Online-Backup.dk Manager v9

Quick Start Guide for Linux (GUI)

Ahsay Systems Corporation Limited

11 May 2022

Copyright Notice

© 2022 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, Oracle Database, Java and MySQL are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

OpenJDK is a registered trademark of Oracle America, Inc.

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

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

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

Ubuntu is a registered trademark of Canonical Ltd.

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

Rocky is a registered trademark of Rocky Brands.

ShadowProtect is a registered trademark of StorageCraft Technology Corporation.

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

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

Disclaimer

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

Revision History

Date	Descriptions	Version
25 January 2022	▪ Ch. 9.5 – added Deduplication	9.1.0.0
7 March 2022	▪ Ch. 12.2 – updated note for Migrate Data	9.1.0.0

Table of Contents

1 Overview 1

1.1 What is this software? 1

1.2 System Architecture 1

1.3 Mobile Backup Server 2

1.4 Two-Factor Authentication 5

2 Requirements for Ahsay Mobile app 8

2.1 Backup Software Version Requirement 8

2.2 Network Connection 8

2.3 Android and iOS Version Requirement 8

3 Requirements for AhsayOBM on Linux (GUI) 9

3.1 Supported Platforms 9

3.2 GUI Desktop Environment 9

3.3 Two-Factor Authentication Requirements 9

3.4 Mobile Backup Requirements 9

3.5 Best Practices and Recommendations 9

3.6 Linux Packages 10

3.7 Network Bandwidth 10

4 Getting Started 11

5 Download and Install AhsayOBM 12

5.1 Online Installation 13

5.1.1 SH online installer 13

5.1.2 RPM online installer 16

5.1.3 DEB online installer 18

5.2 Offline Installation 21

TAR GZ offline installer 21

Check Version of AhsayOBM 26

6 Register device for 2FA in AhsayOBM 27

6.1 Using Ahsay Mobile Authenticator 27

6.1.1 Without Mobile Add-on Module 27

6.1.2 With Mobile Add-on Module 39

6.2 Using Microsoft Authenticator 45

6.3 Using Google Authenticator 53

7 Logging in to AhsayOBM 60

7.1 Login to AhsayOBM without 2FA 60

7.2 Login to AhsayOBM with 2FA using Ahsay Mobile Authenticator 61
7.3 Login to AhsayOBM with 2FA using Microsoft Authenticator 67
7.4 Login to AhsayOBM with 2FA using Google Authenticator 69
7.5 Login to AhsayOBM with 2FA using Twilio 71
8 Unable to log in to AhsayOBM with 2FA 73
9 AhsayOBM Overview 75
9.1 Profile 76
9.1.1 General 76
9.1.2 Contacts 78
9.1.3 Time Zone 80
9.1.4 Encryption Recovery 81
9.1.5 Authentication 82
9.1.6 Password 91
9.1.7 Security Settings 93
9.2 Language 95
9.3 Information 95
9.4 Backup 95
9.5 Backup Sets 96
Backup Set Settings 96
9.6 Report 138
9.6.1 Backup 138
9.6.2 Restore 142
9.6.3 Usage 146
9.7 Restore 148
9.8 Settings 148
9.8.1 Proxy 148
9.8.2 Mobile Backup 149
9.9 Utilities 159
9.9.1 Data Integrity Check 160
9.9.2 Space Freeing Up 176
9.9.3 Delete Backup Data 180
9.9.4 Decrypt Backup Data 186
9.10 Online Help 187
10 Creating a File Backup Set 188
11 Overview on the Backup Process 198
11.1 Periodic Data Integrity Check (PDIC) Process 199
11.2 Backup Set Index Handling Process 201

11.2.1 Start Backup Job 201
11.2.2 Completed Backup Job 202
11.3 Data Validation Check Process 203
12 Running Backup Jobs 204
12.1 Login to AhsayOBM 204
12.2 Start a Manual Backup 204
13 Restoring Data 208
13.1 Login to AhsayOBM 208
13.2 Restore Data 208
13.3 Restore Filter 215
14 Contacting Ahsay 220
14.1 Technical Assistance 220
14.2 Documentation 220
Appendix 221
Appendix A: Uninstall AhsayOBM (SH online installer) 221
Appendix B: Uninstall AhsayOBM (RPM online installer) 224
Appendix C: Uninstall AhsayOBM (DEB online installer) 226
Appendix D: Handling of Non-regular Files 228
Appendix E: Script Files 229
RunConfigurator.sh 229
ListBackupSet.sh 236
ListBackupJob.sh 241
RunBackupSet.sh 248
Restore.sh 269
Decrypt.sh 284
RunDataIntegrityCheck.sh 298
Appendix F: Example Scenarios for Restore Filter 308
Appendix G: Create Free Trial Account in AhsayOBM 316
Appendix H: Manually Upgrade AhsayOBM 320

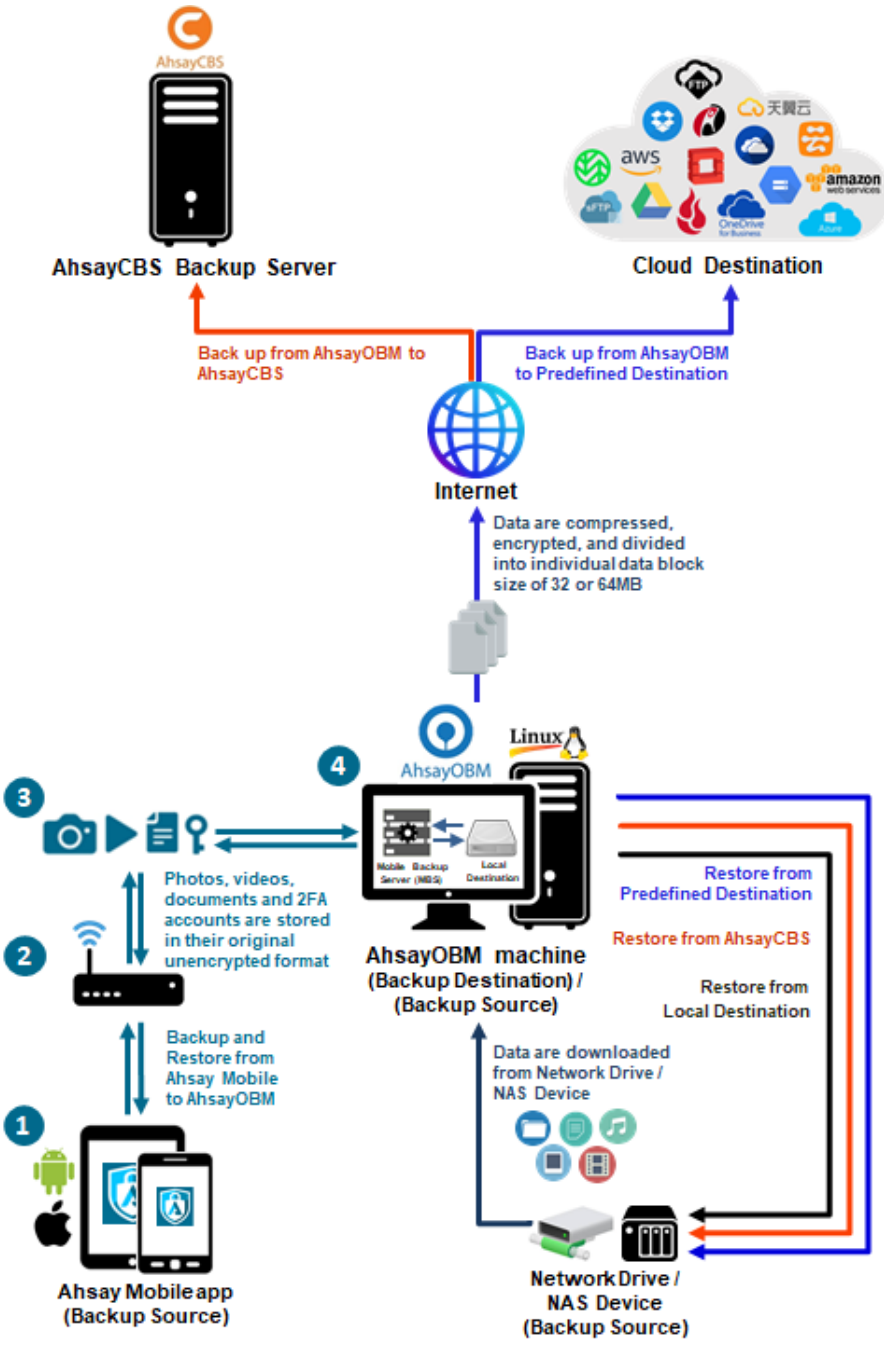
1 Overview

1.1 What is this software?

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

1.2 System Architecture

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



1.3 Mobile Backup Server

The Mobile Backup Server (MBS) will be utilized to handle mobile backup and restore of Ahsay Mobile app. It is an integral part of AhsayOBM.

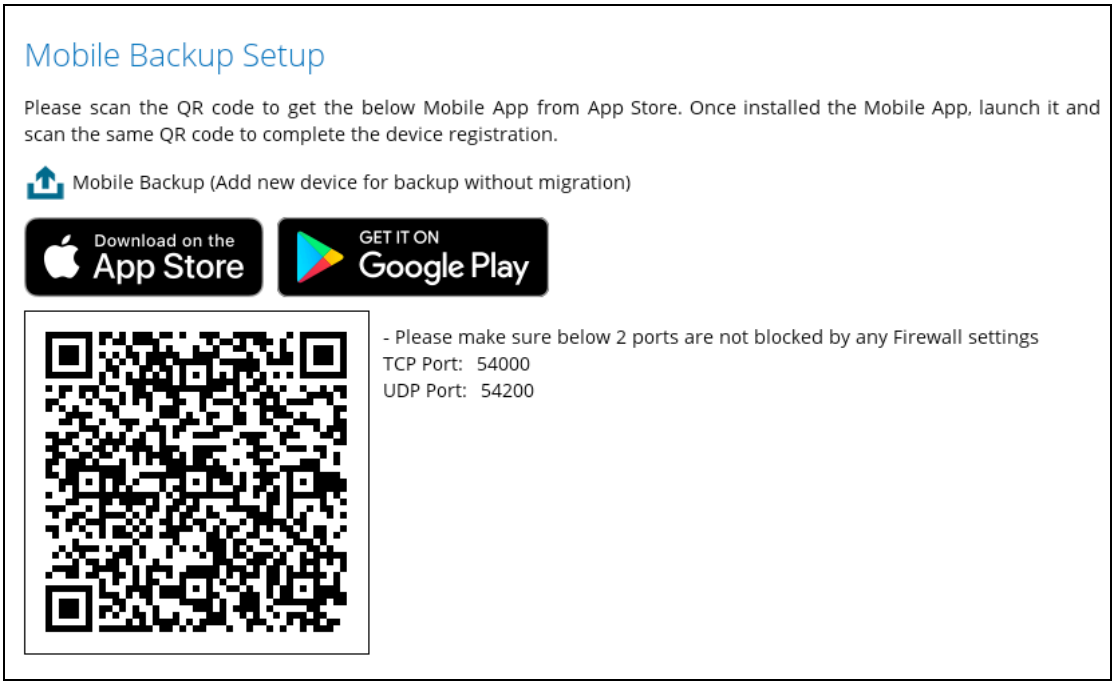
The MBS will be activated automatically when a mobile device installed with the Ahsay Mobile app is successfully registered for mobile backup with AhsayOBM. Afterwards, it will be automatically restarted whenever the AhsayOBM services is restarted or when the AhsayOBM machine is rebooted or powered on.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

The MBS will use the following port ranges:

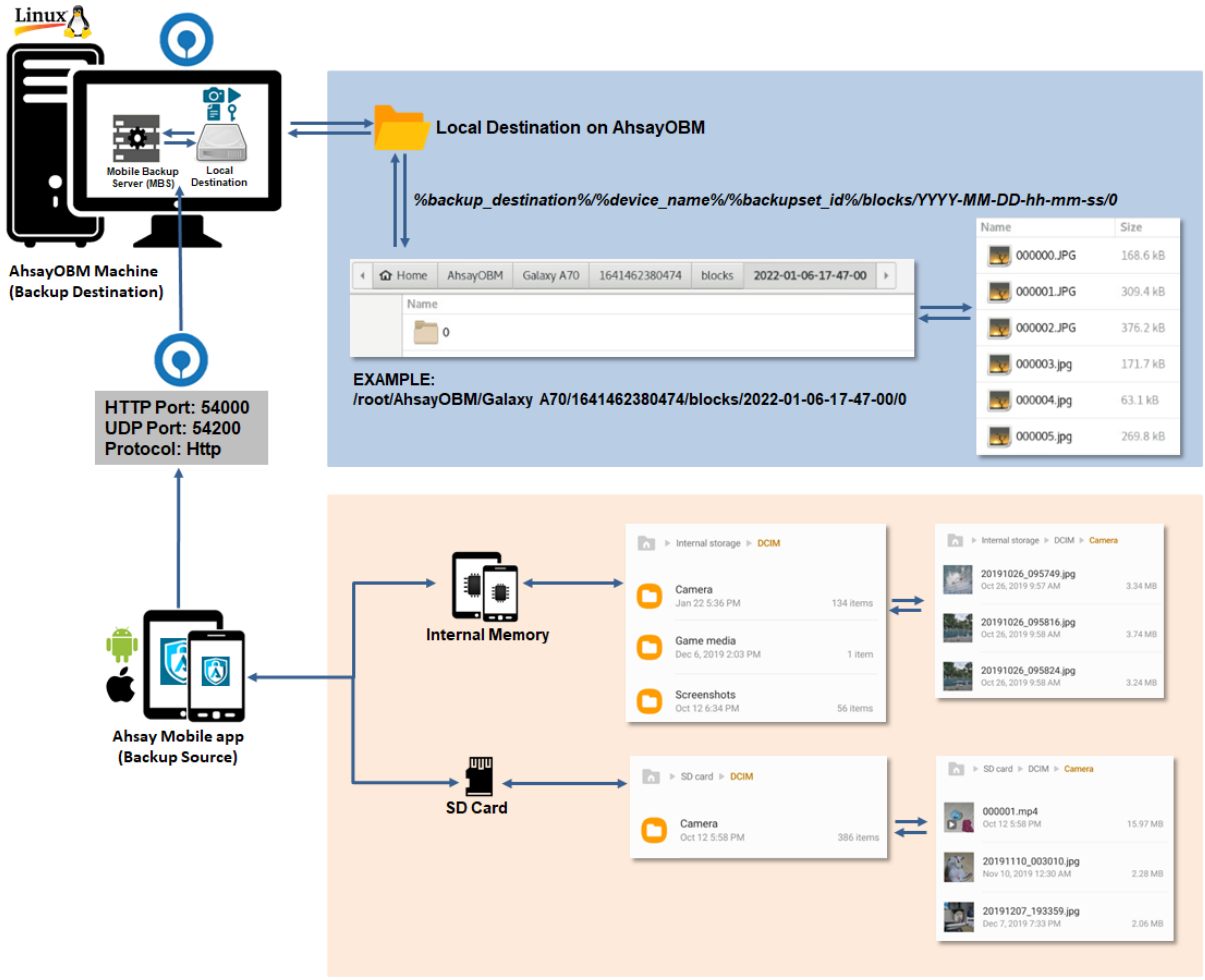
- **TCP Port:** 54000 to 54099
- **UDP Port:** 54200 to 54299
- **Protocol**: Http, for the request of Ahsay Mobile app

The default TCP and UDP ports are 54000 and 54200. If these ports are already used by other applications or services, then the MBS will automatically acquire another port(s).

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



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

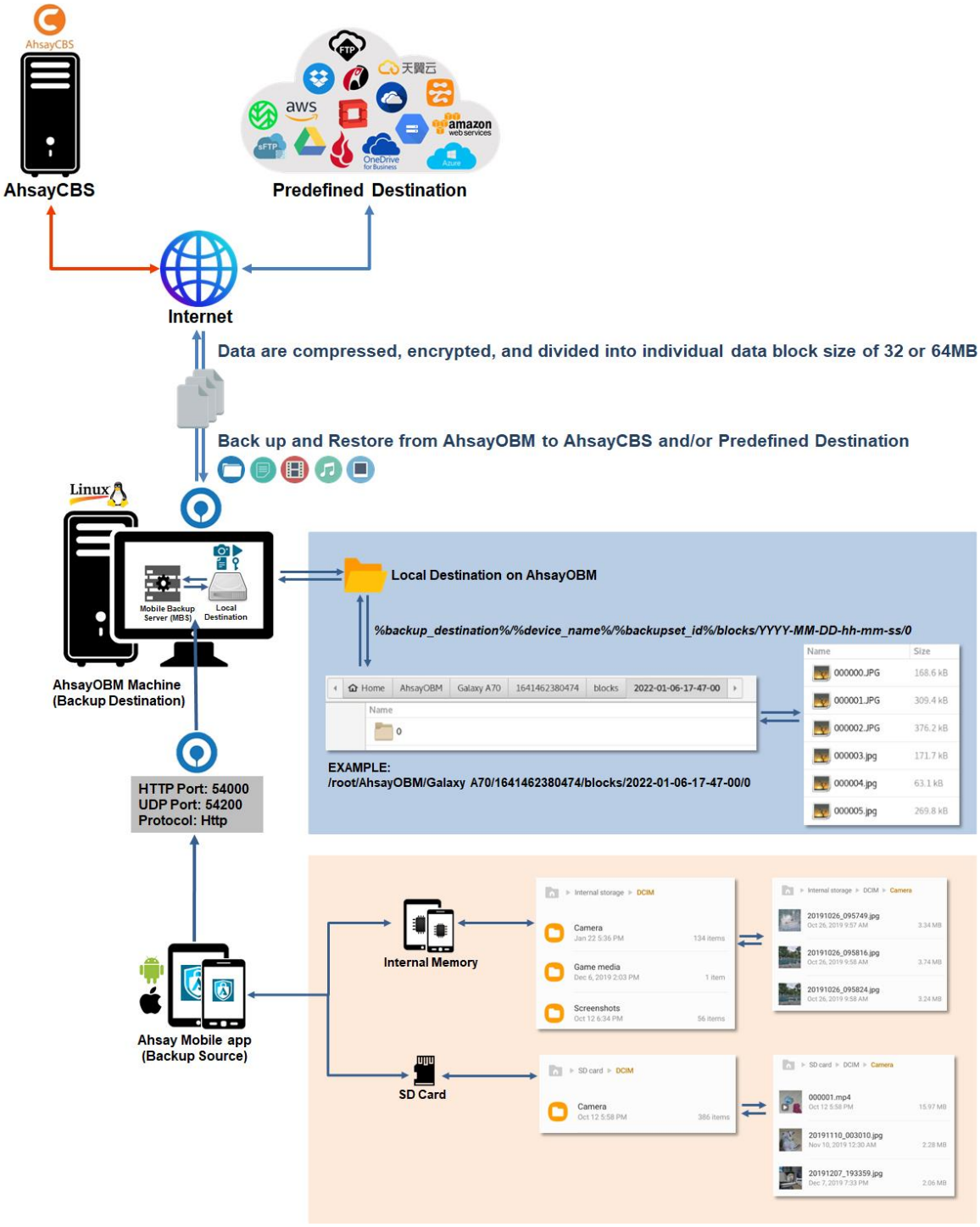


If storage of photos, videos, documents and 2FA accounts to AhsayCBS and/or Predefined Destination is required, then this can be done using AhsayOBM to perform a secondary backup and restore of the photos, videos, documents and 2FA accounts on the local drive to AhsayCBS and/or Predefined Destination.

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

1st: Back up photos, videos, documents and 2FA accounts from Ahsay Mobile app to AhsayOBM local destination.

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



1.4 Two-Factor Authentication

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

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

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

If Ahsay Mobile is used as the authenticator app:

- you will either accept the login request via push notification in the Ahsay Mobile app;

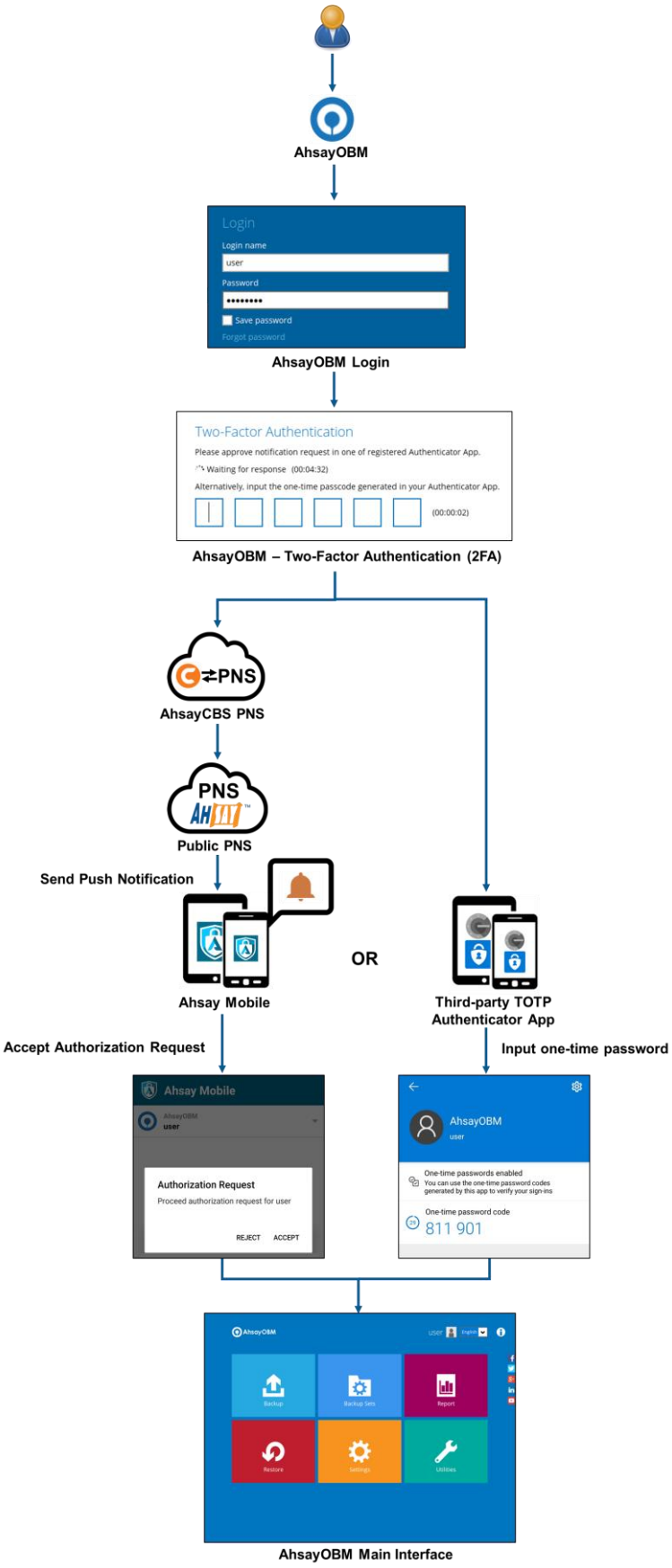
  or

- enter the one-time password generated in the Ahsay Mobile app.

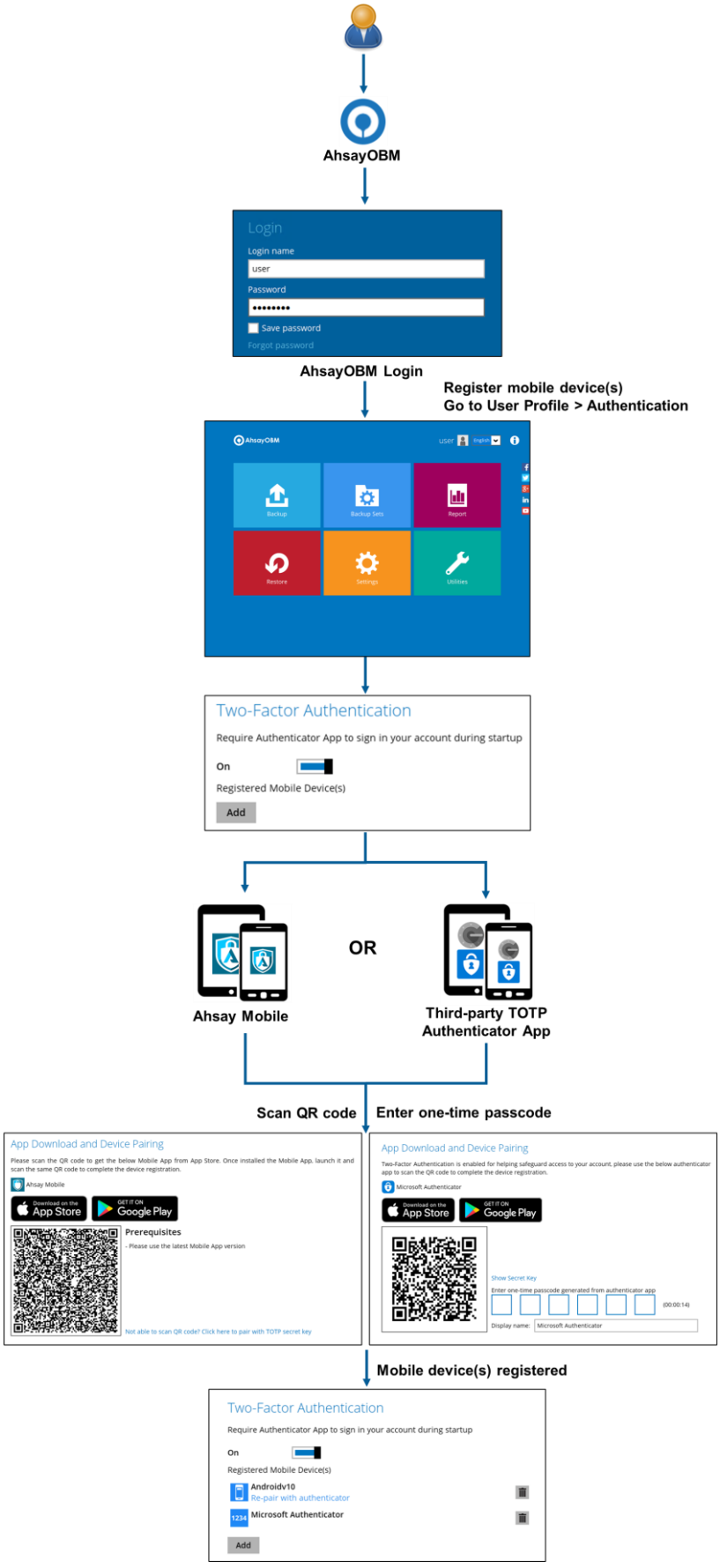
If a third-party authenticator app is used:

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

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



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



2 Requirements for Ahsay Mobile app

2.1 Backup Software Version Requirement

- Download and install the latest version of AhsayOBM v9.0.0.0 or above.
- Download and install the latest version of Ahsay Mobile app on the Play Store for Android mobile devices and on the App Store for iOS mobile devices.

2.2 Network Connection

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

2.3 Android and iOS Version Requirement

- For Android 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 Linux (GUI)

3.1 Supported Platforms

Refer to the following article for the list of supported operating systems:

FAQ: Ahsay Software Compatibility List (SCL) for version 9.1 or above

3.2 GUI Desktop Environment

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

3.3 Two-Factor Authentication Requirements

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

3.4 Mobile Backup Requirements

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

3.5 Best Practices and Recommendations

Periodic Backup Schedule

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

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

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

- Hardware – to achieve optimal performance, compatible hardware requirements is a must. Ensure you have the backup machine's appropriate hardware specifications to accommodate frequency of backups,
  - so that the data is always backed up within the periodic backup interval
  - so that the backup frequency does not affect the performance of the production server
- Storage – ensure you have enough storage quota allocated based on the amount of new data and changed data you will 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.

3.6 Linux Packages

The following packages have to be present on the Linux machine in order for AhsayOBM version 9 to be installed.

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

  The installed 'GNU LIBC' version must at least be 2.14 for OpenJDK 8 to work.

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

  The 'psmisc' package which contains the 'fuser' components must be installed for the auto update agent (AUA) process to work properly for AhsayOBM on Linux.

- **curl** https://curl.haxx.se

  The 'curl' command is used by both the AhsayOBM SH online installer and RPM online installer to download components from AhsayCBS server during the installation process.

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

  The 'tar' command is used by both the AhsayOBM TAR GZ offline installer and RPM online installer to uncompress and extract installation files or components downloaded from the AhsayCBS backup server onto the Linux machine.

- **rpm** http://rpm.org

  The 'rpm' package must be installed to use the AhsayOBM RPM online installer method on CentOS and Red Hat Enterprise Linux platforms.

- **dpkg**

  Debian https://packages.debian.org/buster/dpkg

  Ubuntu https://packages.ubuntu.com/trusty/dpkg

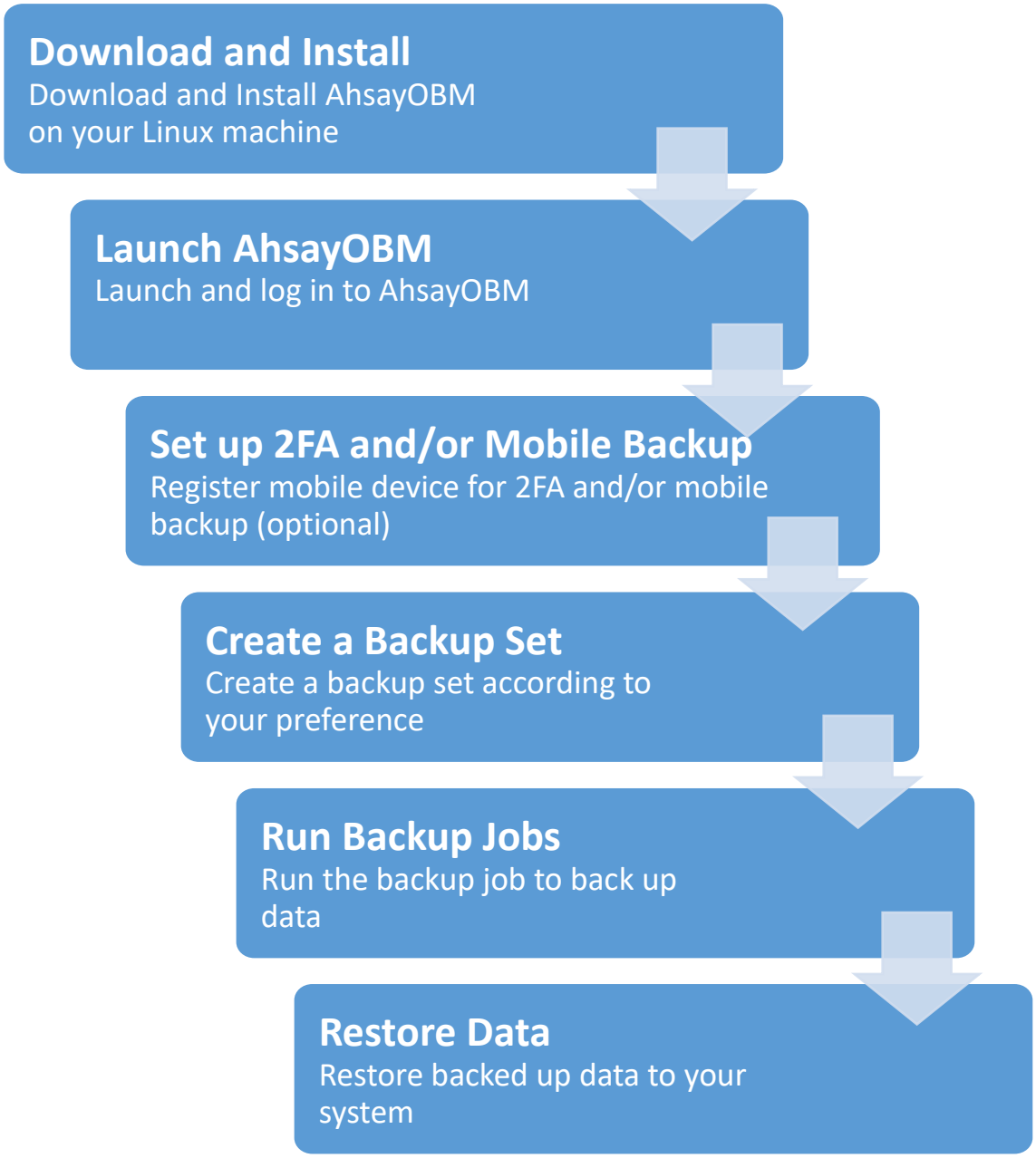
  The 'dpkg' package must be installed to support AhsayOBM DEB online installer method on Debian and Ubuntu platforms.

3.7 Network Bandwidth

10 Mbps or above connection speed.

4 Getting Started

This quick start guide will walk you through the following 5 major parts to get you started with using AhsayOBM.



5 Download and Install AhsayOBM

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

	Online Installation	Offline Installation
Installation Time	➢ 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 80MB to 132MB 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.

NOTE

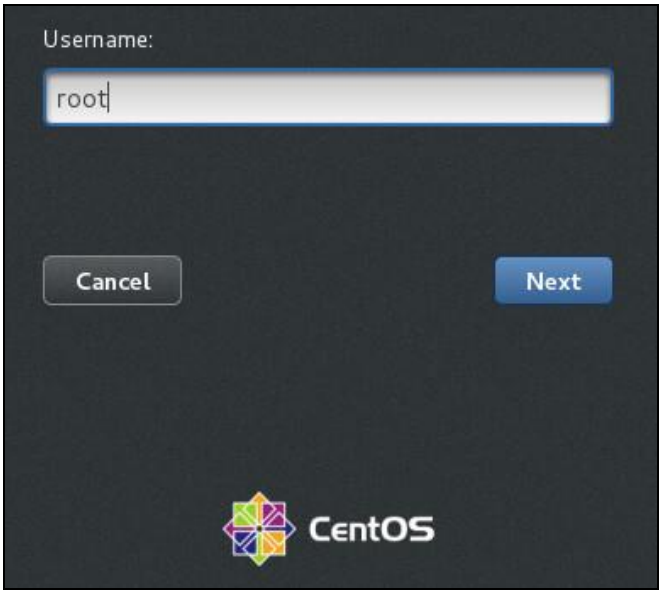
The following platforms only support online installation:

- Debian and Ubuntu – using deb package
- CentOS and Red Hat – using rpm package

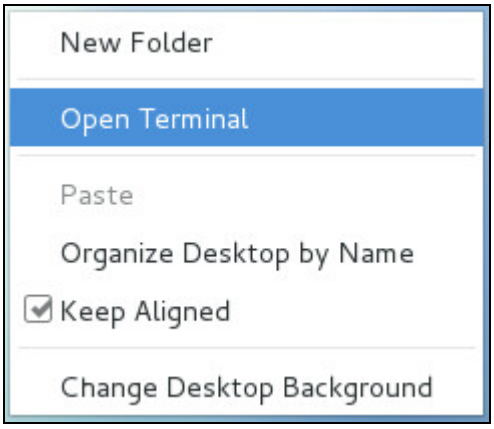
5.1 Online Installation

5.1.1 SH online installer

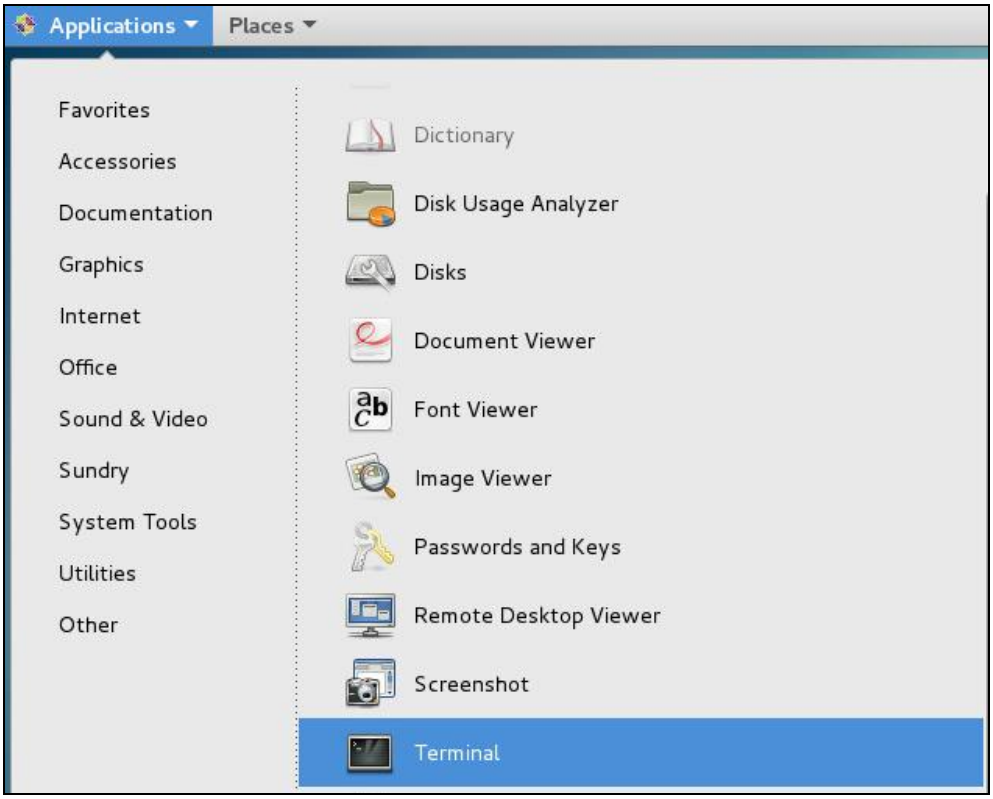
1. Log in to a Linux machine using the root account. (Alternatively, you can remotely invoke the GUI of another Linux machine using SSH client.)



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



Alternatively, you can also click the **Applications** menu bar then select **Utilities > Terminal**.



3. Create a new directory for AhsayOBM installation using the following script.

```
# mkdir -p /usr/local/obm

# cd /usr/local/obm
```

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

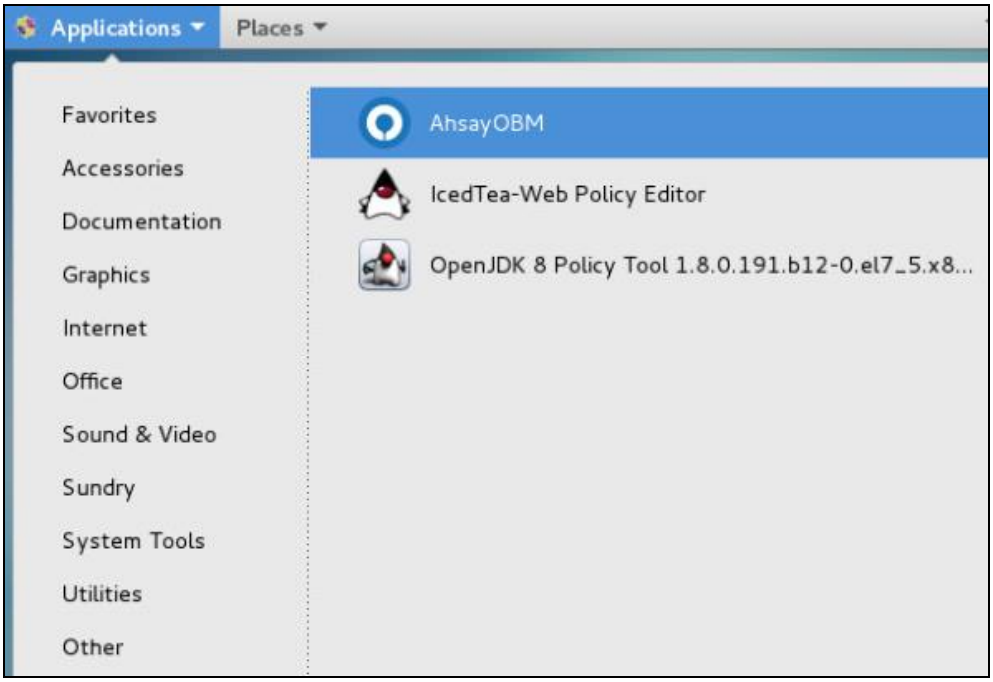
5. Run the AhsayOBM installation script. At the end of the script, the installation path and "Done" will be shown to indicate that the AhsayOBM installation is successful.

NOTE: *The .sh script file should be copied and run under the directory path where you want the AhsayOBM application to be installed, i.e., /usr/local/obm*

```
# ./obm-nix-443-10.90.10.12-https-00.sh
Log Time: Mon Dec 27 18:42:40  HKT 2021
Host address: https://10.3.121.17:443
Downloading file... jre-std-linux-amd64.tar.gz
% Total    % Received % Xferd  Average Speed   Time
Current
Dload  Upload   Total   Spent    Left  Speed
100 91.3M  100 91.3M    0     0  3672k      0  0:00:25  0:00:25 -
-:--:-- 12.0M
Download file completed
Untar component file to /tmp/_obm.190114184240/jvm
Downloading file... app-common.tar.gz
% Total    % Received % Xferd  Average Speed   Time
Current
Dload  Upload   Total   Spent    Left  Speed
100 34.9M  100 34.9M    0     0  1126k      0  0:00:31  0:00:31 -
-:--:-- 4478k
Download file completed
     .
     .
     .
Untar component file to /tmp/_obm.190114184240
Downloading file... aua-inst-nix-obm.tar.gz
% Total    % Received % Xferd  Average Speed   Time
Current
Dload  Upload   Total   Spent    Left  Speed
100 54564  100 54564    0     0   329k      0 --:--:-- --:--:-- -
-:--:--  330k
Download file completed
Untar component file to /tmp/_obm.190114184240
No old application found, begin fresh install
Install Application Path: /usr/local/obm
Done
```

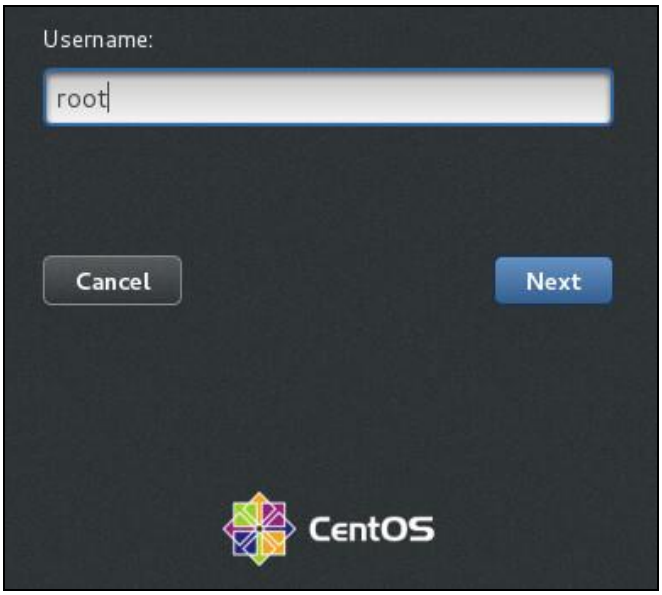
6. After successful installation, an AhsayOBM icon will be added to the desktop.

Another way is to click the **Applications** menu bar, then select **Other** to access **AhsayOBM**.



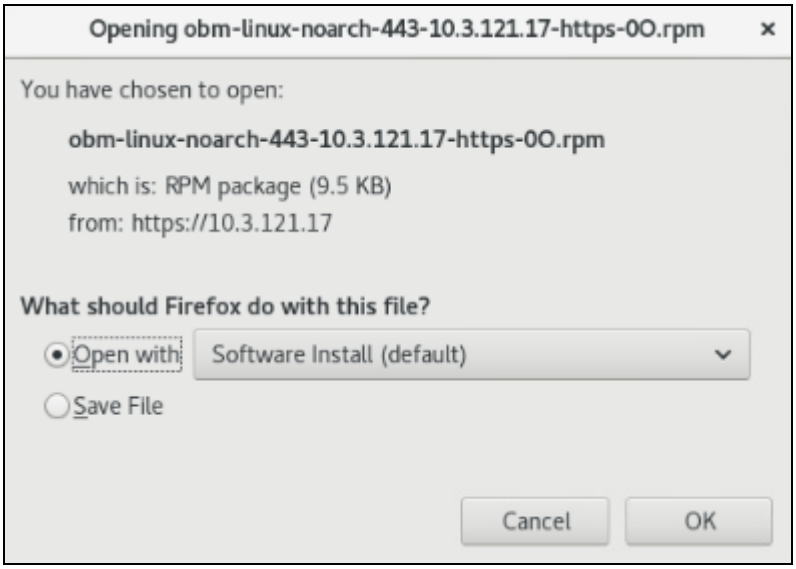
5.1.2 RPM online installer

1. Log in to a Linux machine using the root account. (Alternatively, you can remotely invoke the GUI of another Linux machine using SSH client.)



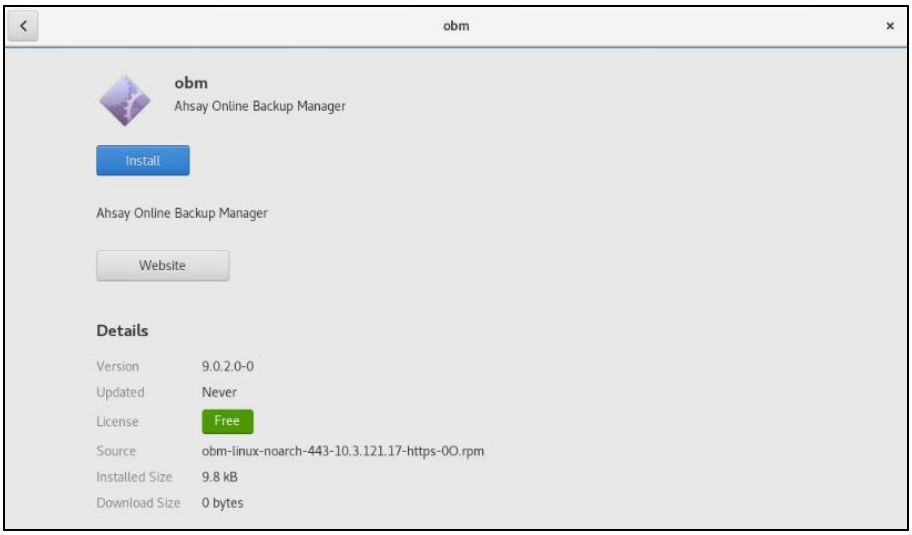
2. Go to the download page of your backup service provider's website and download the AhsayOBM **RPM online installer**.

3. Click **OK** to proceed with the downloading of file.



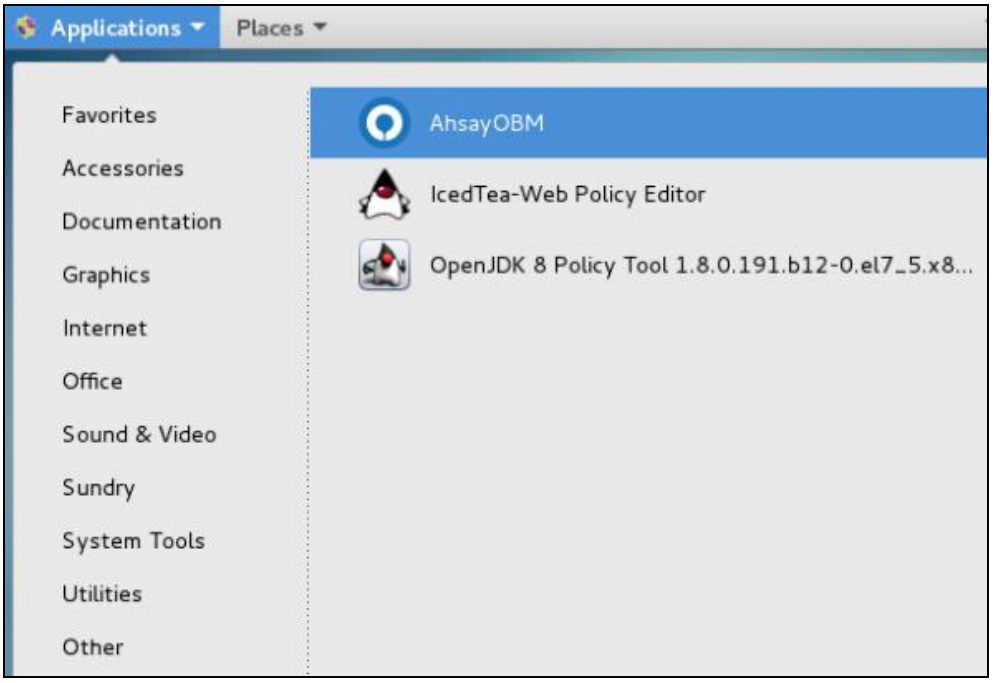
4. When a notification message "Application Installer Software is ready" appears, click the **Software** tab to proceed.

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



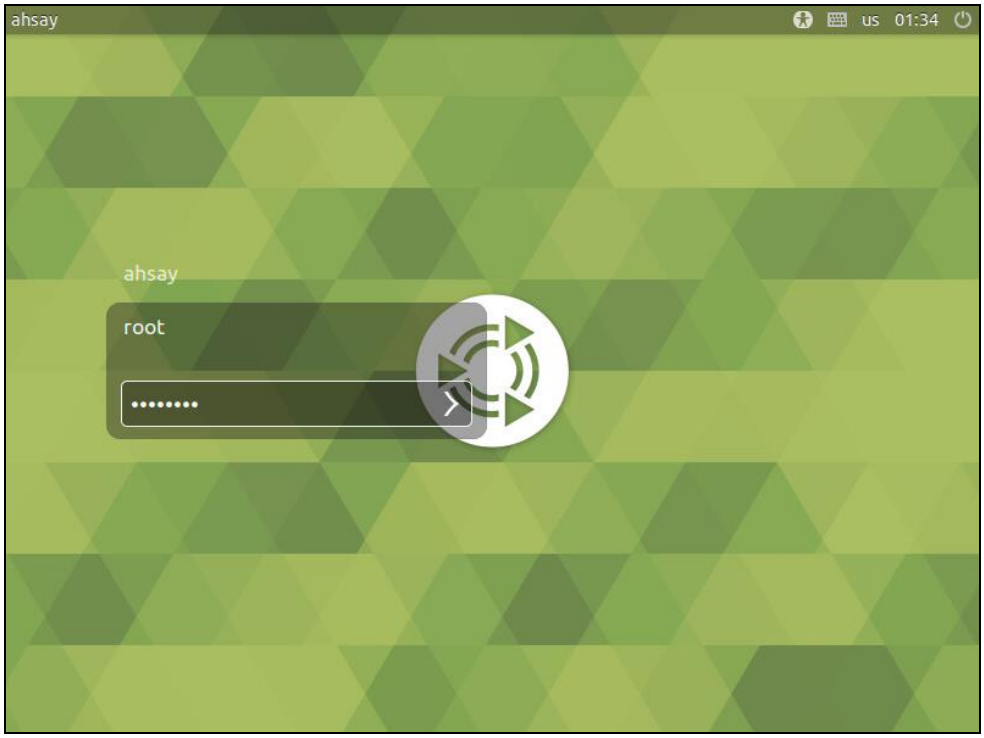
6. After successful installation, an AhsayOBM icon will be added to the desktop.

Another way is to click the **Applications** menu bar, then select **Other** to access **AhsayOBM**.



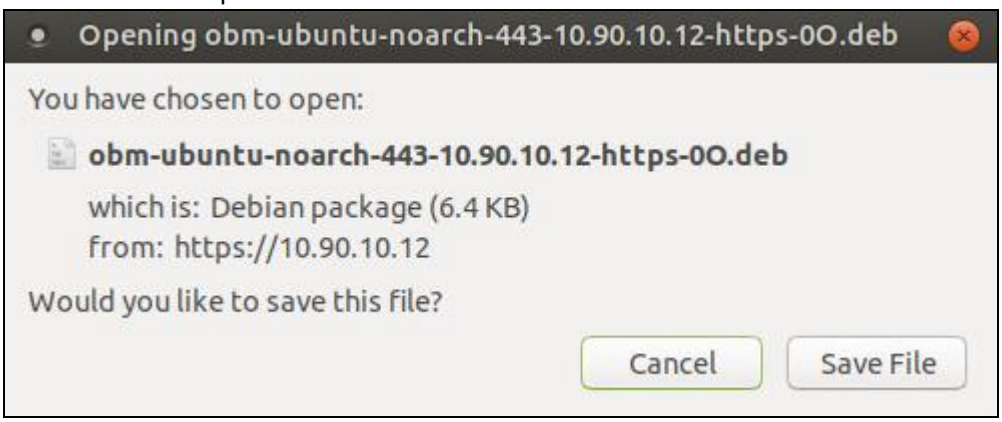
5.1.3 DEB online installer

1. Log in to a Debian or Ubuntu machine using the root account. (Alternatively, you can remotely invoke the GUI of another Debian or Ubuntu using SSH client.)

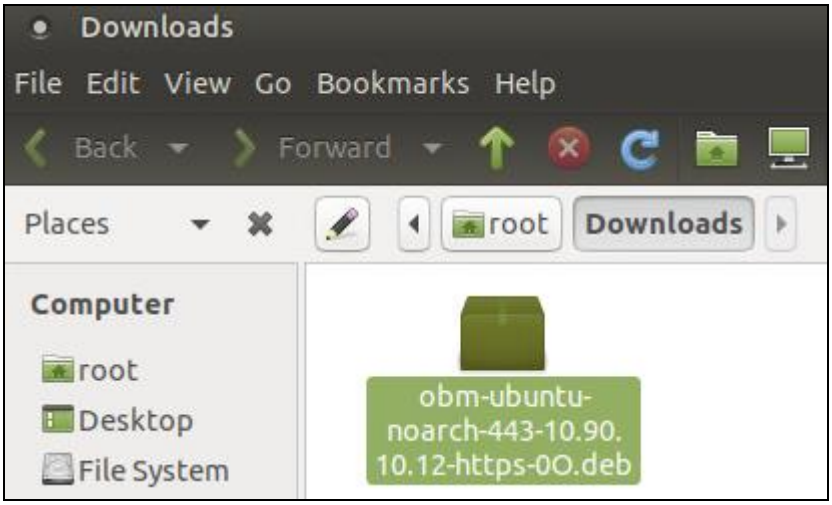


2. Go to the download page of your backup service provider's website and download the AhsayOBM **DEB online installer**.

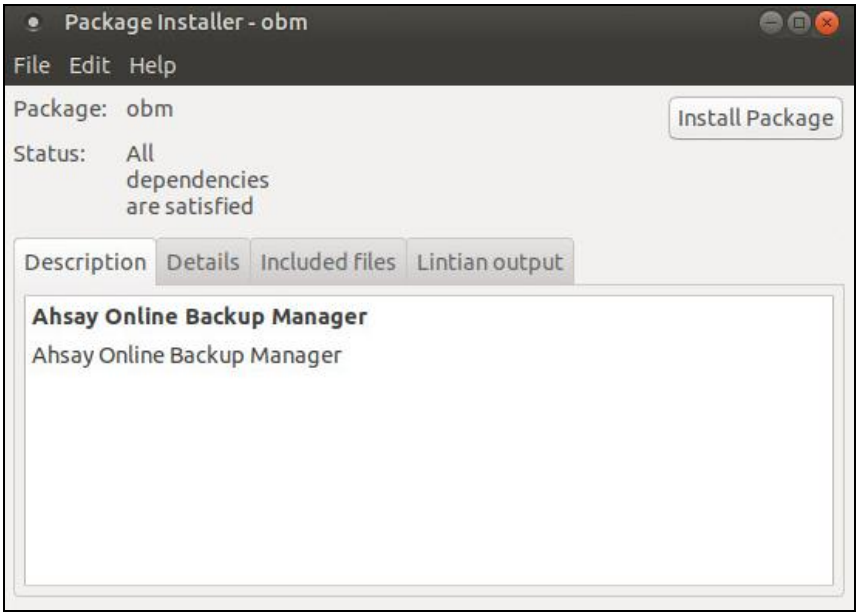
3. Click **Save File** to proceed.



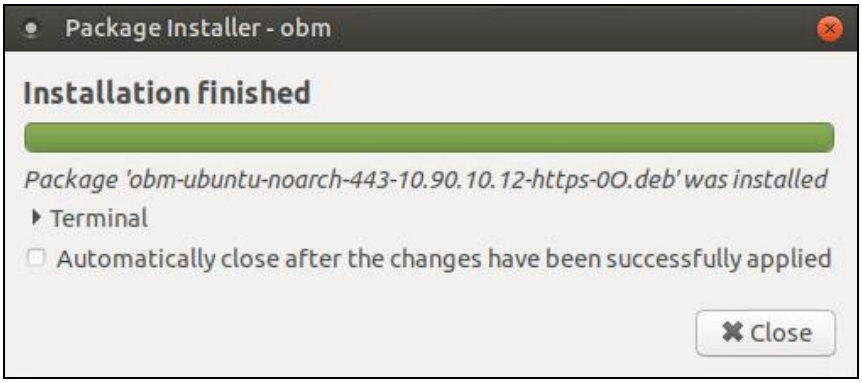
4. Go to **Downloads** folder and double click the downloaded file.



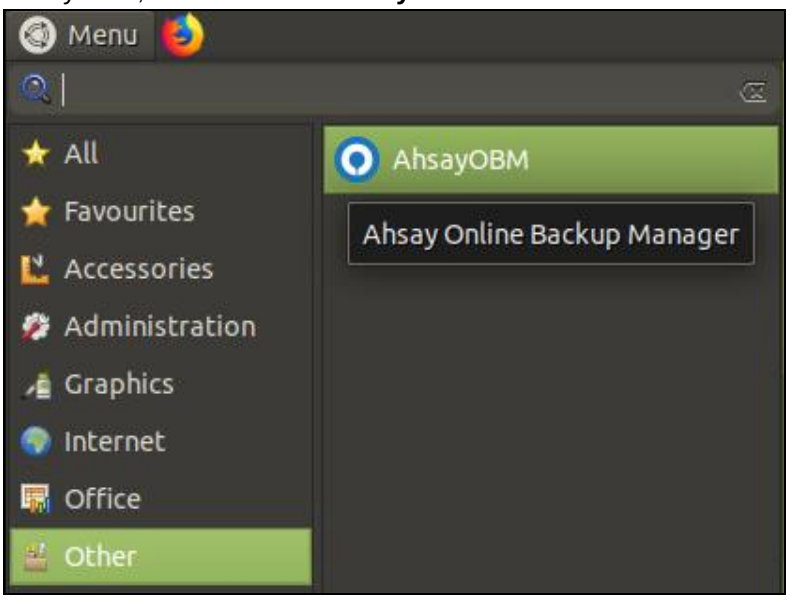
5. Click **Install Package** to start the installation.



6. Once the installation is completed, the following screen will be displayed.



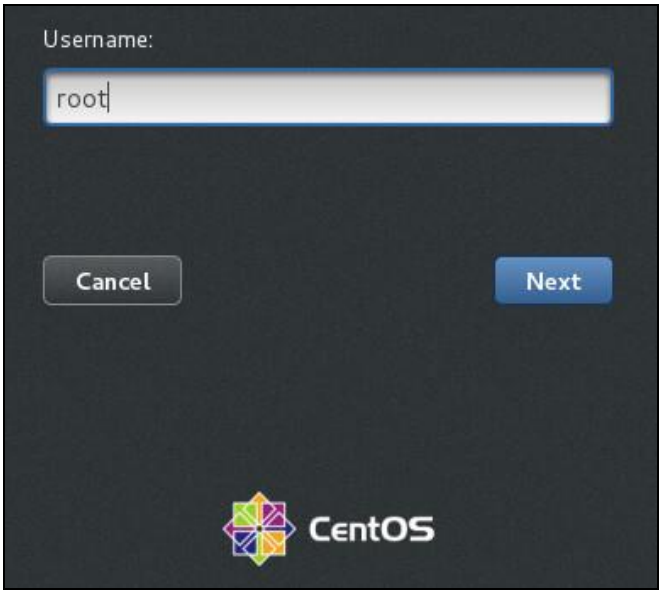
7. After successful installation, AhsayOBM will be added to the menu bar. To access AhsayOBM, select **Other > AhsayOBM**.



5.2 Offline Installation

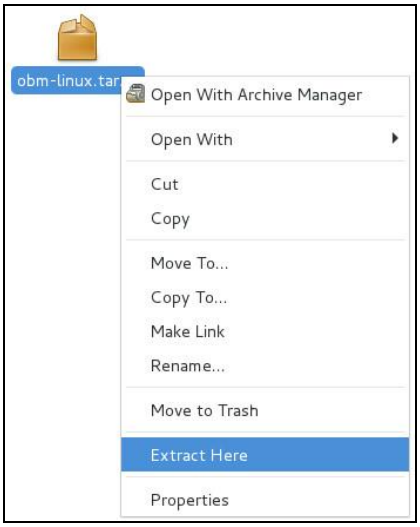
TAR GZ offline installer

1. Log in to a Linux machine using the root account. (Alternatively, you can remotely invoke the GUI of another Linux machine using SSH client.)

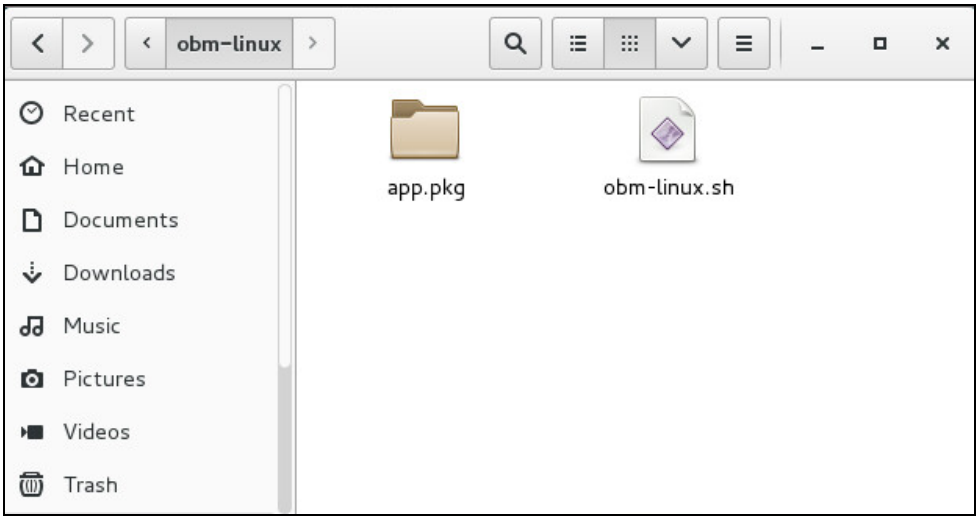


2. Go to the download page of your backup service provider's website and download the AhsayOBM **TAR GZ offline installer**.

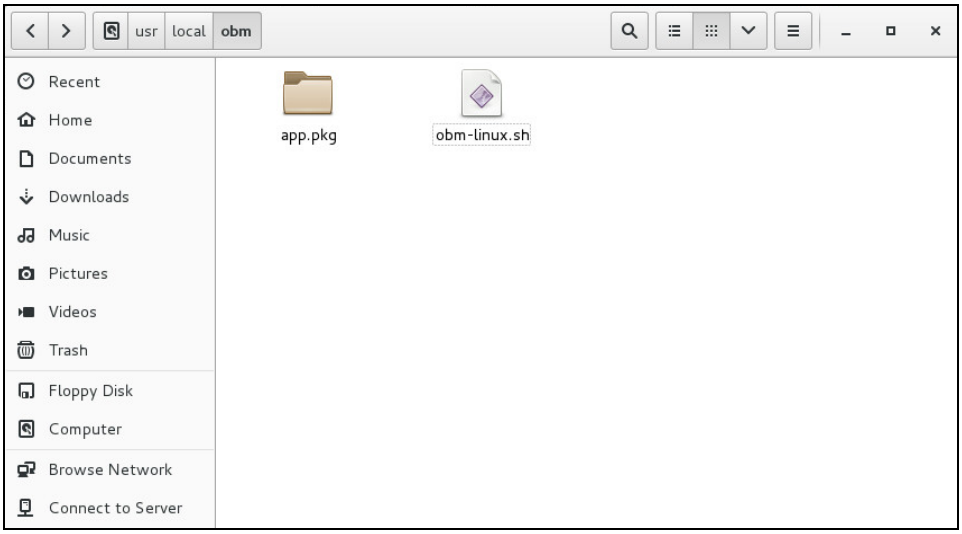
3. Right click on the AhsayOBM installation package **.gz** file to extract.



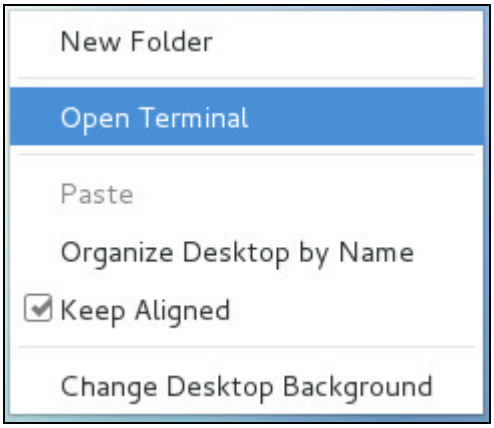
4. Open the folder to check the extracted installation package.



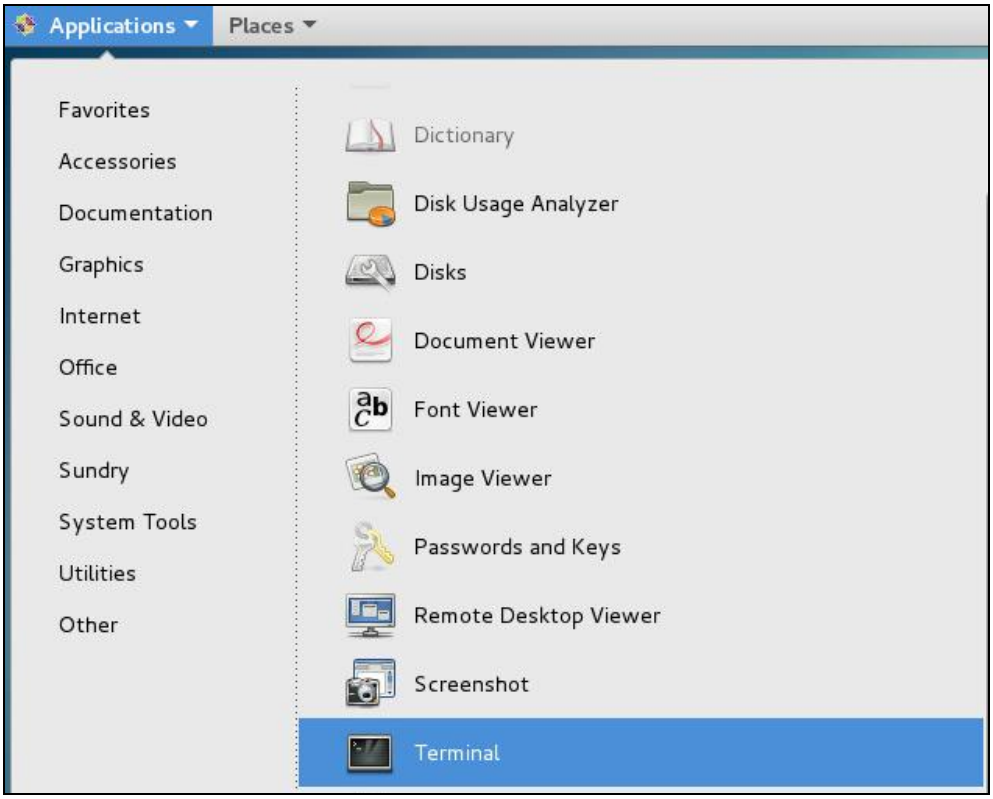
5. Create a folder for AhsayOBM under the **/usr/local** directory, then move the extracted **obm-linux.sh** file to the obm folder.



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



Alternatively, you can also click the **Applications** menu bar then select **Utilities > Terminal**.



7. Go to the **/usr/local/obm** directory.

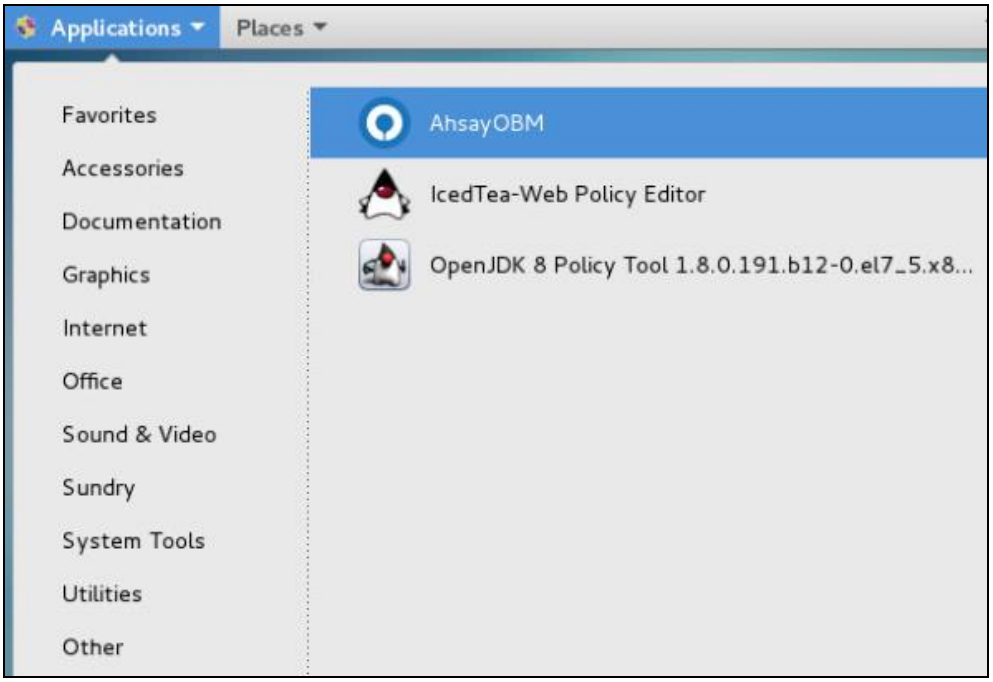
```
# cd /usr/local/obm
```

8. Use the **sh** command to install AhsayOBM.

```
sh obm-linux.sh
Log Time: Fri May  7 10:32:21 +08 2021
Using package in /usr/local/obm/app.pkg
Package version: 9.0.2.0
Untar jre-std-linux-amd64.tar.gz to /tmp/_obm.210507103221/jvm
Untar app-common.tar.gz to /tmp/_obm.210507103221
Untar app-native-nix-x64.tar.gz to /tmp/_obm.210507103221
Untar app-nix-obm.tar.gz to /tmp/_obm.210507103221
Untar aua-common.tar.gz to /tmp/_obm.210507103221
Untar aua-native-nix-x64.tar.gz to /tmp/_obm.210507103221
Untar aua-nix-obm.tar.gz to /tmp/_obm.210507103221
Untar util-common.tar.gz to /tmp/_obm.210507103221
Untar util-nix-obm.tar.gz to /tmp/_obm.210507103221
Untar properties-common.tar.gz to /tmp/_obm.210507103221
Untar app-inst-nix-obm.tar.gz to /tmp/_obm.210507103221
Untar aua-inst-nix-obm.tar.gz to /tmp/_obm.210507103221
Backup user setting files
Backup finished
Uninstall previous version...
Remove previous application files
Remove file obm-linux.tar.gz
Remove application files finished
Install Application Path: /usr/local/obm
Restore Previous Setting backup...
Previous Setting backup restored
 Done
```

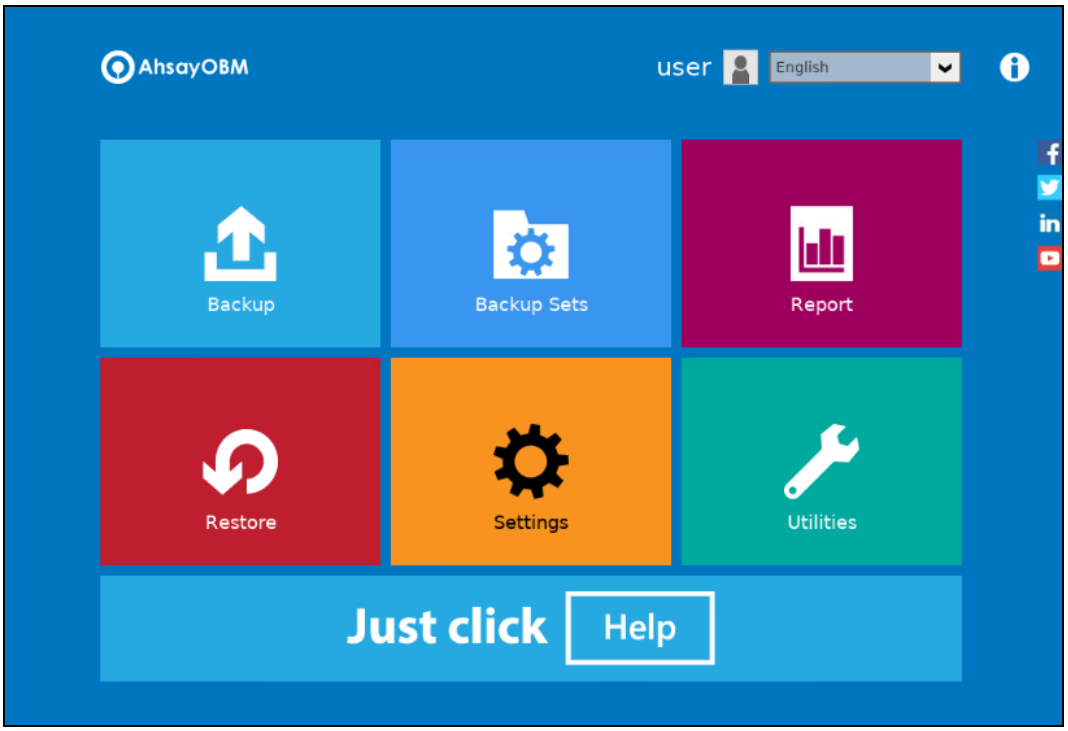
9. After successful installation, an AhsayOBM icon will be added to the desktop.

Another way is to click the **Applications** menu bar, then select **Other** to access **AhsayOBM**.

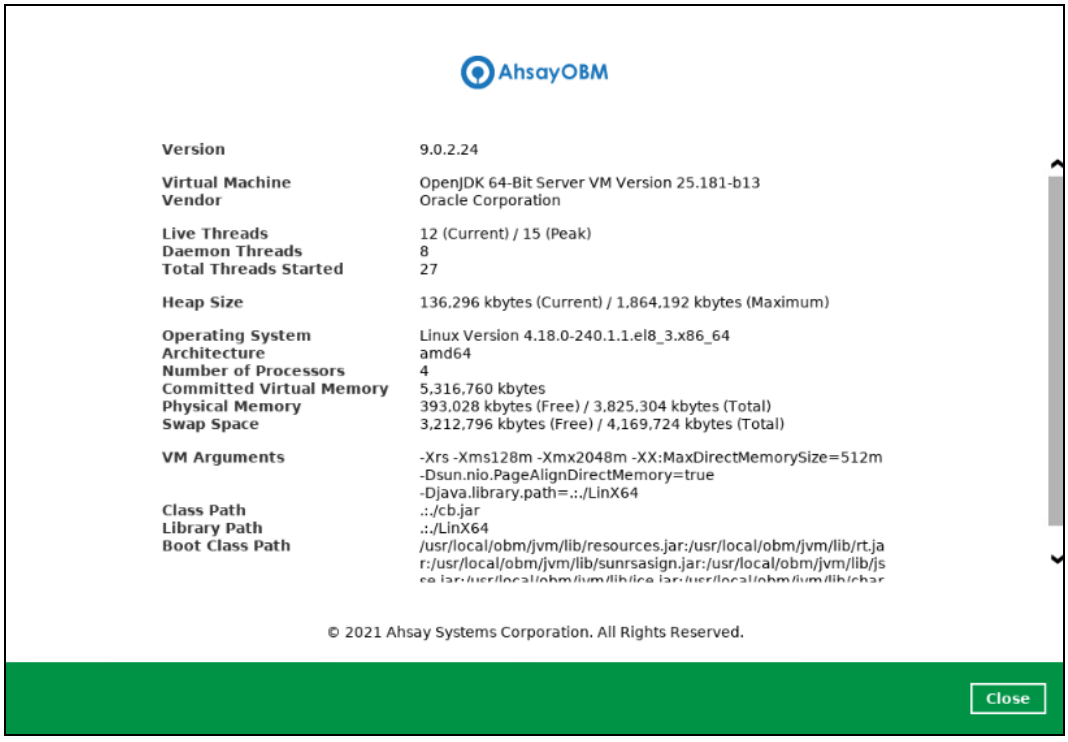


Check Version of AhsayOBM

1. Log in to AhsayOBM application according to the instructions in Login to AhsayOBM.
2. Click the Information icon at the top right corner.



3. The **version** of the installed AhsayOBM will be displayed.



6 Register device for 2FA in AhsayOBM

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

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

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

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

6.1 Using Ahsay Mobile Authenticator

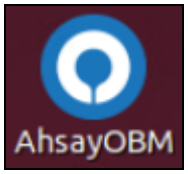
To register a device for 2FA in AhsayOBM using Ahsay Mobile, here are the two scenarios:

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

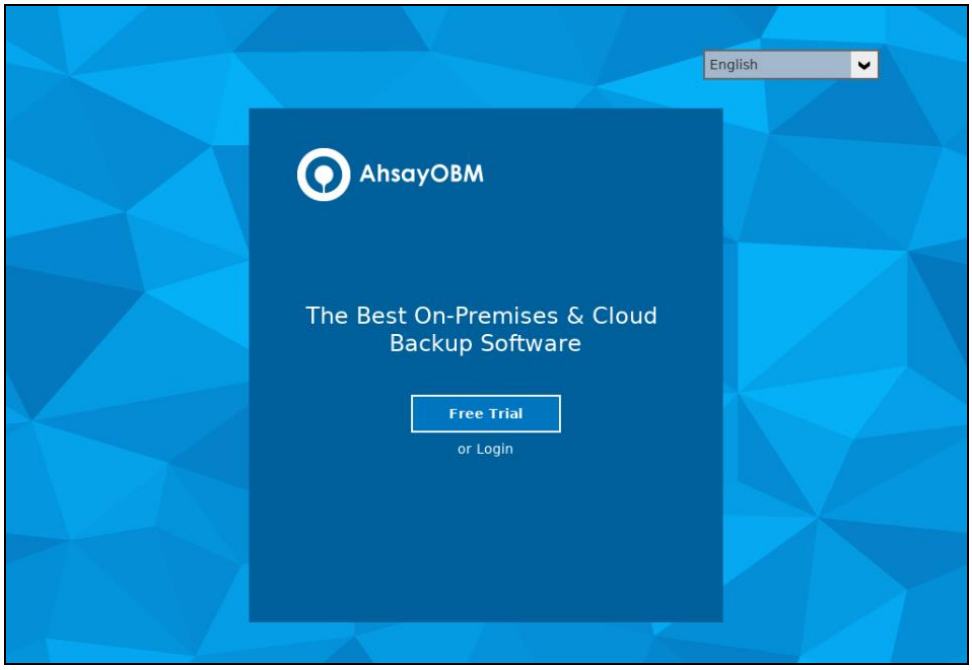
6.1.1 Without Mobile Add-on Module

To register a device for 2FA without Mobile Add-on Module, please follow the steps below:

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



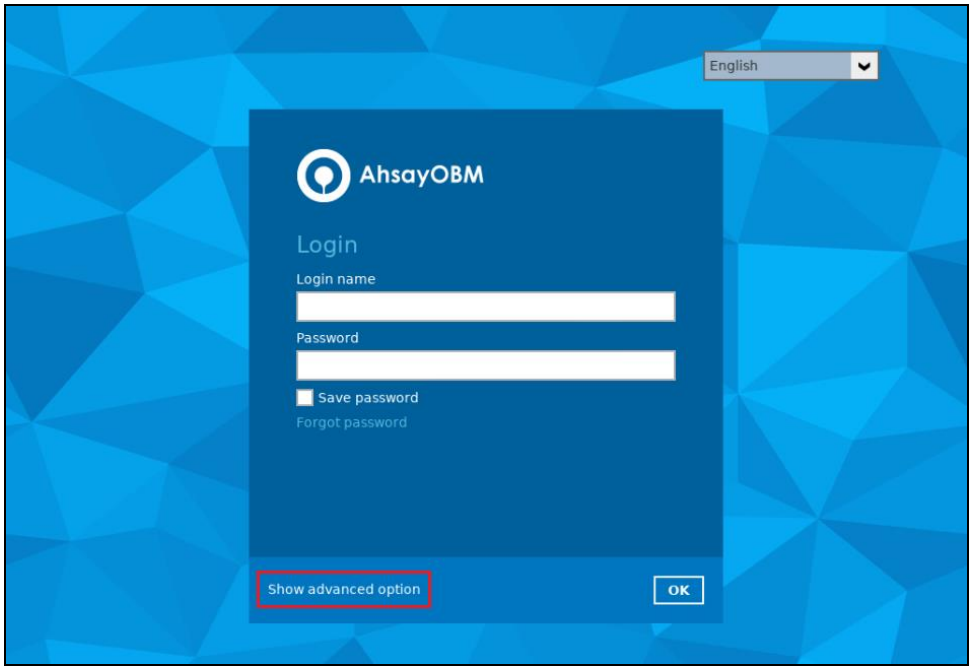
2. The Free Trial Registration option may be displayed when you login for the first time. If you want to create a free trial account please proceed to Appendix G. Otherwise, click **Login** if you already have an AhsayOBM account.



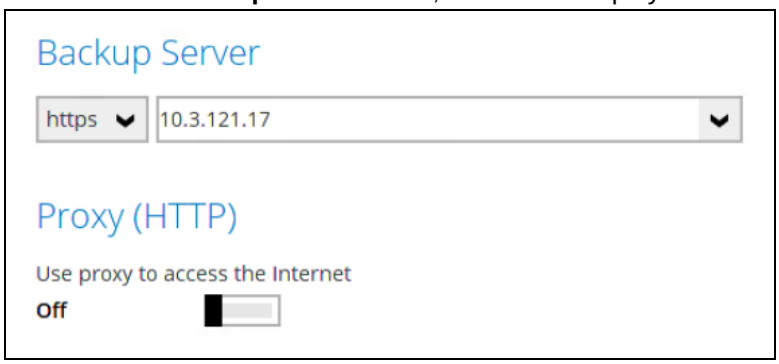
NOTE

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

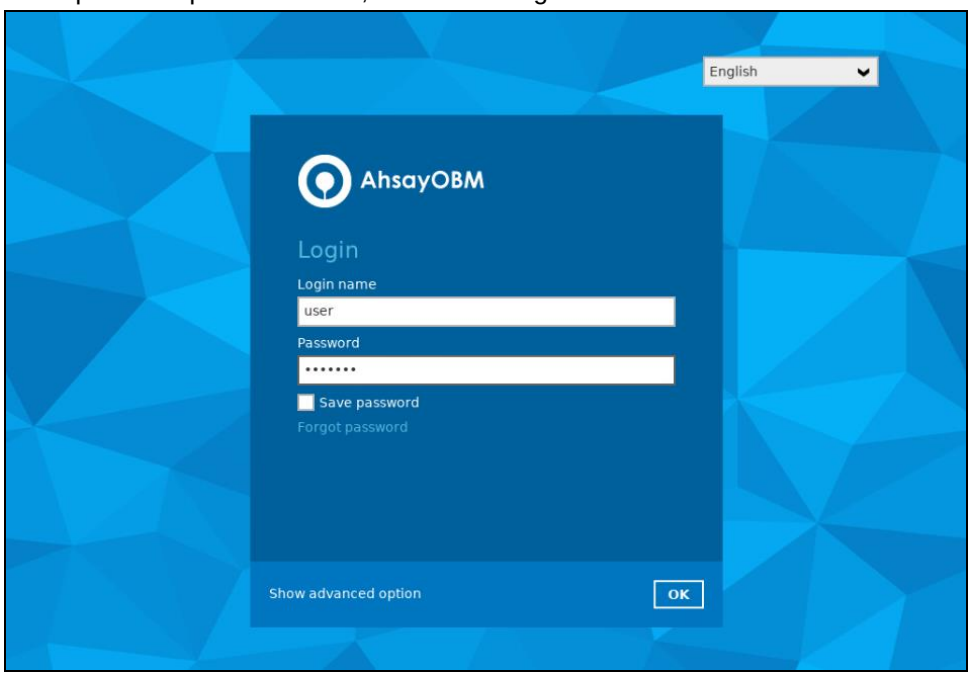
3. The **Show advanced option** may not be available if the backup server settings are already setup by your backup service provider. Please contact your backup service provider for more information.



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



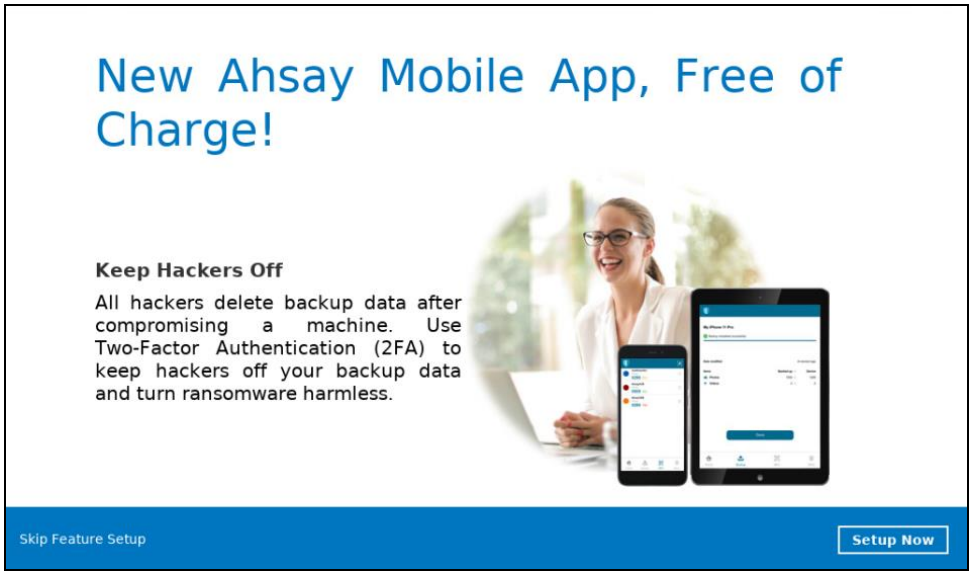
4. Enter the login name and password of your AhsayOBM account provided by your backup service provider. Then, click **OK** to log in.



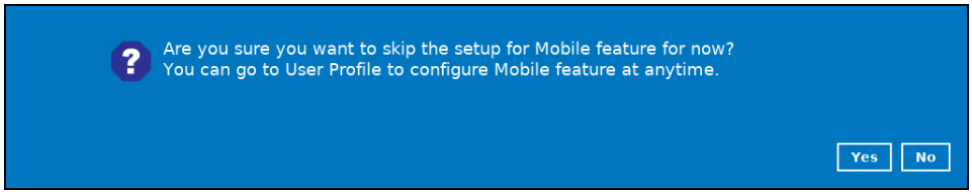
NOTE

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.

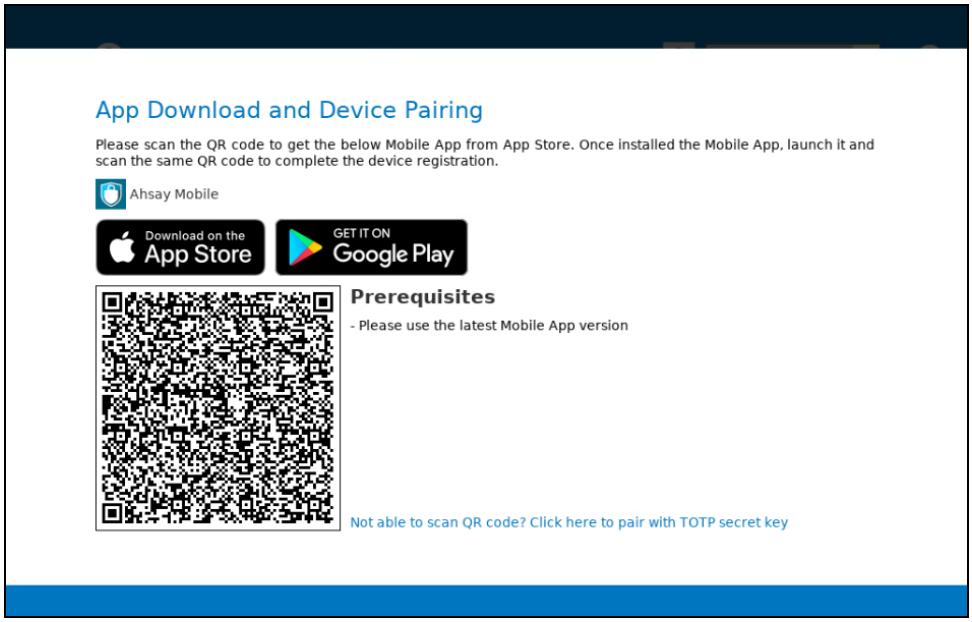
5. You will have the option to set up your 2FA. Click **Setup Now.**



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:

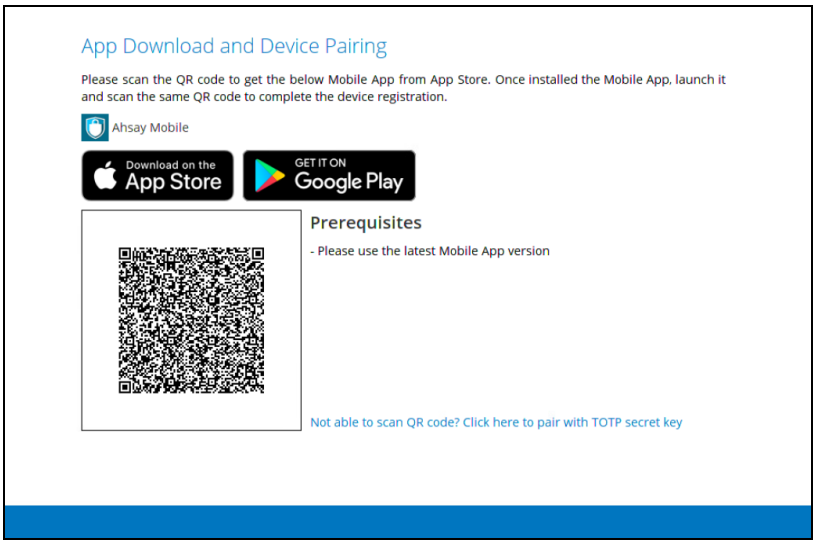
- Push Notification and TOTP (default mode)

  or

- TOTP only

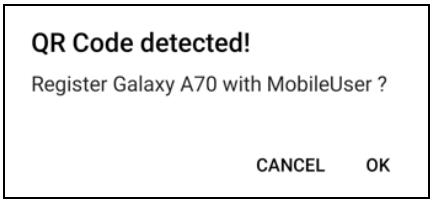
Push Notification and TOTP (default mode)

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

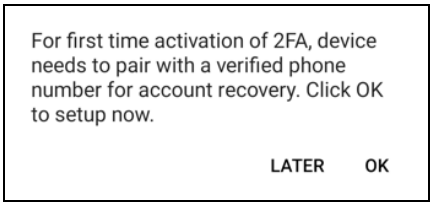


In this example, the Ahsay Mobile app is installed on a mobile device named “Galaxy A70”.

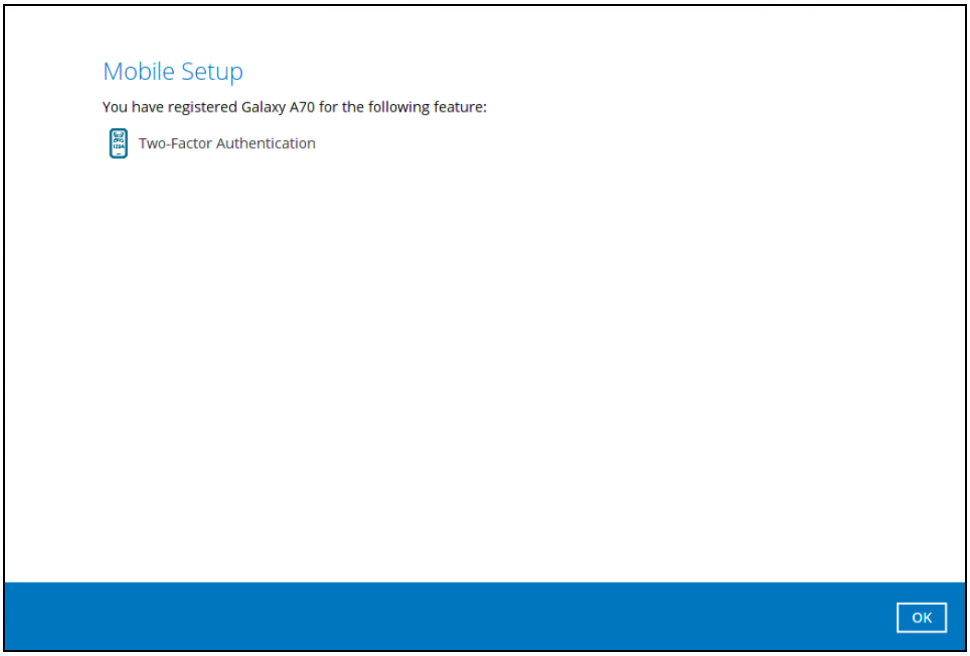
ii. Tap **OK** to continue.



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 the "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.

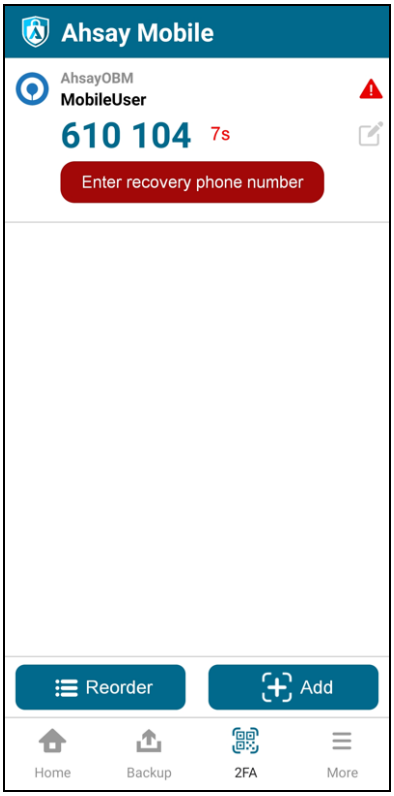


Phone number verification for account recovery

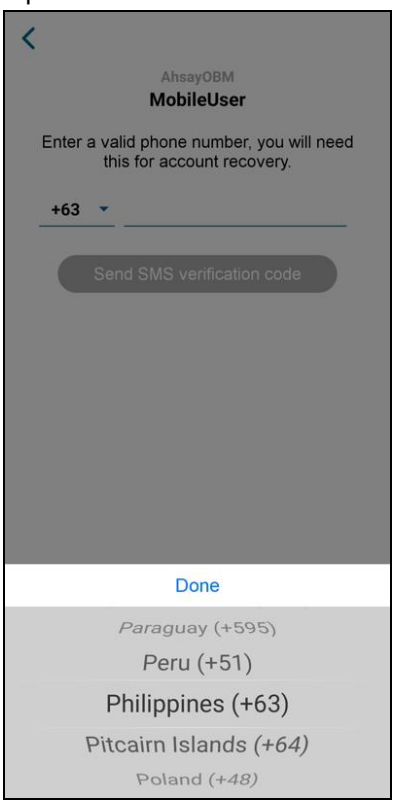
iv. In the Ahsay Mobile app, go to 2FA then enter the phone number for account recovery. Tap **Enter recovery phone number.**

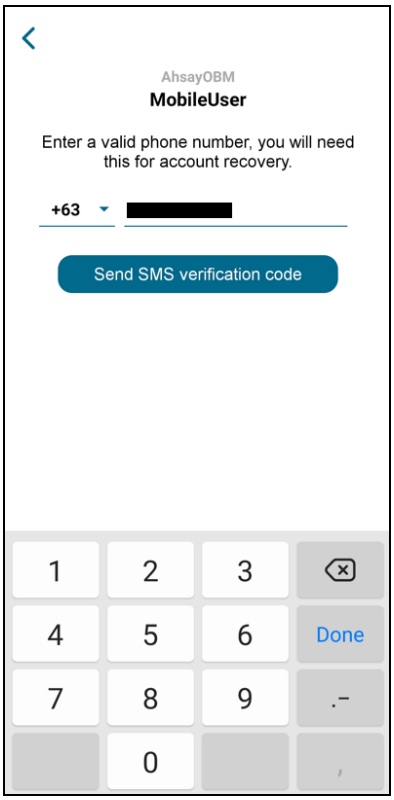
NOTE

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.

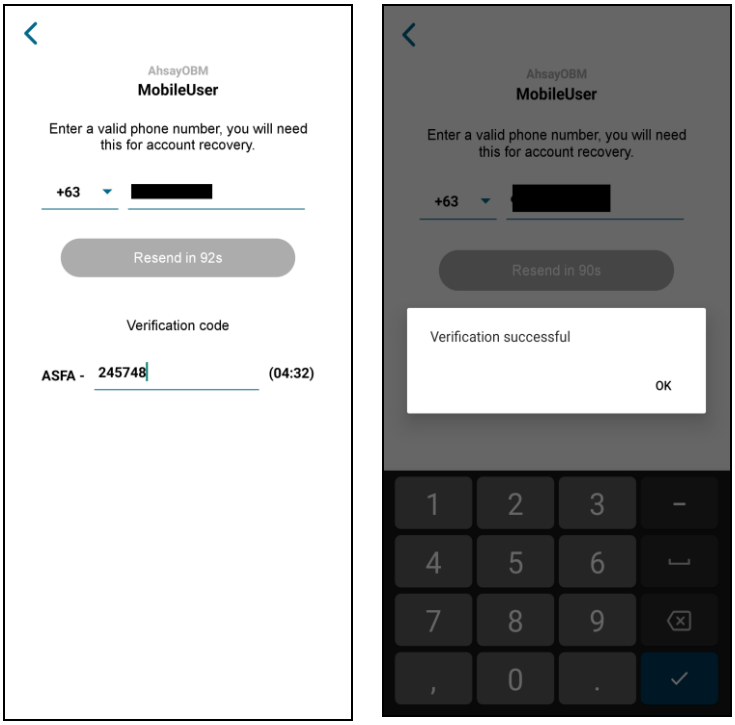


Select your country code and tap **Done**. Enter your phone number then tap **Send SMS verification code**.



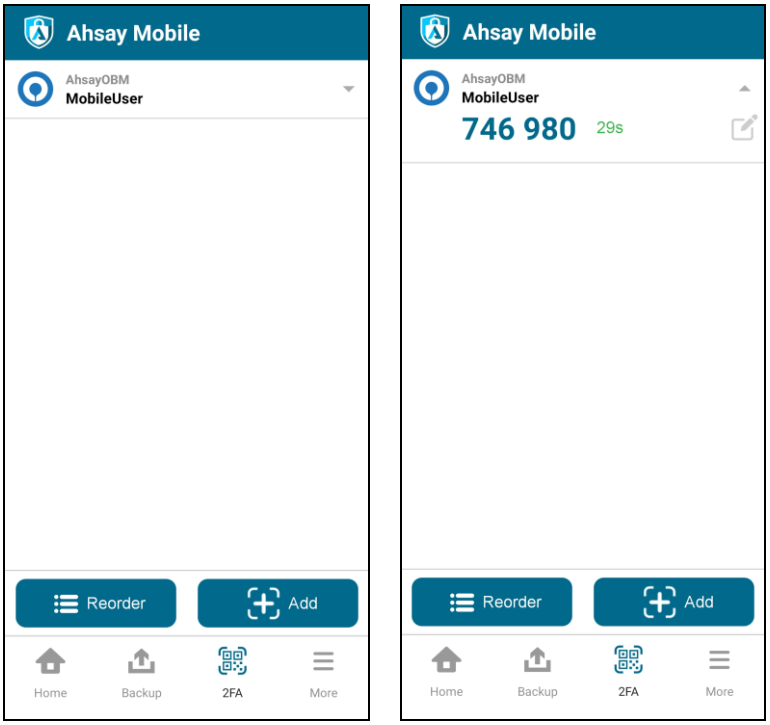


Enter the verification code sent to your mobile device.



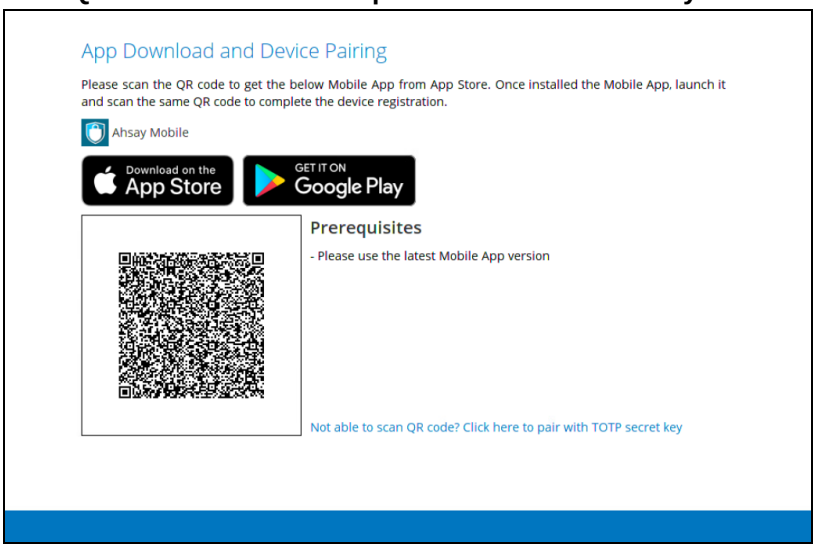
Example of verification code.

Your phone number for account recovery is successfully verified.

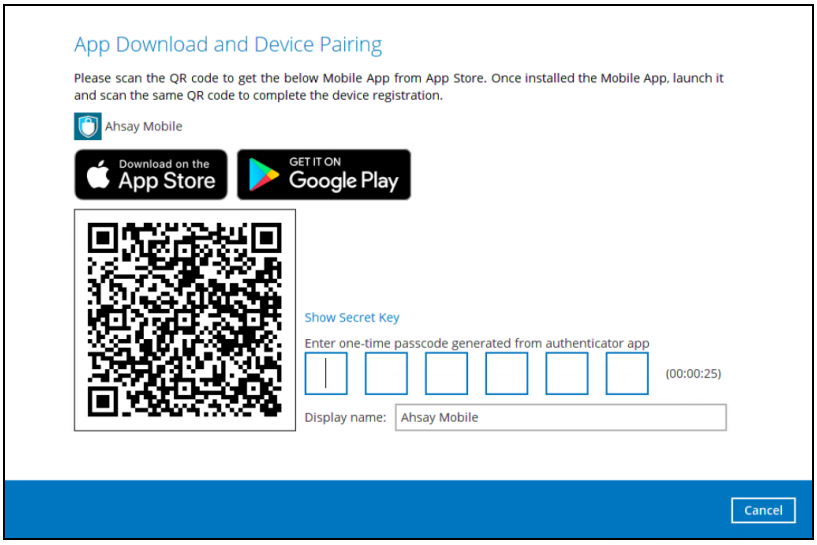


TOTP only

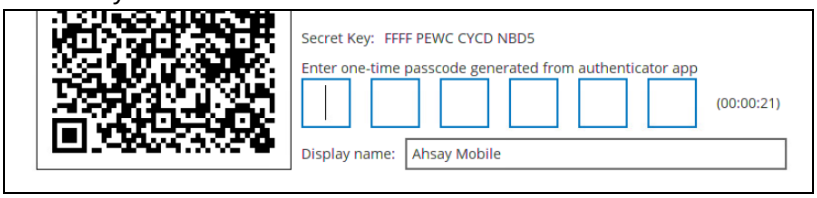
i. To configure a TOTP only 2FA with Ahsay Mobile, click the **"Not able to scan QR code? Click here to pair with TOTP secret key"** link.



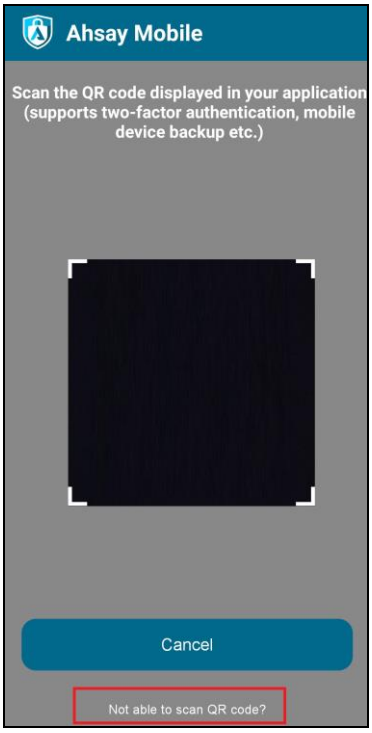
ii. After clicking the **"Not able to scan QR code? Click here to pair with TOTP secret key"** link, the QR code for the TOTP only authenticator will be displayed.

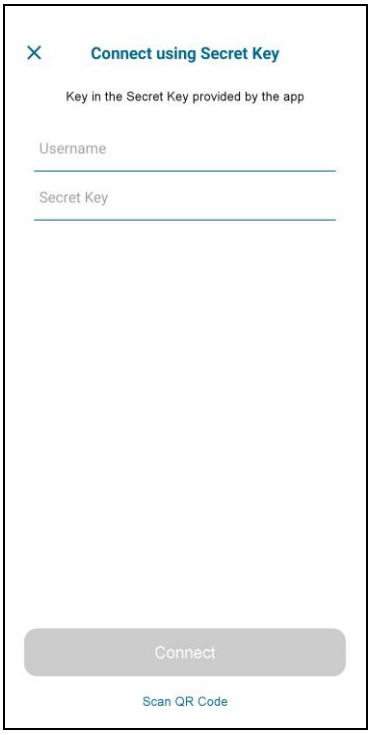


To show the secret key, click the **Show Secret Key** link to display the 16-character alphanumeric secret key. The display name will be "Ahsay Mobile" by default.

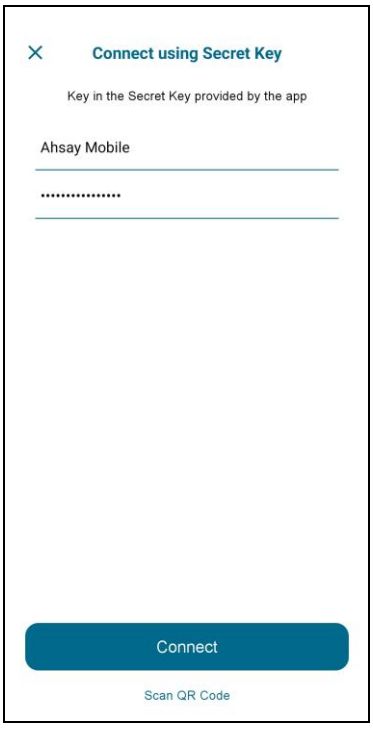


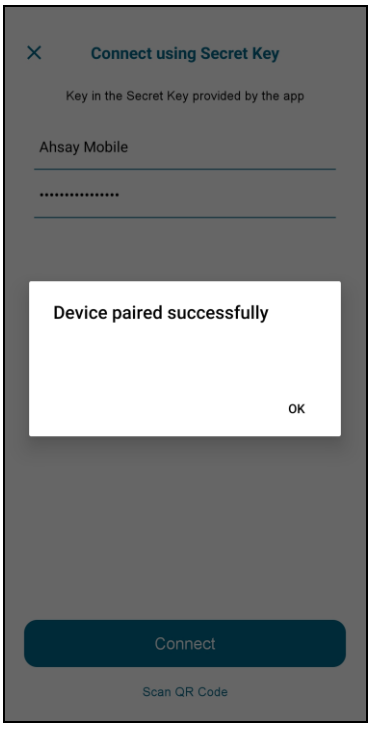
iii. In the Ahsay Mobile app, go to **2FA**. Tap the **Not able to scan QR code?** link.



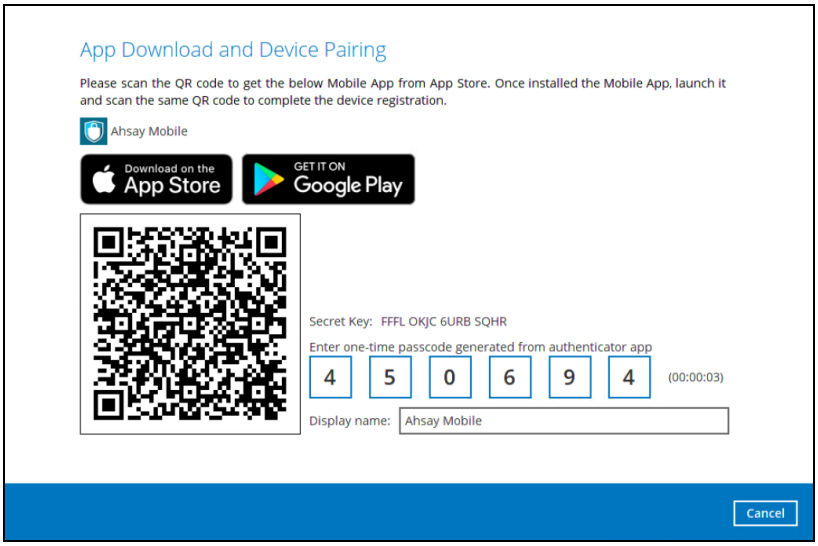


iv. Enter the Username and Secret Key shown in the AhsayOBM then tap **Connect**. Once the device is paired successfully, tap **OK** to continue.

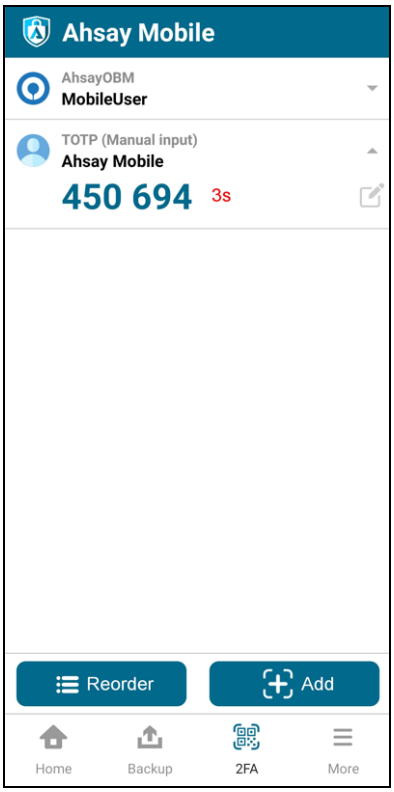




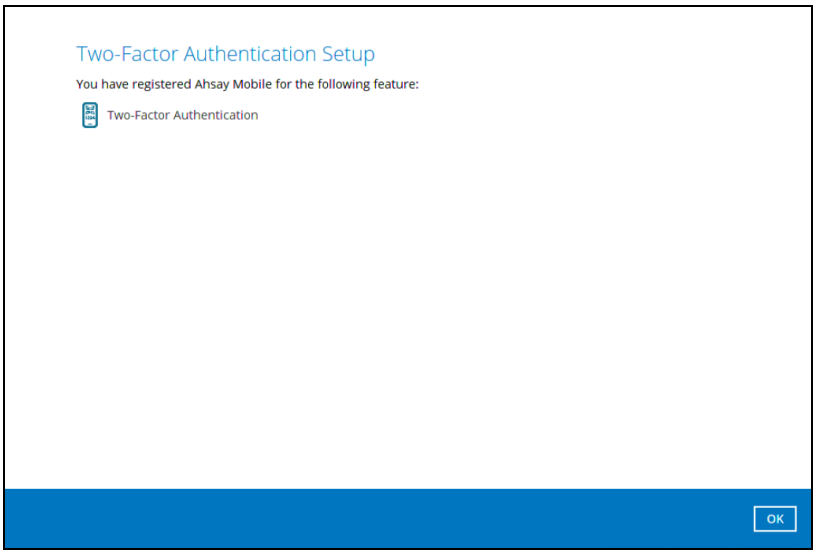
v. Enter the one-time passcode from the Ahsay Mobile app.



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

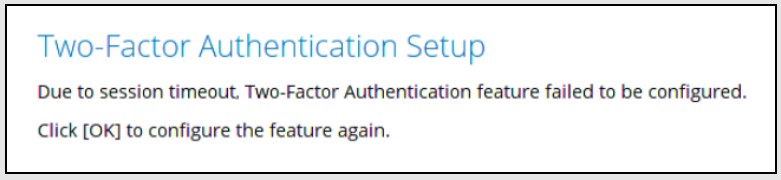


vi. Once the registration is successful, the following screen will be displayed. You have now registered Ahsay Mobile for TOTP only 2FA.

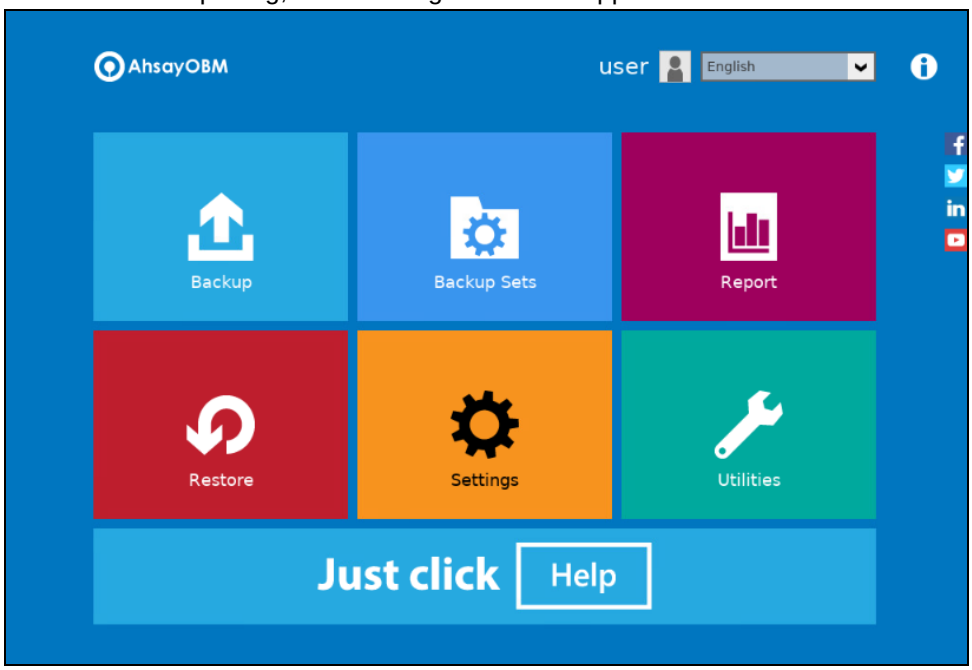


NOTE

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



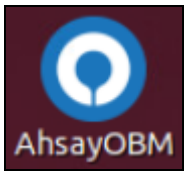
8. After successful pairing, the following screen will appear.



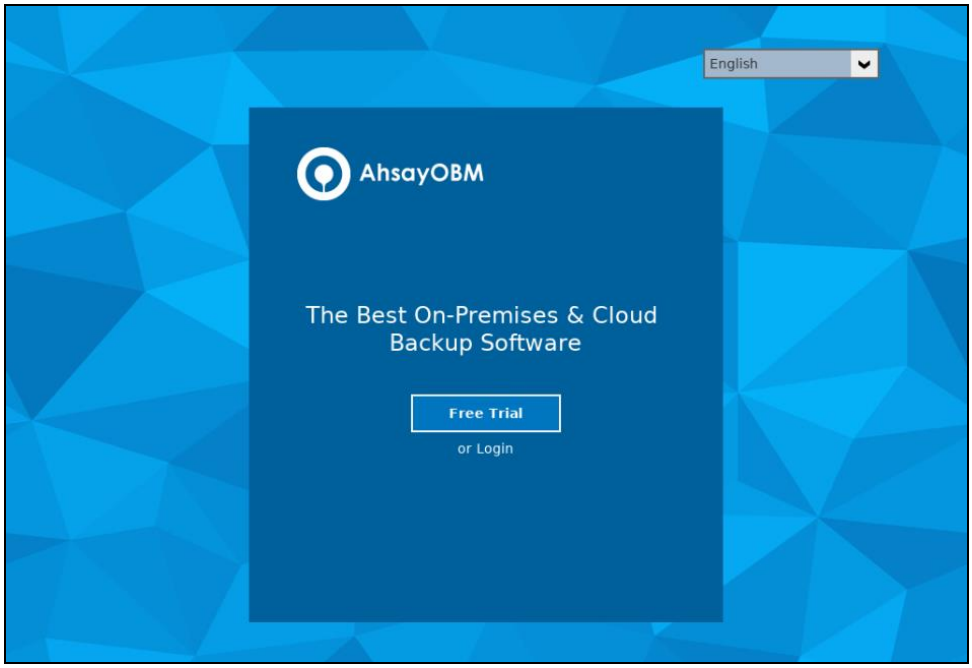
6.1.2 With Mobile Add-on Module

To register a device for 2FA with Mobile Add-on Module enabled, please follow the steps below:

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



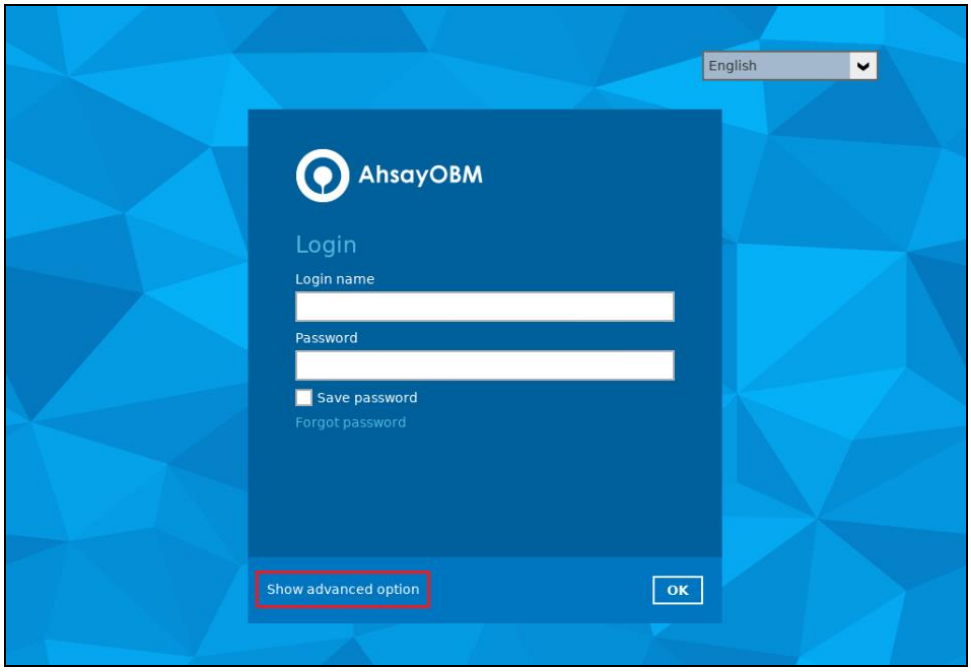
2. The Free Trial Registration option may be displayed when you login for the first time. If you want to create a free trial account please proceed to Appendix G. Otherwise, click **Login** if you already have an AhsayOBM account.



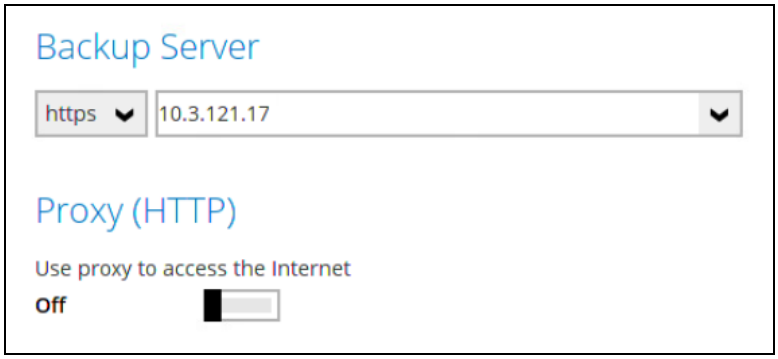
NOTE

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

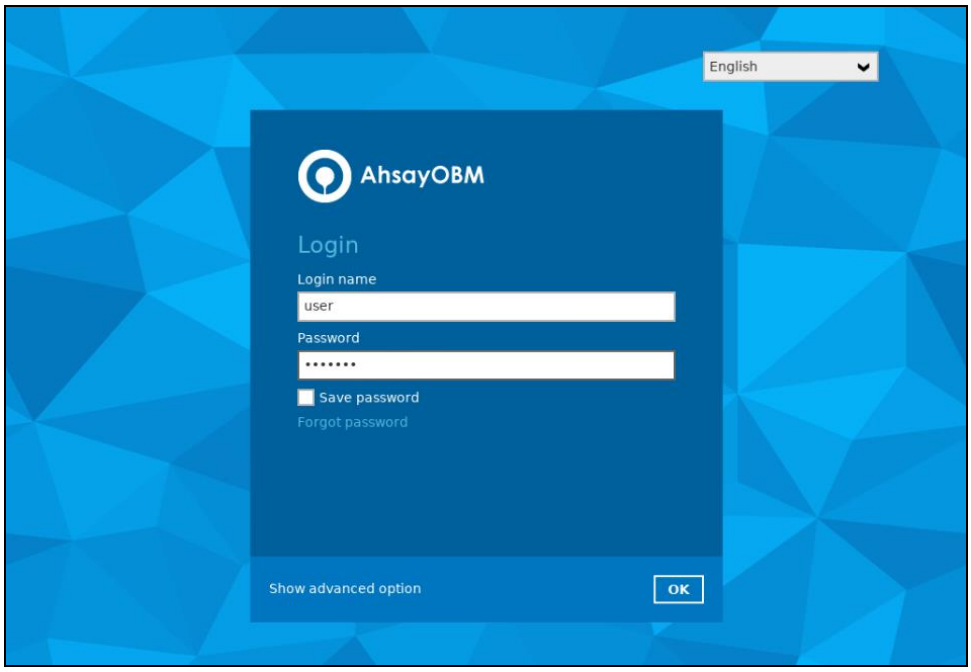
3. The **Show advanced option** may not be available if the backup server settings are already setup by your backup service provider. Please contact your backup service provider for more information.



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



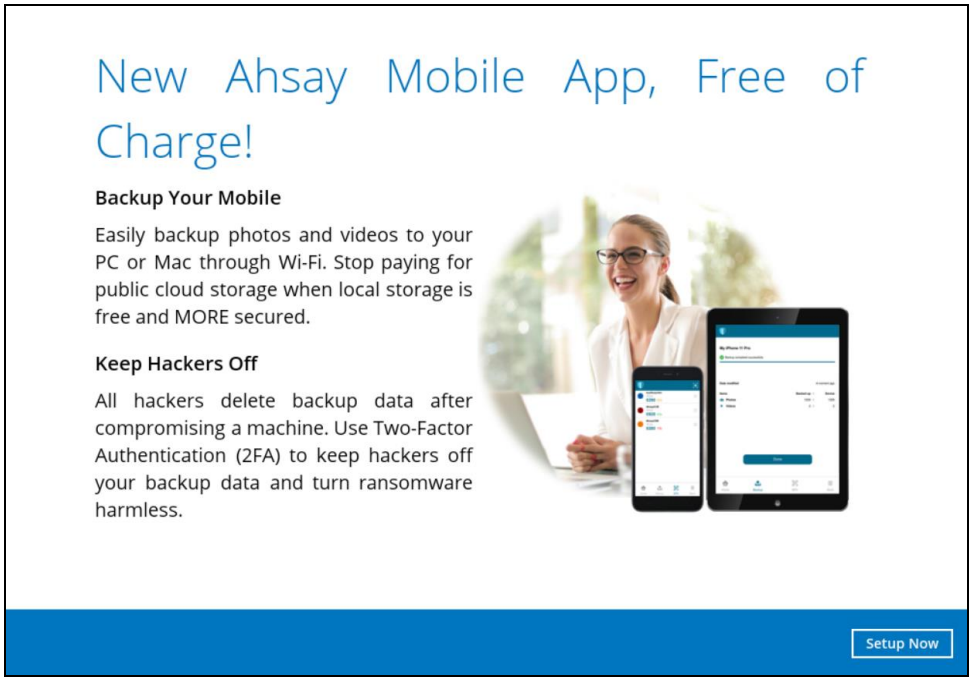
4. Enter the login name and password of your AhsayOBM account provided by your backup service provider. Then, click **OK** to log in.



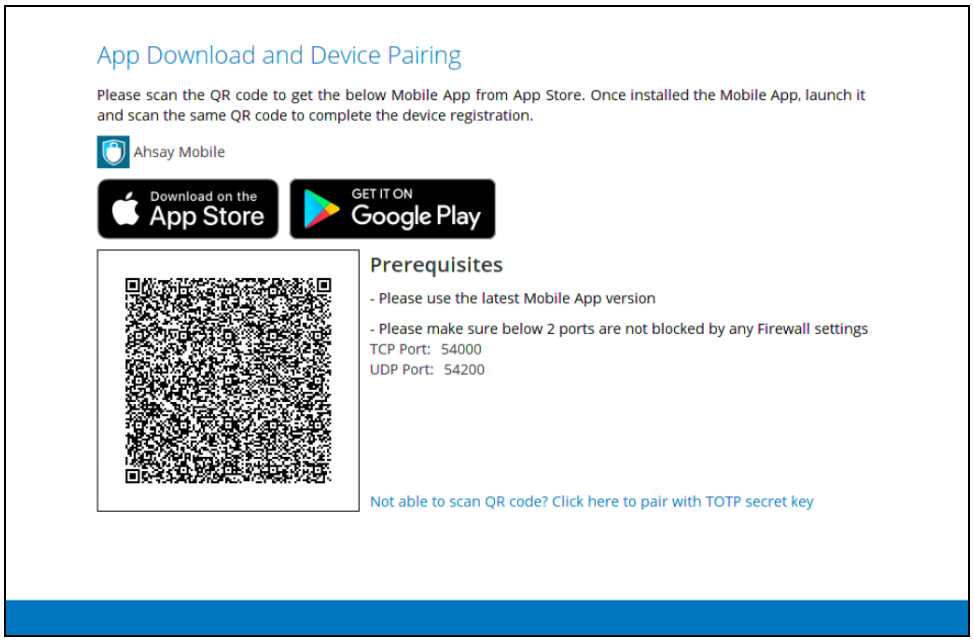
NOTE

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.

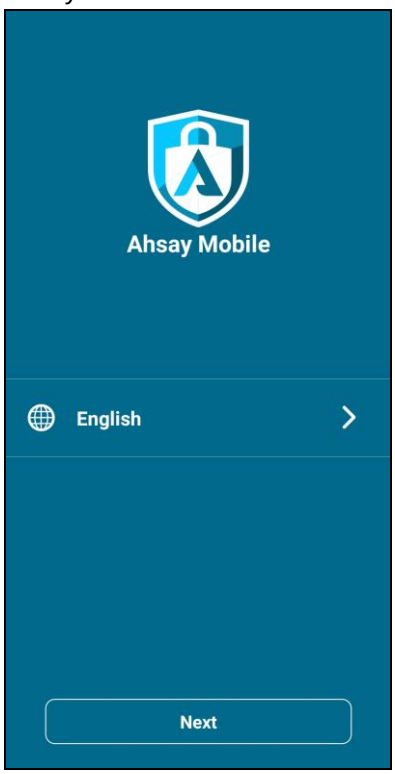
5. You will have the option to set up your 2FA. Click **Setup Now.**



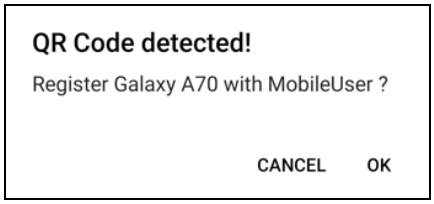
6. Download the Ahsay Mobile app from the App Store / Google Play Store. Ensure that the displayed Prerequisites are met.



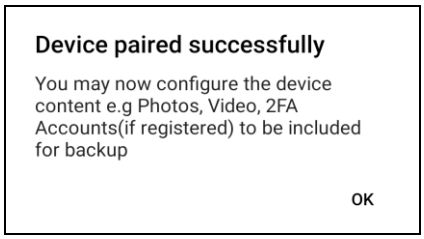
7. Using the Ahsay Mobile app, tap **Next** and scan the QR code displayed in AhsayOBM.



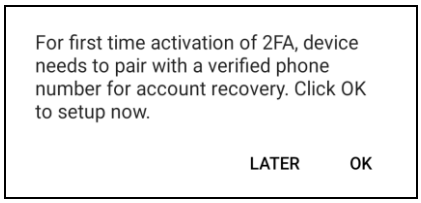
Tap **OK** to continue.



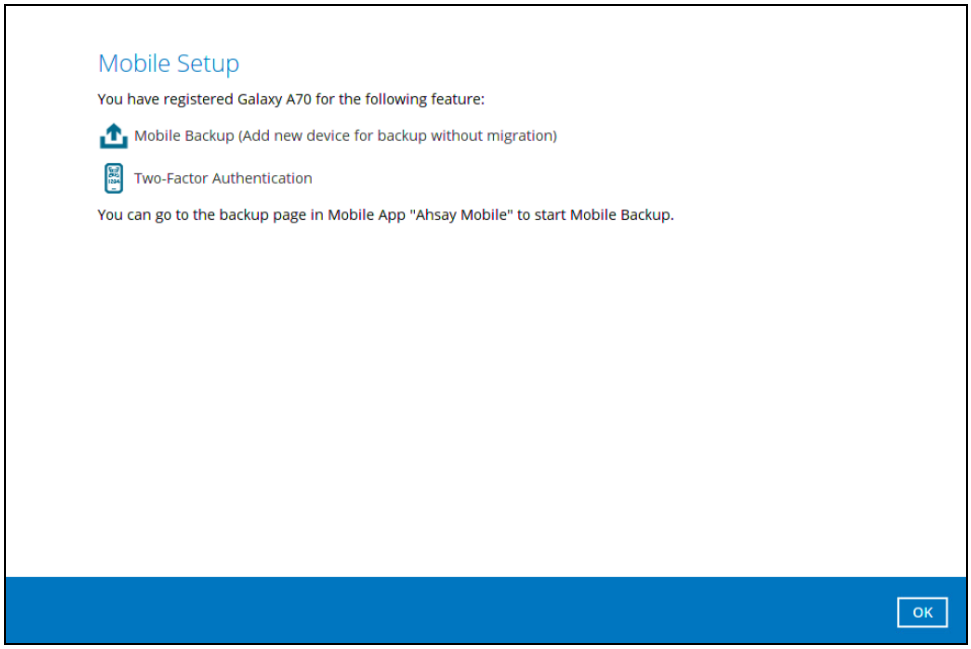
Once the device is successfully paired for mobile backup, the following message will be displayed in the Ahsay Mobile app. Tap **OK** to continue.



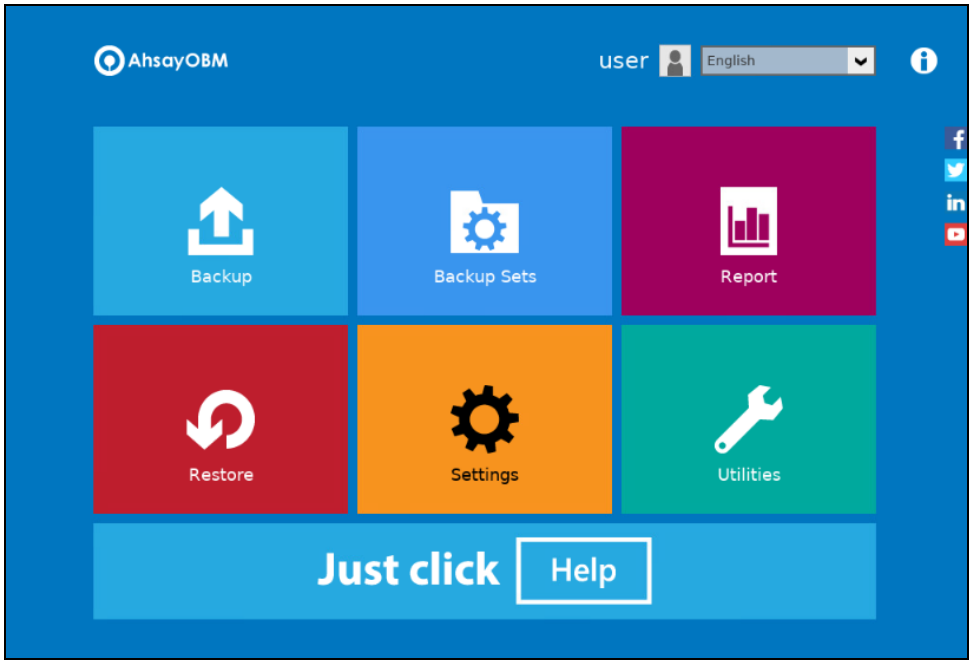
Once the device is successfully paired for 2FA, the following message will be displayed in the Ahsay Mobile app. You can set up a recovery number here that will be used in the "Authentication Recovery" procedure by tapping **OK**. You may refer to Phone number verification for account recovery in Chapter 6.1.1 for the following setup. Otherwise, tap **LATER** to set it up later on.



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



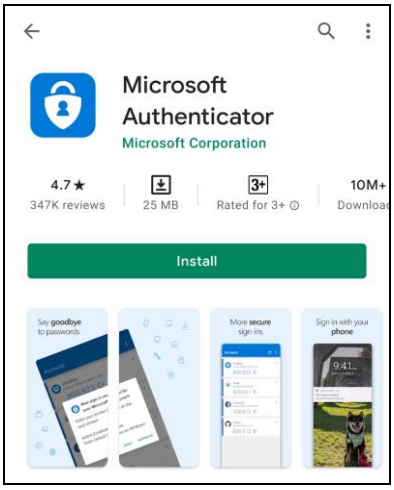
9. After successful pairing, the following screen will appear.



6.2 Using Microsoft Authenticator

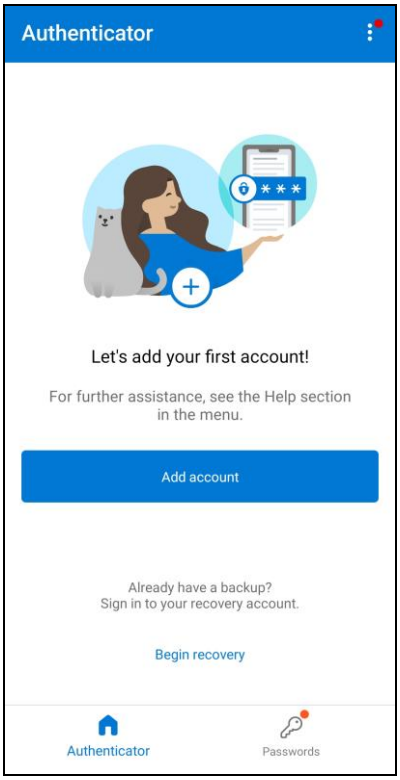
To register a device for TOTP 2FA in AhsayOBM using Microsoft Authenticator, please follow the steps below:

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

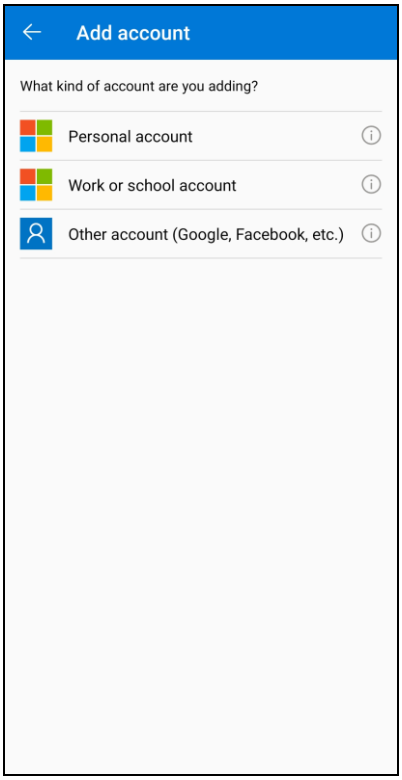


2. Launch the Microsoft Authenticator app.

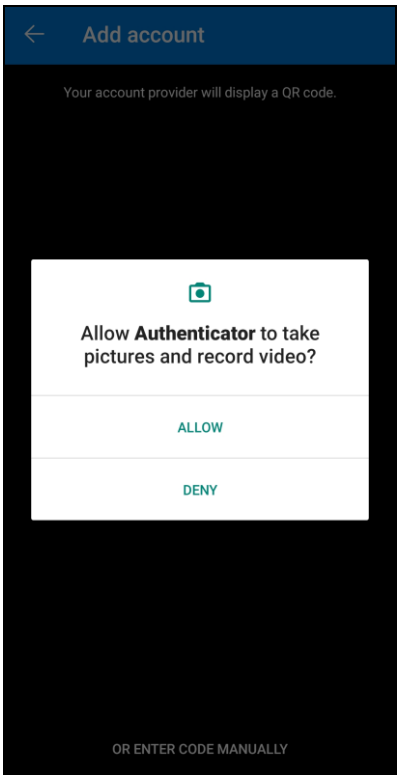
3. Tap **Add account**.



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



5. Allow permission to take pictures and record video.

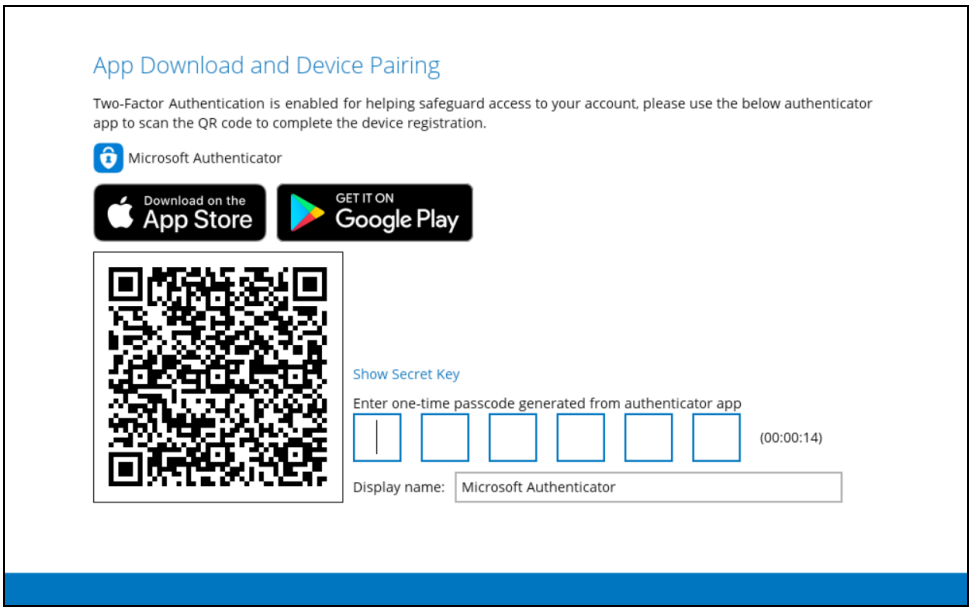


6. Set up the account by selecting from the following methods: Scan the QR code or Enter code manually.

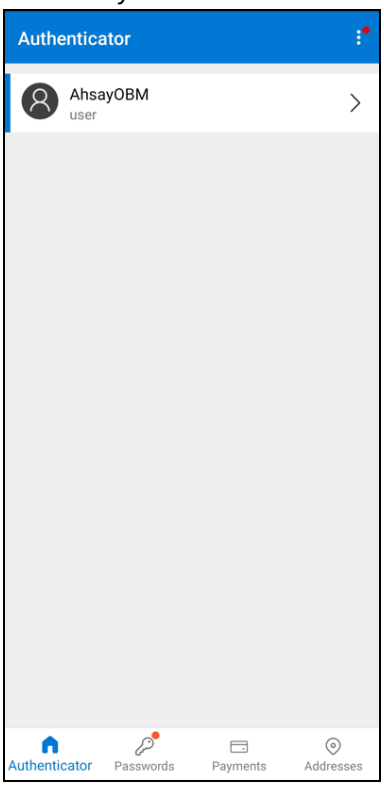
Method 1: Scan the QR code

i. Scan the QR code on AhsayOBM.

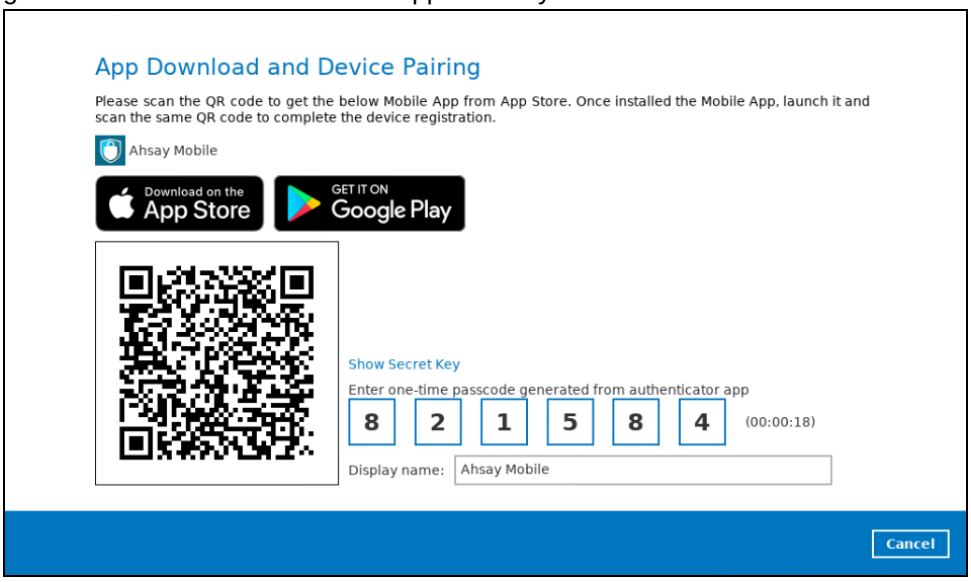
Example of the displayed QR code:



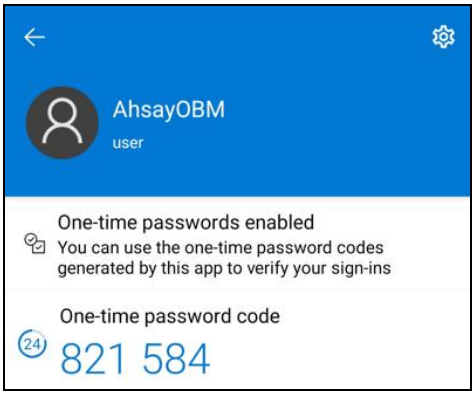
ii. The AhsayOBM account is successfully added to Microsoft Authenticator.



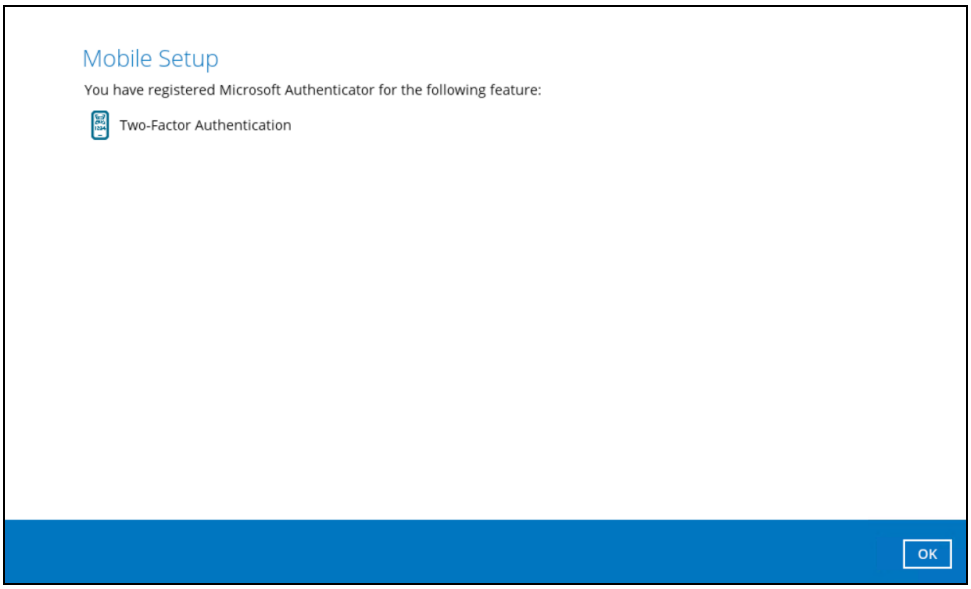
iii. Once the account is added to Microsoft Authenticator, enter the one-time passcode generated from the authenticator app in AhsayOBM.



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.

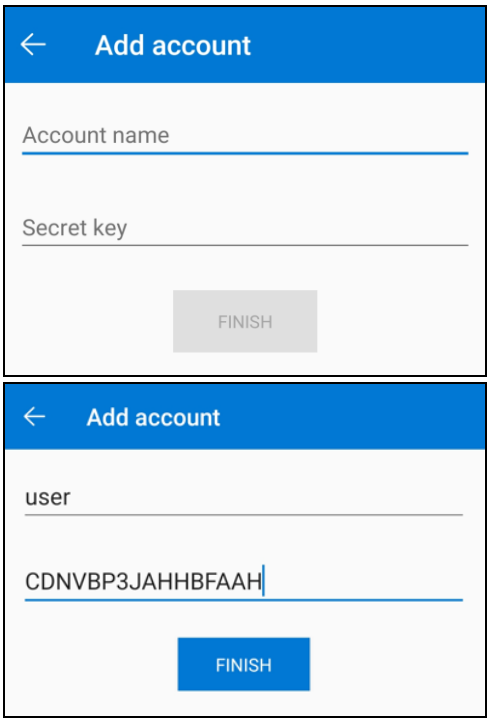


Method 2: Enter Code Manually

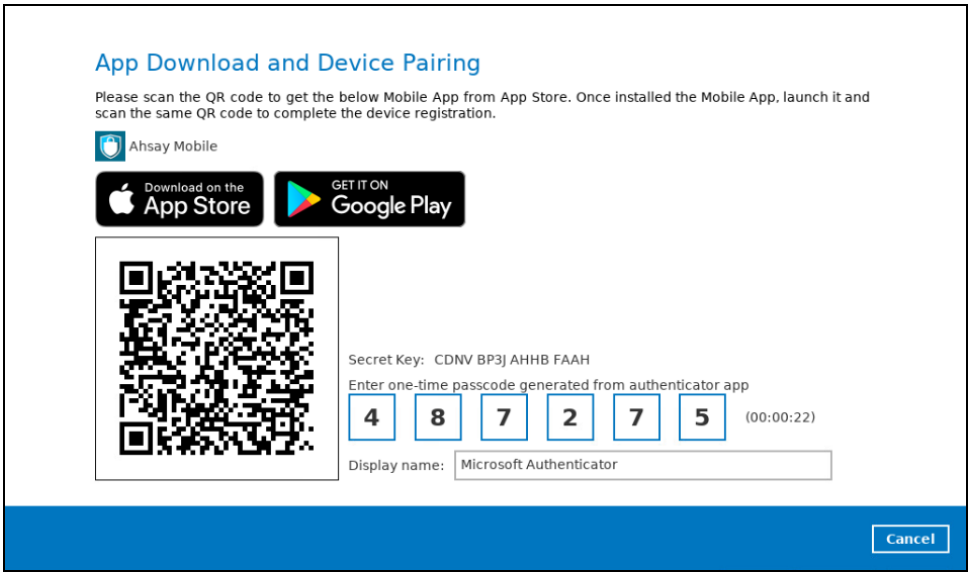
i. Tap **OR ENTER CODE MANUALLY**.

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

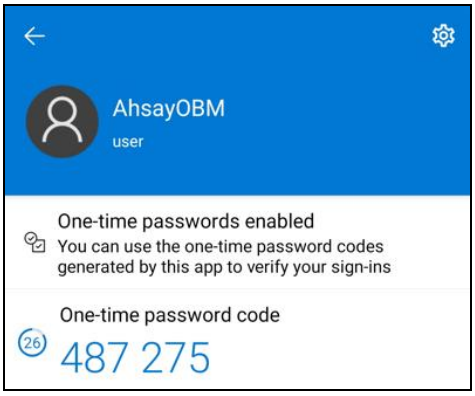
iii. On the Microsoft Authenticator app, input an account name, then enter the displayed Secret Key in the AhsayOBM. Tap **FINISH** to proceed.



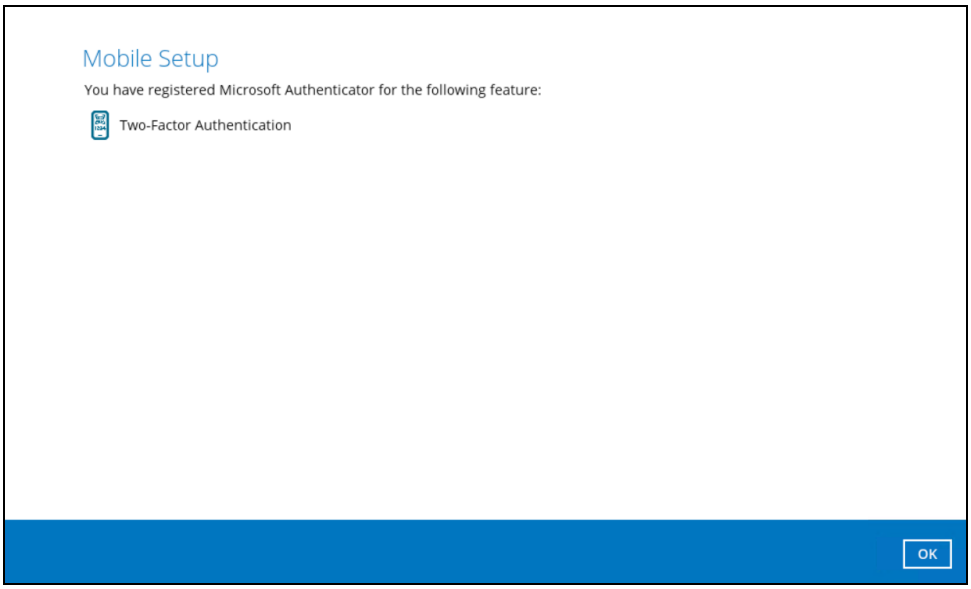
iv. Once the account is added to Microsoft Authenticator, enter the one-time passcode generated from the authenticator app in AhsayOBM.



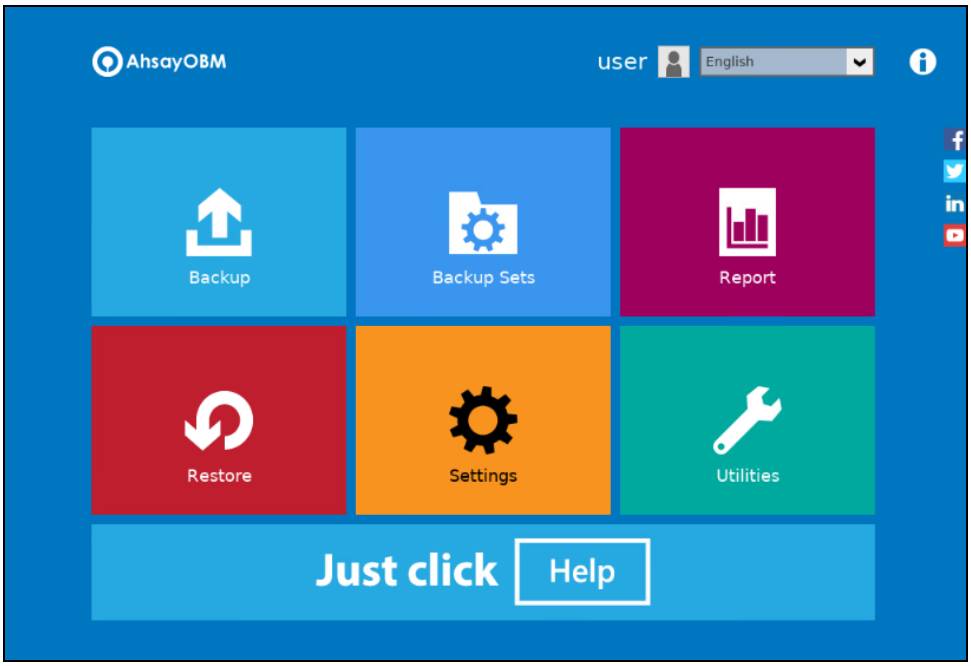
Example of the one-time passcode generated:



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



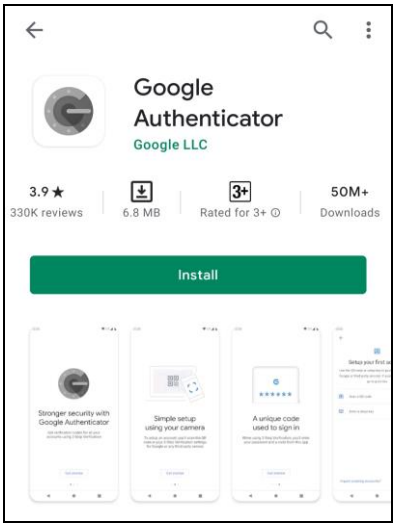
7. After successful pairing, the following screen will appear.



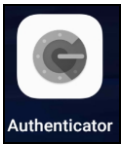
6.3 Using Google Authenticator

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

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



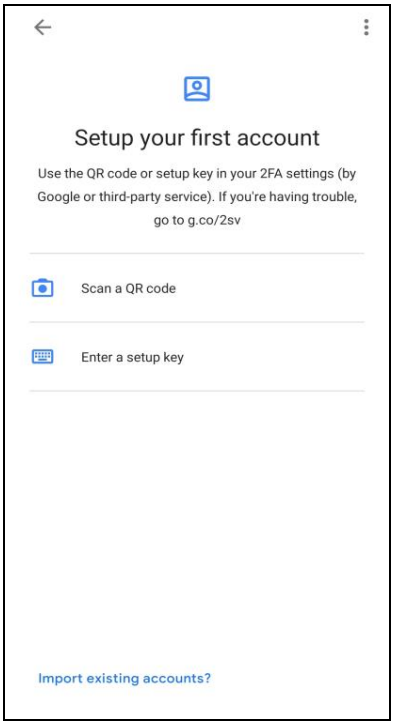
2. Launch the Google Authenticator app.



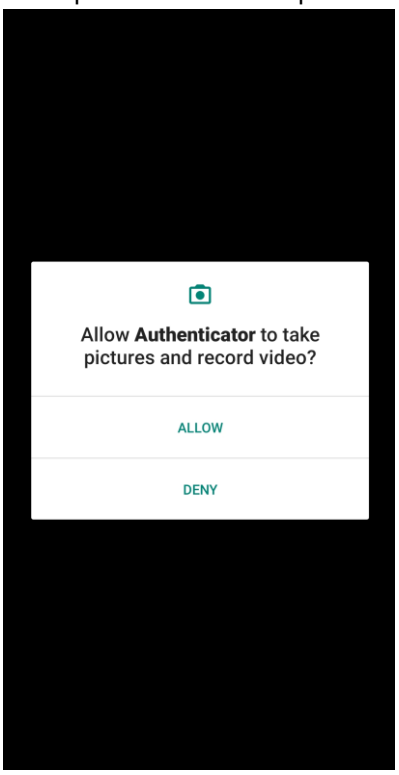
3. Set up the account by selecting from the following methods: Scan the QR code or Enter a setup key manually.

Method 1: Scan the QR code

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

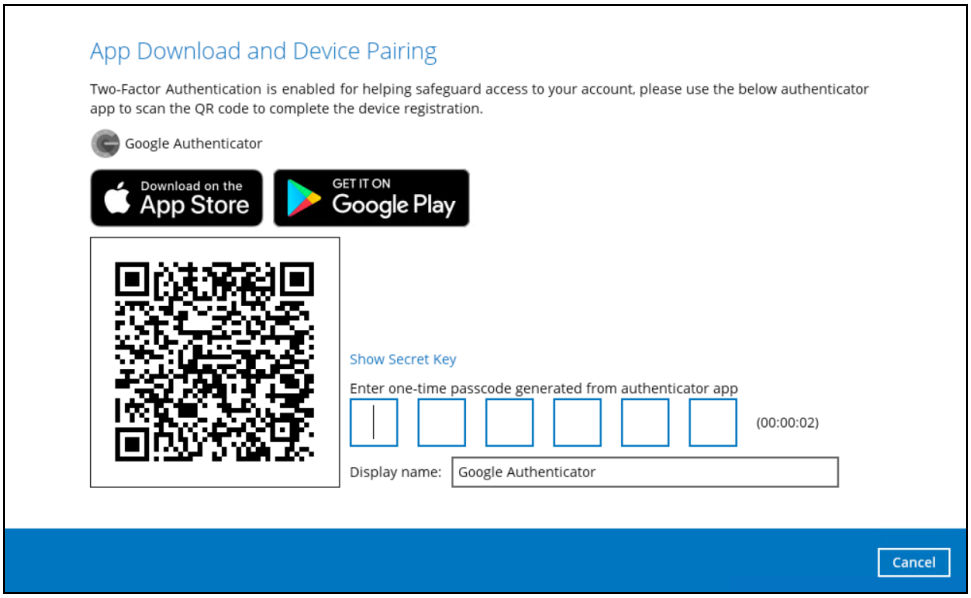


ii. Allow permission to take pictures and record video.

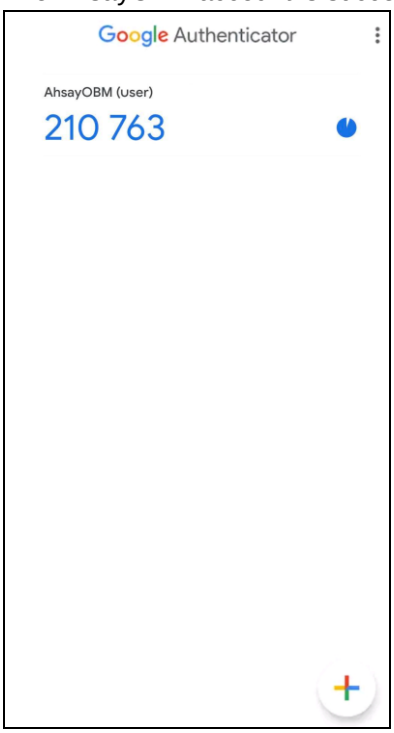


iii. Scan the QR code on AhsayOBM.

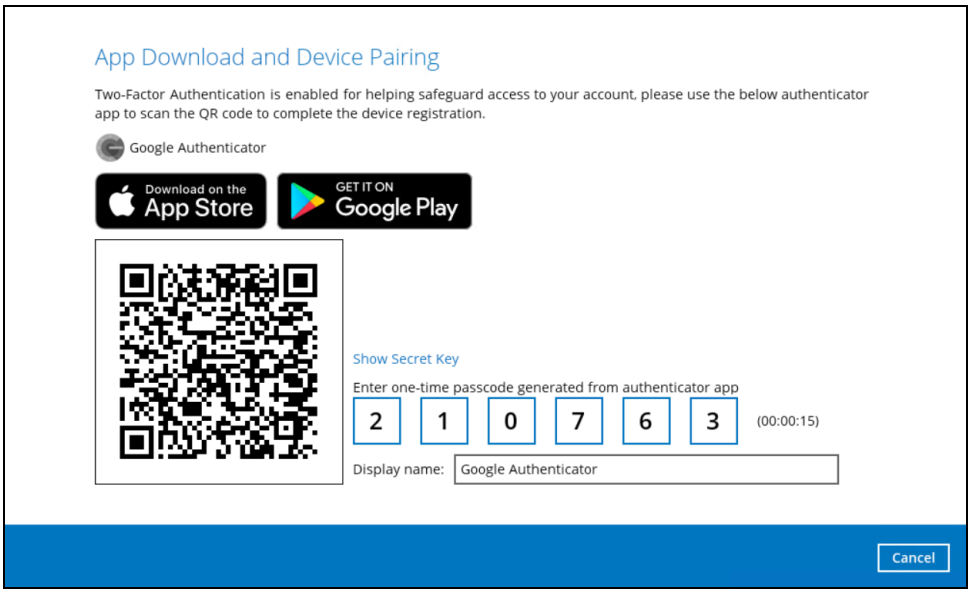
Example of the displayed QR code:



iv. The AhsayOBM account is successfully added to Google Authenticator.

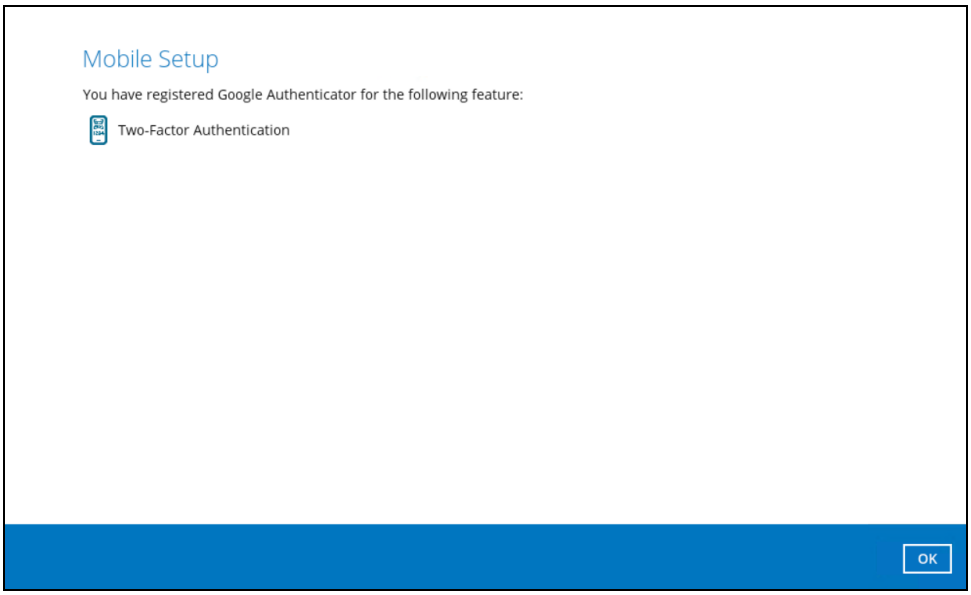


v. Once the account is added to Google Authenticator, enter the one-time passcode generated from the authenticator app in AhsayOBM.



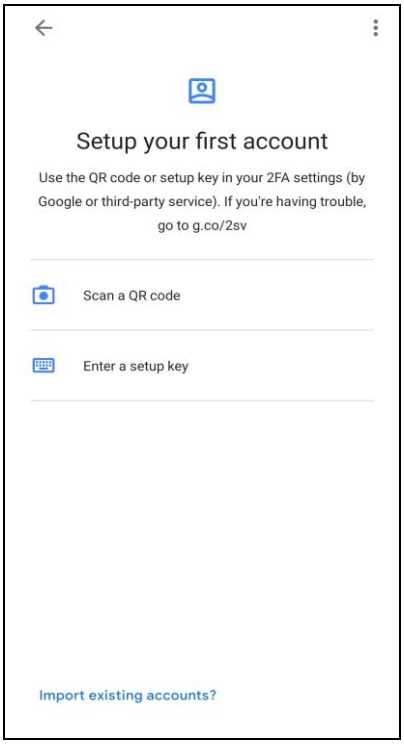
Example of the one-time passcode generated:

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

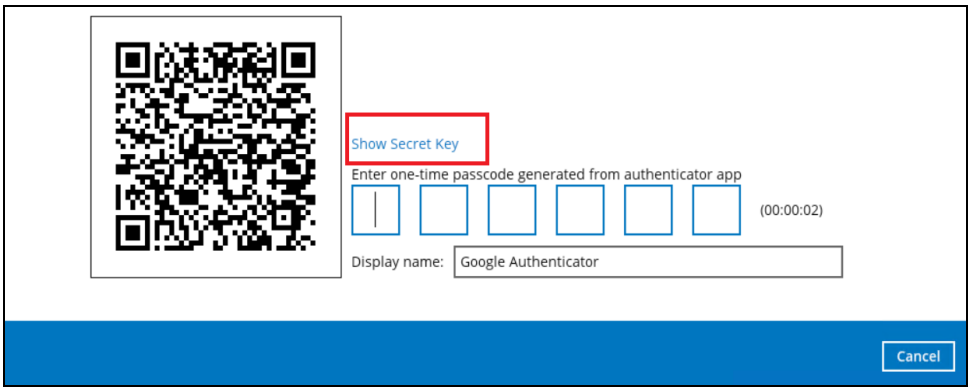


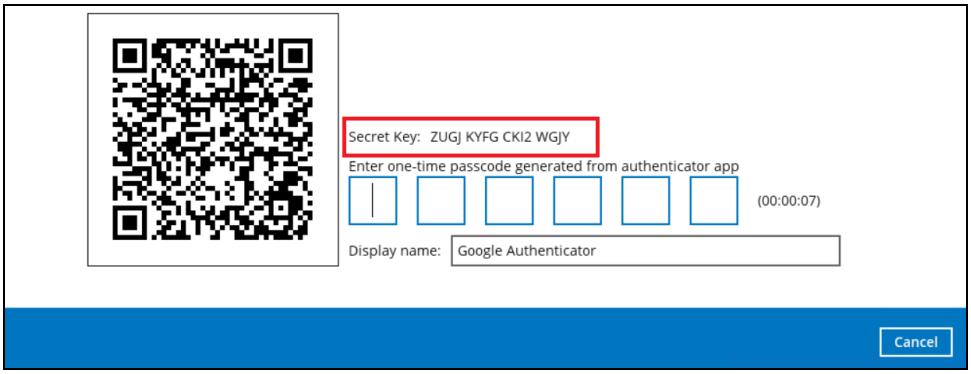
Method 2: Enter a setup key manually

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

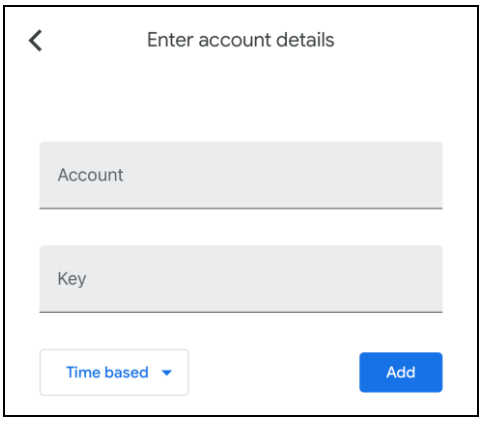


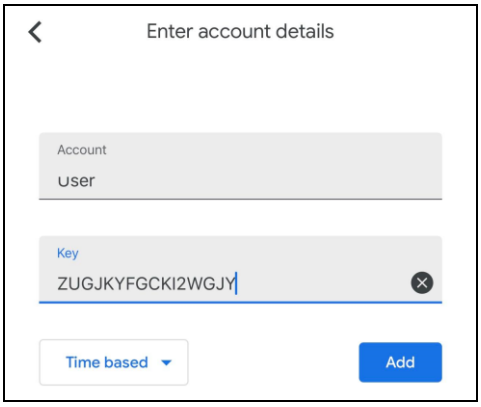
ii. Click the **Show Secret Key** link in the AhsayOBM to display the Secret Key which must be entered manually in Google Authenticator.



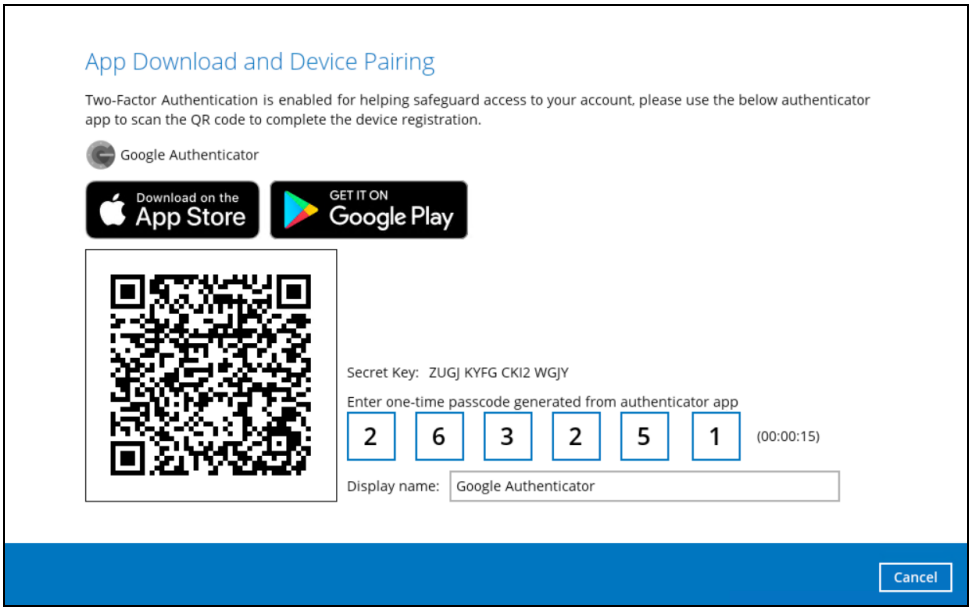


iii. On the Google Authenticator app, input an account name, then enter the displayed Secret Key in the AhsayOBM. Tap **Add** to proceed.

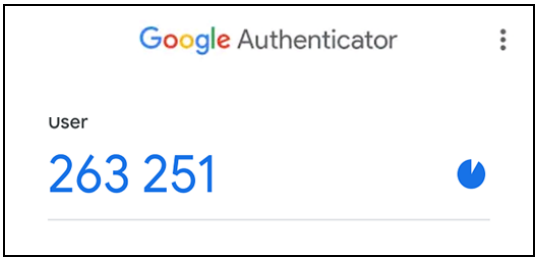




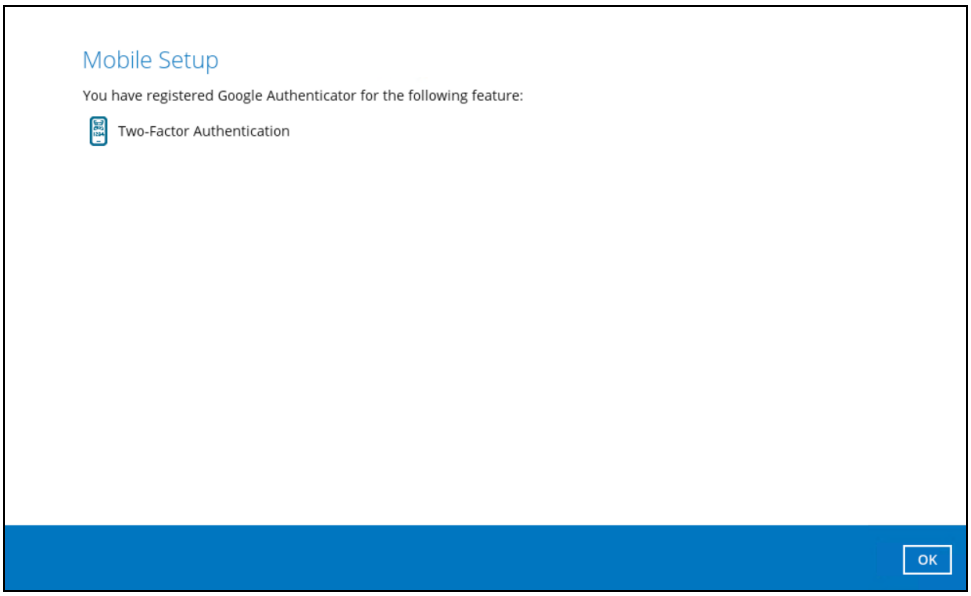
iv. Once the account is added to Google Authenticator, enter the one-time passcode generated from the authenticator app in AhsayOBM.



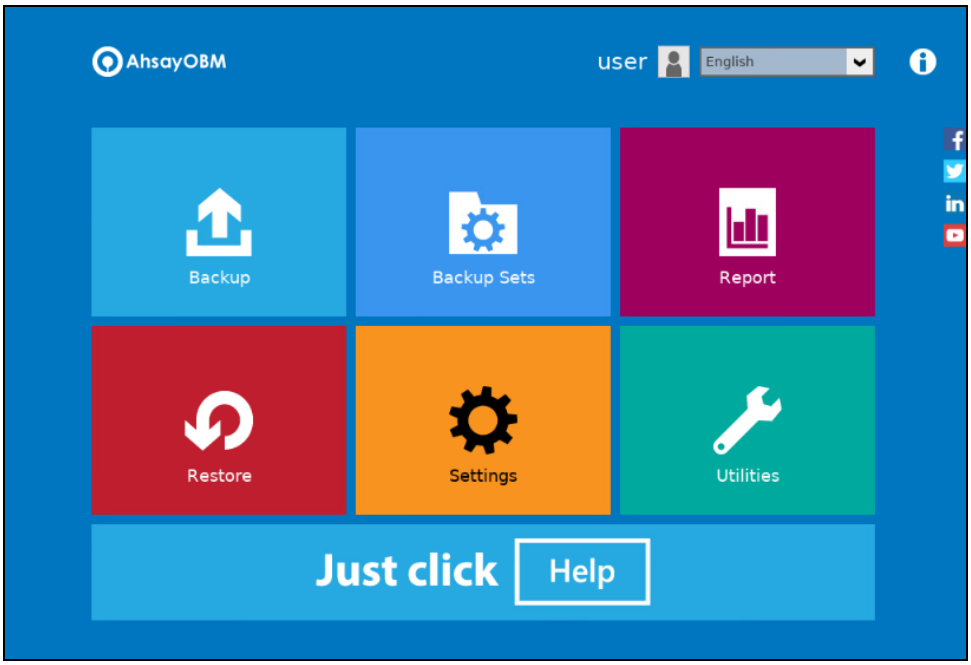
Example of the one-time passcode generated:



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



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



7 Logging in to AhsayOBM

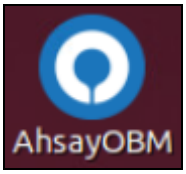
Login steps without 2FA and with 2FA using the different types of authenticator will be discussed in this chapter.

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

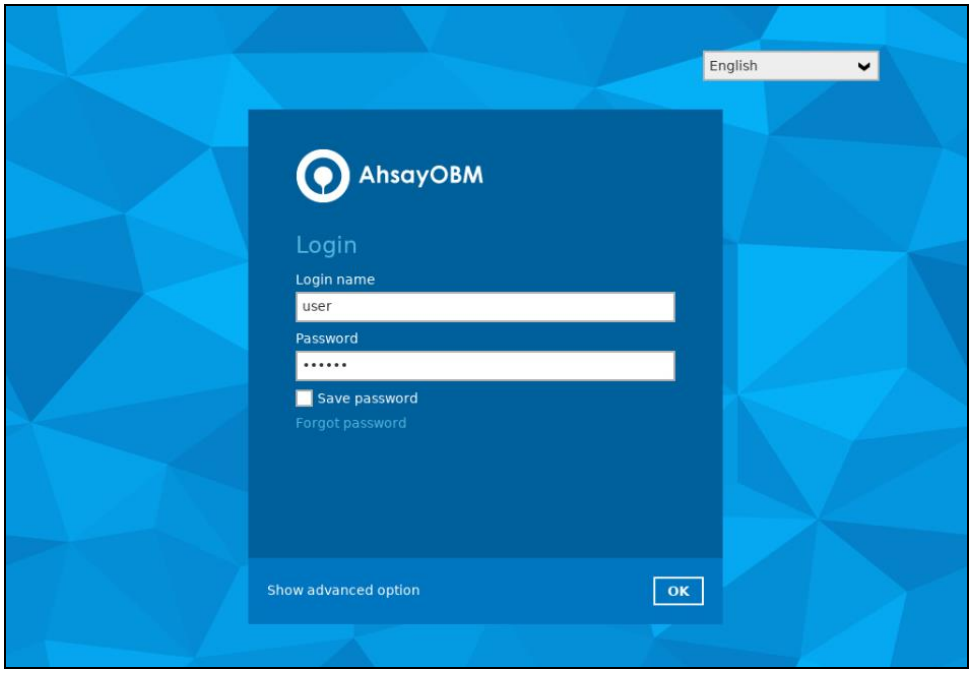
7.1 Login to AhsayOBM without 2FA

When logging in to AhsayOBM without Two-Factor Authentication, please follow the steps below:

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



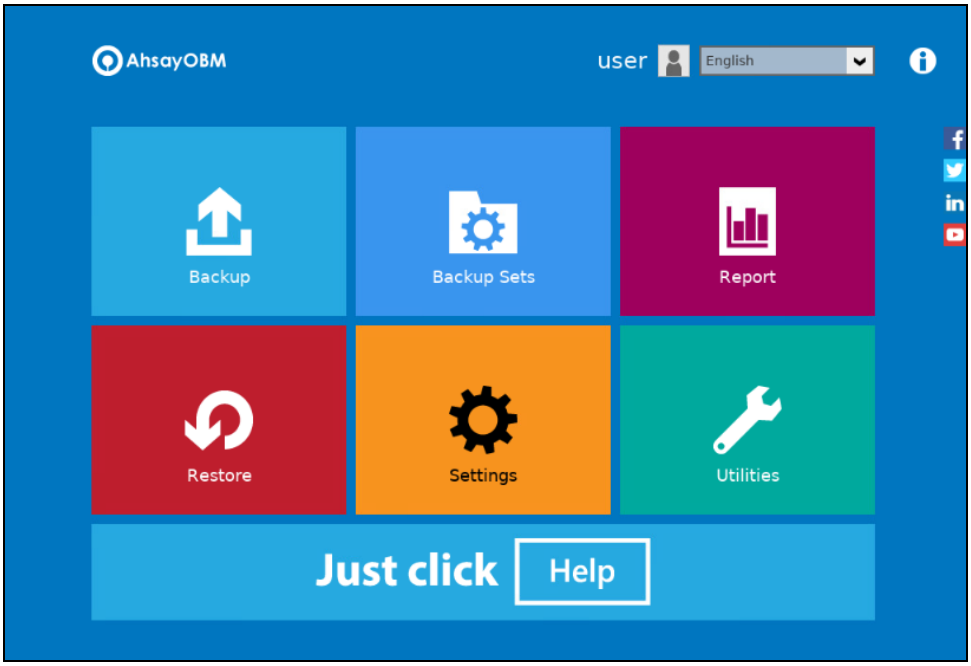
2. Enter the login name and password of your AhsayOBM account provided by your backup service provider. Then, click **OK** to login.



NOTE

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

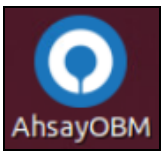
3. After successful login, the following screen will appear.



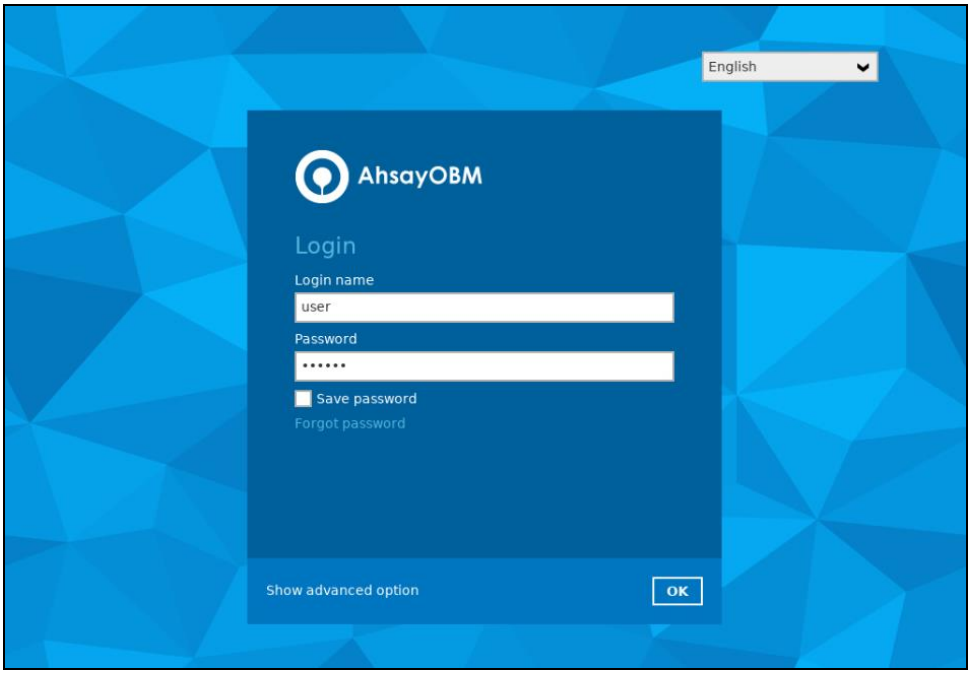
7.2 Login to AhsayOBM with 2FA using Ahsay Mobile Authenticator

When logging in to AhsayOBM with Two-Factor Authentication using Ahsay Mobile Authenticator, please follow the steps below:

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



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



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.

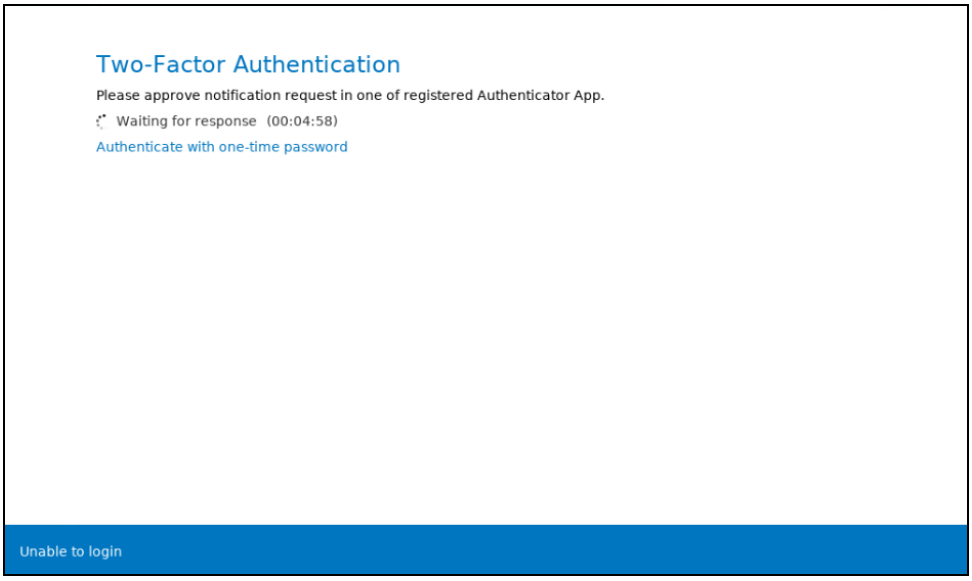
Please refer to the Ahsay Mobile User Guide for Android and iOS – Appendix A: Troubleshooting Login if you are experiencing problems logging into AhsayOBM with Two-Factor Authentication using Ahsay Mobile app.

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

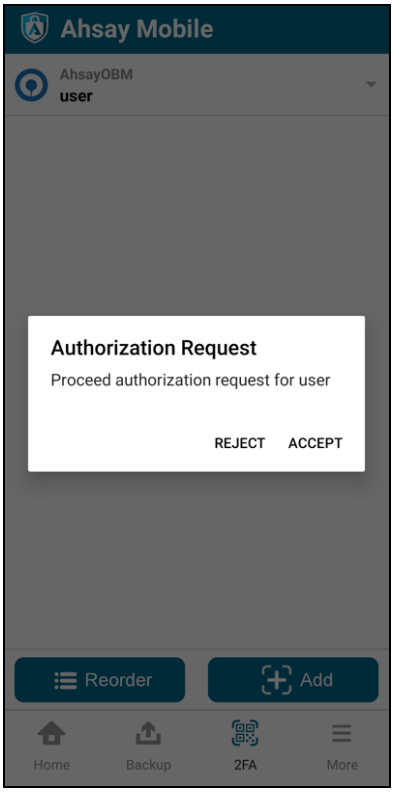
- **Push Notification and TOTP (default mode)**

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

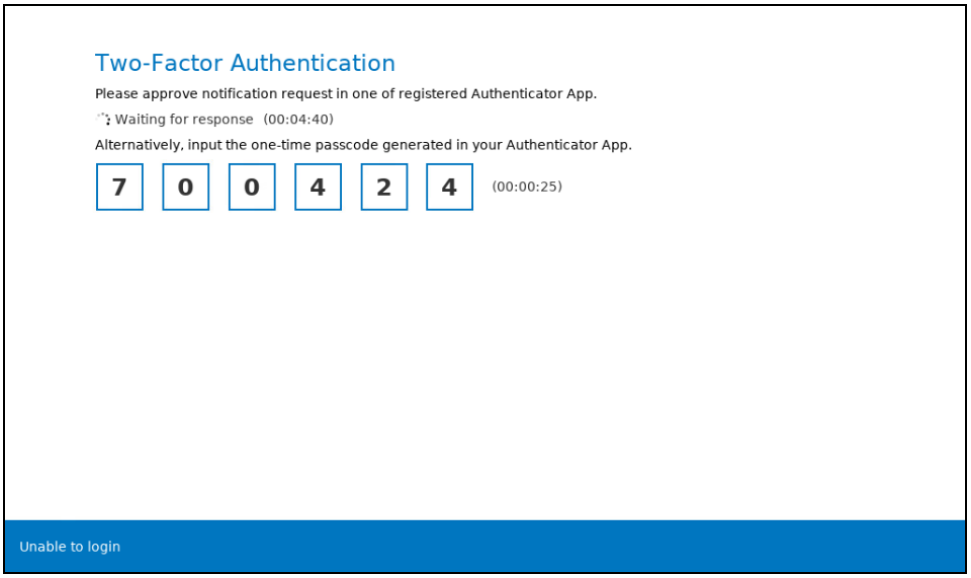
  Example of the 2FA alert screen on AhsayOBM after login with correct username and password:



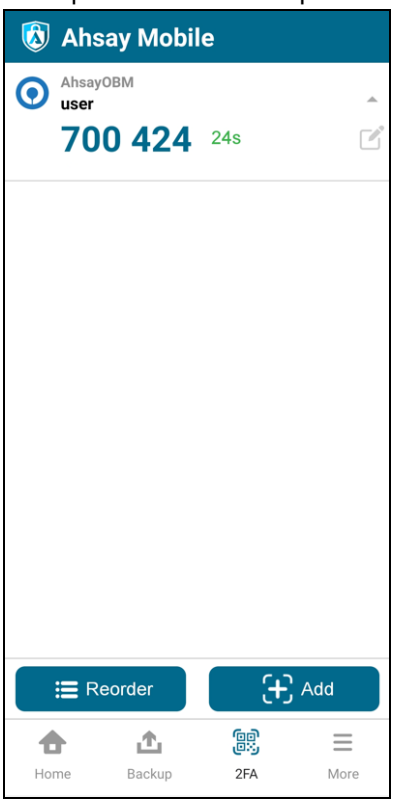
Example of the login request sent to the Ahsay Mobile:



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.

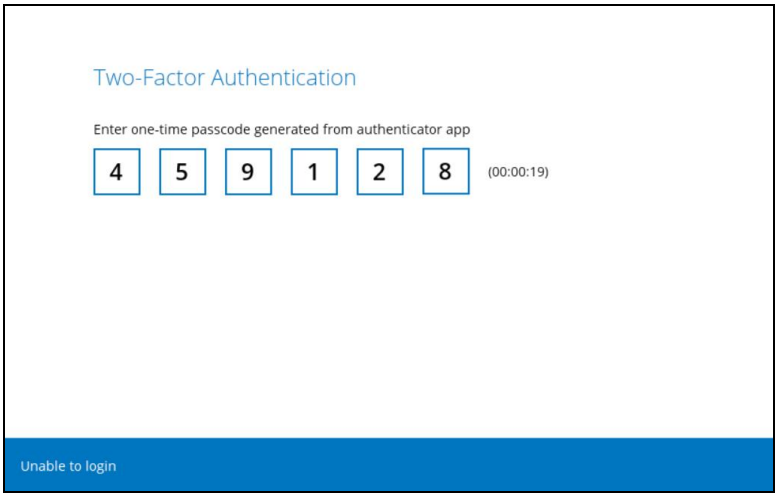


Example of the one-time password generated by Ahsay Mobile:

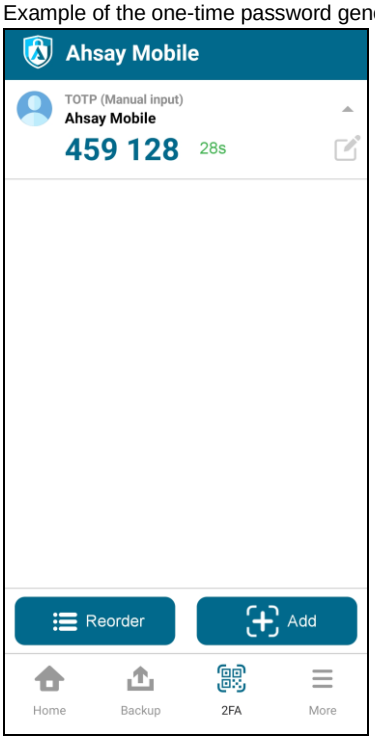


- **TOTP only**

  Input the one-time password generated by Ahsay Mobile to complete the login. Example of the 2FA alert screen on AhsayOBM after login with correct username and password.



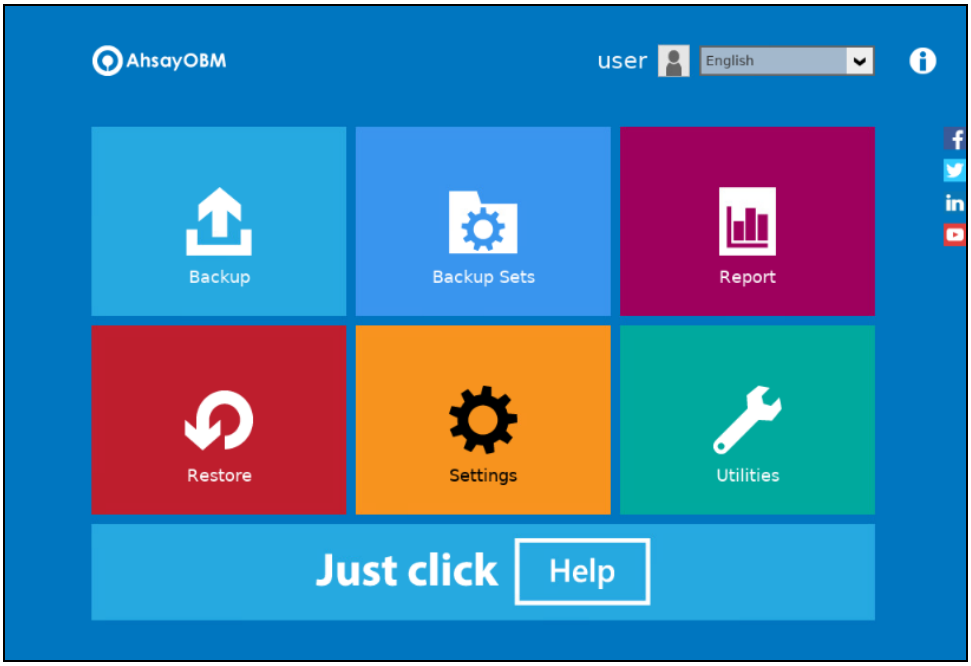
Example of the one-time password generated by Ahsay Mobile:



NOTE

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

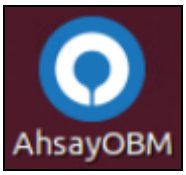
4. After successful login, the following screen will appear.



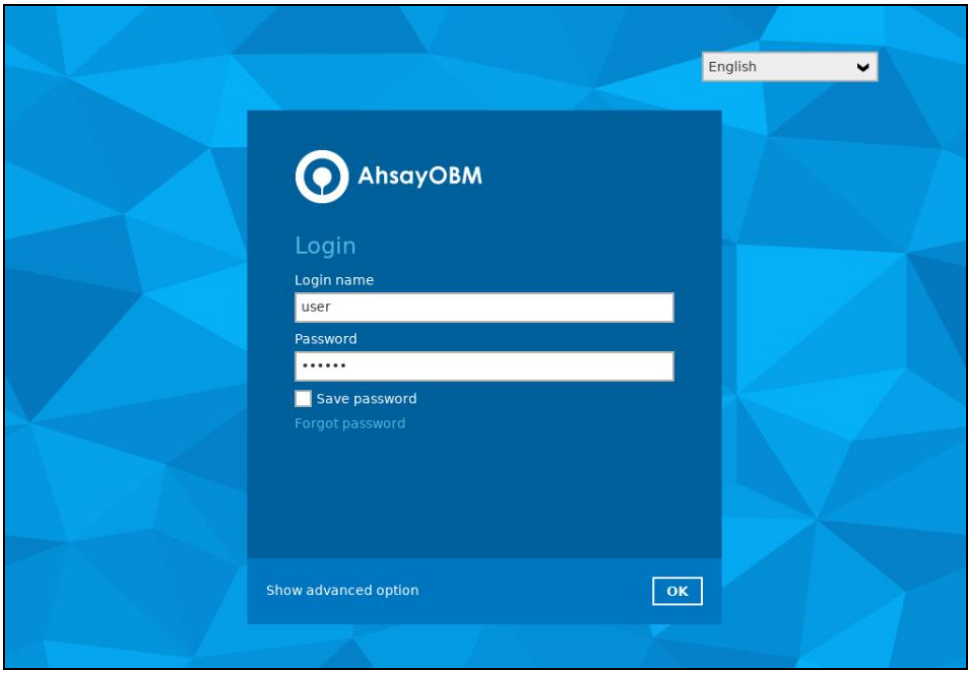
7.3 Login to AhsayOBM with 2FA using Microsoft Authenticator

When logging in to AhsayOBM with Two-Factor Authentication using Microsoft Authenticator, please follow the steps below:

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



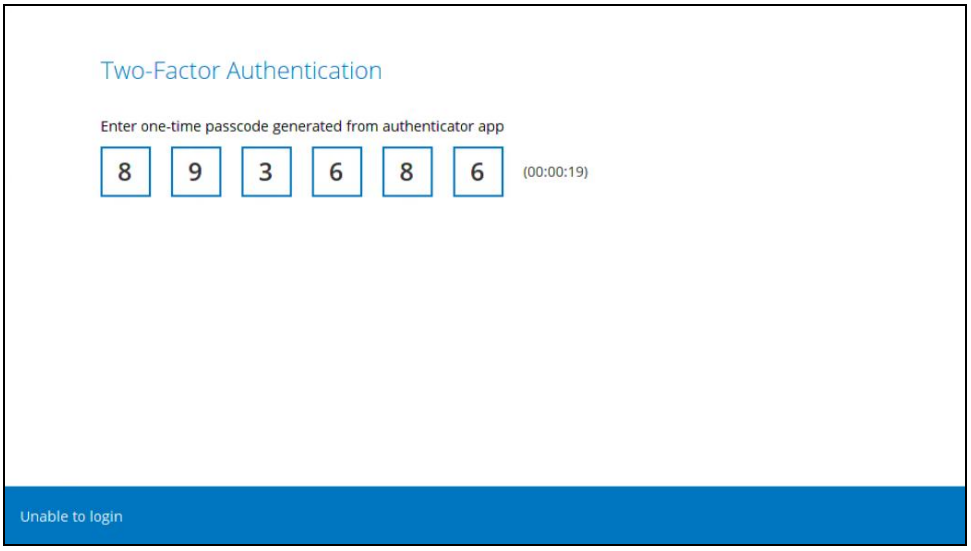
2. Enter the login name and password of your AhsayOBM account provided by your backup service provider. Then, click **OK** to log in.



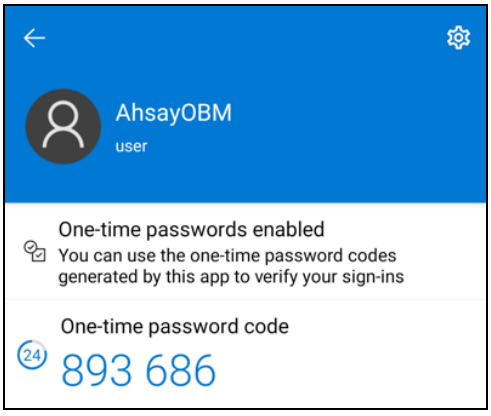
NOTE

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.

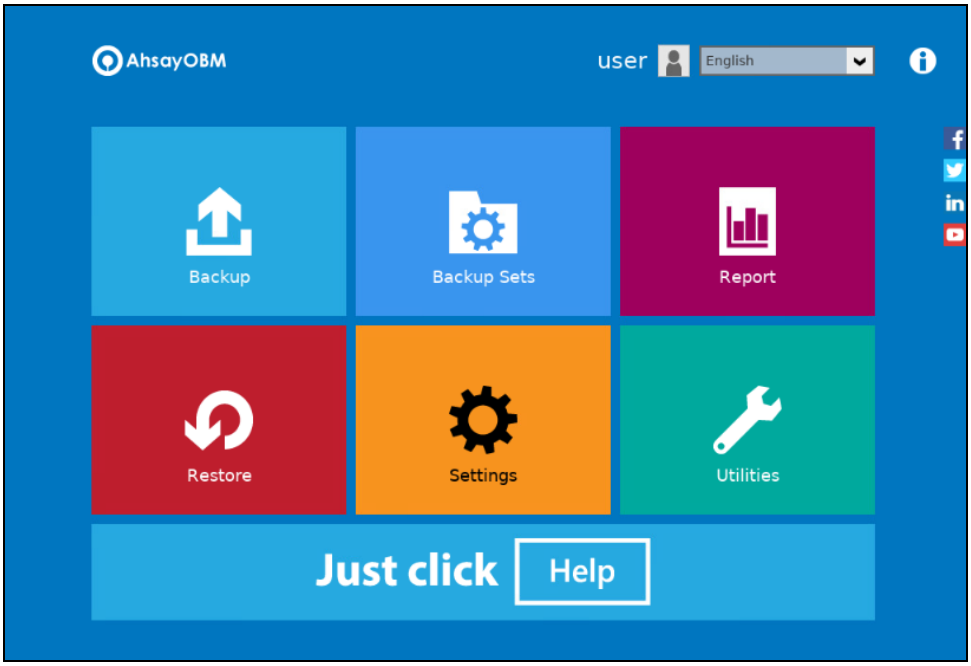
3. Enter the one-time passcode generated from the Microsoft Authenticator app.



Example of the one-time passcode generated:



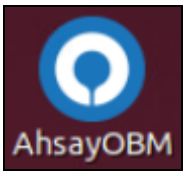
4. After successful login, the following screen will appear.



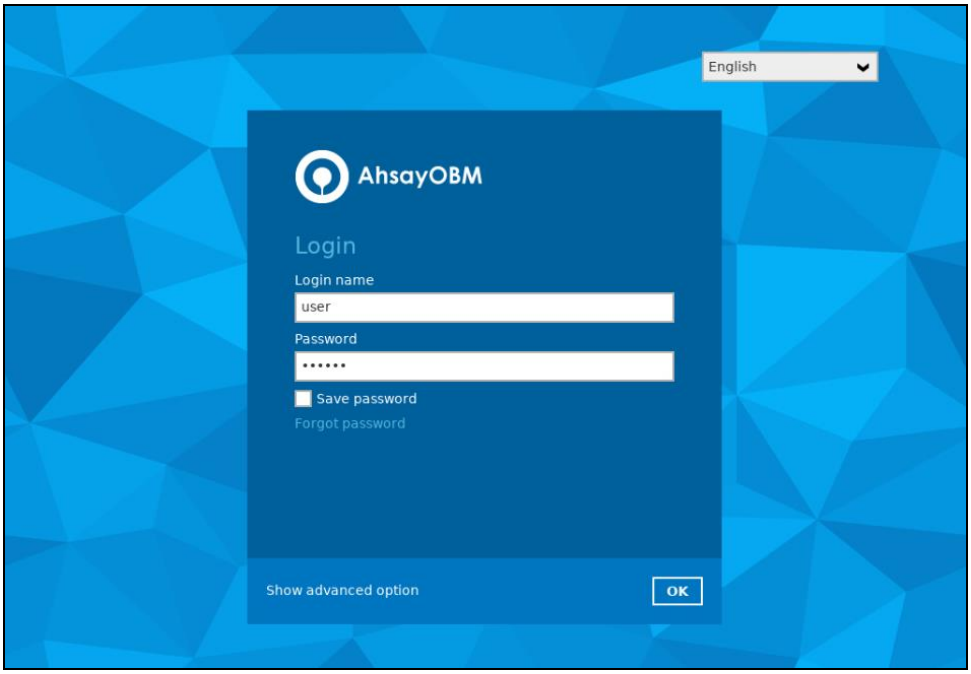
7.4 Login to AhsayOBM with 2FA using Google Authenticator

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

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



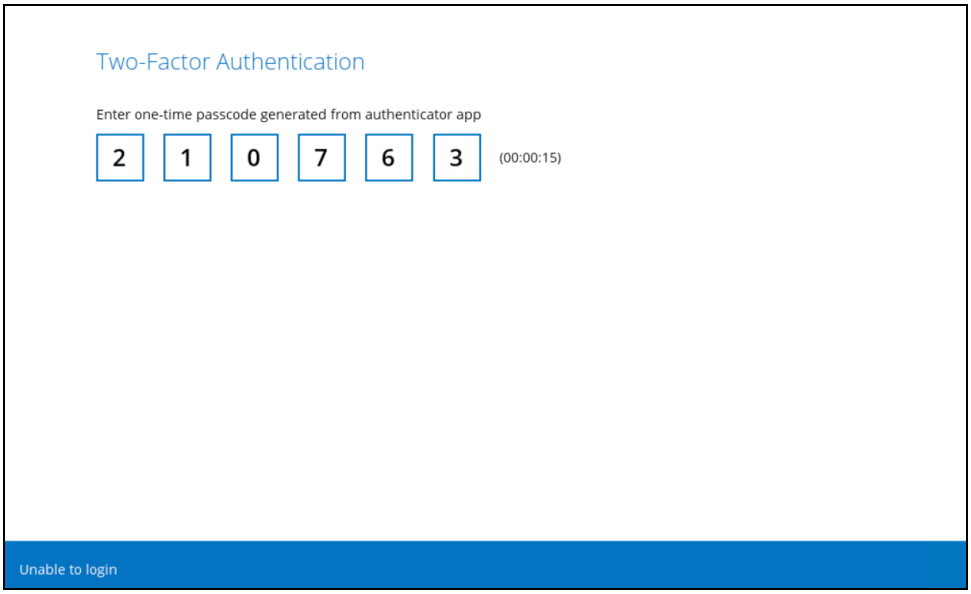
2. Enter the login name and password of your AhsayOBM account provided by your backup service provider. Then, click **OK** to log in.



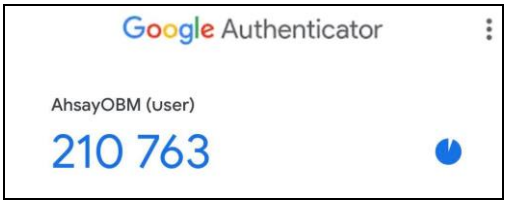
NOTE

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.

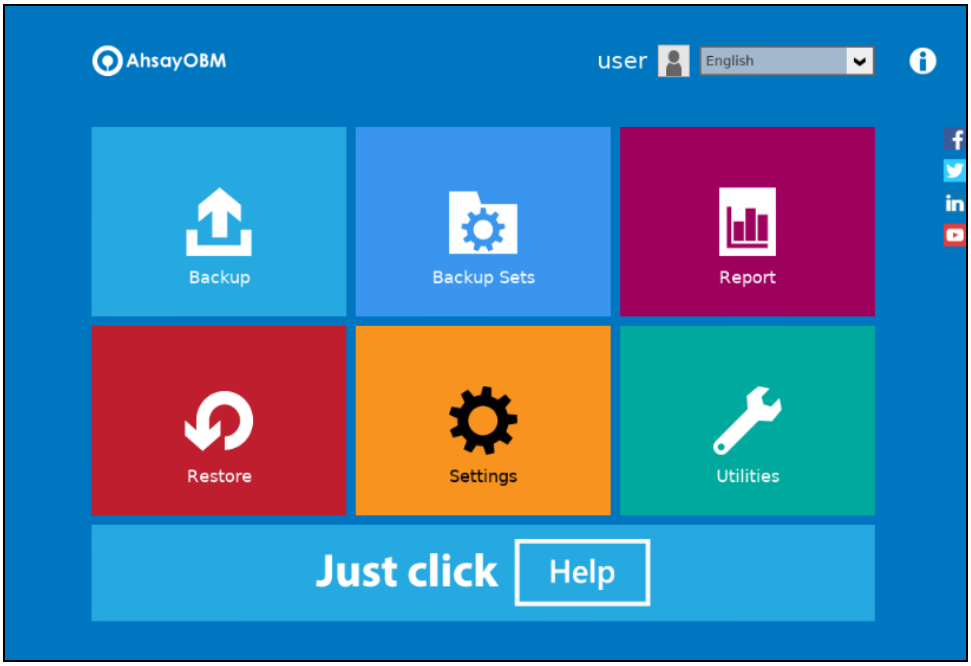
3. Enter the one-time passcode generated from the Google Authenticator app.



Example of the one-time passcode generated:



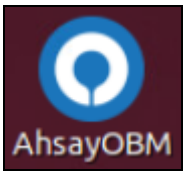
4. After successful login, the following screen will appear.



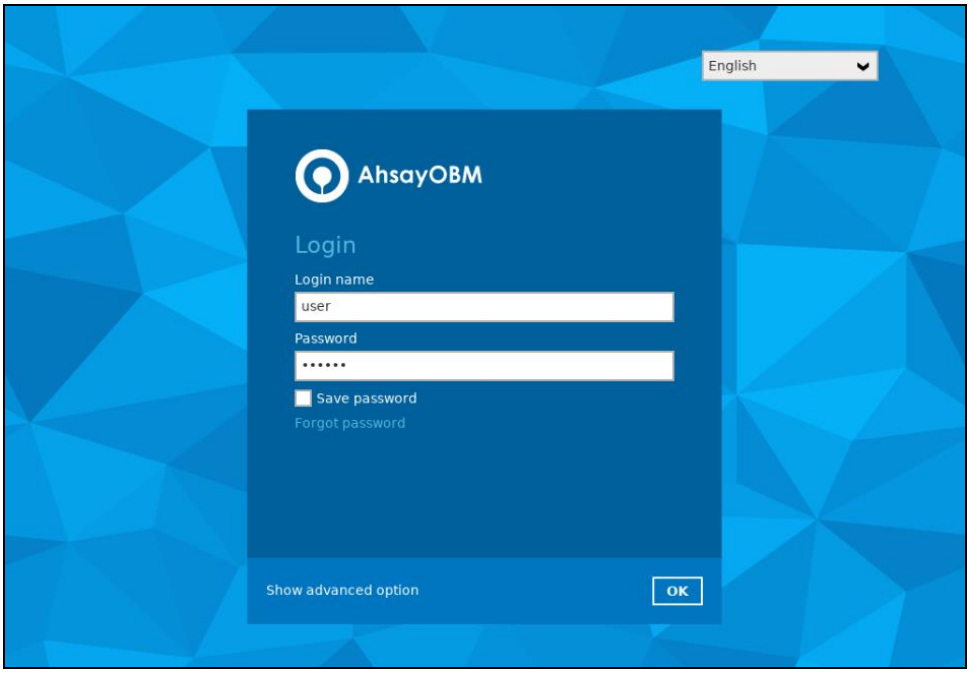
7.5 Login to AhsayOBM with 2FA using Twilio

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

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



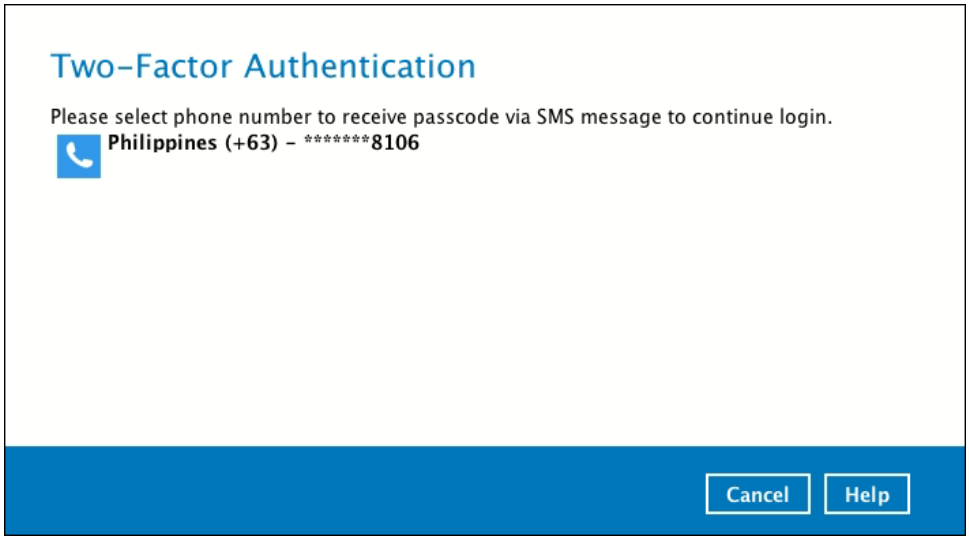
2. Enter the login name and password of your AhsayOBM account provided by your backup service provider. Then, click **OK** to login.



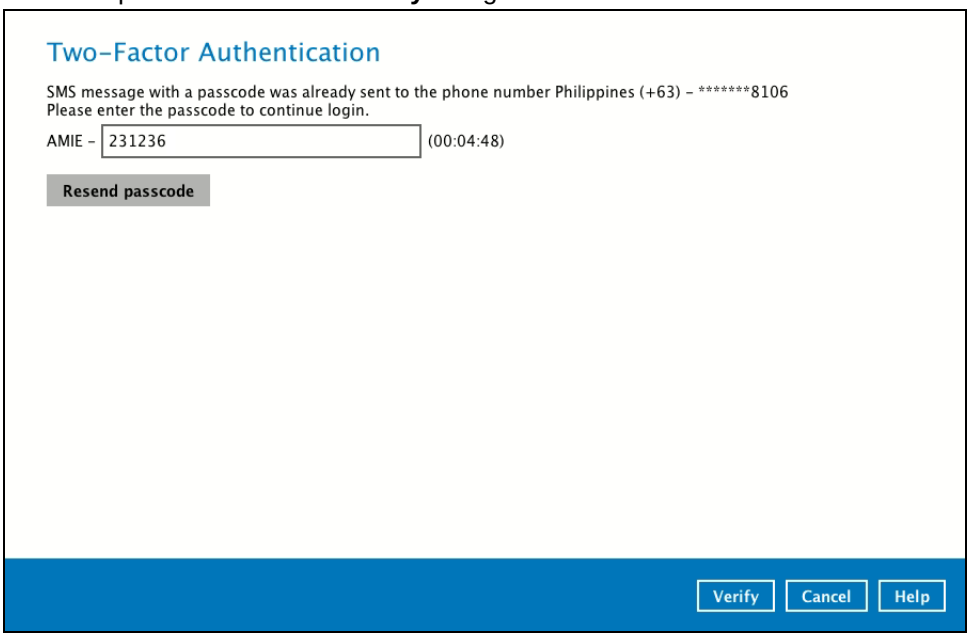
NOTE

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.

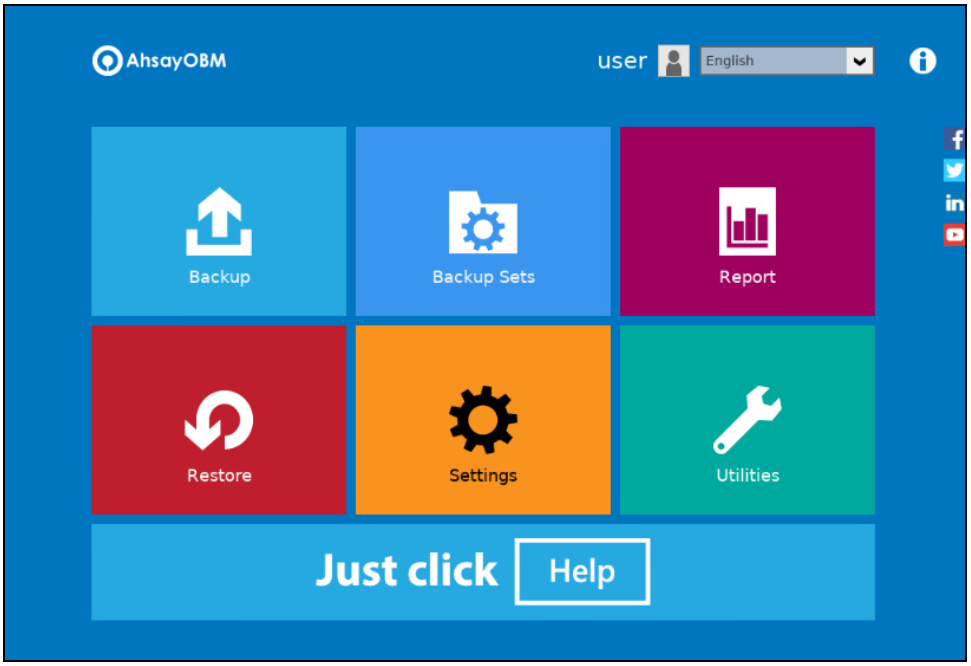
3. Select your phone number to receive the passcode.



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



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

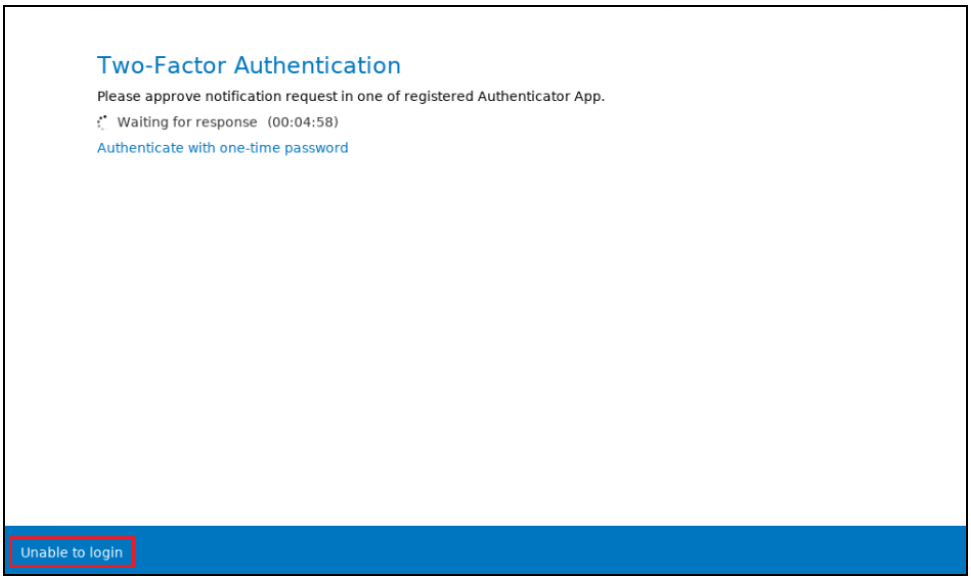


8 Unable to log in to AhsayOBM with 2FA

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

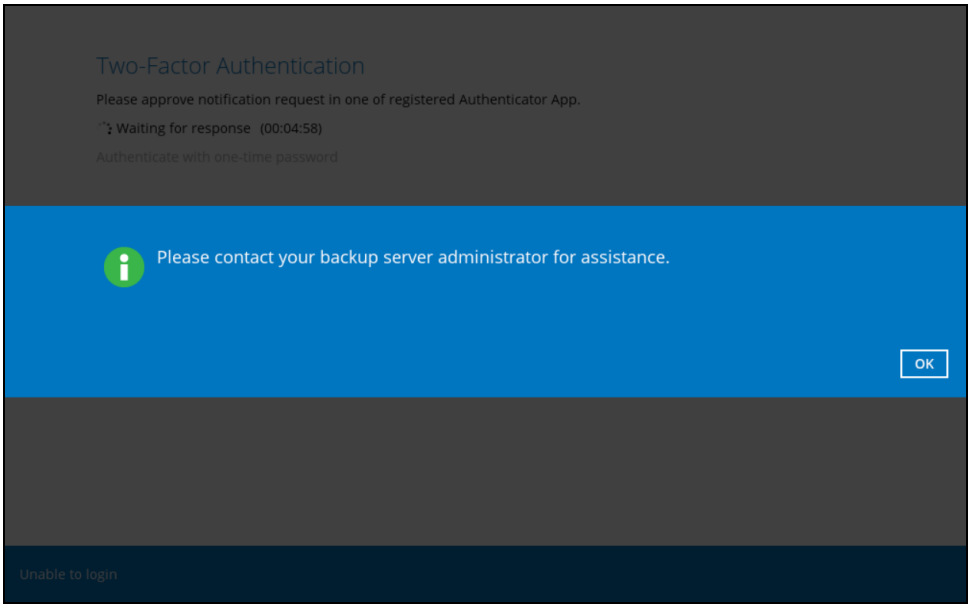
Here are the three scenarios after clicking the **Unable to login** link:

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



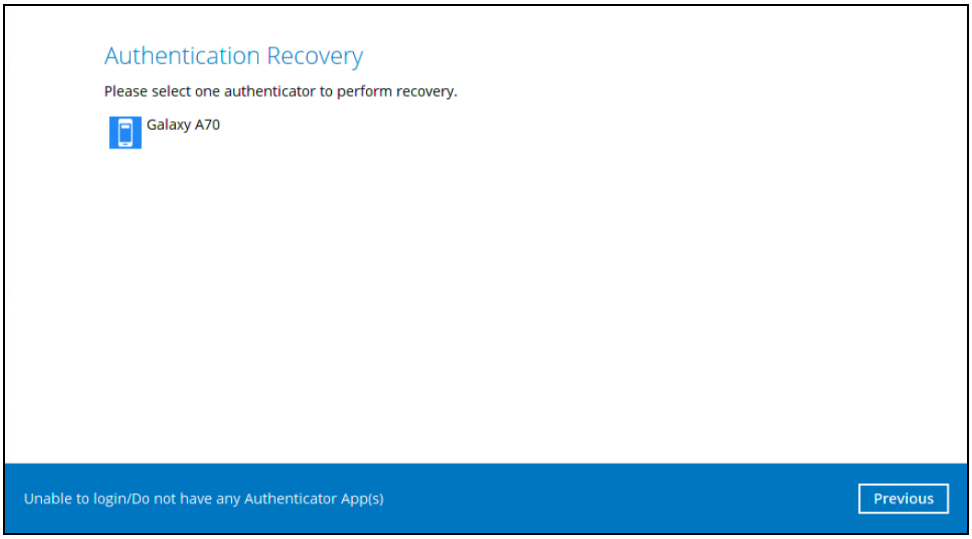
No recovery number was registered on Ahsay Mobile for the 2FA account

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.



"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.

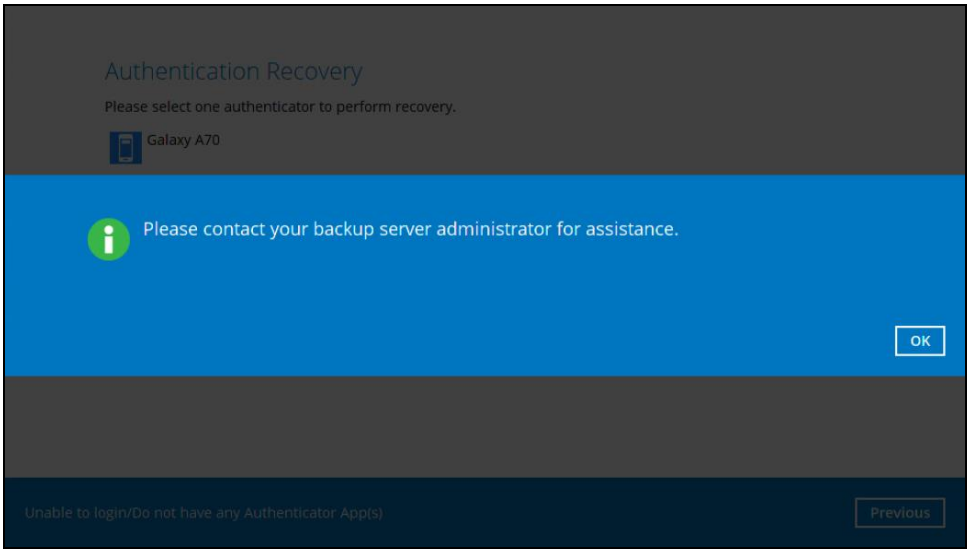


NOTE

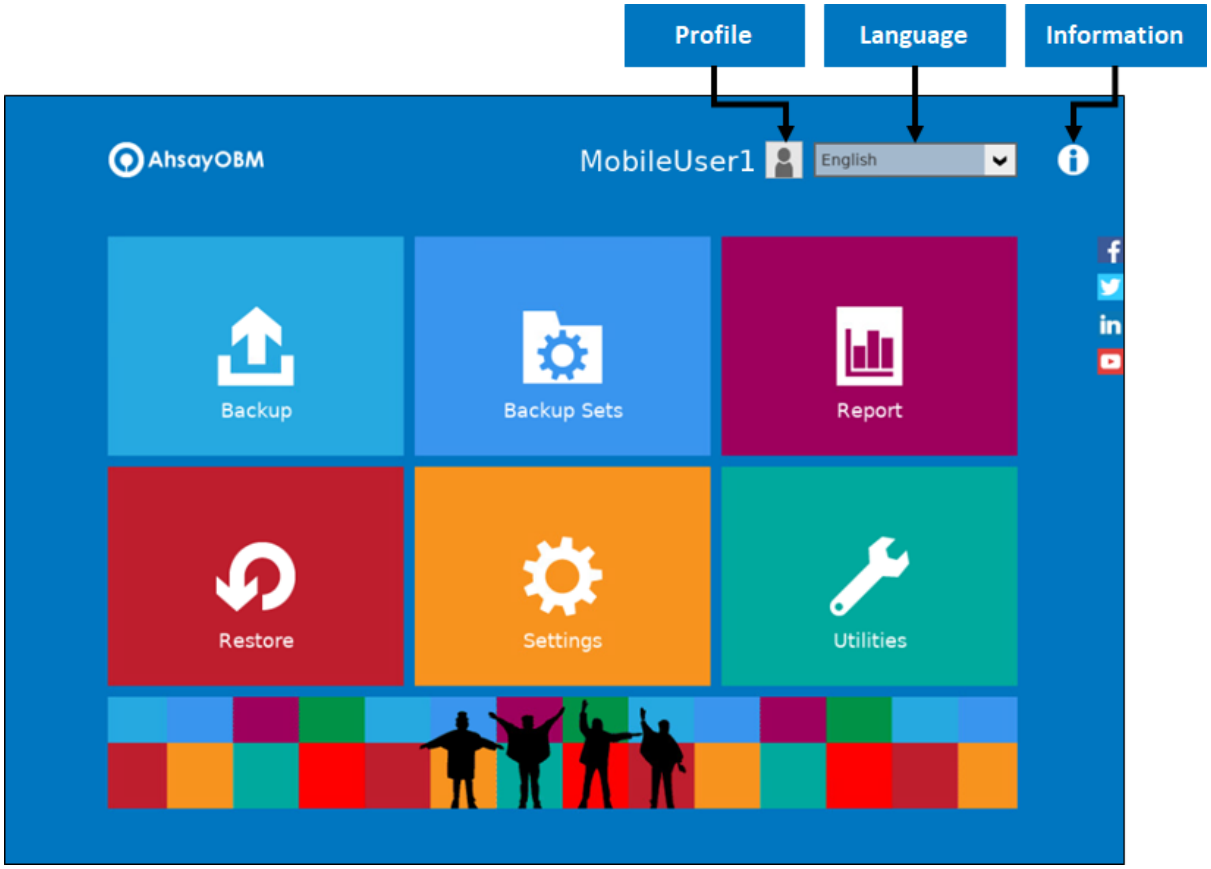
For the detailed steps in performing Authentication Recovery, please refer to the Ahsay Mobile User Guide for Android and iOS – Appendix A: Troubleshooting Login.

Unable to perform the "Authentication Recovery" procedure

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



9 AhsayOBM Overview



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

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

9.1 Profile

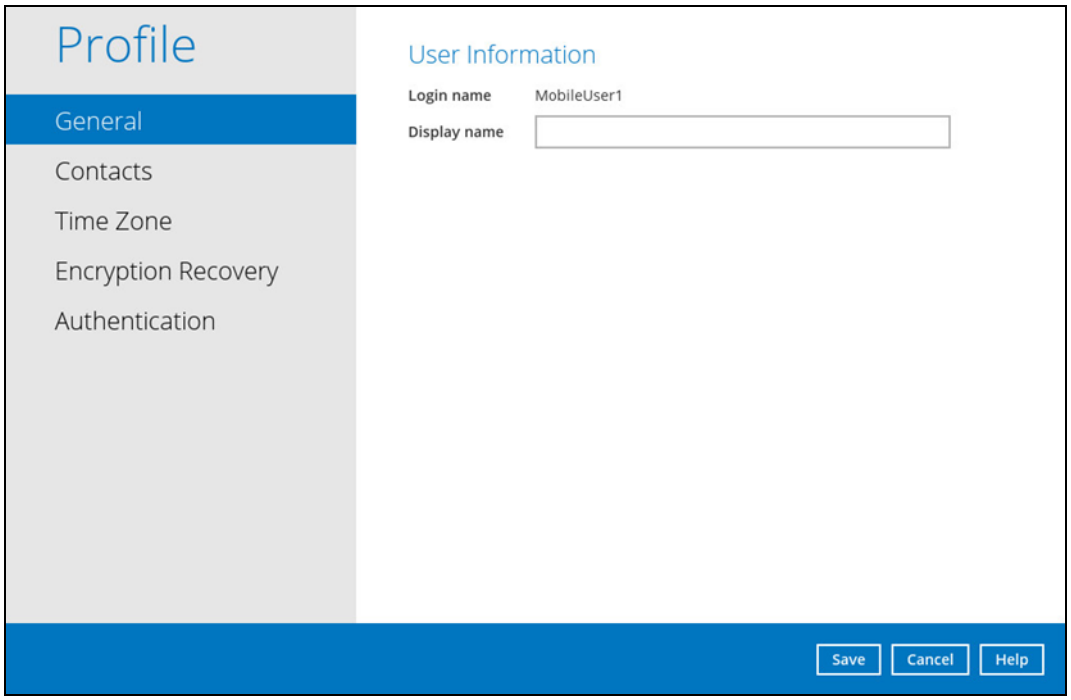
The **Profile** icon shows the settings that can be modified by the user. The features that will be shown will depend on the user account if it was using Twilio for Two-Factor Authentication prior to upgrading to v9.0.0.0 or above and will continue to use Twilio.

There are seven (7) available features:

- General
- Contacts
- Time Zone
- Encryption Recovery
- Authentication
- Password (Only shown for backup accounts created prior to AhsayOBM v9.0.0.0 and using Twilio for two-factor authentication.)
- Security Settings (Only shown for backup accounts created prior to AhsayOBM v9.0.0.0 and using Twilio for two-factor authentication.)

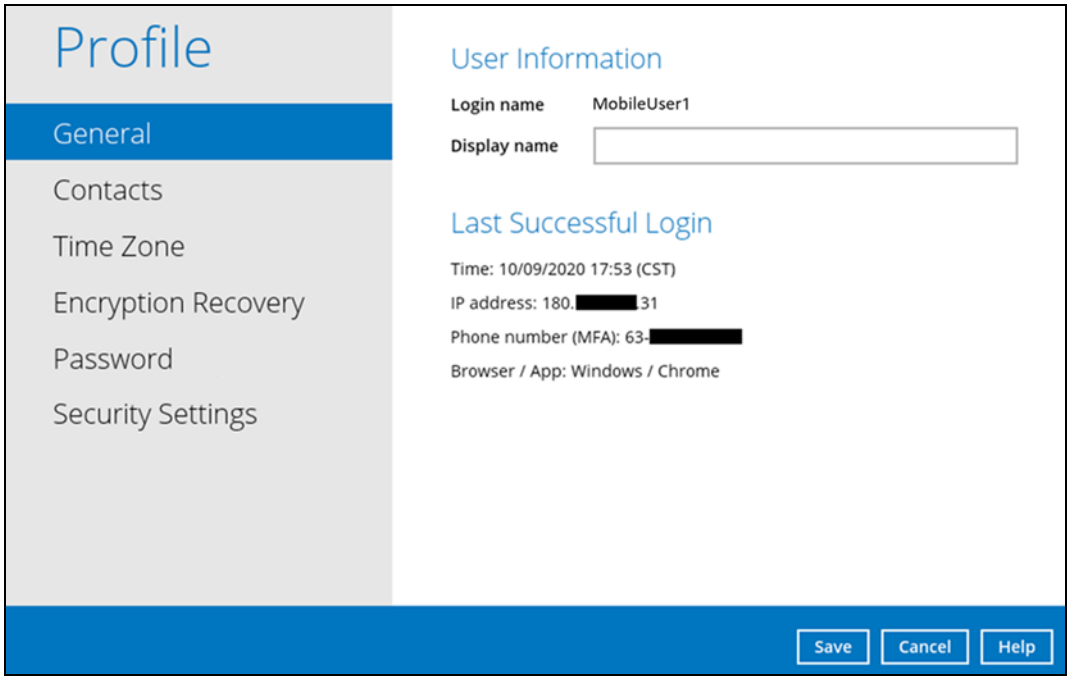
9.1.1 General

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.

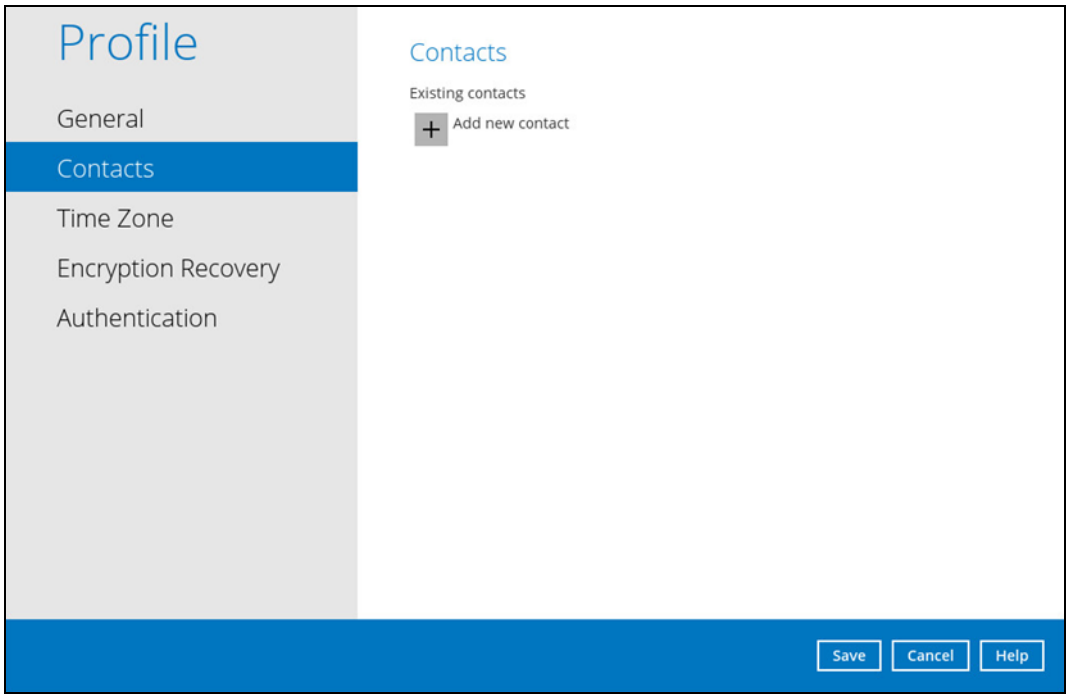
This will be the General tab for old backup account using Twilio for two-factor authentication.



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 login.
Phone number (MFA)	The phone number where sms authentication will be sent when 2FA is enabled.
Browser / App	The browser or app used to login in to AhsayCBS User Web Console or AhsayOBM.

9.1.2 Contacts

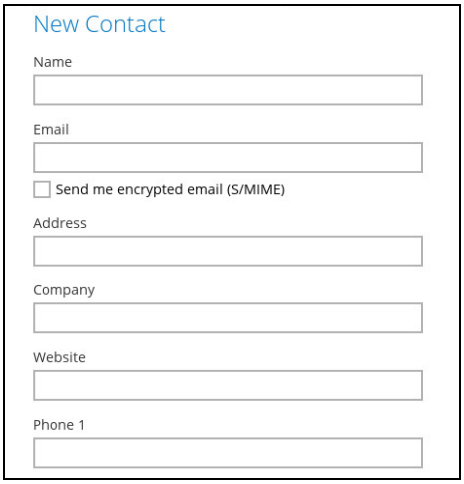
This refers to the contact information of the user. You can also add multiple contacts or modify an existing contact information. Having this filled up will help us to send backup and daily reports and even recovered backup set encryption key in case it was forgotten or lost.



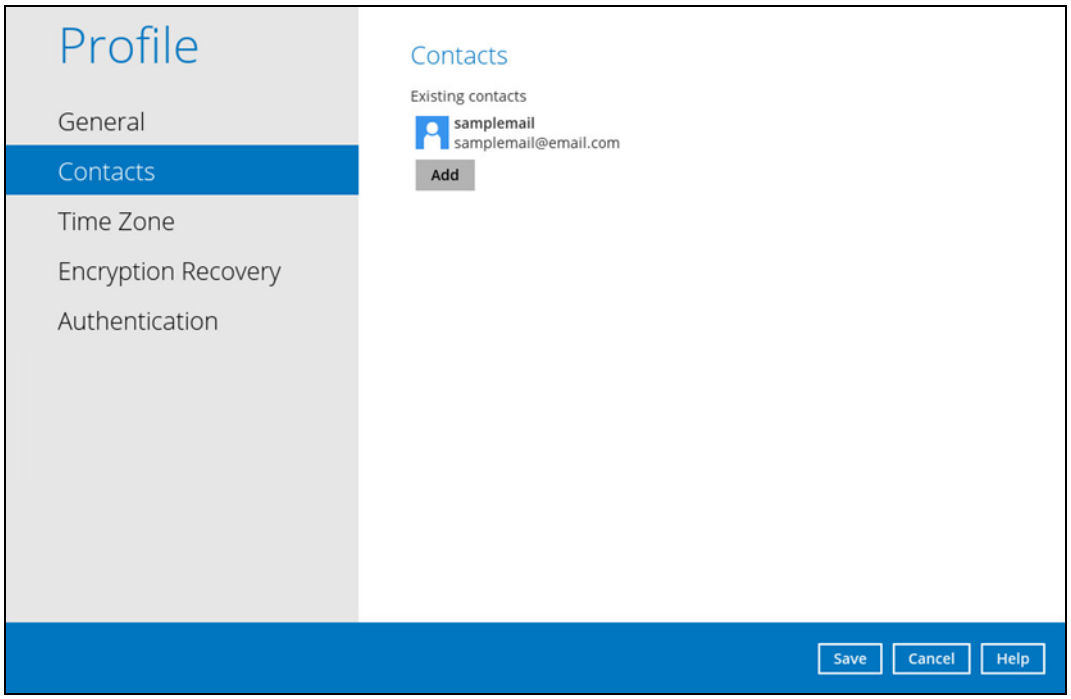
To add a new contact, follow the instructions below:

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

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

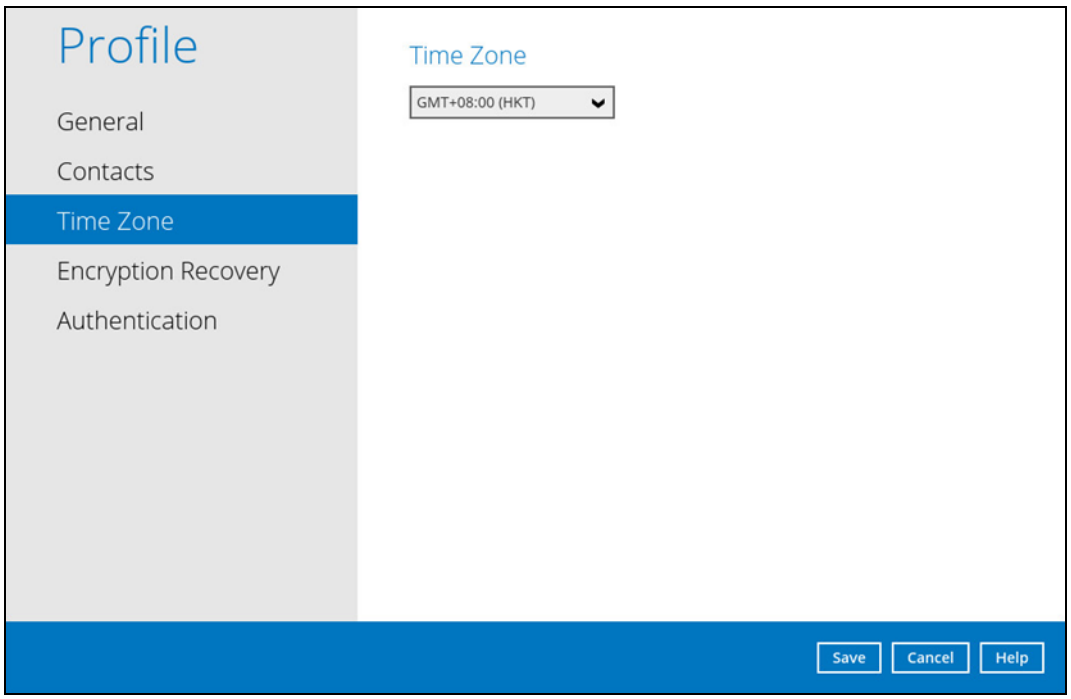


3. Click **Save** to store the contact information.



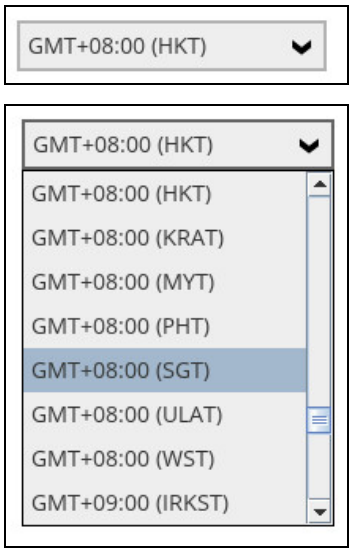
9.1.3 Time Zone

The time zone indicated



To modify the time zone, follow the instructions below:

1. Select from the dropdown list.

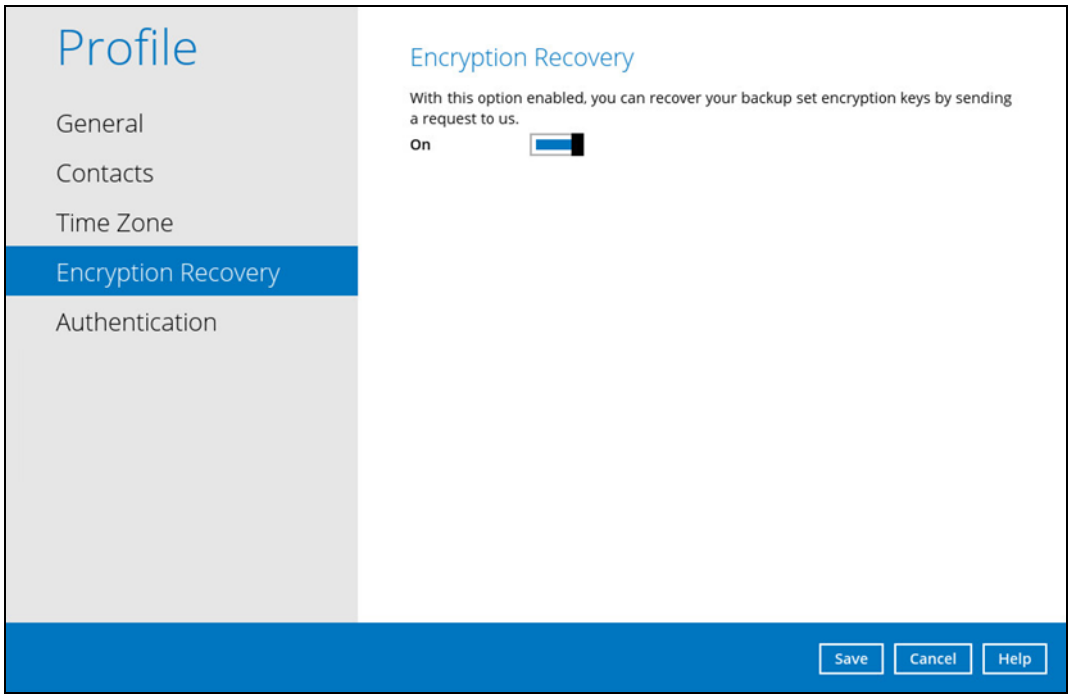


2. Click **Save** to save the updated time zone.

9.1.4 Encryption Recovery

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

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



9.1.5 Authentication

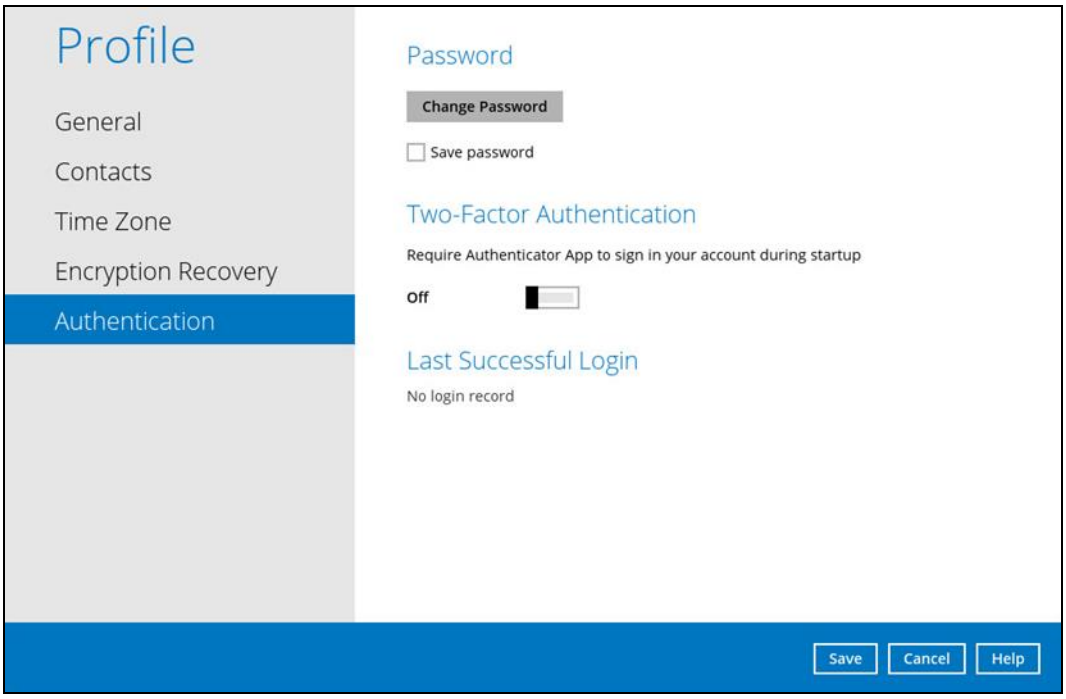
You can use the Authentication function to:

- 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 User Guide for Android and iOS – Chapter 6.3.1 for the detailed step-by-step procedure.

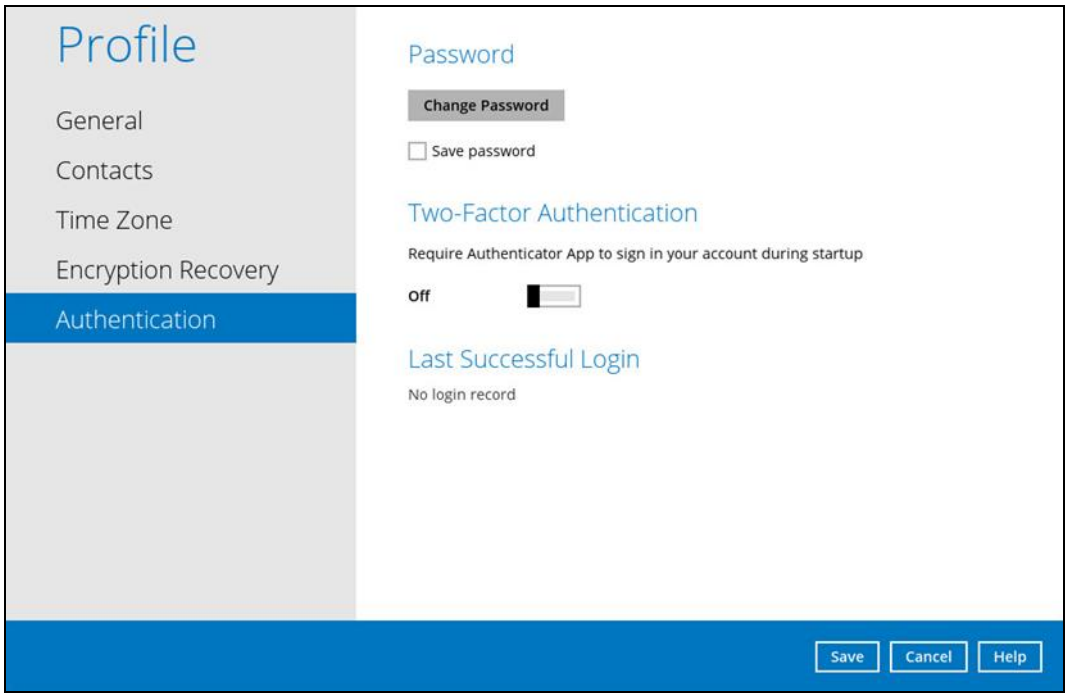
- Remove one or more device(s) registered for Two-Factor Authentication (2FA).
- Re-pair mobile device with AhsayOBM account.
- View details of the "Last Successful Login".

> **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, LastPass Authenticator etc.).



Password

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

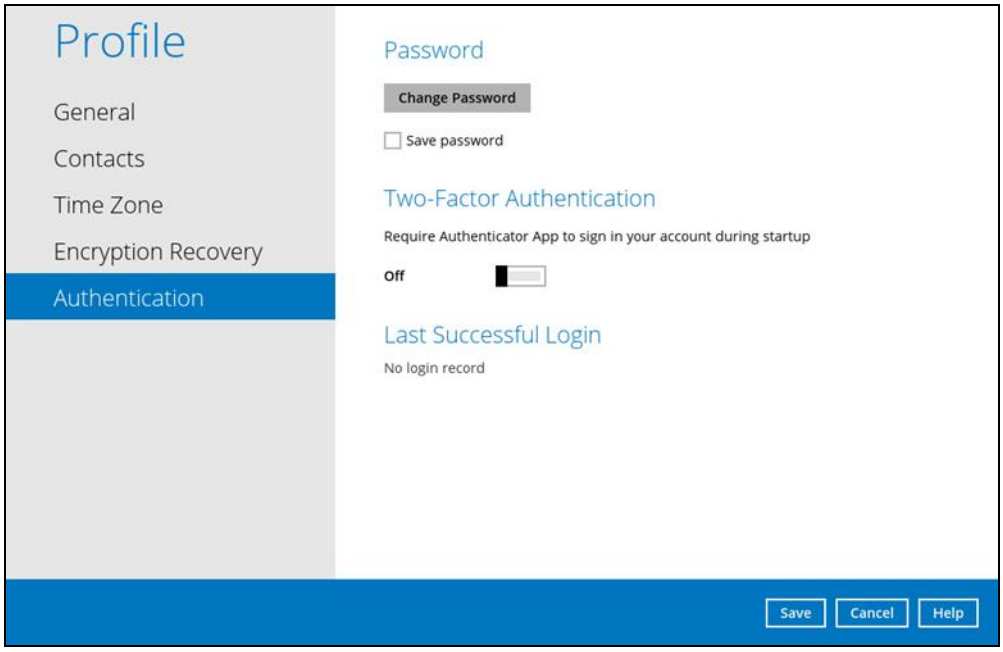


NOTE

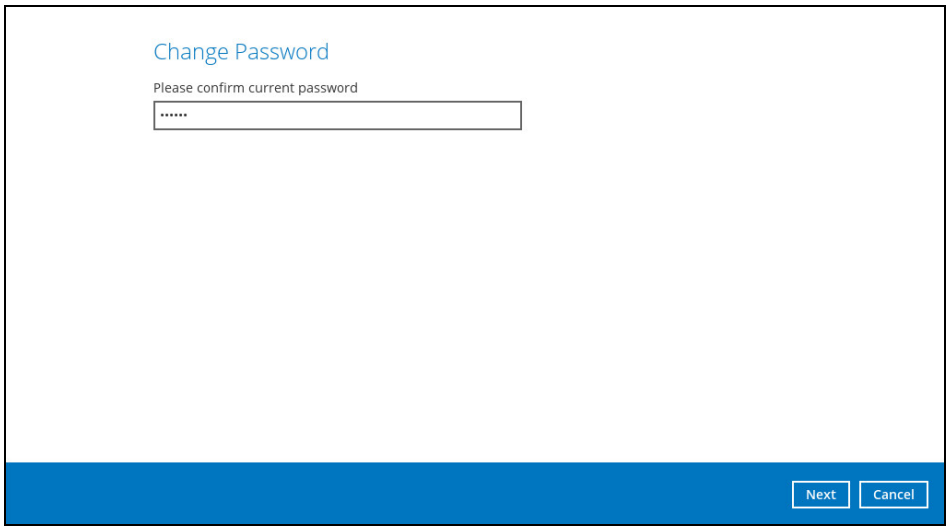
The Save password option may not be available. This depends on the settings of your backup service provider. Please contact your backup service provider for more information.

To change the password, follow the instructions below:

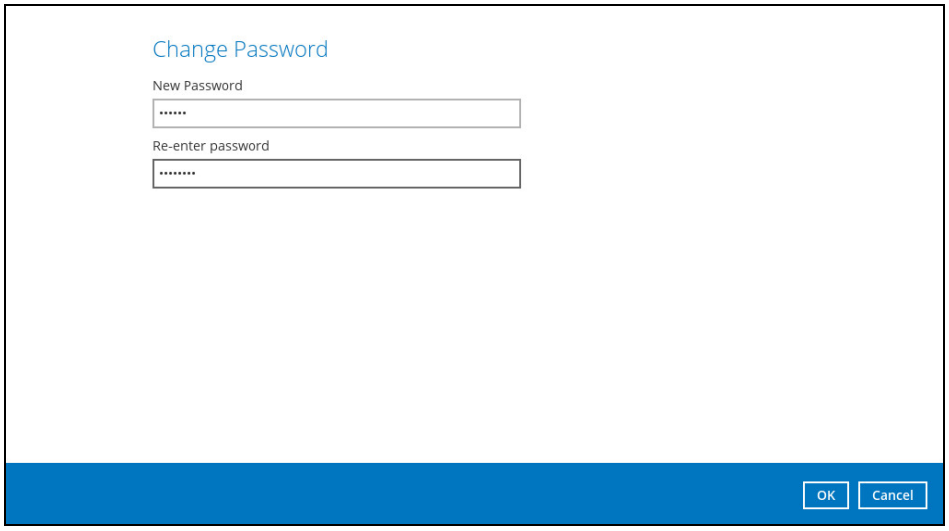
1. Click the **Change Password.**



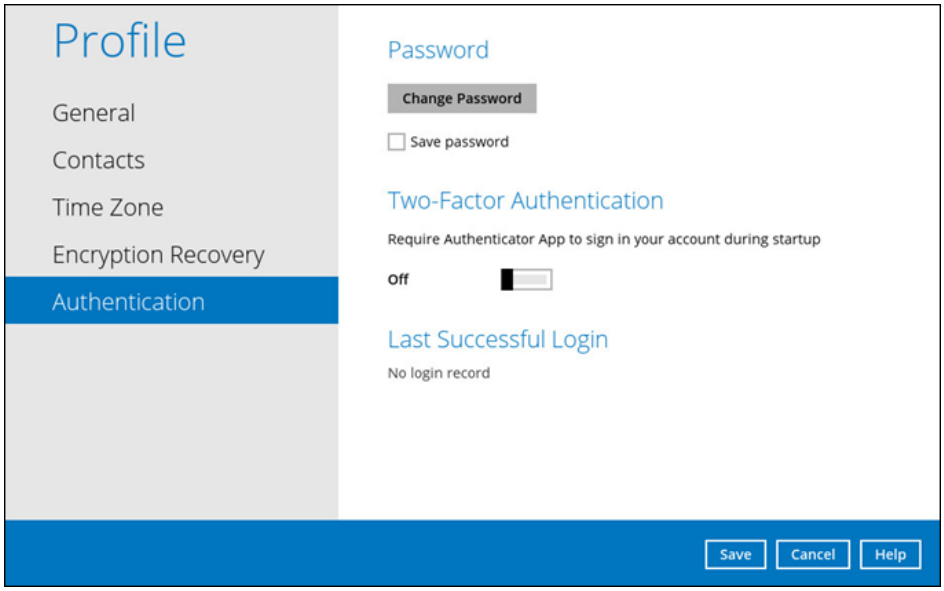
2. Enter the current password.



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.

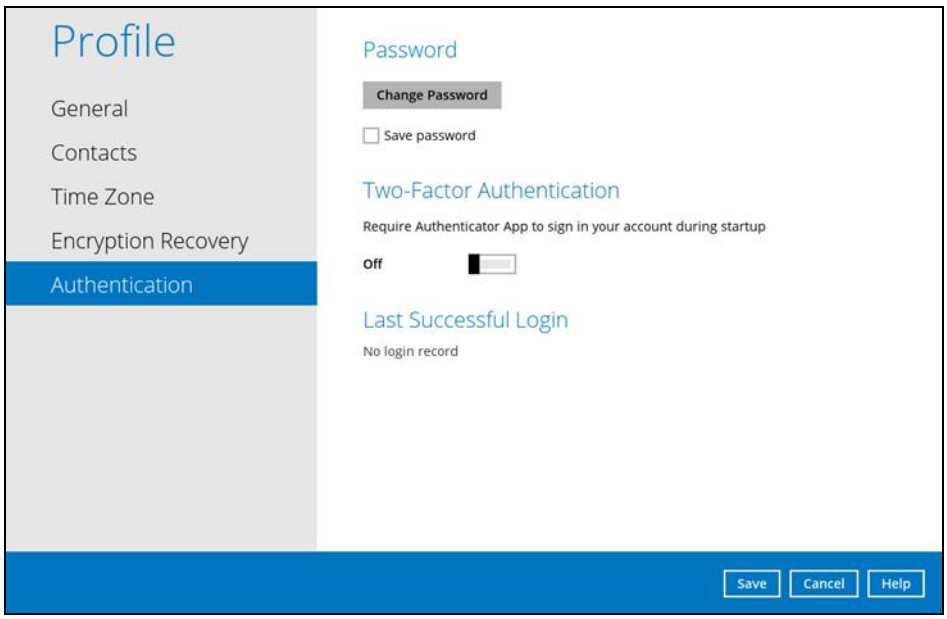


Two-Factor Authentication

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

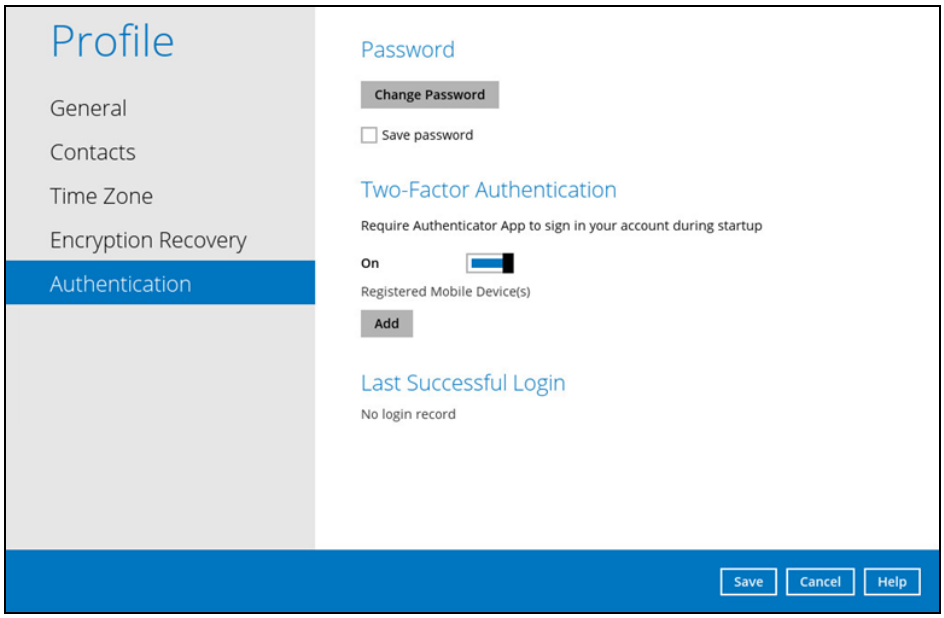
NOTE
The Ahsay Mobile app or a third-party authenticator apps is needed for 2FA.

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



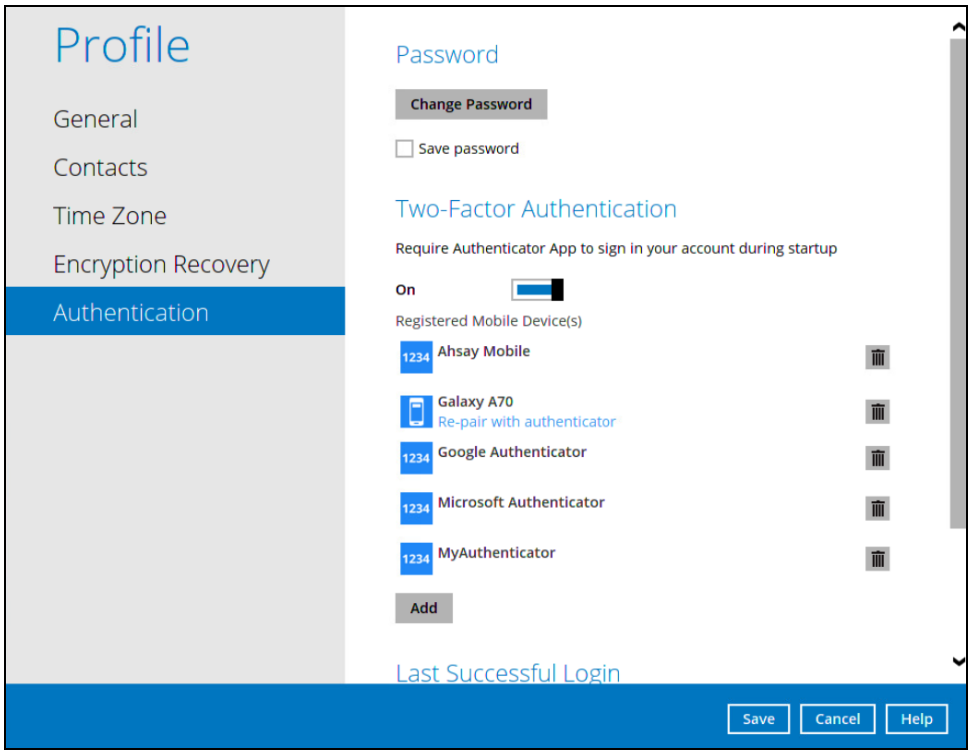
2. Swipe lever to the right to turn it on.

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

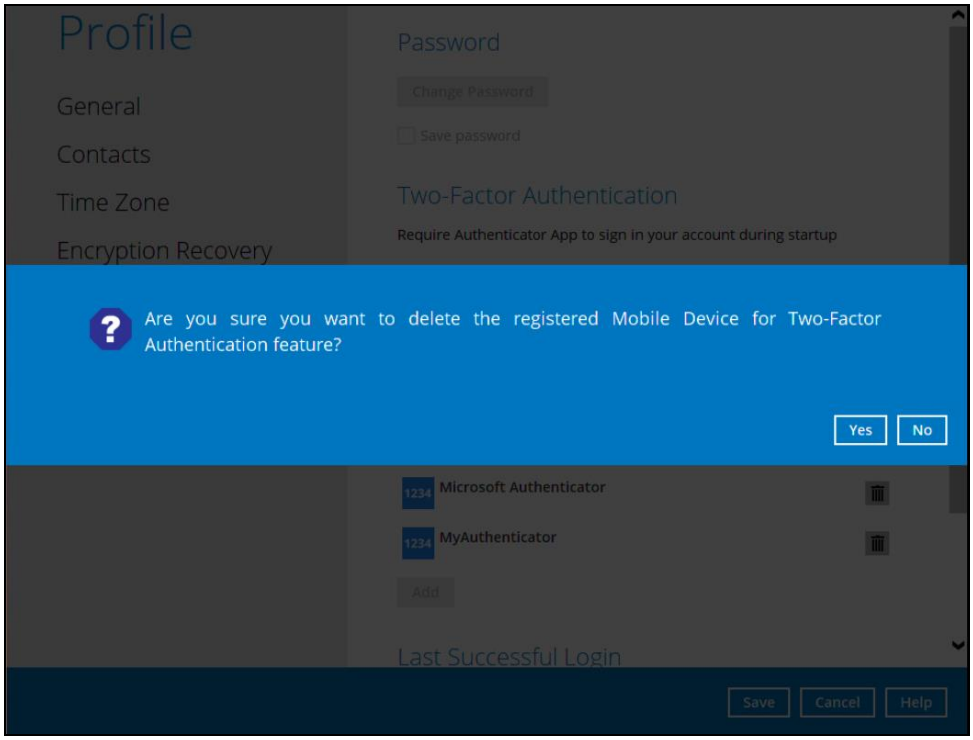


To remove a mobile device, follow the instructions below:

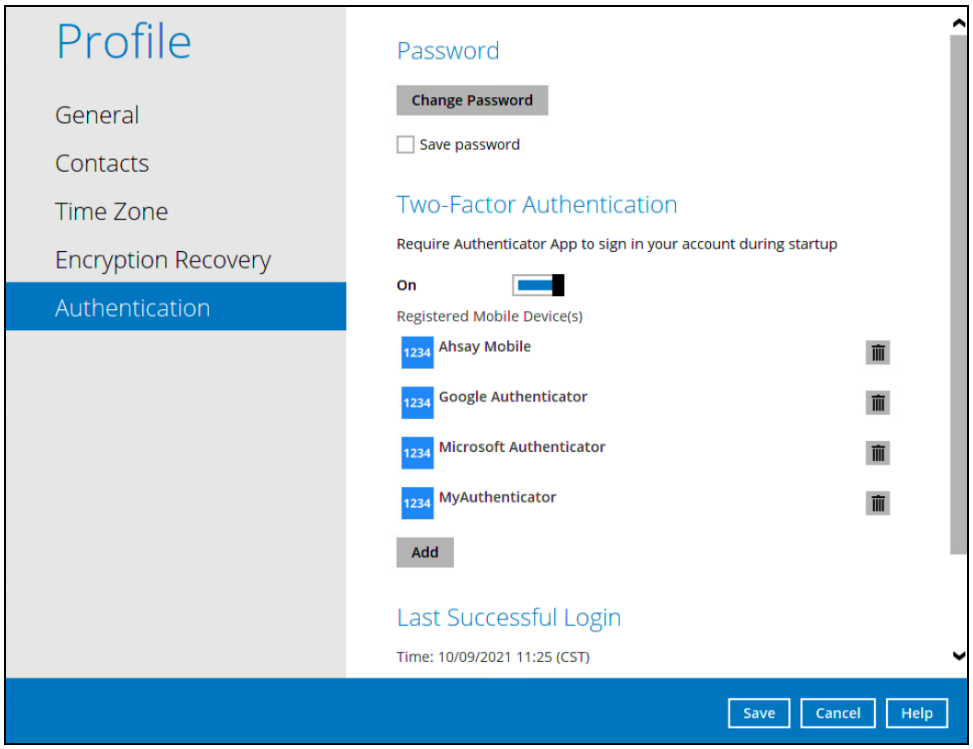
1. Click the button on the right side of the registered mobile device. In this example we are going to delete the mobile device named “Galaxy A70”.



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



3. Mobile device is successfully removed.

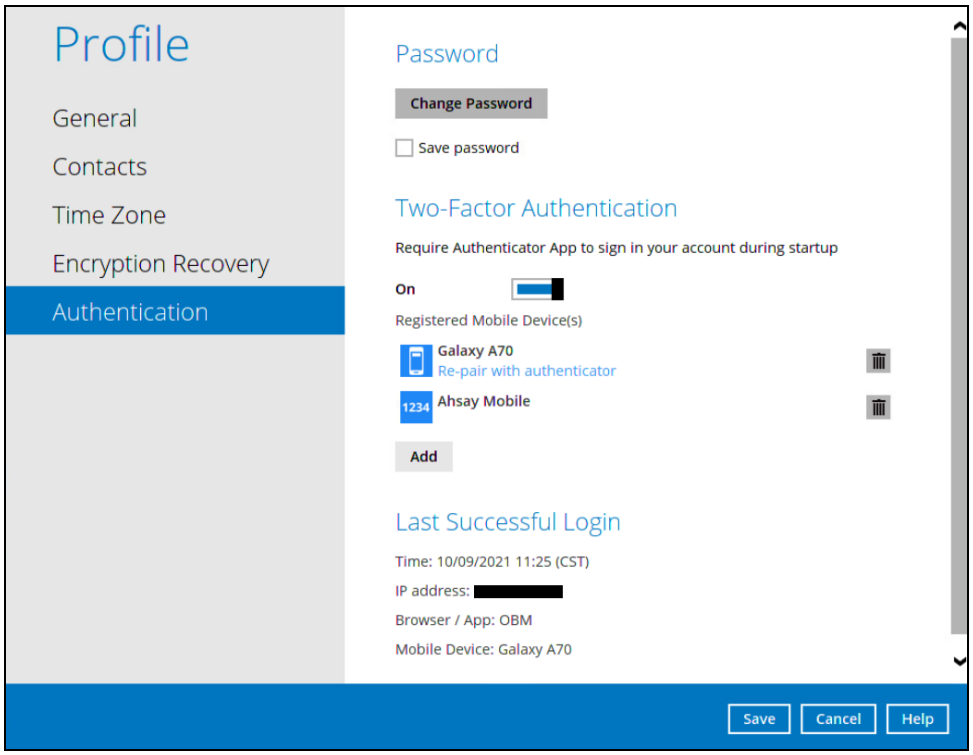


To disable the two-factor authentication feature, follow the instructions below:

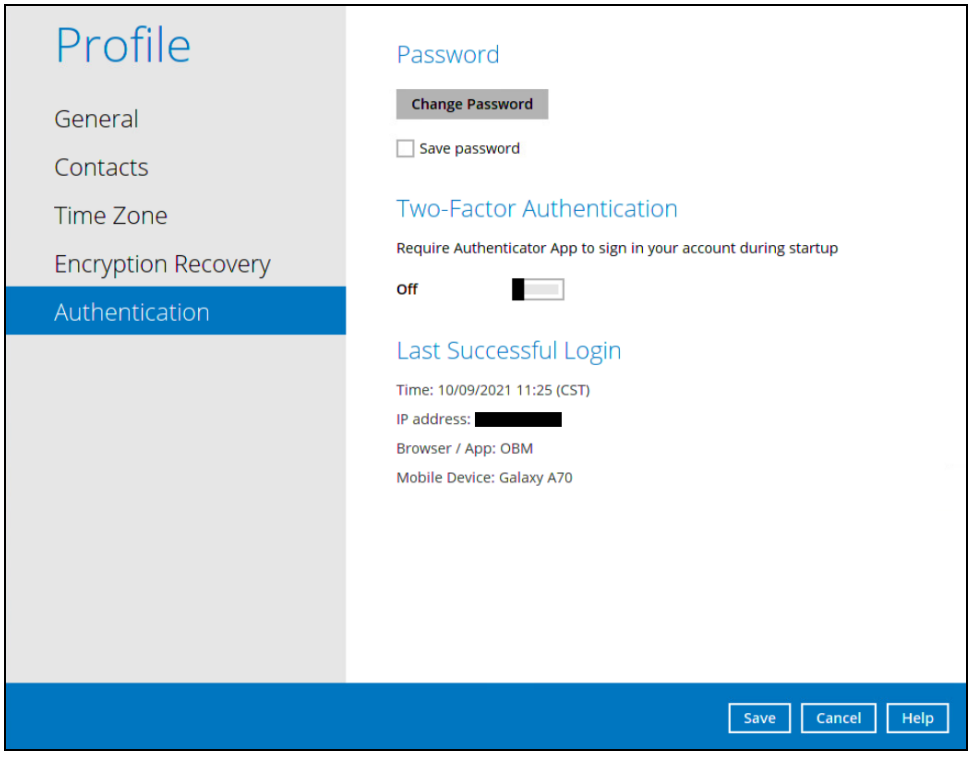
NOTE

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.



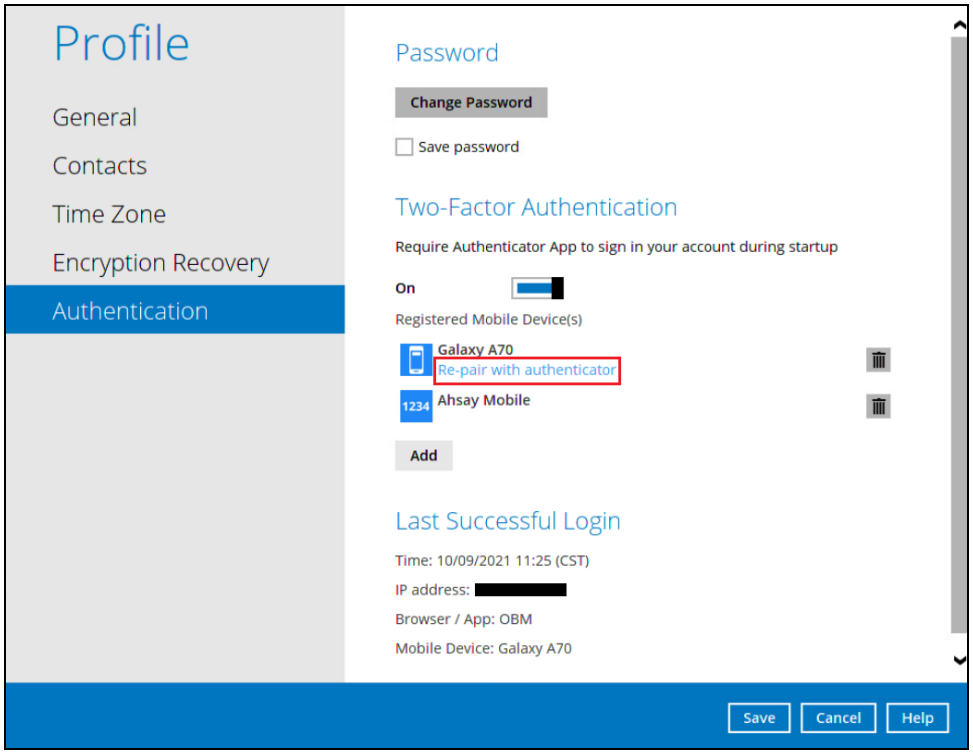
2. Click **Save** to save the settings.



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 2FA is still registered in AhsayOBM. This feature is used when:

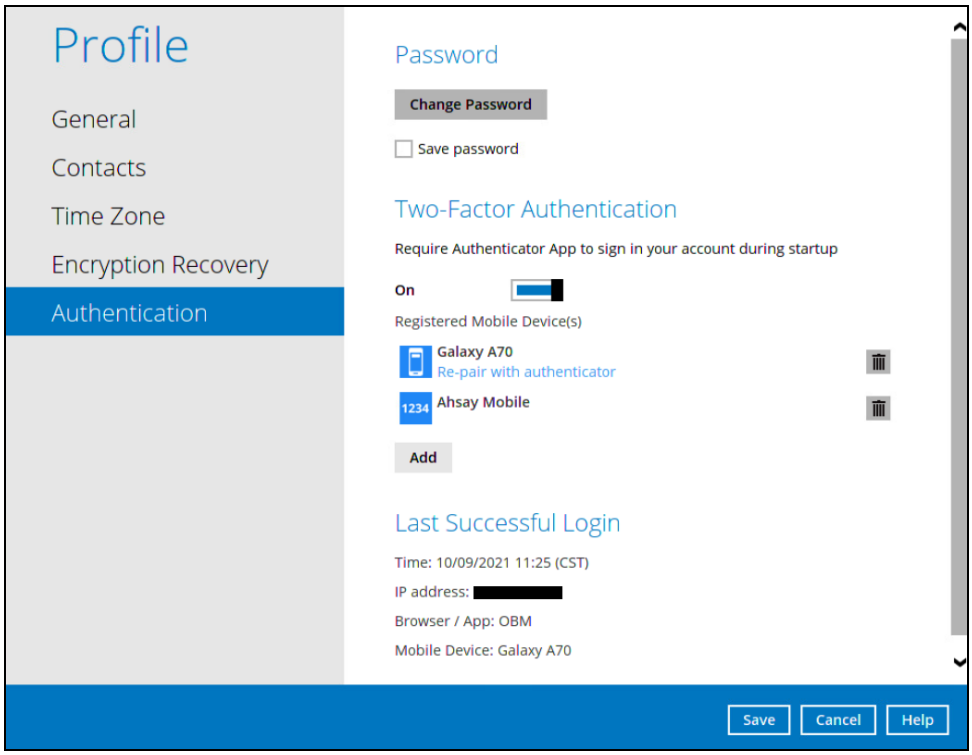
- the registered profile for the 2FA is removed from the Ahsay Mobile app.
- the Ahsay Mobile app is accidentally uninstalled from the mobile device.



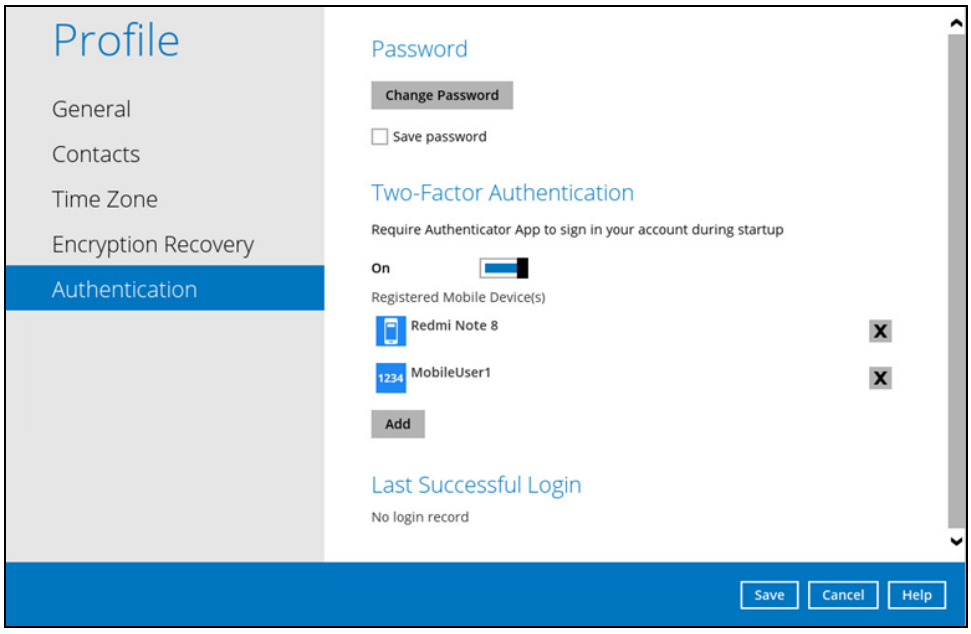
Last Successful Login

Displays the Date, Time, IP address, and Browser / App and the registered Mobile Device used during last log in.

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

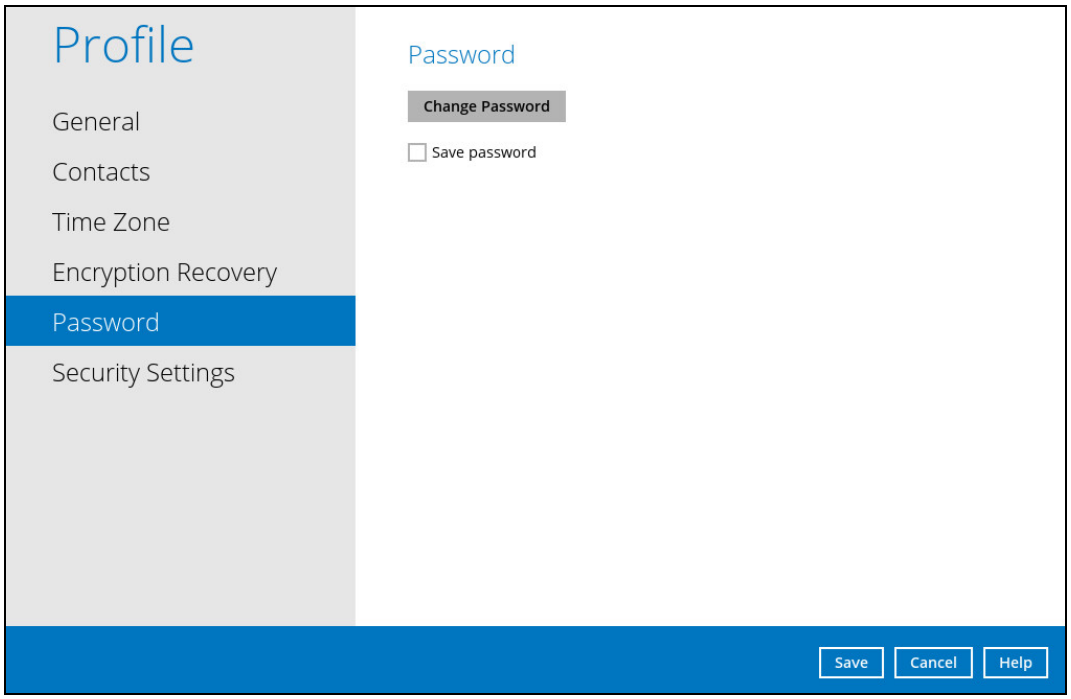


Below is the screenshot if there is no login record yet.



9.1.6 Password

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



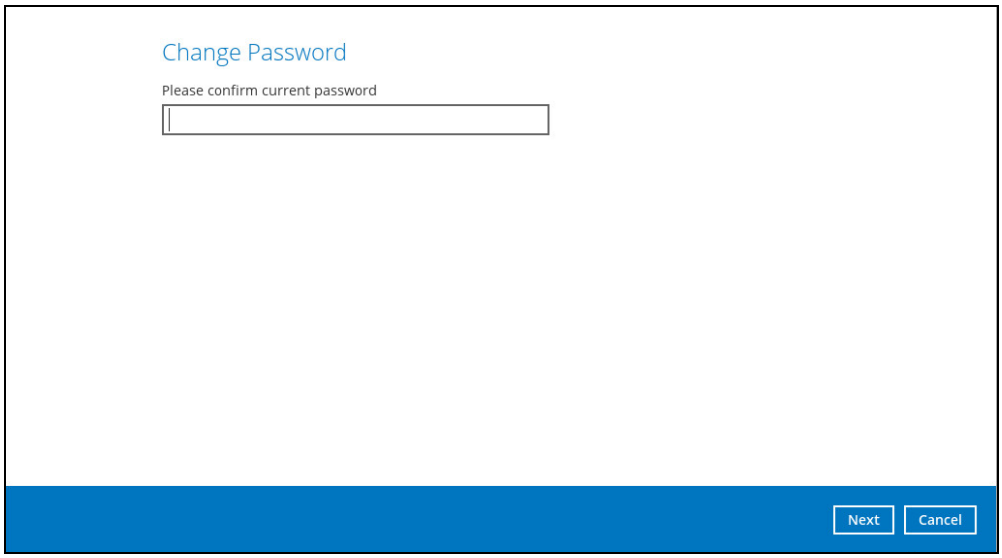
NOTE

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.

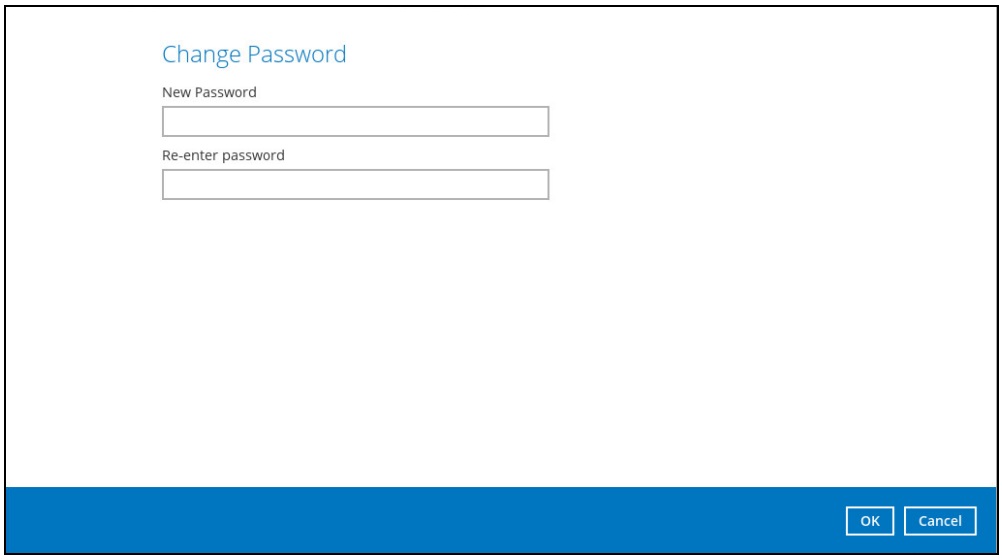
To modify the password, follow the instructions below:

1. Click **Change Password** button.

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



3. Enter the New Password and re-enter the new password then click **OK** to return to the main screen.

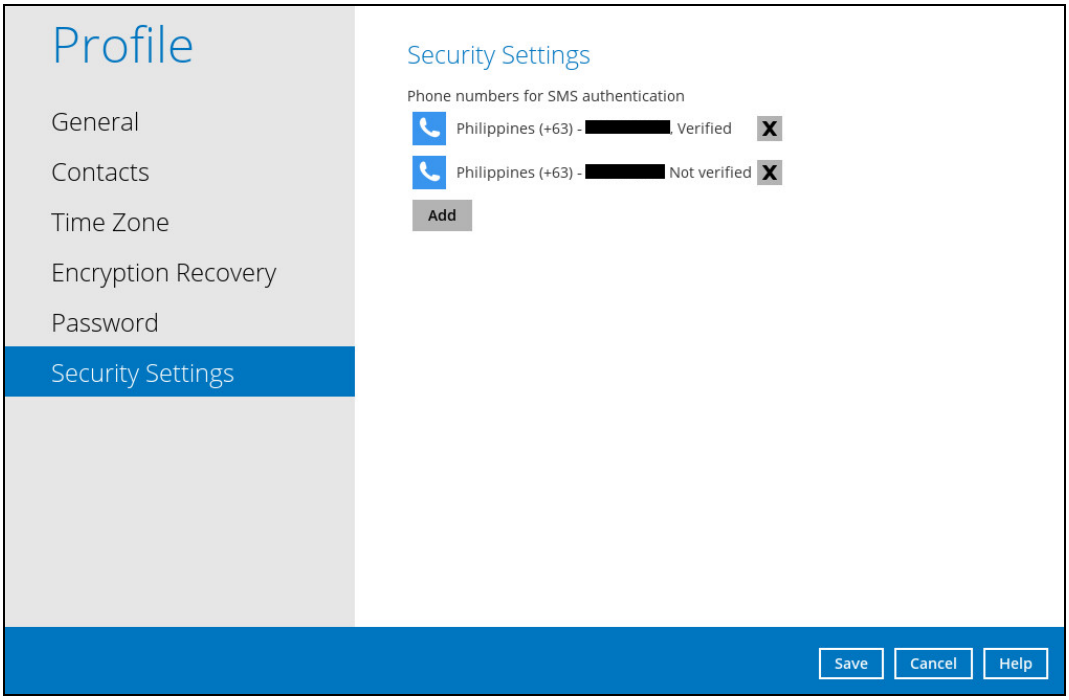


4. Click **Save** to store the updated password.

9.1.7 Security Settings

The Security Settings option is for backward compatibility with Twilio Two-Factor Authentication. It will only be visible if Twilio Two-Factor Authentication was enabled on the user account on pre-v9.0.0.0 AhsayOBM versions.

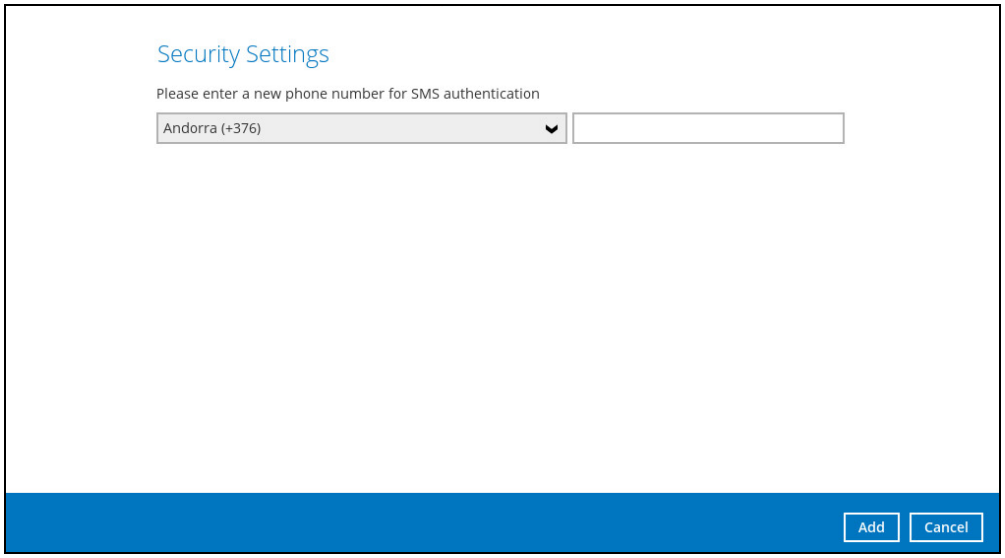
Phone numbers that will be used for sending sms authentication will be listed here and will show the status if it is verified or not. You can also add phone numbers here that can be used for sending the sms authentication.



To add a phone number, follow the instructions below:

1. Click the **Add**.

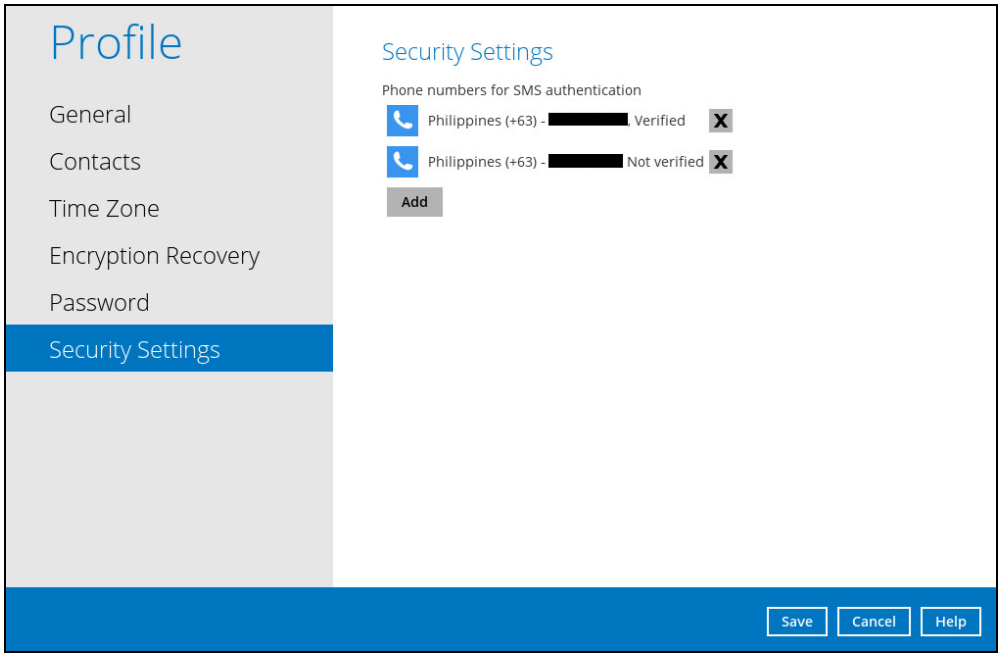
2. Select the country code and enter the phone number then click **Add**.



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

To delete a phone number, follow the instructions below:

1. Click the **X** button next to the phone number that you want to delete.



2. Click **Save** to delete the phone number.

9.2 Language

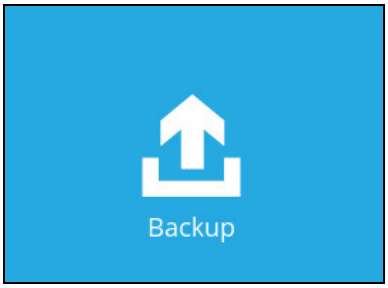
The list of available languages depends on the backup service provider.

9.3 Information

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

9.4 Backup

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



To start backing up, follow the instructions on Chapter 10: Running Backup Jobs.

9.5 Backup Sets

A backup set is a place for files and/or folders of your backed-up data. This feature allows 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 10: Creating a File Backup Set.

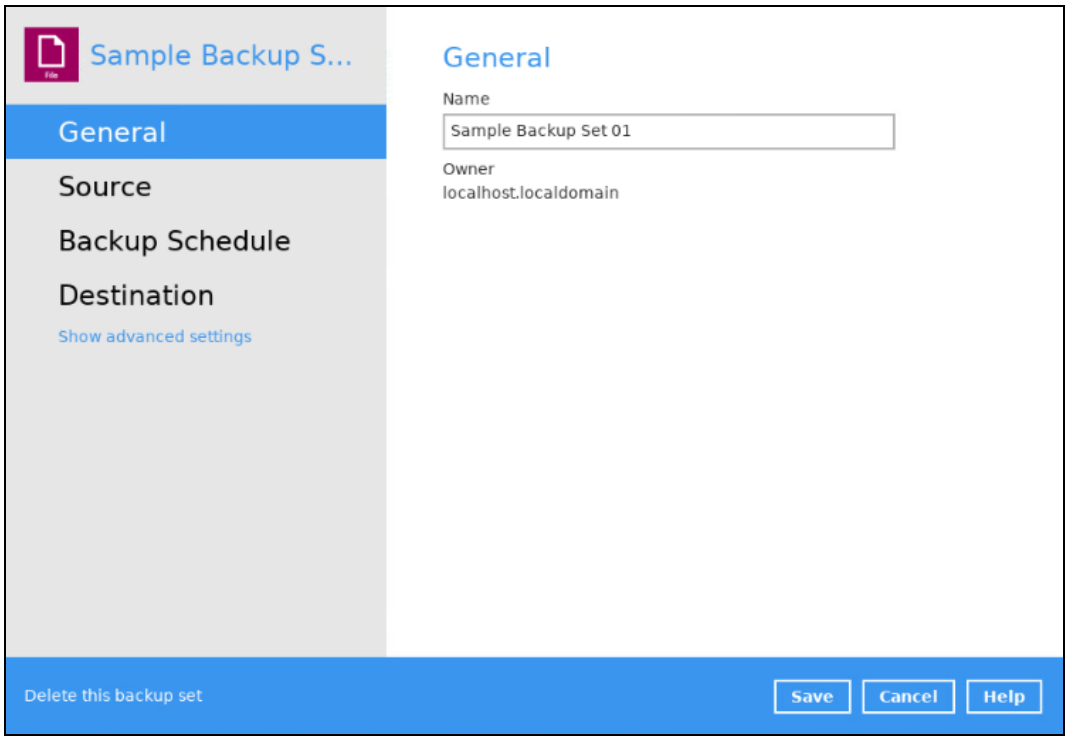
Backup Set Settings

Below is the list of configurable items under the Backup Sets:

- General
- Source
- Backup Schedule
- Destination
- Deduplication
- Retention Policy
- Command Line Tool
- Bandwidth Control
- Others

General

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

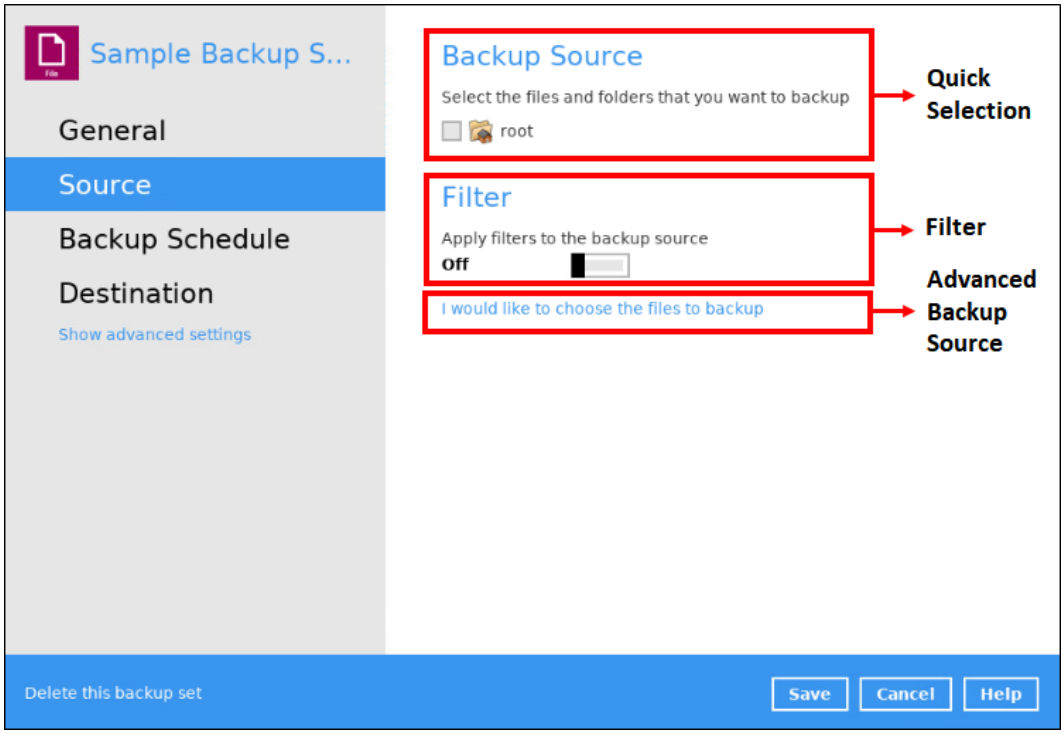


To modify the backup set name, follow the instructions below:

1. Enter the new backup set name on the Name field.
2. Click the **Save** button to save the new backup set name.

Source

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



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

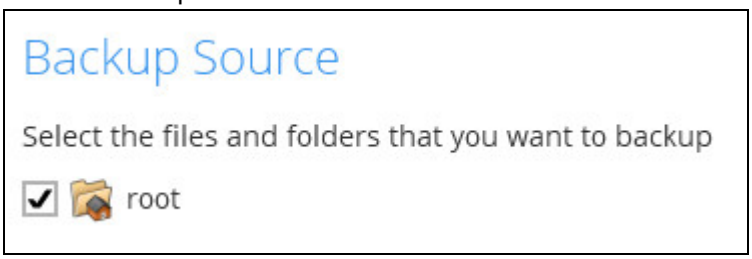
Option	Description
Quick Selection	This allows the user to back up files and/or folders in the selected backup source entirely.
Filter	This allows the user to select or exclude files and/or folders from the backup job.
Advanced Backup Source	This allows the user to select files and/or folders individually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

Option no. 1: Quick Selection

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

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

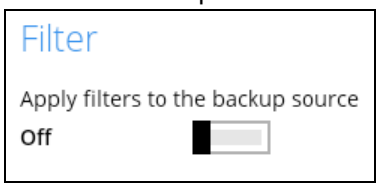
1. Select a backup source.



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

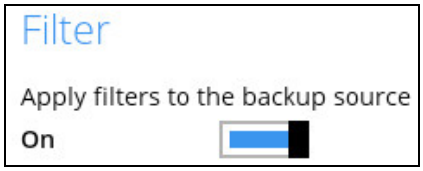
Option no. 2: Filter

The Filter Backup Source is an alternative way to select a backup source.

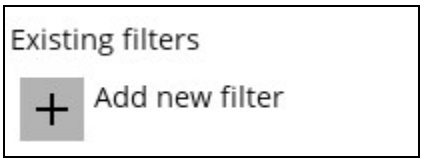


To select files and/or folders to back up using the Filter Backup Source, follow the steps below:

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

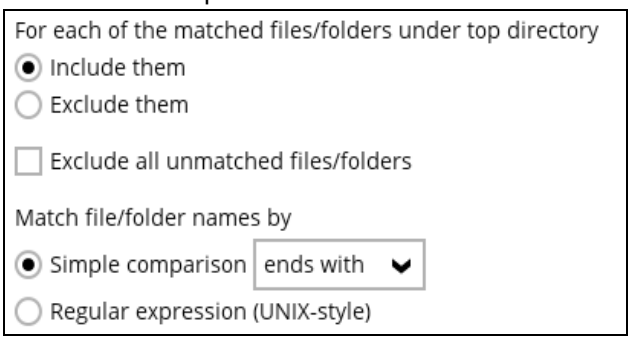


2. Click the **Add** button to create filter.

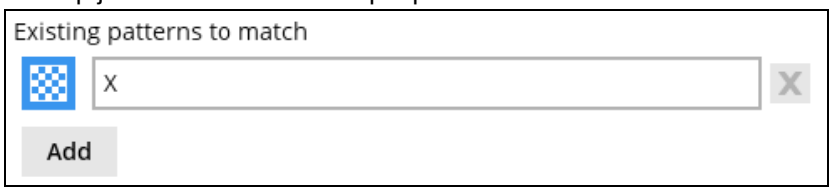


3. Assign a desired name to the backup filter.

4. Select from the options below.



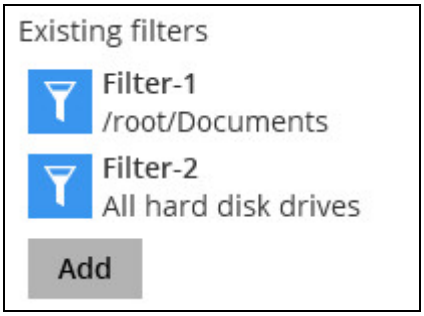
5. In this example, all files and/or folders that end with the letter 'X' will be included in the backup job. You can add multiple patterns here.



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

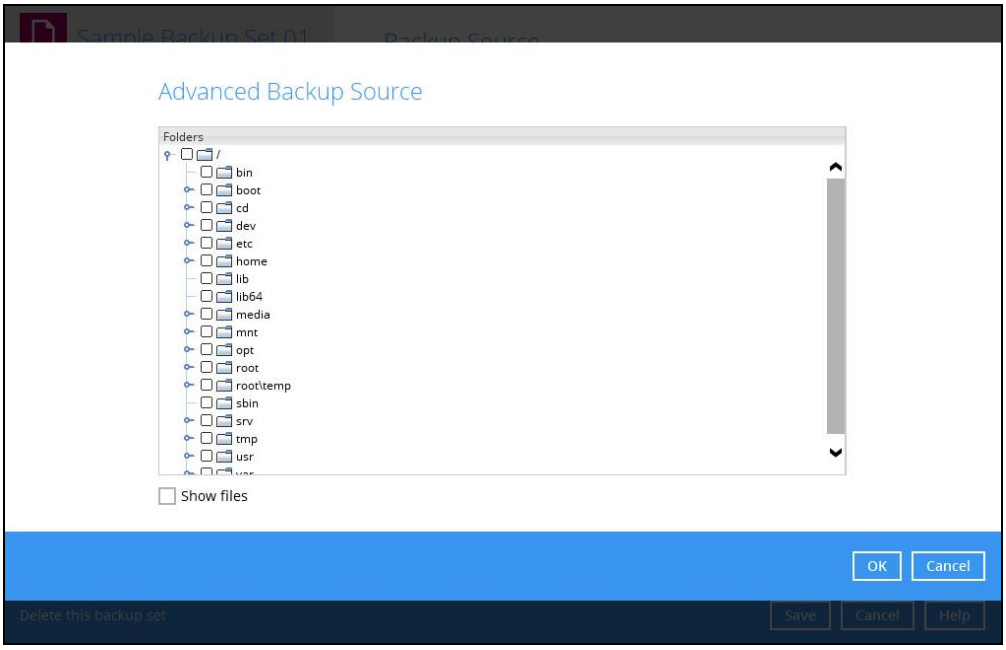
7. Click the **OK** button to save the created filter, then click the **Save** button to save the settings. Once you run a backup, all files and/or folders that match the applied filter will be backed up.

8. Multiple backup filters can be created.



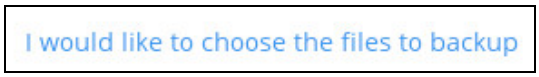
Option no. 3: Advanced Backup Source

The Advanced Backup Source is another way to select a backup source.

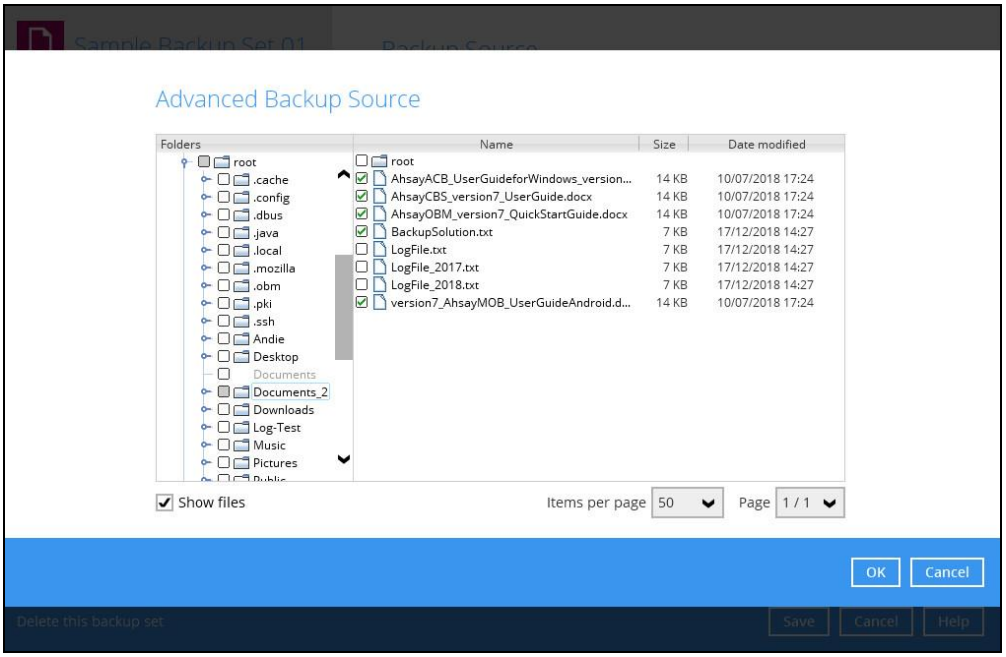


To select files and/or folders using the Advanced Backup Source, follow the steps below:

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



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



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

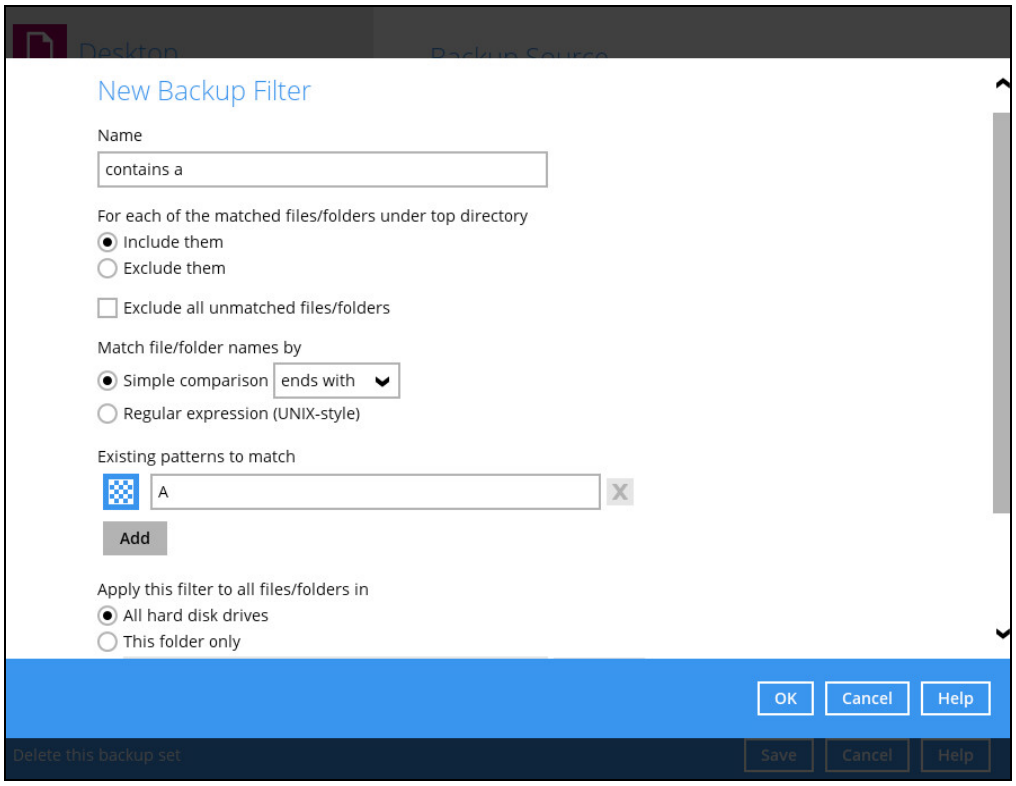
In selecting files and/or folders to back up, the three (3) options are combinable and can be used simultaneously. Please refer to the example scenarios below for details:

Scenario 1 (Quick Selection + Filter)

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

1. Choose a backup source.

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

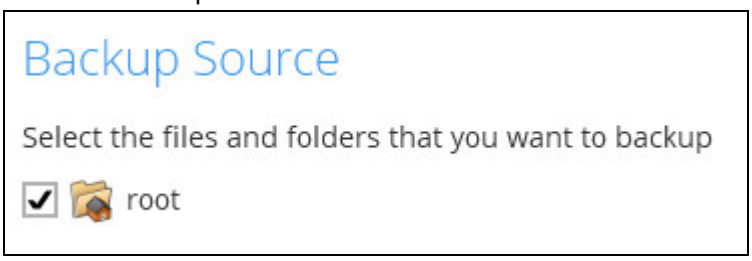


3. Click the **OK** button to save the created filter, then click the **Save** button to save settings.

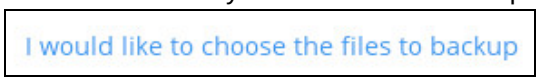
Scenario 2 (Quick Selection + Advanced Backup Source)

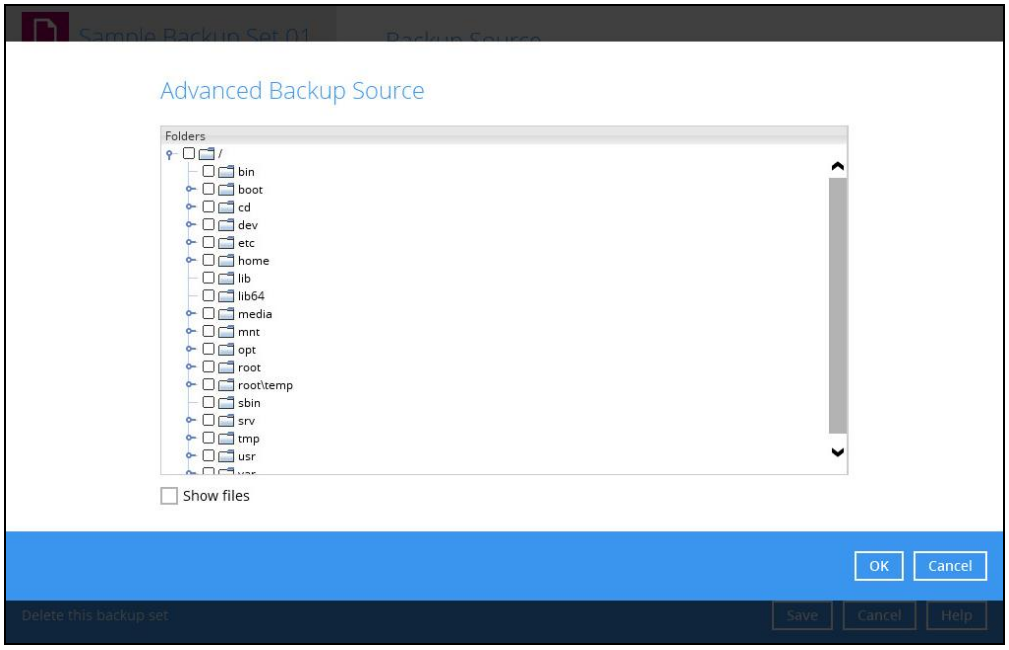
You can use the quick selection option and select files and/or folders in the advanced backup source at the same time. To use this type of combination, follow the steps below:

1. Choose a backup source.



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



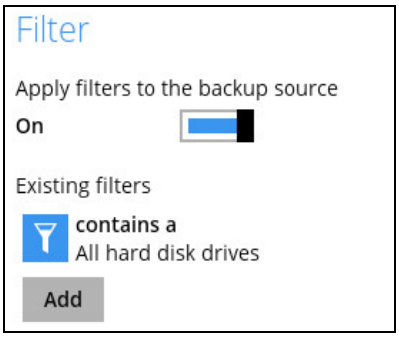


3. Click the **OK** button to save the selection, then click the **Save** button to save settings.

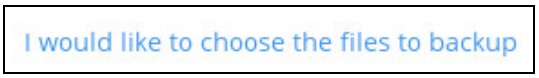
Scenario 3 (Filter + Advanced Backup Source)

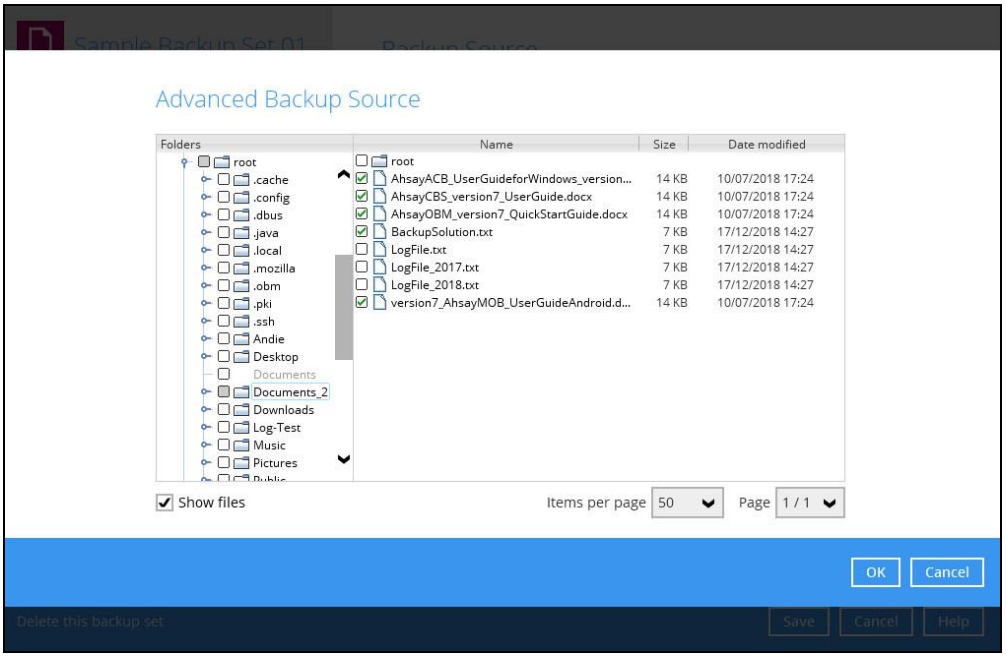
You can use the filter backup source and choose files and/or folders in the advanced backup source at the same time. To use this type of combination, follow the steps below:

1. Create a filter.



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

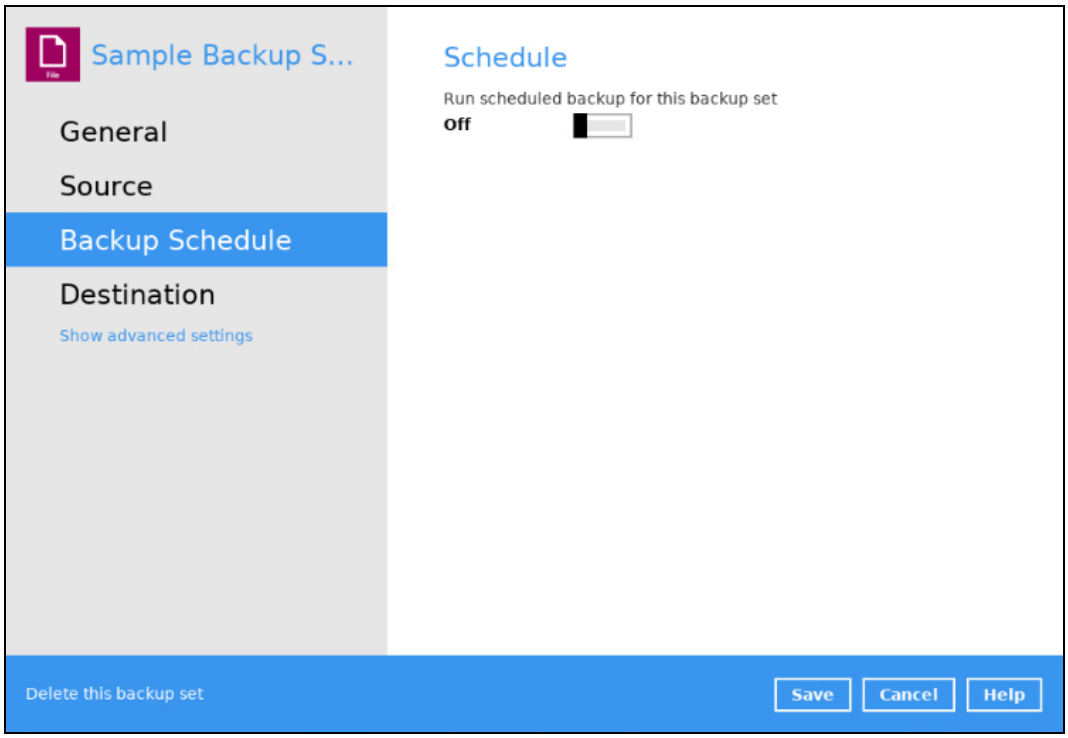




3. Click the **OK** button to save the selection, then click the **Save** button to save settings.

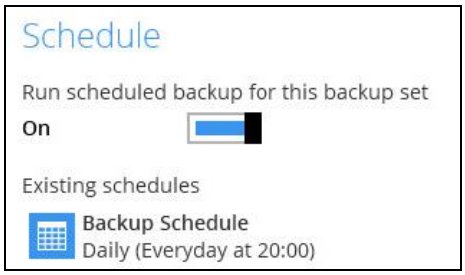
Backup Schedule

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

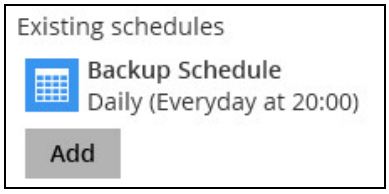


To configure a backup schedule, follow the steps below:

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

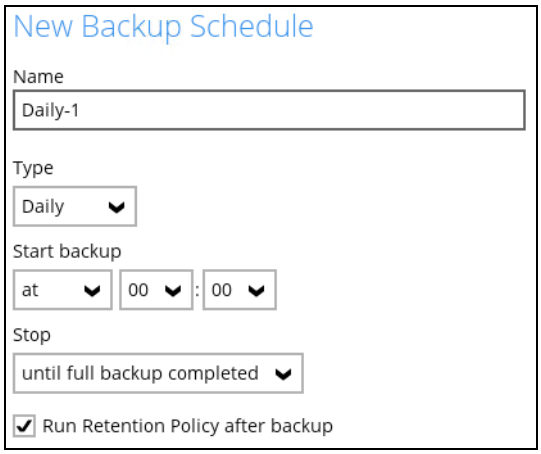


2. Select an existing backup schedule to modify or click the **Add** button to create a new one.

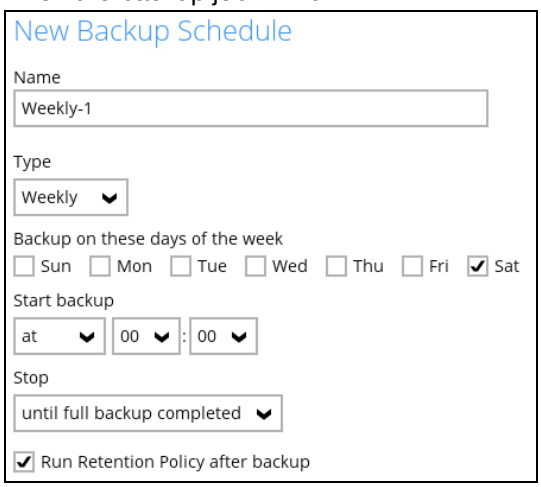


3. In the New Backup Schedule window, configure the following backup schedule settings.
   - **Name** – the name of the backup schedule.
   - **Type** – the type of the backup schedule. There are four (4) different types of backup schedule: Daily, Weekly, Monthly and Custom.

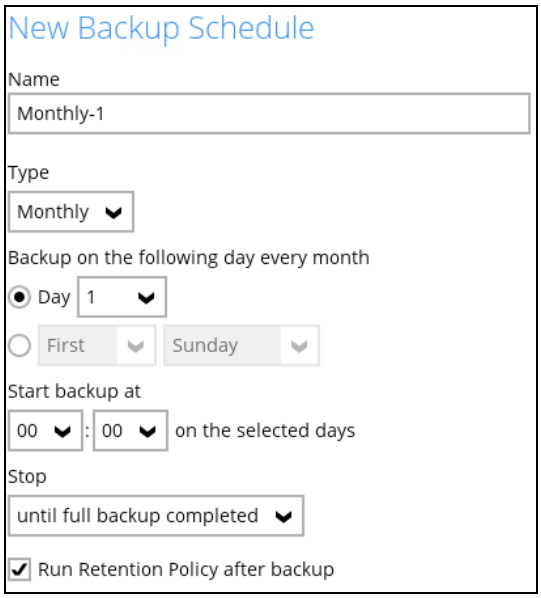
- **Daily** – the time of the day or interval in minutes/hours when the backup job will run.



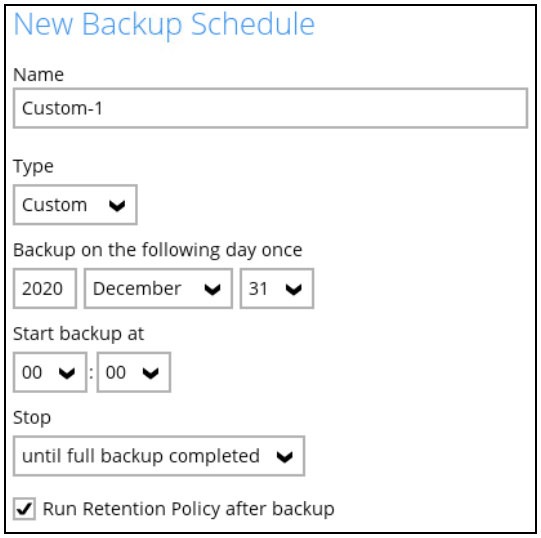
- **Weekly** – the day of the week and the time of the day or interval in minutes/hours when the backup job will run.



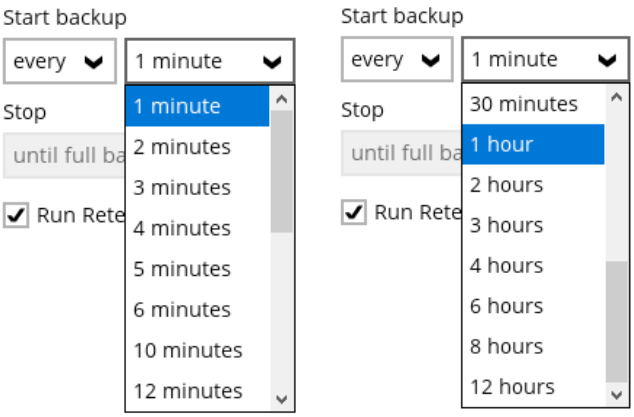
- **Monthly** – the day of the month and the time of the day when the backup job will run.



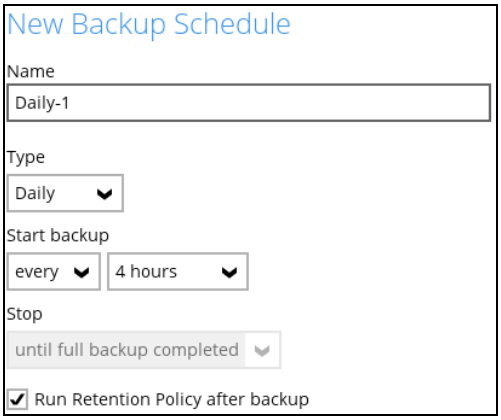
- **Custom** – a specific date and the time when the backup job will run.

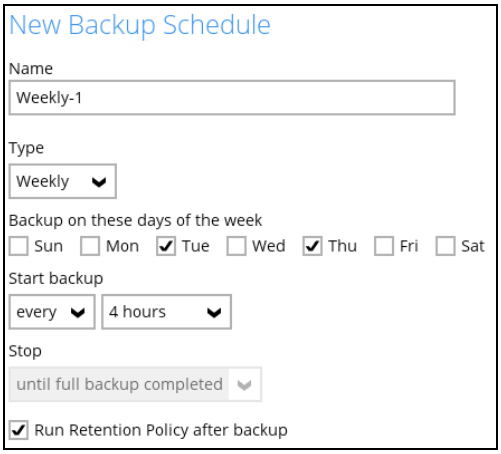


- **Start backup** – the start time of the backup job.
  - **at** – this option will start a backup job at a specific time.
  - **every** – this option will start a backup job in intervals of minutes or hours.
    - minute interval, 1, 2, 3, 4, 5, 6, 10, 12, 15, 20, or 30 minutes
    - hourly interval,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



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





Daily backup schedule runs daily every 4 hours while the weekly backup schedule run on Tuesday and Thursday every 4 hours.

Both are running every 4 hours but the priority backup schedule will still be the Daily backup schedule. Weekly backup schedule will run after the daily backup schedule.

- **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.

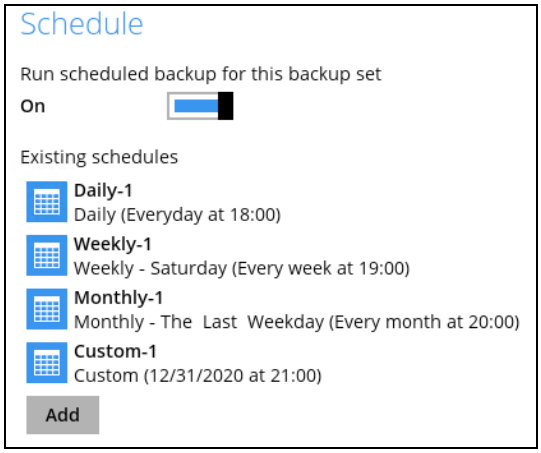
    The partially backed up data will have to be removed by running the data integrity check.

    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.

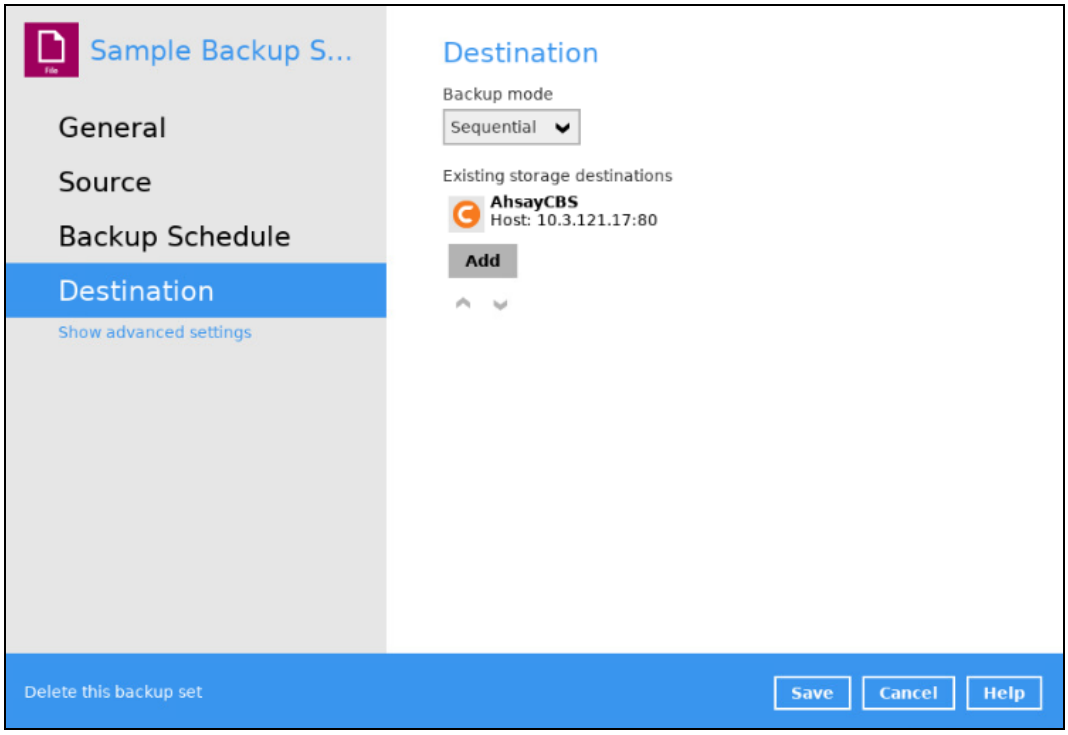
5. Click the **Save** button to save settings.

6. Multiple backup schedules can be created.



Destination

This allows the user to view the current backup mode and existing storage and add additional storage destinations.



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

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

Comparison between Sequential and Concurrent Backup mode

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

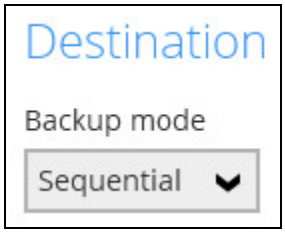
Concurrent	➢ Backup job is faster than in Sequential mode. ➢ Maximum number of concurrent backup destinations can be configured.	➢ Requires more resources in the local machine (e.g. memory, CPU, bandwidth, etc.) to complete a backup job.

To modify the Backup mode, follow the steps below:

1. Go to Backup Sets, then choose a backup set.

1. Select the Destination tab in the backup set settings.

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

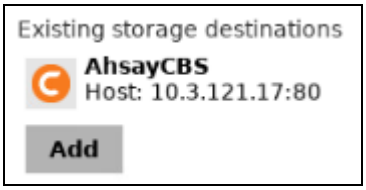


3. If “Concurrent” is selected, click the drop-down button to select the no. of maximum concurrent backup destinations.

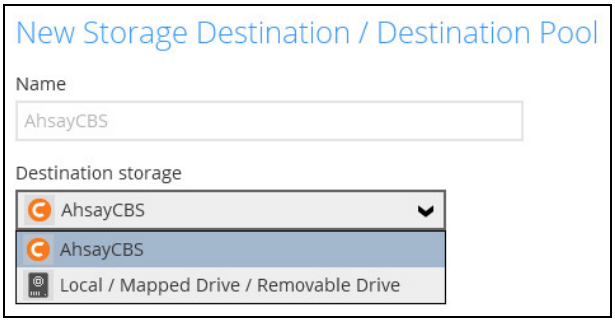
4. Click the **Save** button to save the selected backup mode.

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

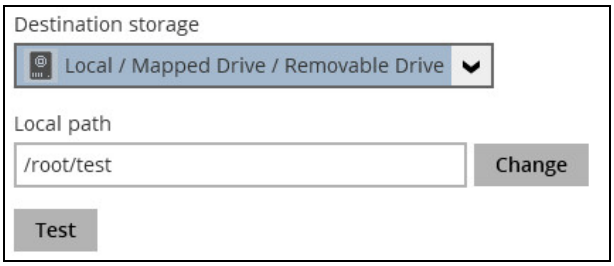
1. Click the **Add** button.



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



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



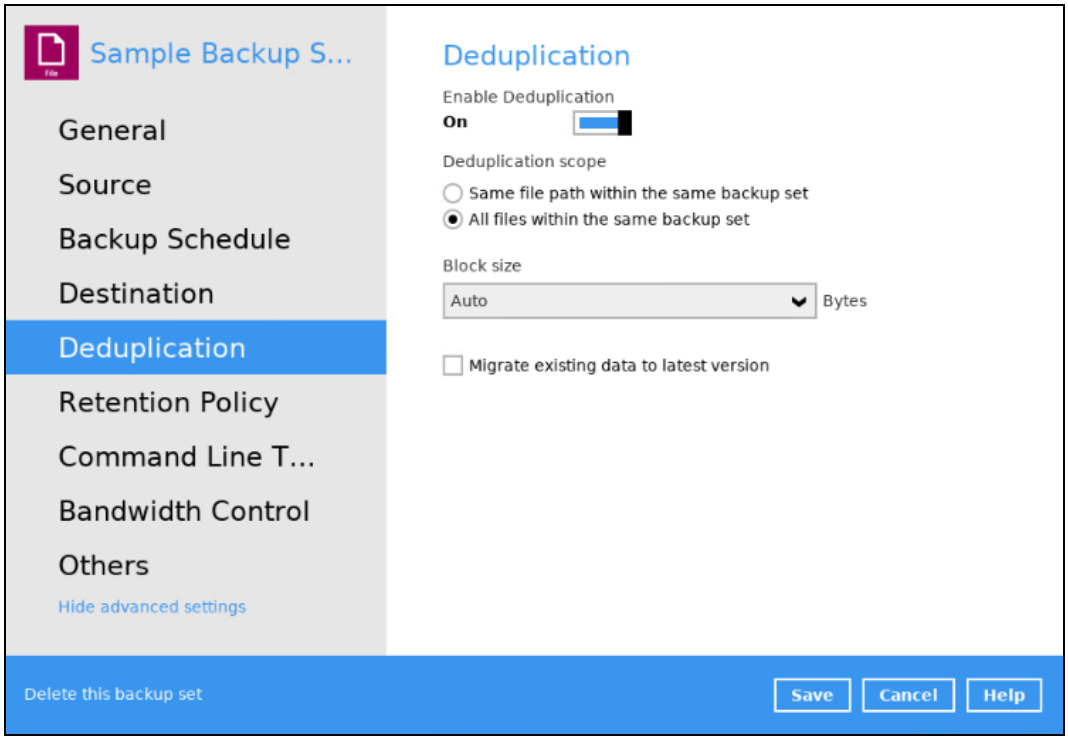
4. If there is an added storage destination, click the **OK** button to save the added one. Then click the **Save** button to save the updated backup mode and the added storage destination.

Deduplication

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

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

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

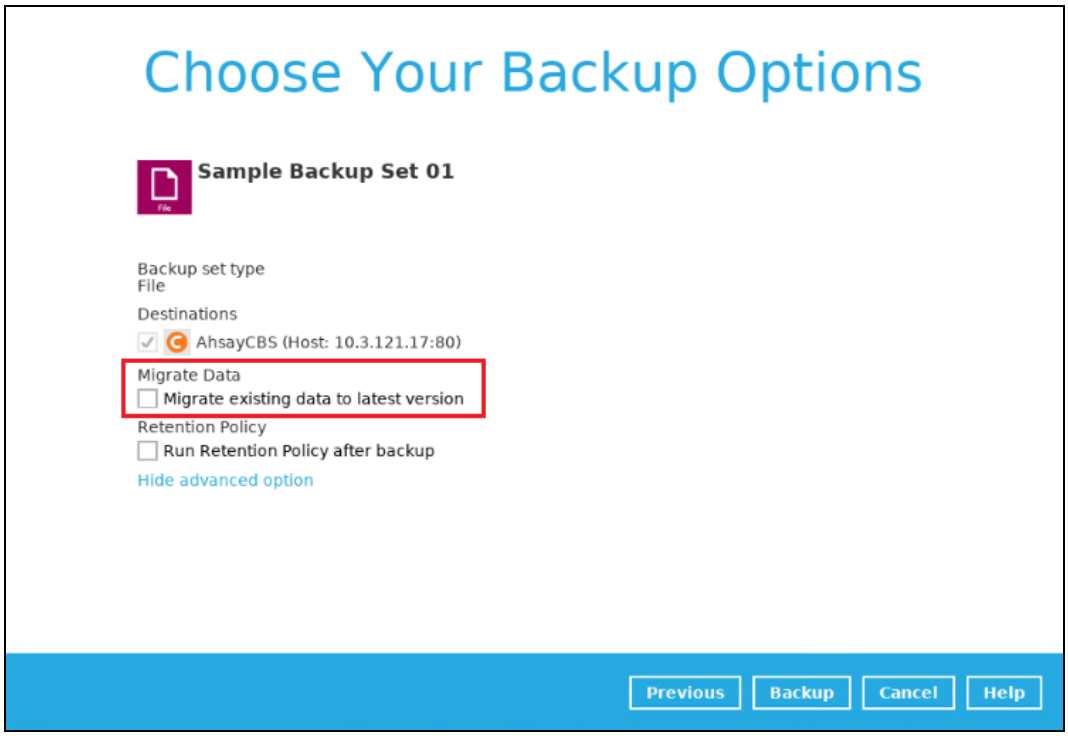


There are two (2) Deduplication scope:

Deduplication	Description
Same file path within the same backup set	This type of Deduplication will deduplicate data under the same path during a backup job.
All files within the same backup set	This type of Deduplication will deduplicate data under the same backup set during a backup job.

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

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



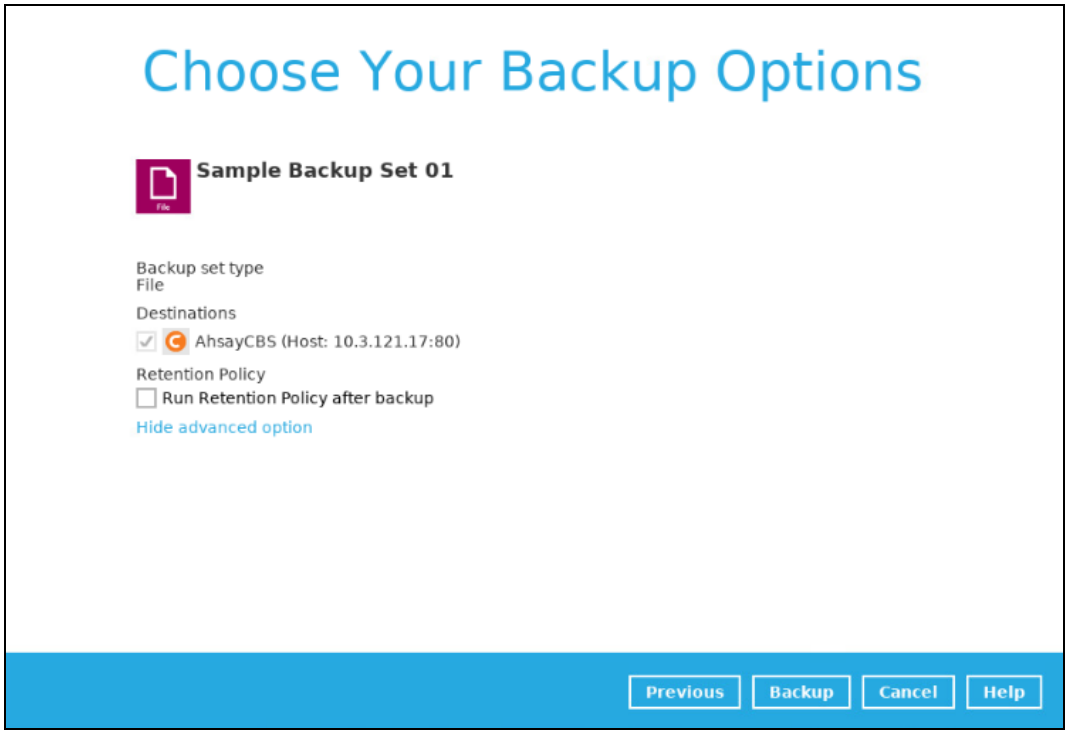
Migrate Data

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

NOTE

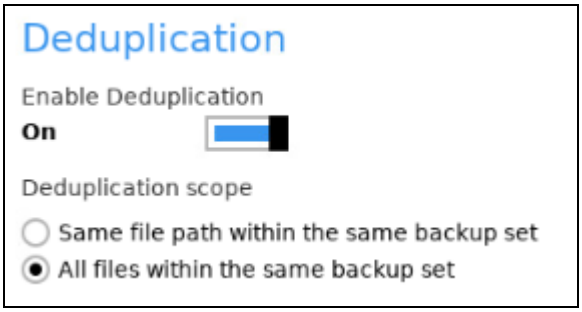
In case the Deduplication setting is disabled for the backup set, the Migrate Data option will not be displayed.

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

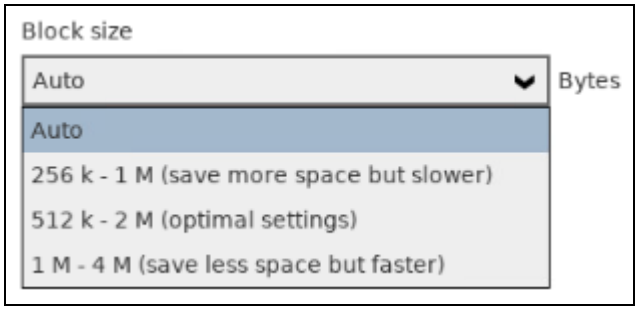


To configure the deduplication settings, follow the instructions below:

1. Select the Deduplication scope.



2. Click the drop-down button to select the block size that will be used for the deduplicated data. This option is configured to use “Auto” by default.



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

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

Retention Policy

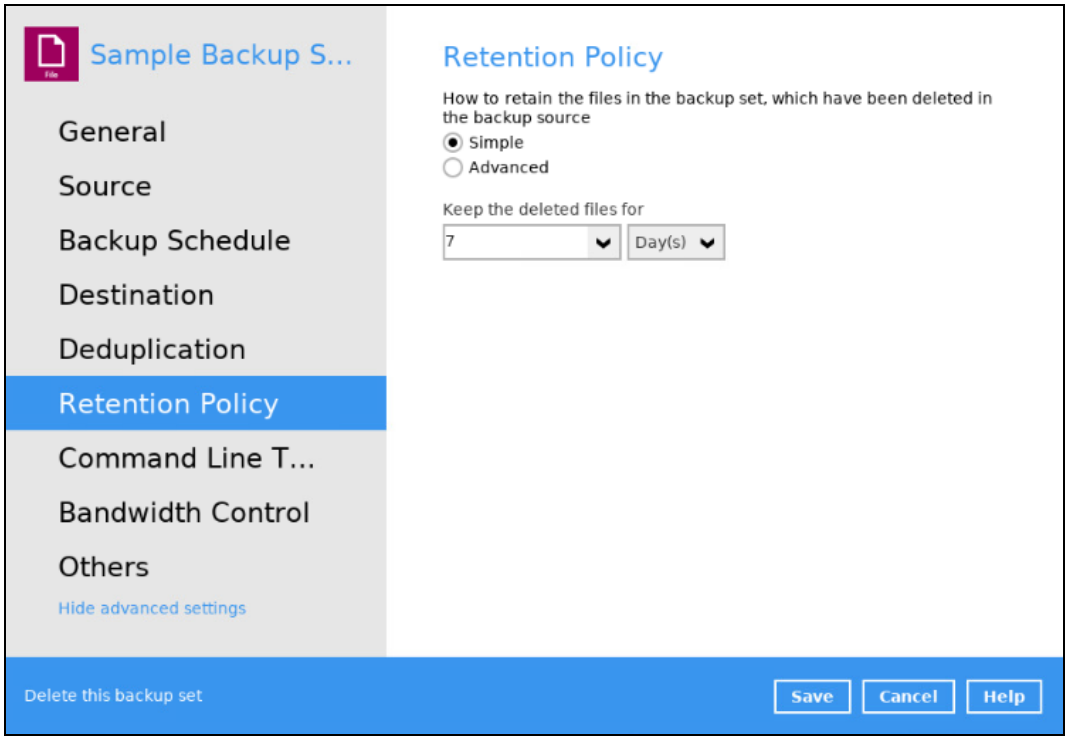
When the AhsayOBM identifies files and/or folders that are deleted, updated, or with updated permission/attributes during a backup job, these files and/or folders will then be moved from the Data Area to the Retention Area.

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

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

The **Retention Policy** is used to control how long these files remain in the Retention Area when they are removed which can be specified in the number of days, weeks, months, or backup jobs. Retained data within all backup destinations (e.g. 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

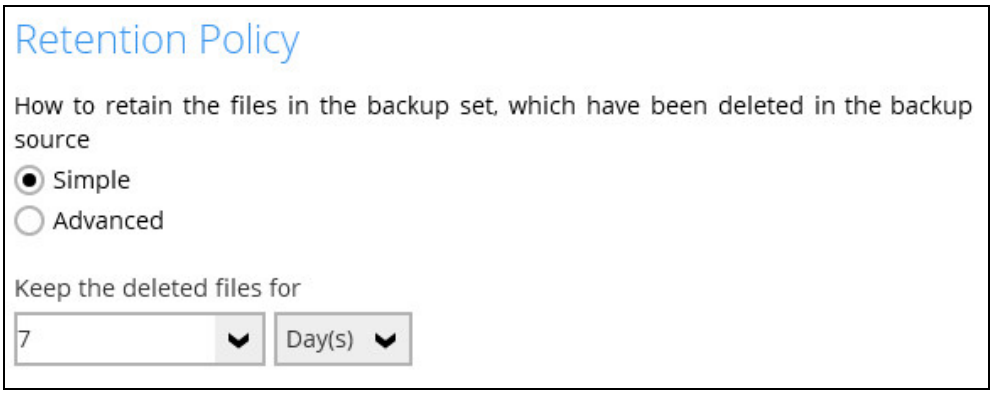
Control	Simple	Advanced
Backup Jobs	Can keep the deleted for specified number of backup job(s)	Not applicable
Days	Can keep the deleted files for specified number of day(s)	Can keep the deleted files for specified number of day(s)
Type	Not applicable	➢ Daily ➢ Weekly ➢ Monthly ➢ Quarterly ➢ Yearly ➢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

WARNING

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

To configure a **Simple Retention Policy** retention policy, follow the instructions below:

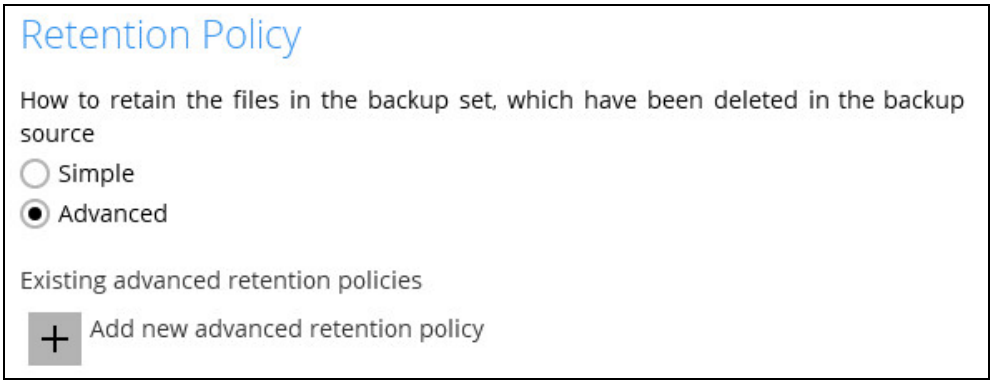
1. Select “Simple” from the options, then click the drop-down button to define the number of day(s) or job(s) when the deleted files will be retained. This is configured as seven (7) days by default.



2. Click the **Save** button to save the configured retention policy settings.

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

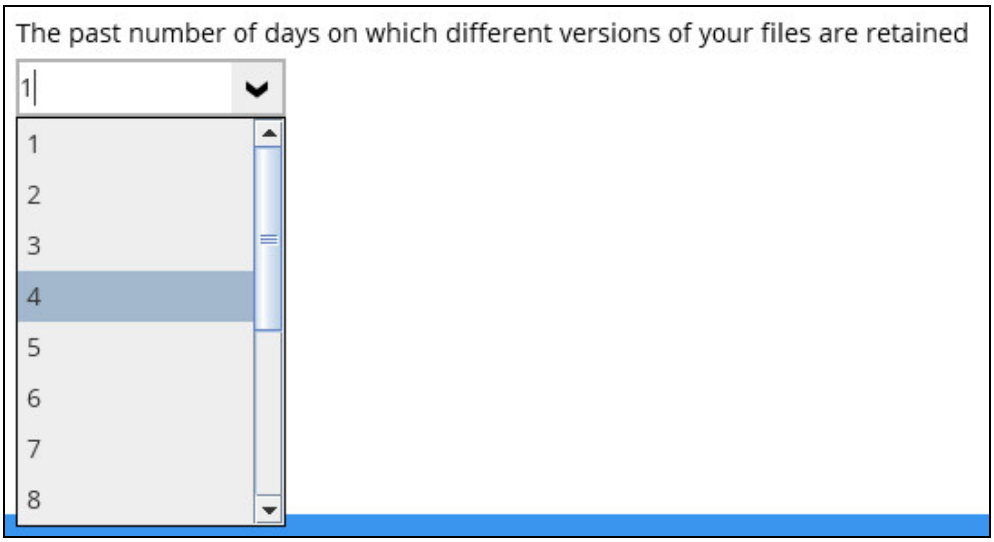
1. Select “Advanced” from the options, then click the **Add** button to create a retention policy.



2. Enter a name for the retention policy.

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

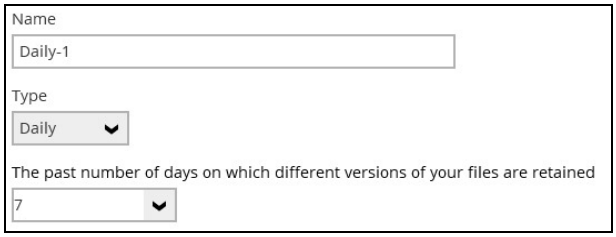
4. Click the drop-down button to specify the period on which the deleted files will be kept in retention.



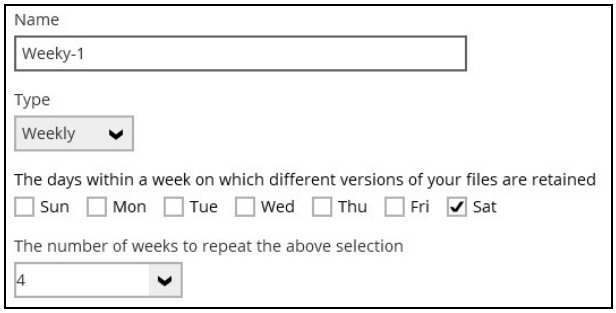
5. Click the **OK** button to save the configured advanced retention policy, then click **Save** to save the settings.

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

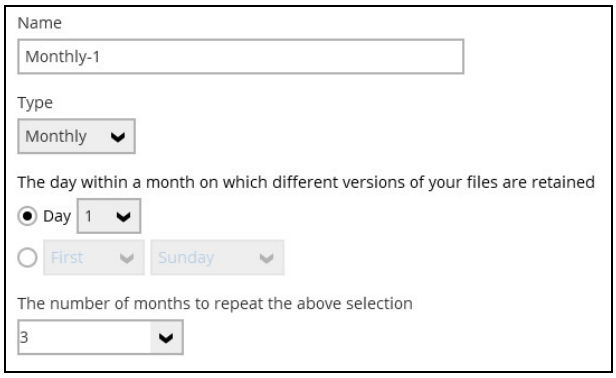
- **Example no. 1**: To keep the retention files for the last seven (7) days:



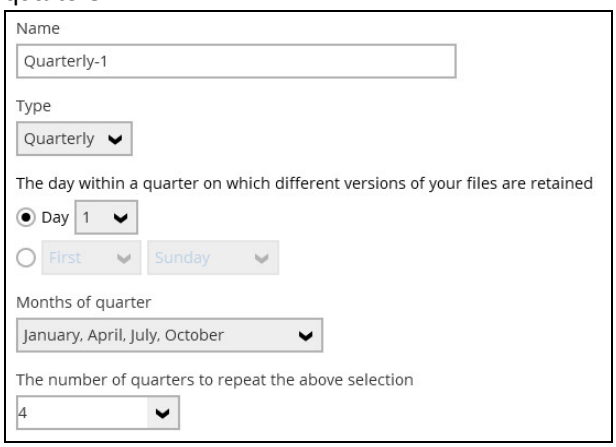
- **Example no. 2**: To keep the retention files for the last four (4) Saturdays:



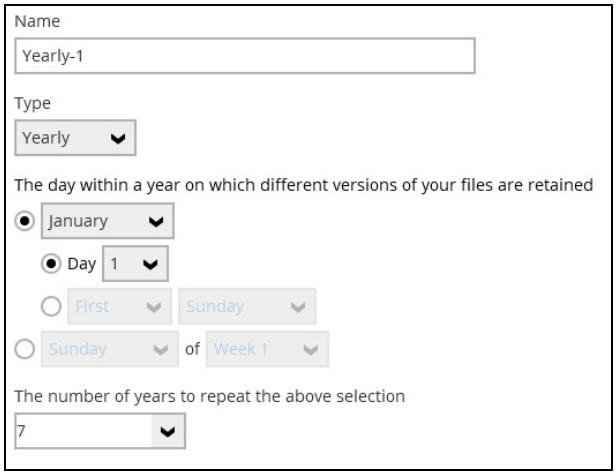
- **Example no. 3**: To keep the retention files for the 1st day of each month for the last three (3) months:



- **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.

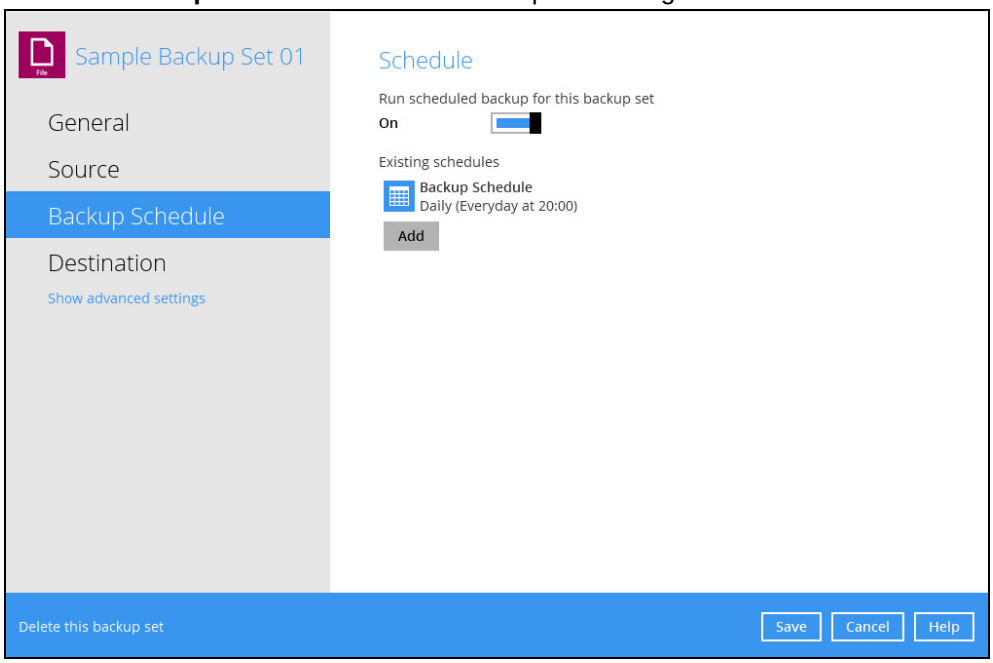
There are three (3) different ways to enable the Retention Policy:

- Backup Scheduler
- Manual Backup
- Space Freeing Up

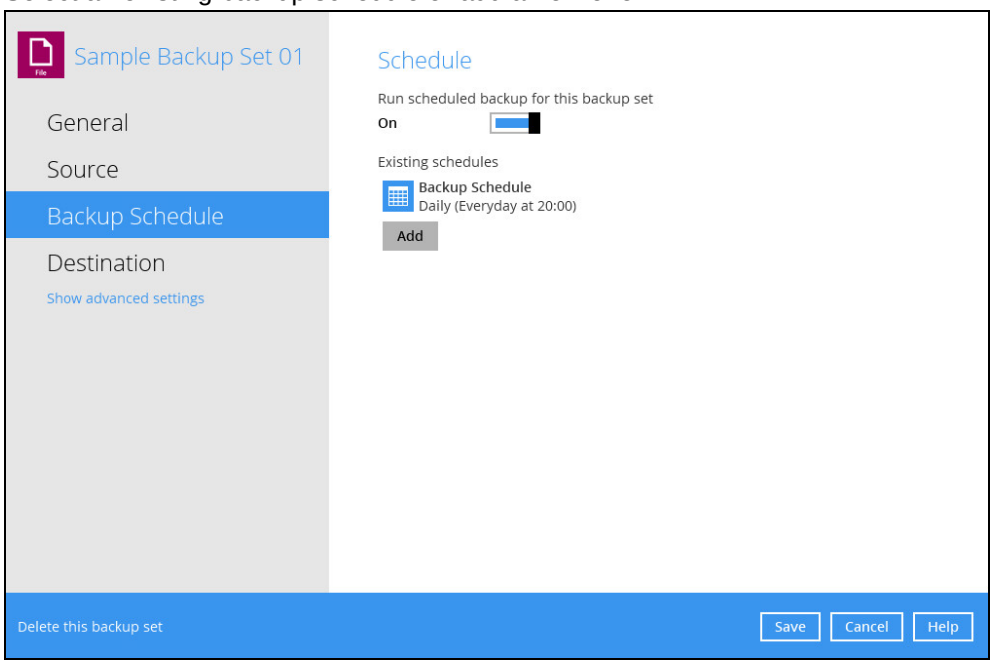
Backup Scheduler (Recommended)

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

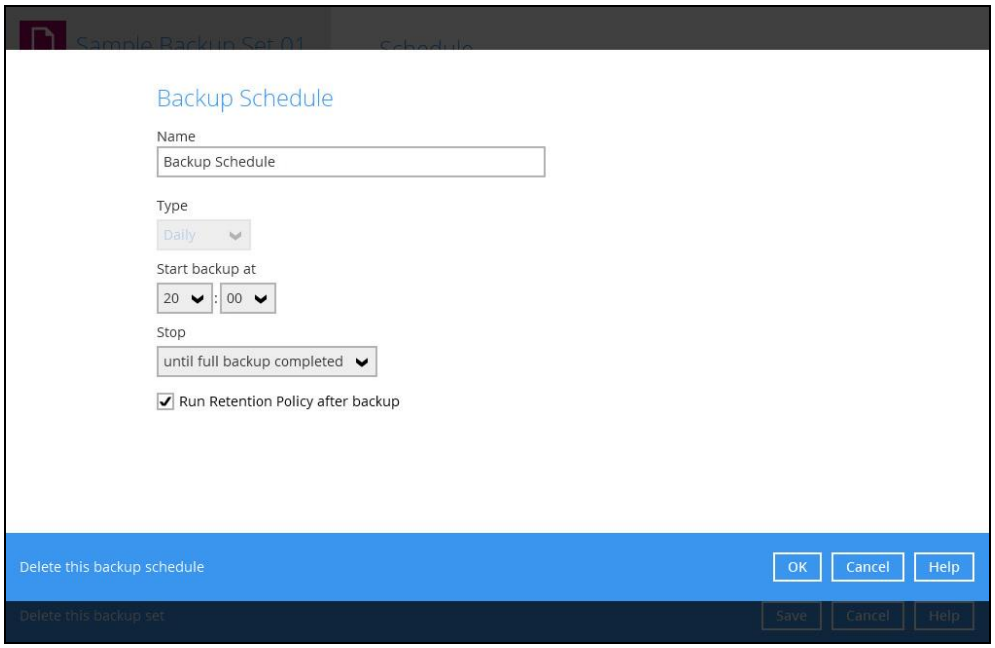
1. Click the **Backup Schedule** tab in the backup set settings.



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



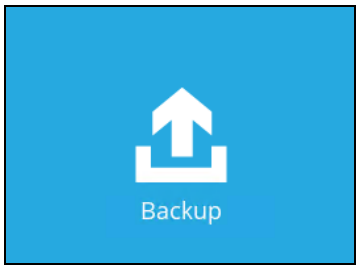
3. In the Backup Schedule window, select ‘Run Retention Policy after backup’ to run a retention policy job after a scheduled backup job.



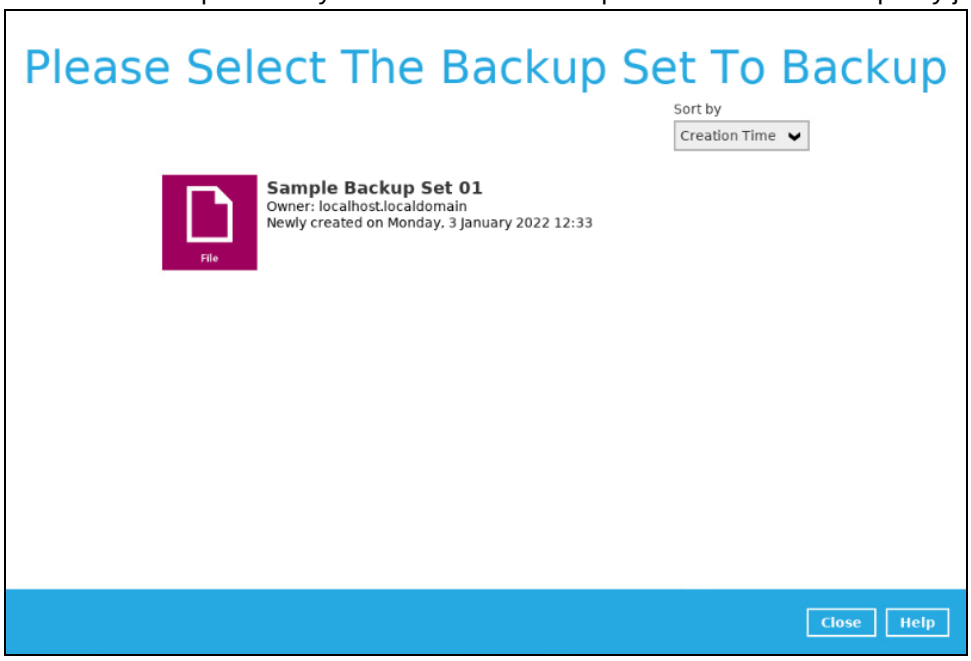
Manual Backup

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

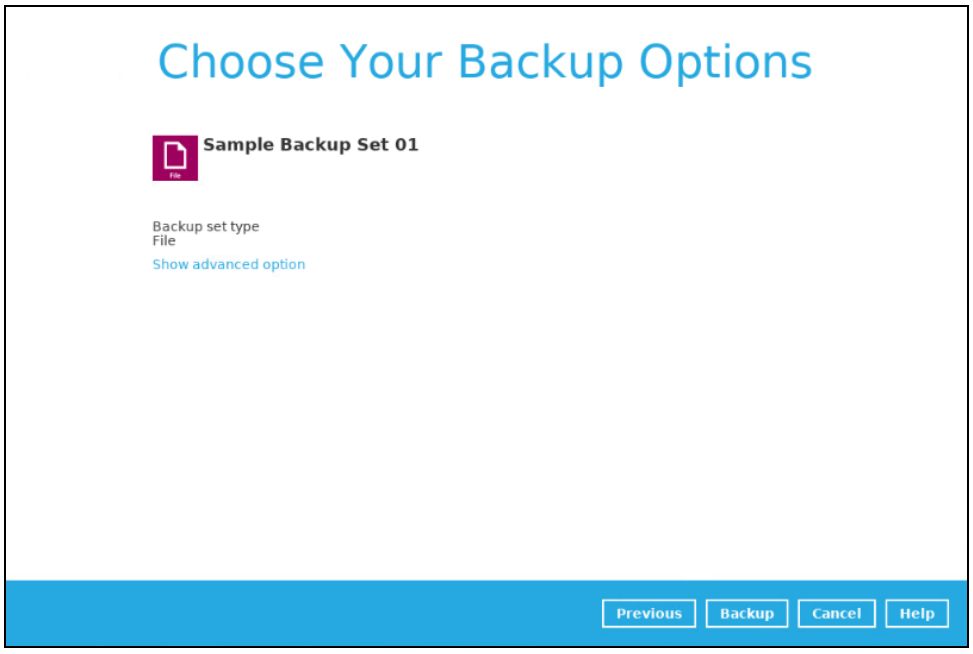
1. Click the **Backup** icon in the AhsayOBM main interface.



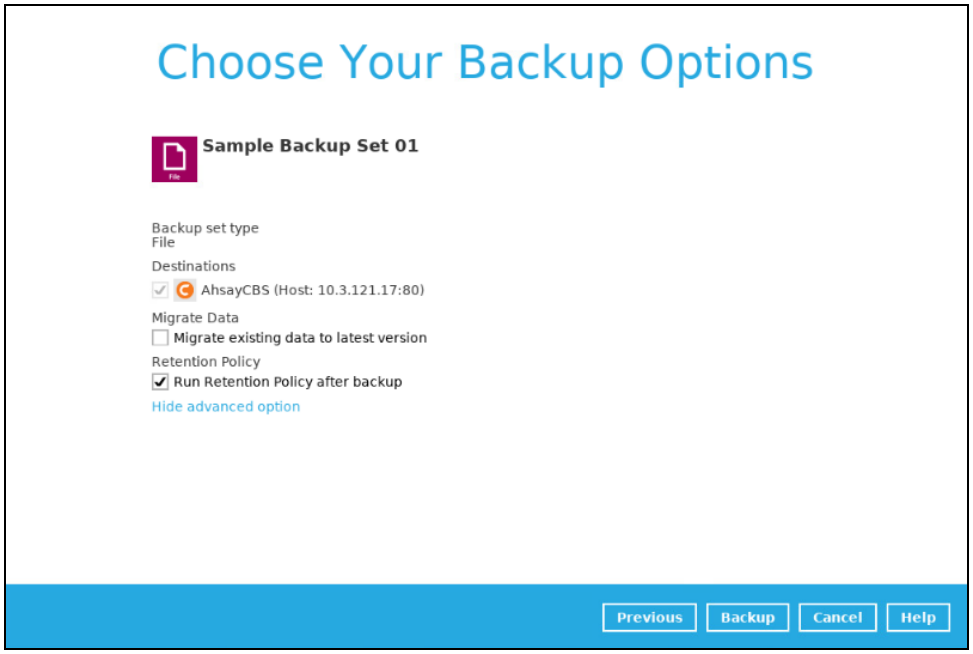
2. Select the backup set that you would like to back up and run the retention policy job on.



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



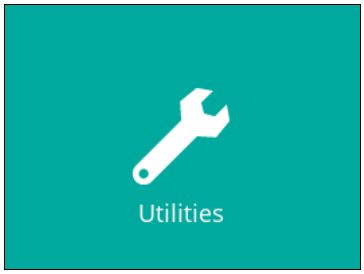
4. Select ‘Run Retention Policy after backup’ to run a retention policy job after a backup job.



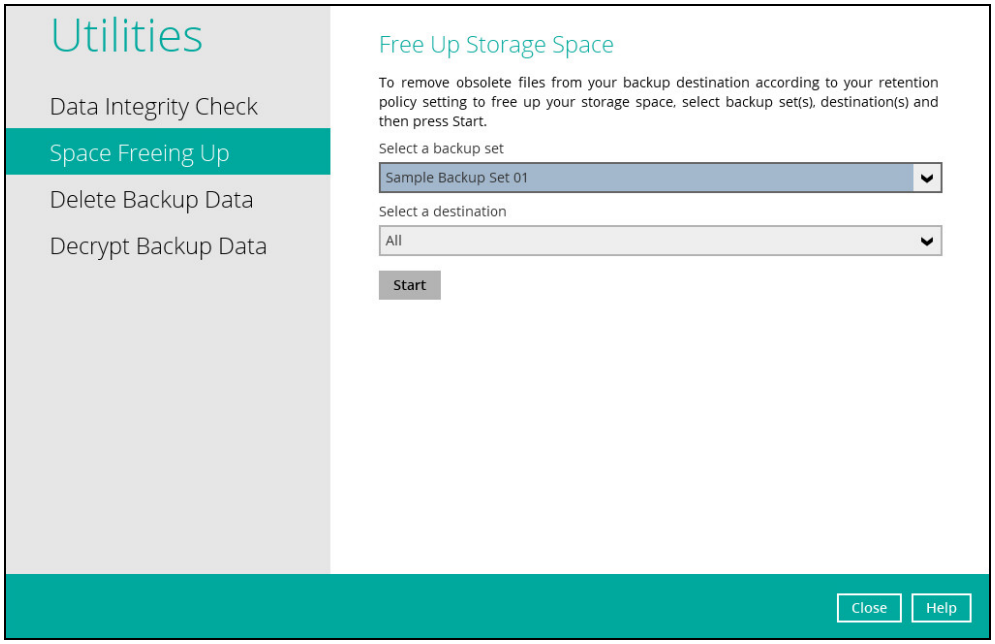
Space Freeing Up

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

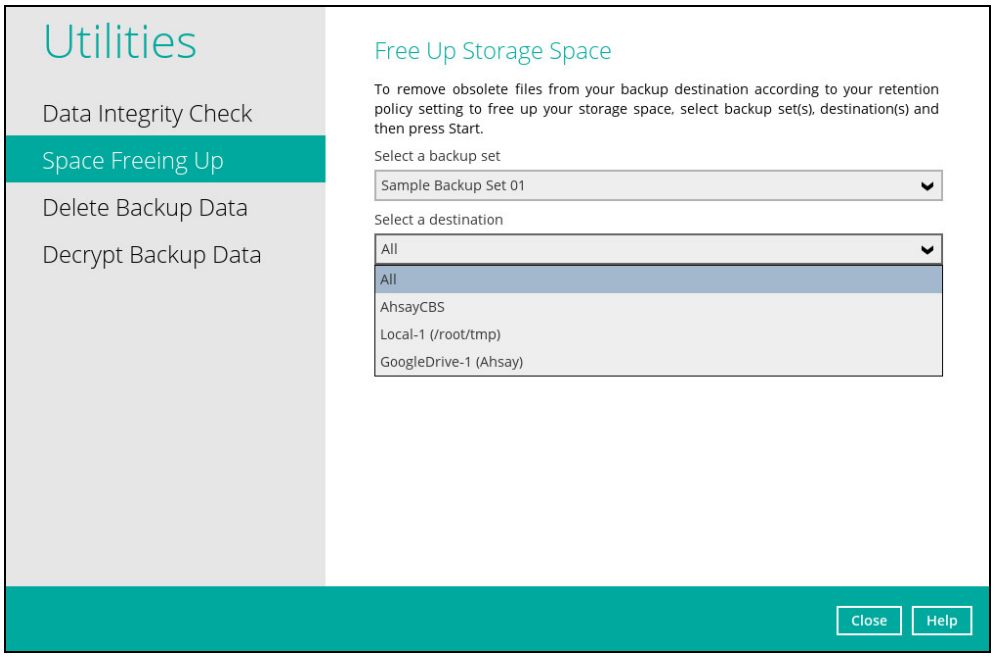
1. Click the **Utilities** icon in the AhsayOBM interface.



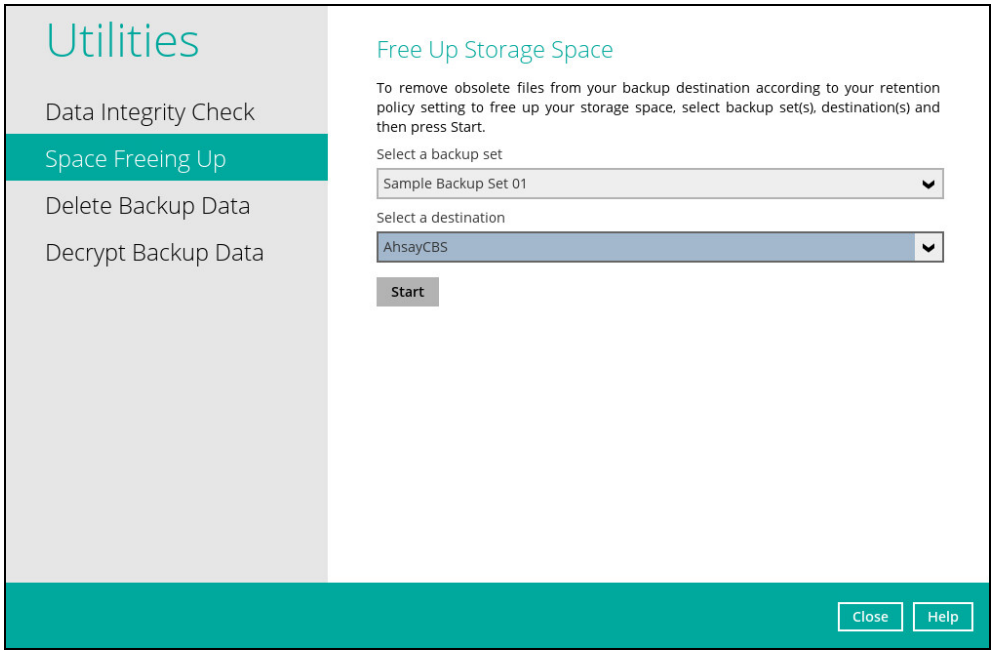
2. Select the **Space Freeing Up** tab in the Utilities settings.



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.



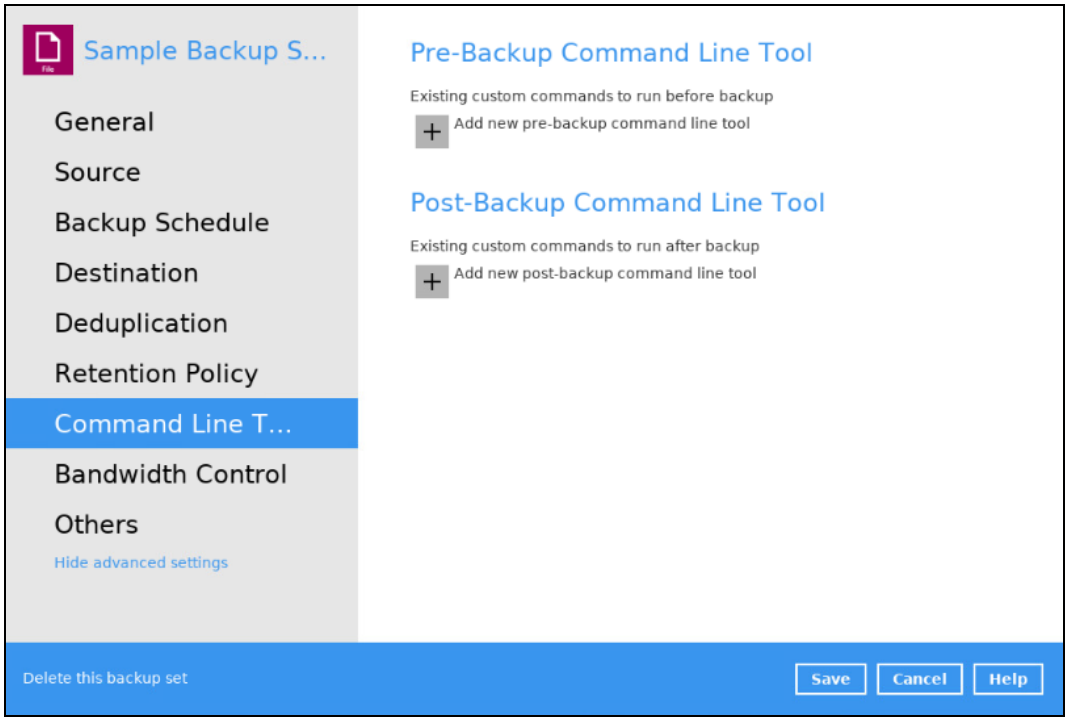
NOTE

For more details about Space Freeing Up, please refer to Space Freeing Up in Chapter 9.9.2.

Command Line Tool

This allows the user to configure 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 after a backup job.

For example: 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 the 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 9.6.

Command or Batch File Compatibility

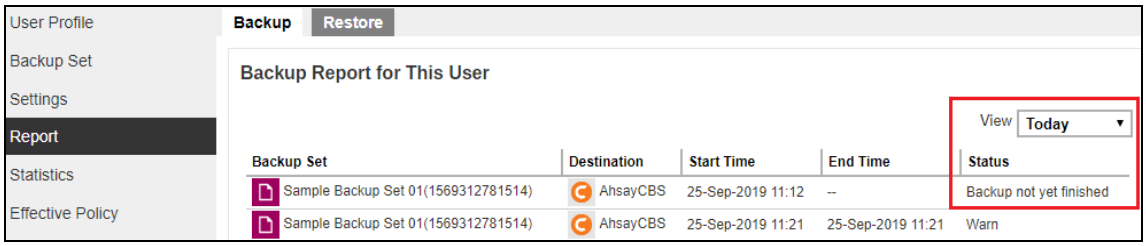
Make sure that each command (pre-backup and post-backup) are tested thoroughly before including them to the backup job.

Scheduled Backup

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

Pre-backup Command Limitation

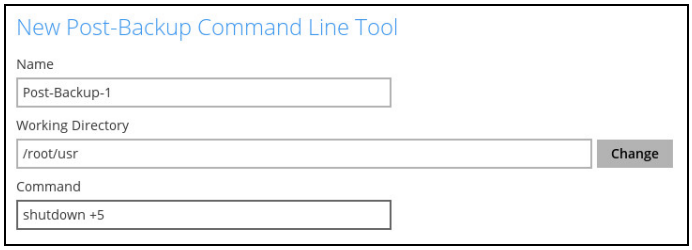
A reboot or shutdown must not be used in the pre-backup command. Otherwise, the machine will shut down immediately that will result to a status indicating “Backup not yet finished”, which can be viewed in the AhsayCBS User Web Console. Please refer to AhsayCBS Backup Reports for more details.



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 9.6.

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

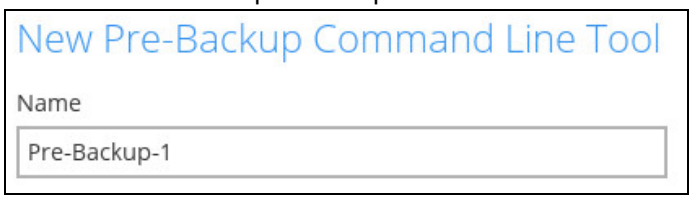
Field	Description
Name	The user-defined name of the pre-backup or post-backup command.
Working Directory	The location in the local machine which the pre-backup or post-backup command will run at, or the location of the command or created batch file.
Command	The **pre-backup** or **post-backup** command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

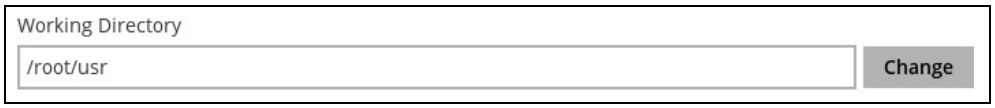
A pre-backup command is used to execute an action or process before the start of a backup job. To create a pre-backup command, follow the steps below:

1. Click the **Add** button.

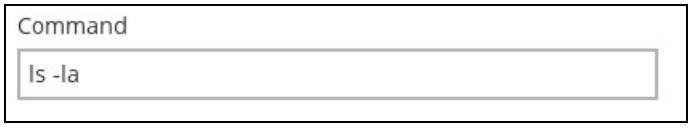
2. Enter a name for the pre-backup command.



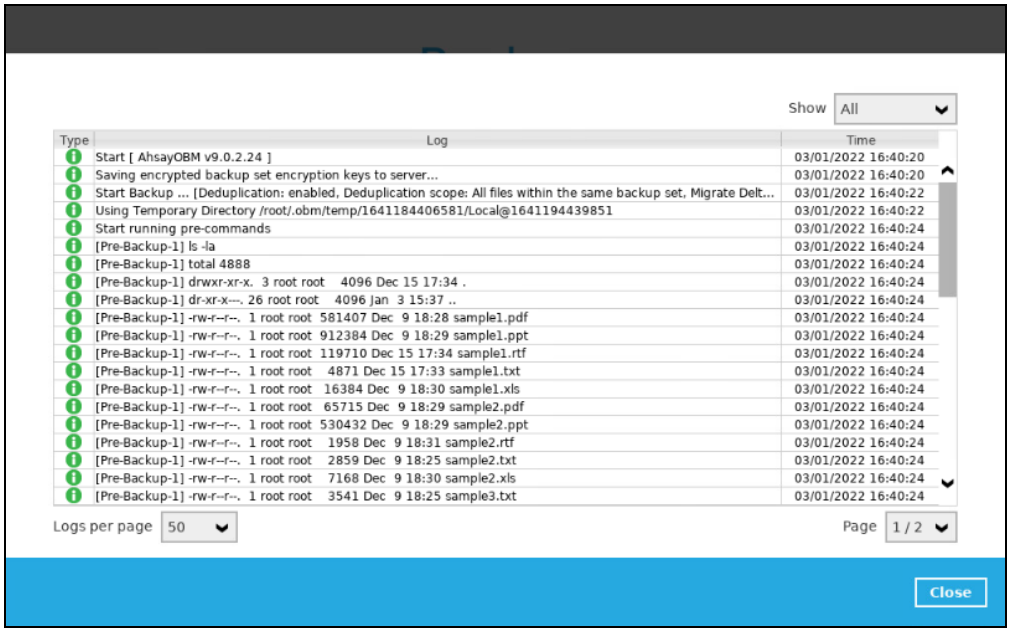
3. Click the **Change** button to locate the working directory of the command.



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

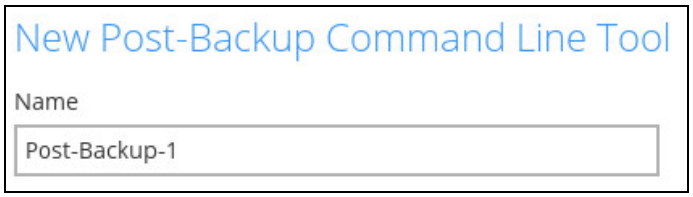


Post-backup Command

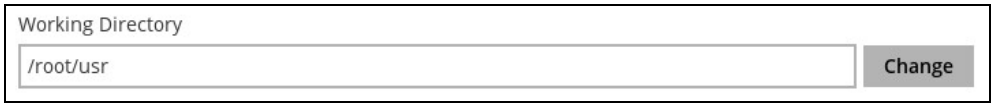
A post-backup command is used to execute an action or process after a backup job. To create a post-backup command, follow the steps below:

1. Click the **Add** button.

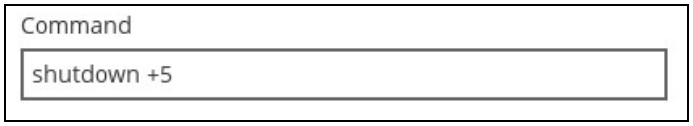
2. Enter a name for the post-backup command.



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

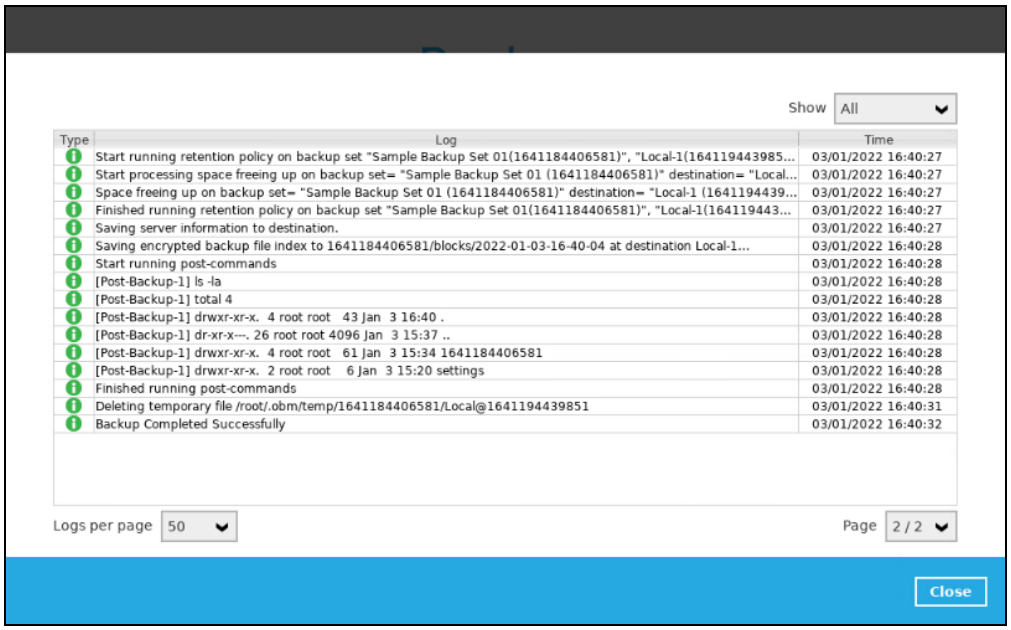


4. Input a command to be run after a backup job. In this example, the post-backup command will shut down the machine five minutes after the backup process.



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.

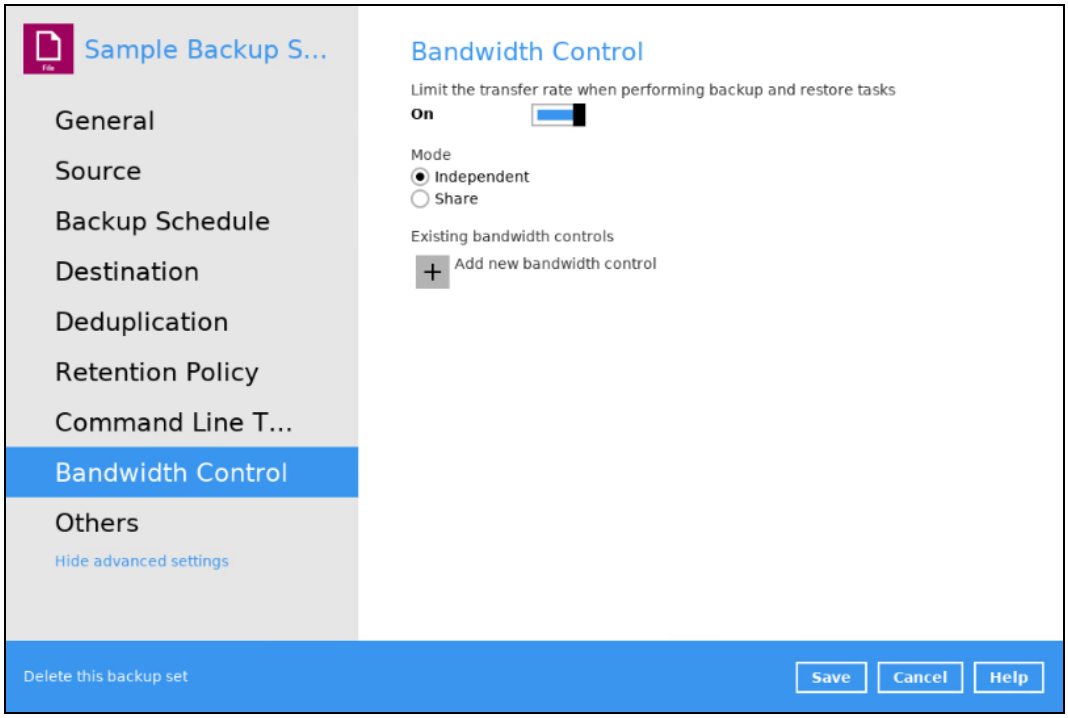


NOTE

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

Bandwidth Control

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



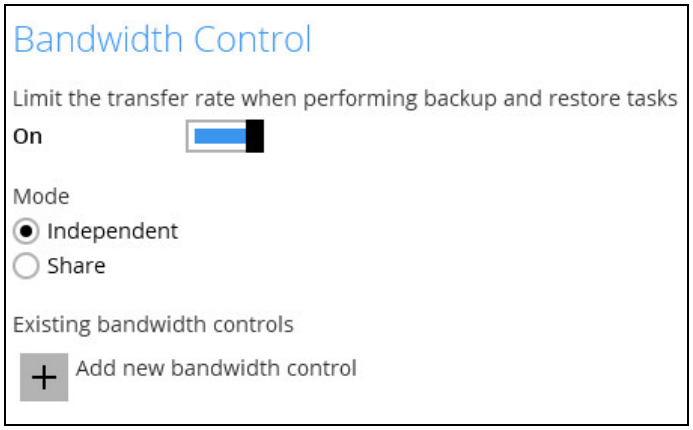
There are two (2) modes in assigning a bandwidth control:

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.

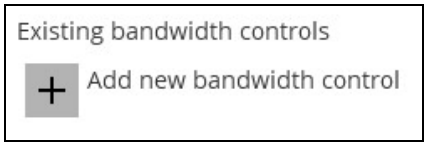
To enable the bandwidth control setting, follow the steps below:

1. Swipe the lever to the right to enable the bandwidth control.



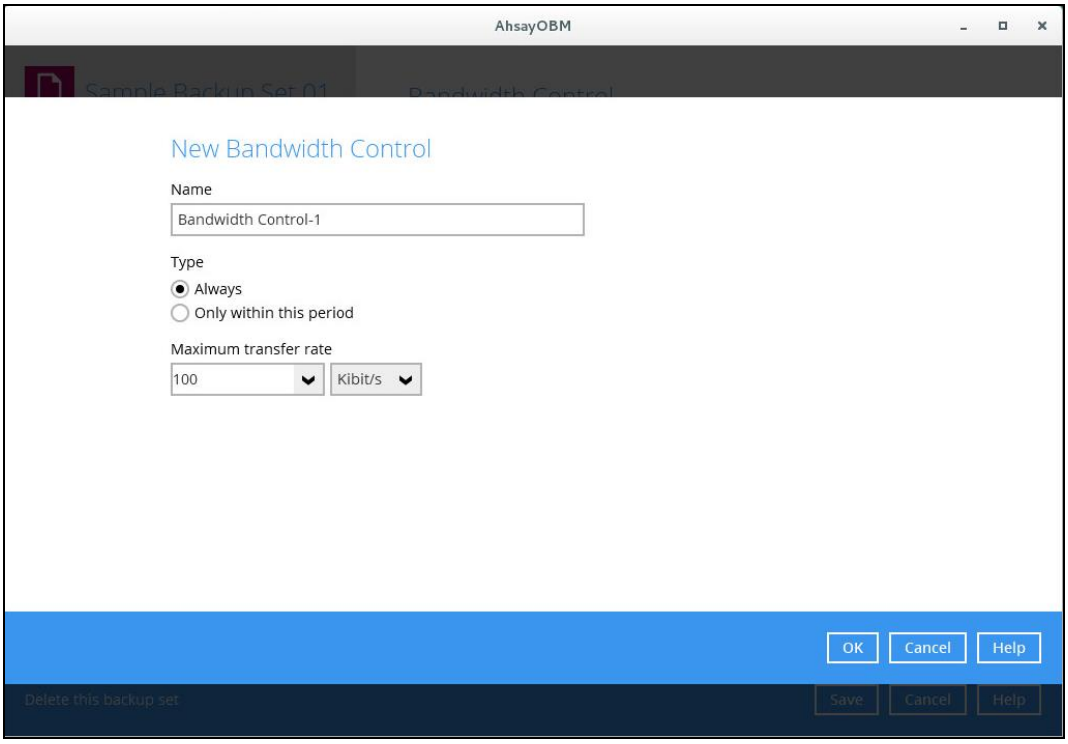
2. Select a mode: Independent or Share.

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



4. Complete the following fields:

   - Name – the name of the bandwidth control set.
   - Type – the type of enforced bandwidth control period.
   - Maximum transfer rate – the maximum bandwidth used.

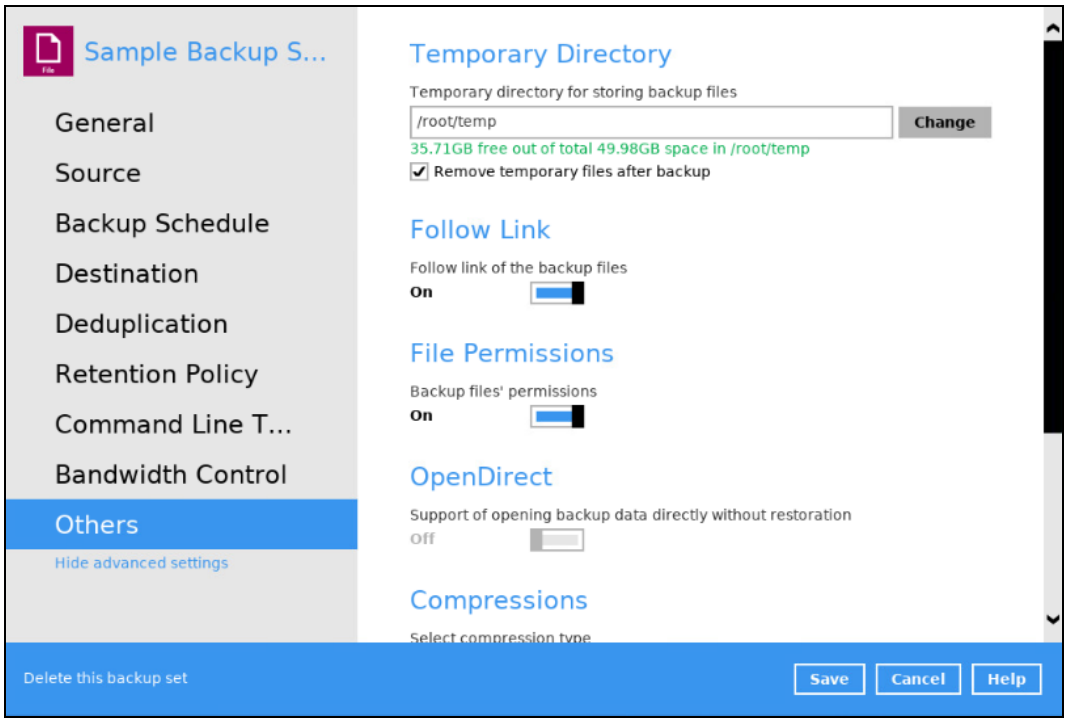


5. Click the **OK** button to save the created bandwidth control set, then click the **Save** button to save settings.

Others

These are the list of other backup set settings that can be configured.

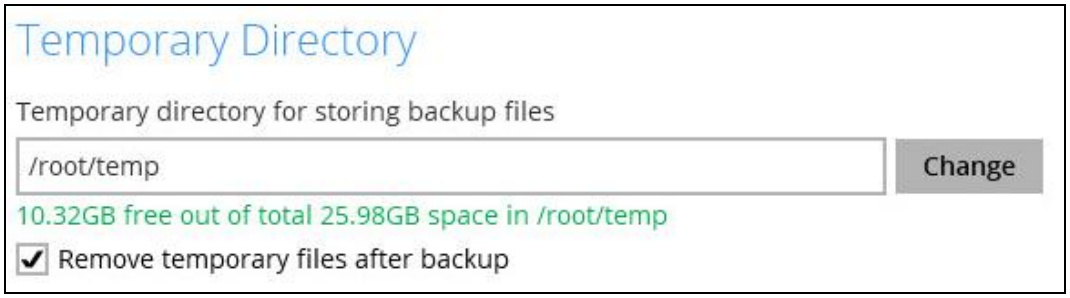
- Temporary Directory
- Follow Link
- File Permissions
- OpenDirect
- Compressions
- Encryption



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:

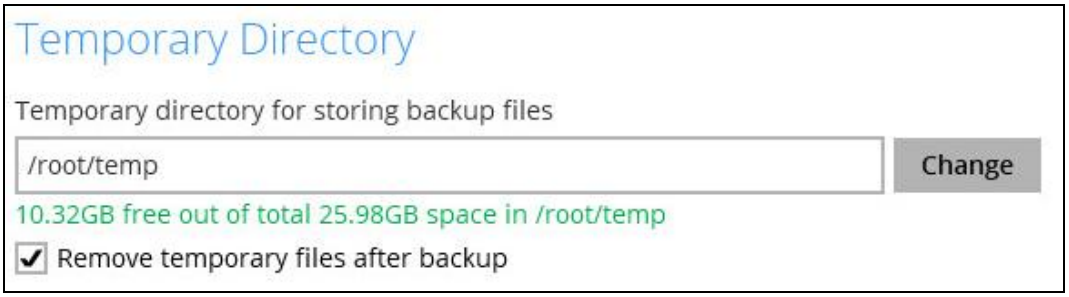
- Full and Incremental/Differential delta files retrieved from the backup destination.
- Merging of the Full and Incremental/Differential delta files as part of the restore process.

NOTES

1. For best practice, the temporary directory should be located on:
   - A local drive for optimal backup and restore performance. And 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.
2. It is recommended to select the 'Remove temporary files after backup' option on the backup set to keep the temporary drive clear.

To change the temporary directory, follow the steps below:

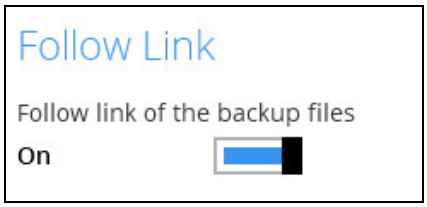
1. Click the **Change** button to select a directory path for storing temporary data.



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

Follow Link

This feature allows the user to enable or disable the follow link which defines the NFTS junction or Linux symbolic link during backup. This option is enabled by default.



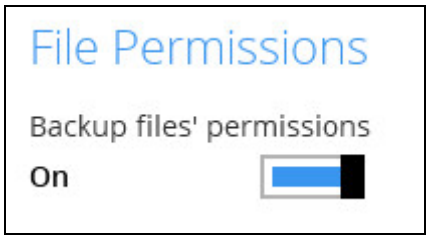
1. Slide the lever to the right to turn on the Follow Link option. Otherwise, slide to the left to turn it off.

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

NOTE
Applicable for File Backup Sets only.

File Permissions

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



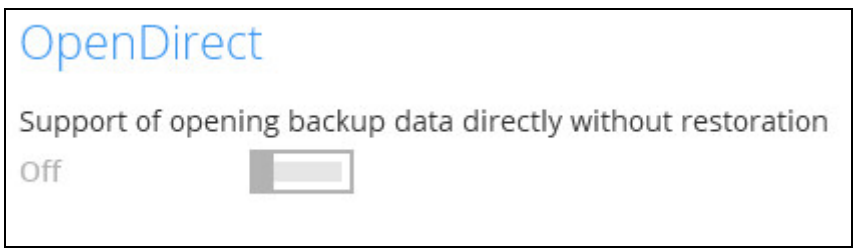
1. Slide the lever to the right to turn on the File Permissions option. Otherwise, slide to the left to turn it off.

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

NOTE
Applicable for File Backup Sets only

OpenDirect

This option is not supported in any Linux platform.



Compressions

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

There are four (4) different data compression types:

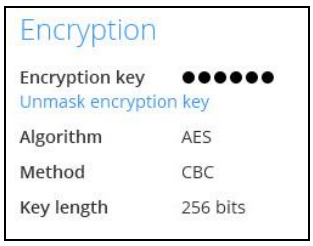
- No Compression
- Normal
- Fast (Compressed size larger than normal)
- Fast with optimization for local

NOTE

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

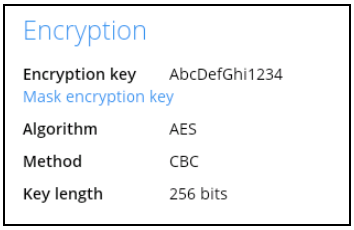
Encryption

This 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.

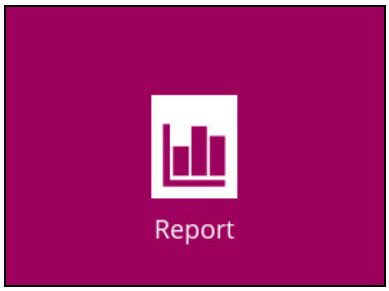


NOTE

For more details about encryption settings, please refer to step no. **13** in Chapter 10 Create a Backup Set.

9.6 Report

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



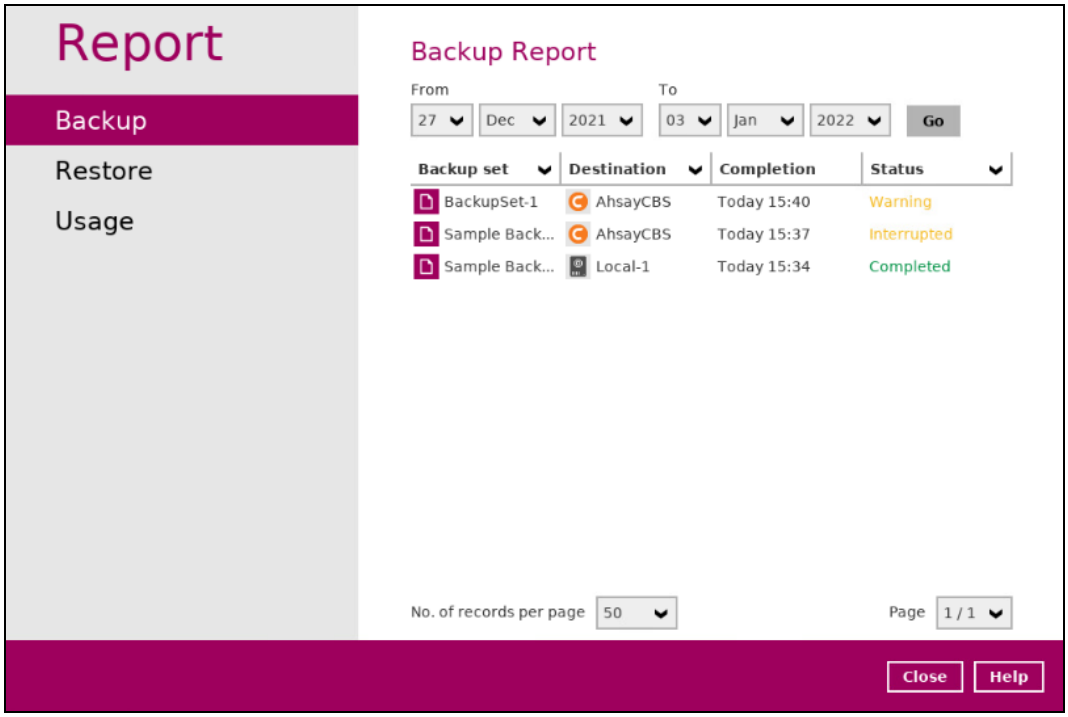
There are three (3) functions available for this feature:

- Backup
- Restore
- Usage

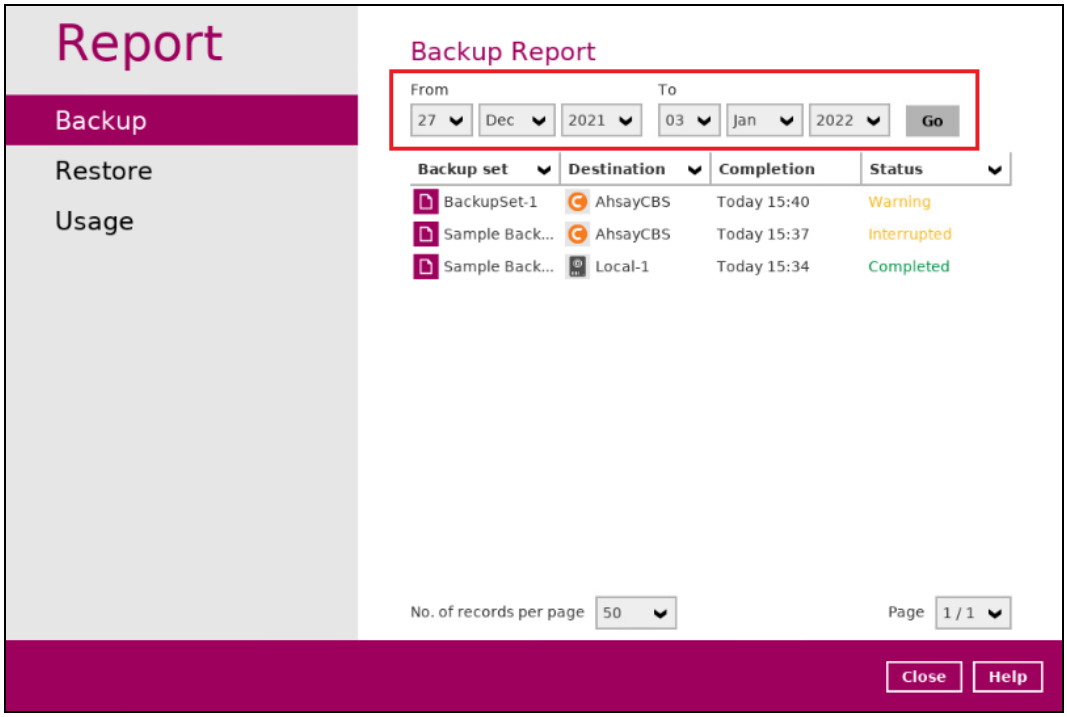
9.6.1 Backup

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

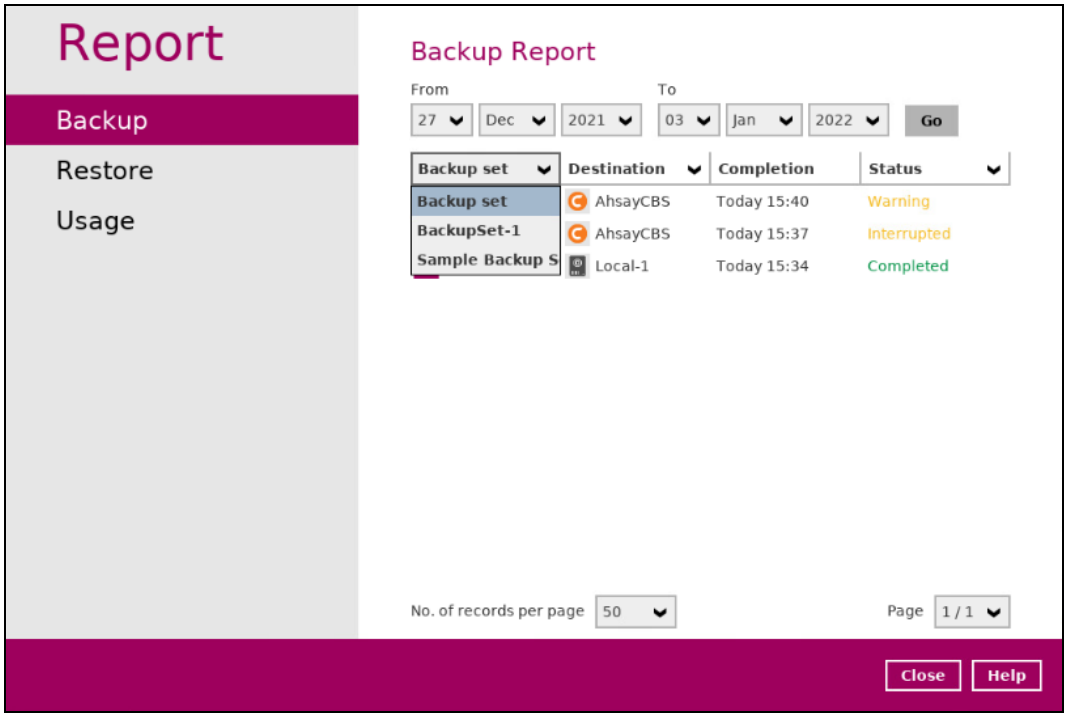
- Date
- Backup Set
- Destination
- Status



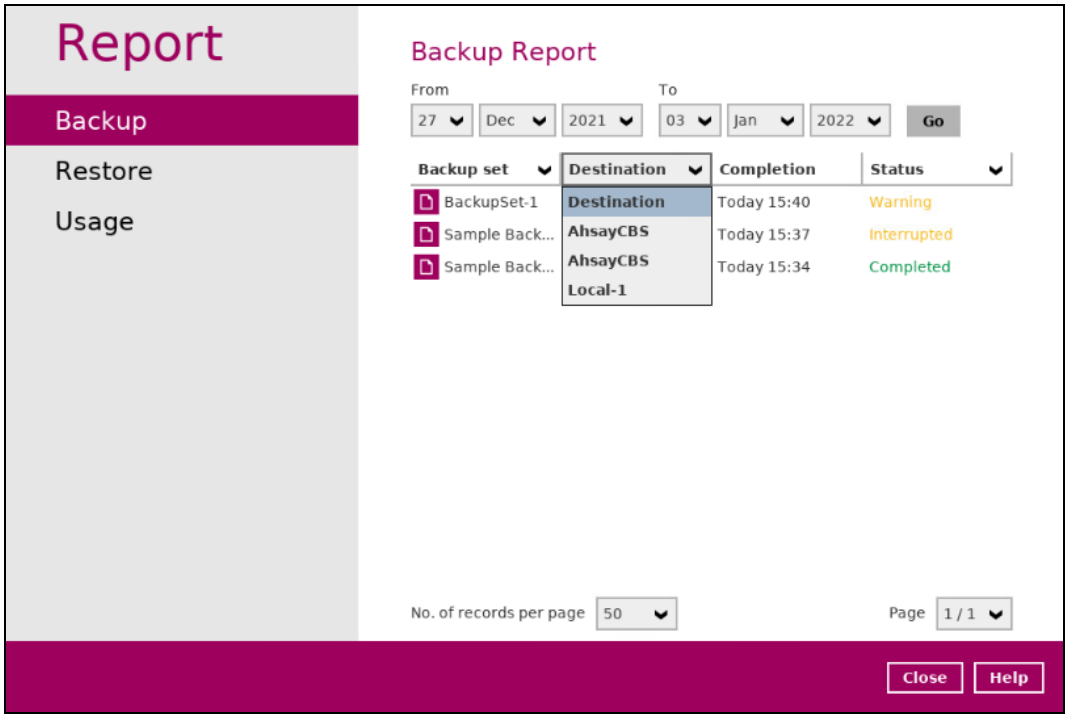
You can filter and view and backup report using the Date filter.



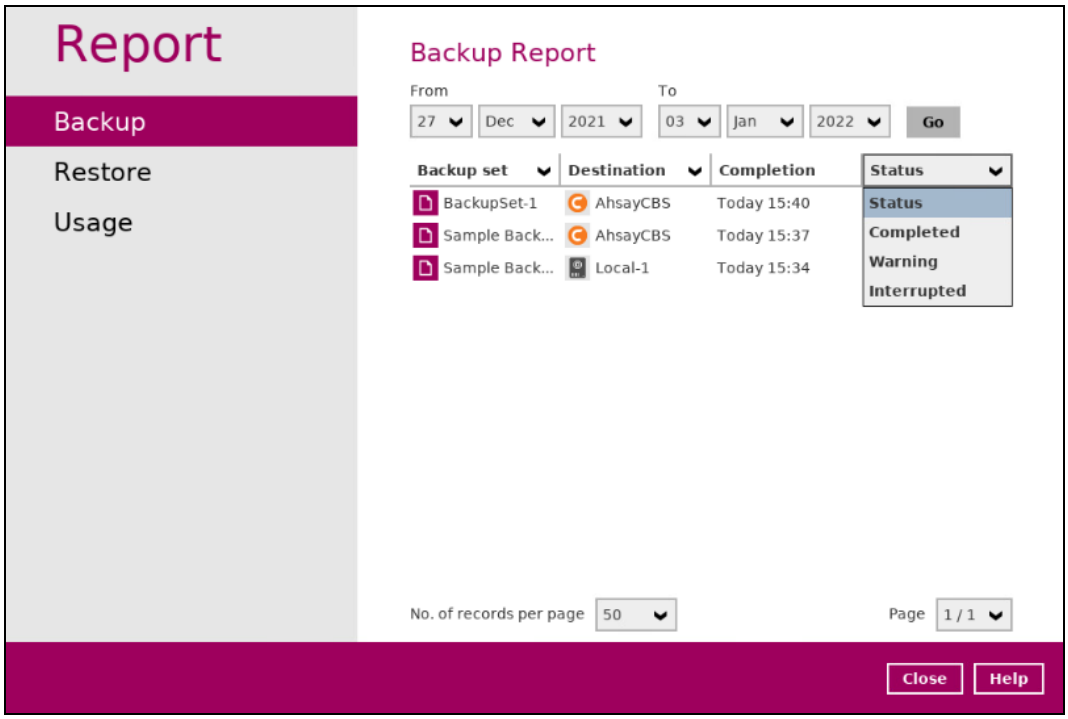
You can filter and view and backup report using the Backup set filter.



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

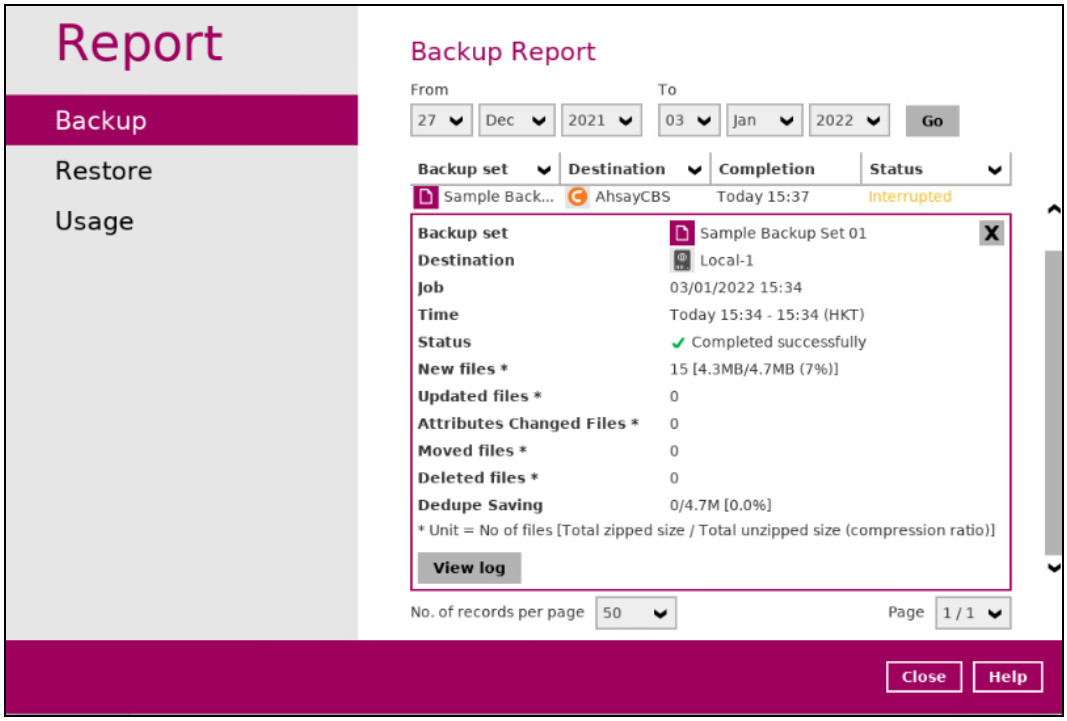


You can filter and view the backup report with the same status using the Status filter.



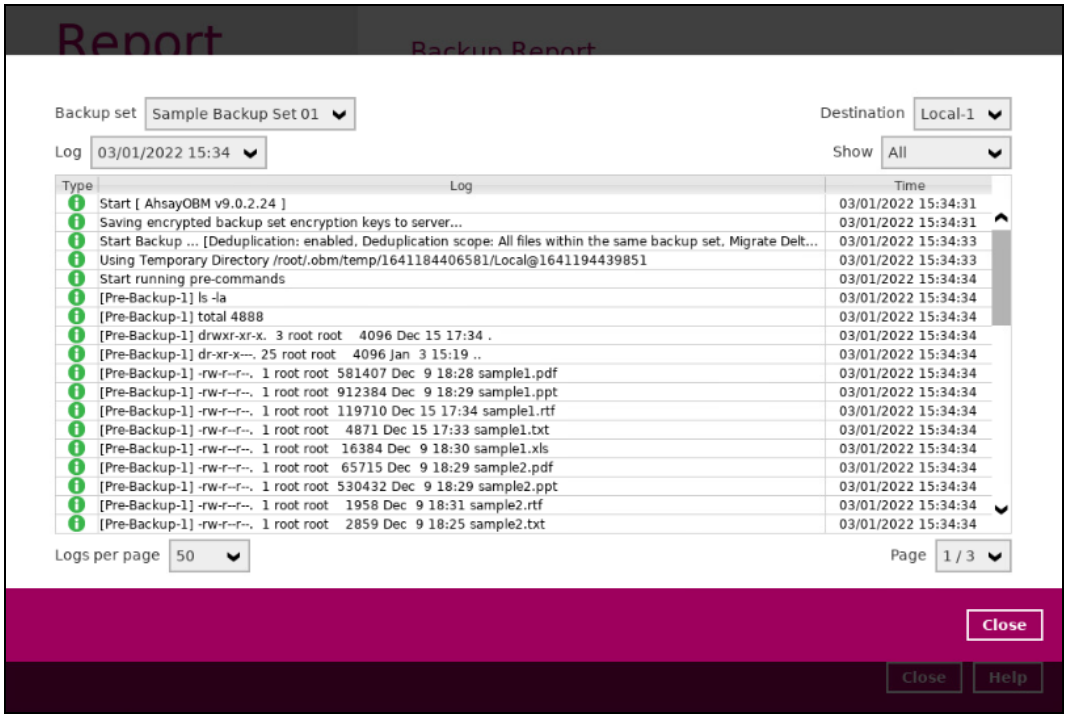
To view the backup log, follow the instructions below:

1. Select and click the backup report.



2. Click the **View log** button.

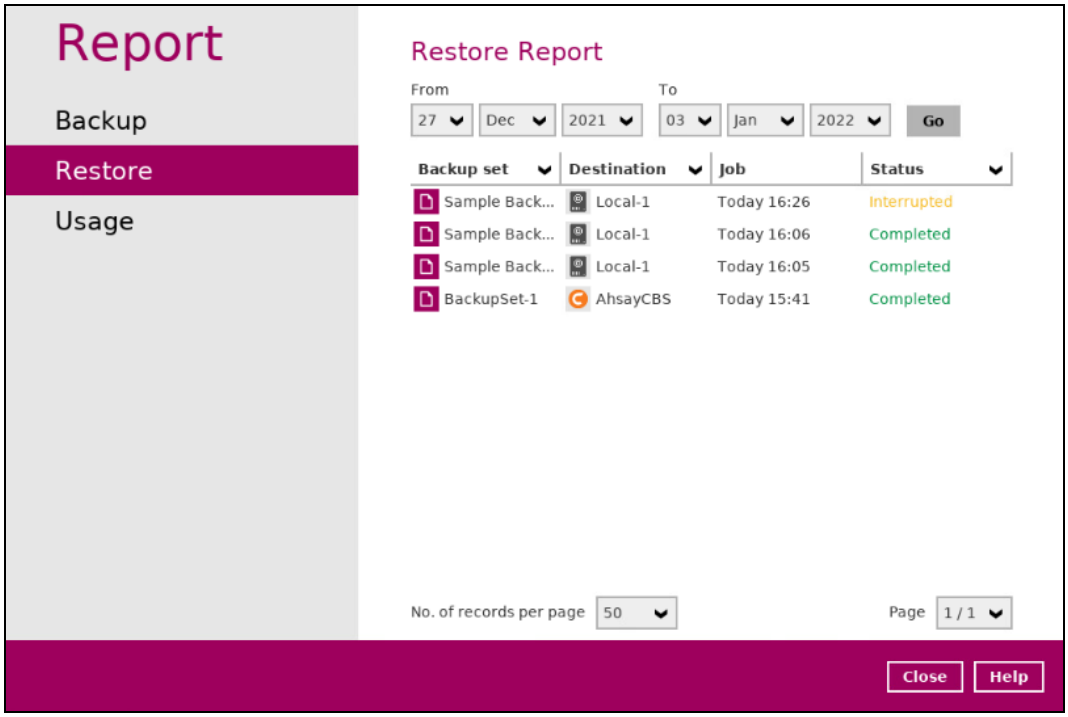
   Backup set, Destination, Log Date and Time, and Status can also be filtered as well as the number of logs per page.



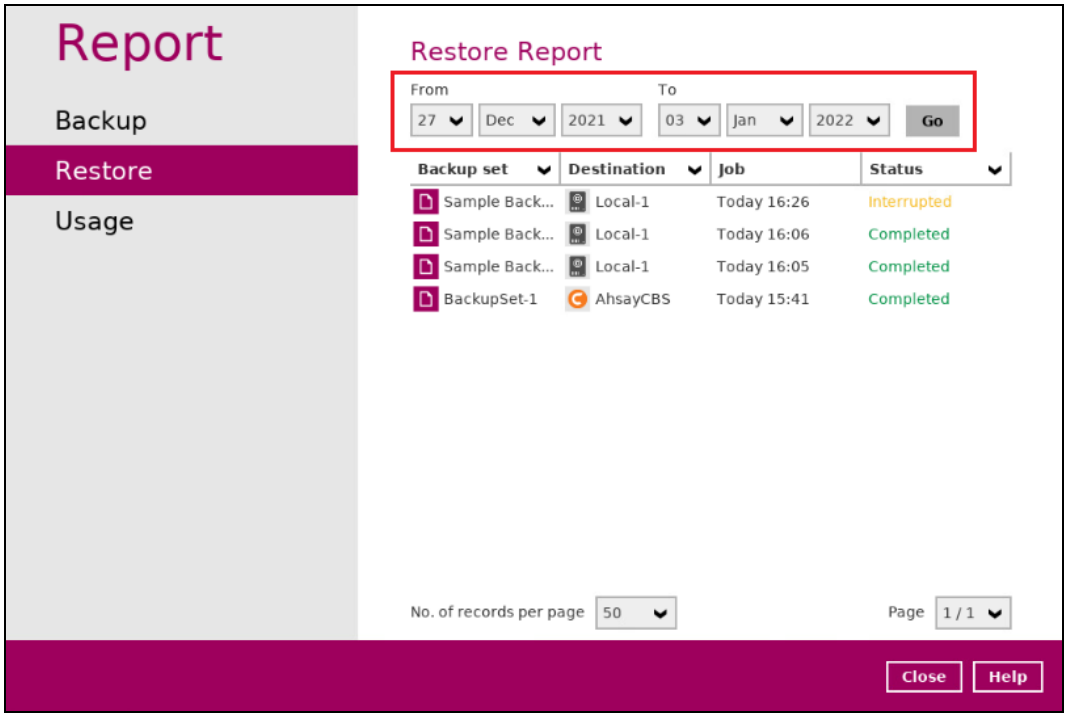
9.6.2 Restore

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

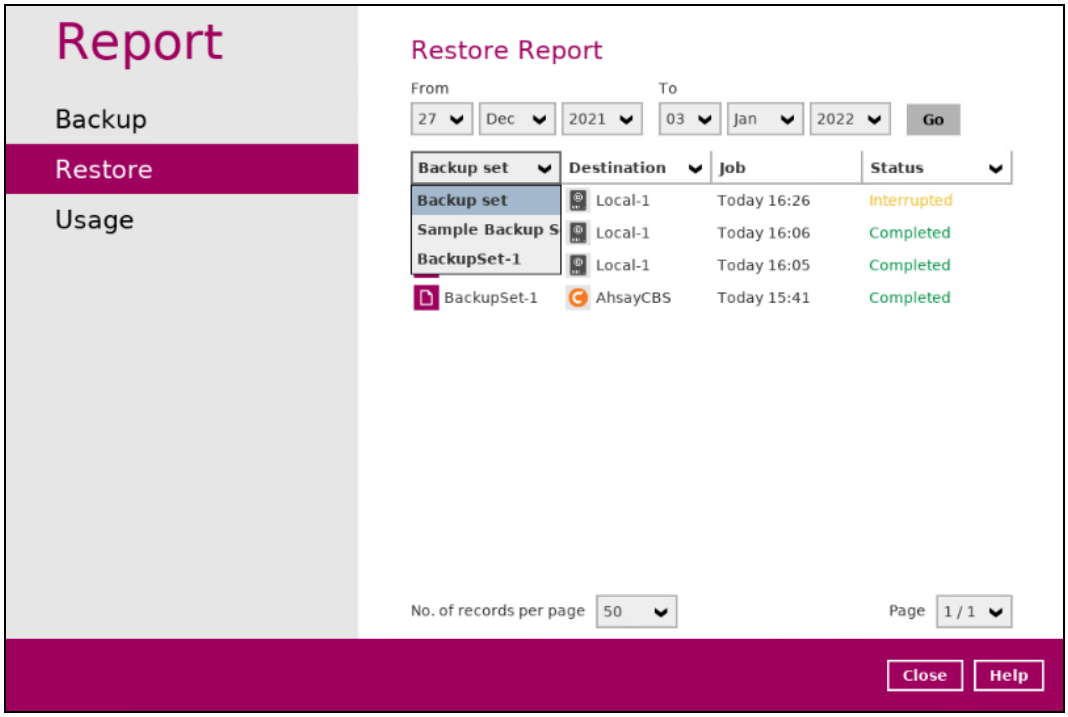
- Date
- Backup Set
- Destination
- Status



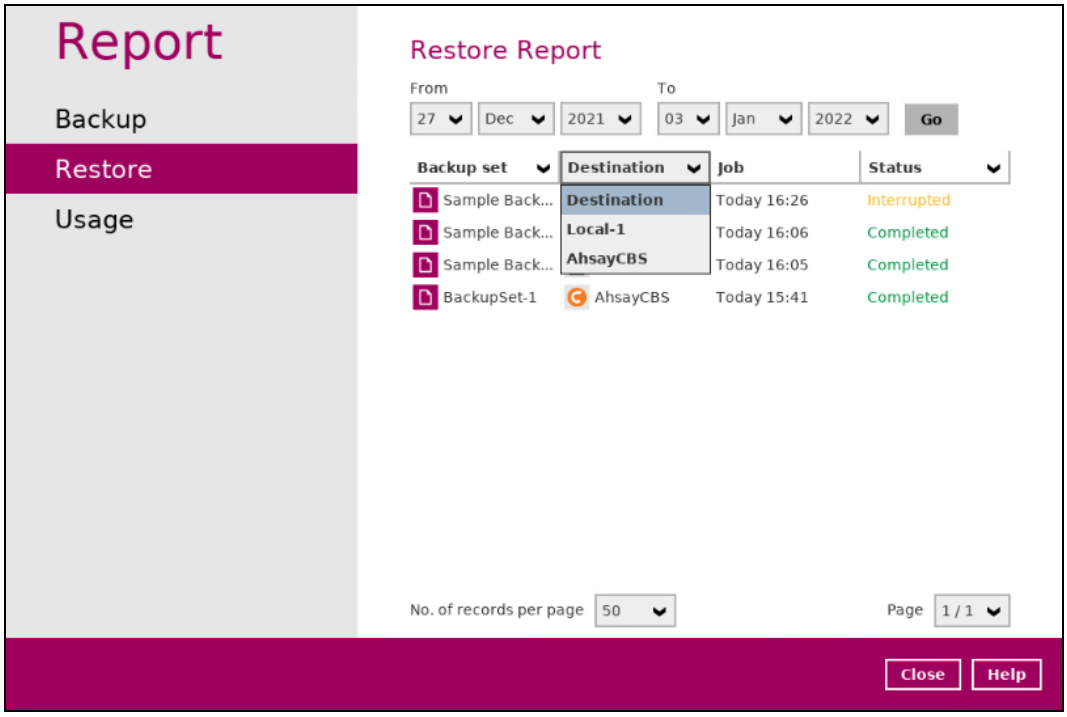
You can filter and view and restore report using the Date filter.



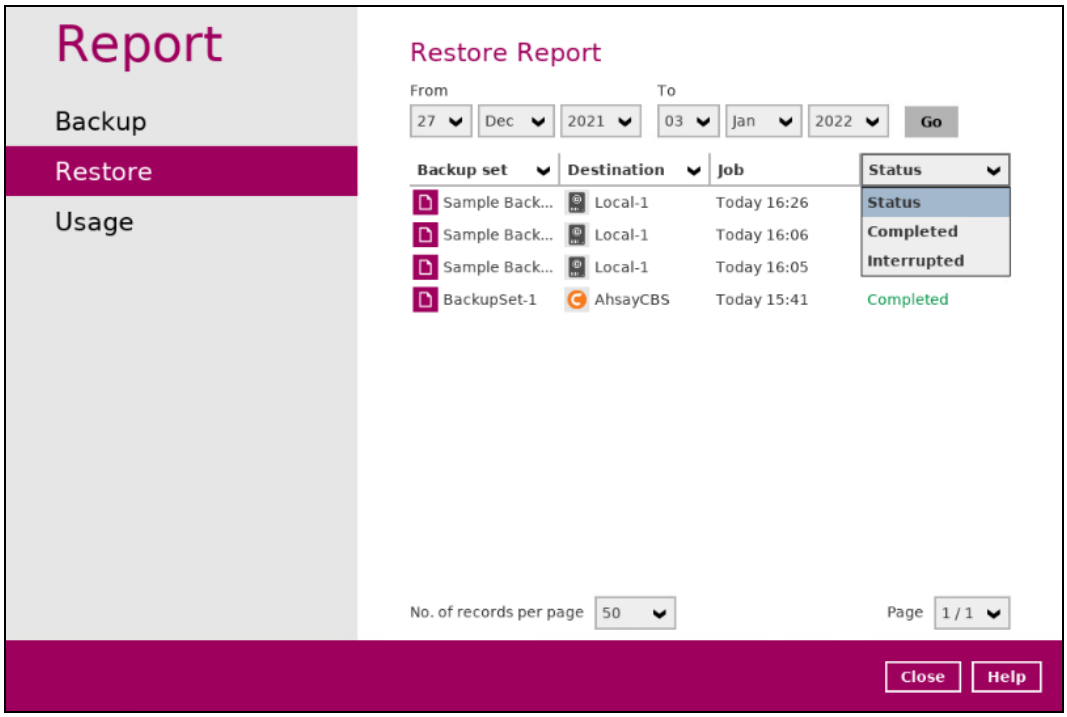
You can filter and view and restore report using the Backup set filter.



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

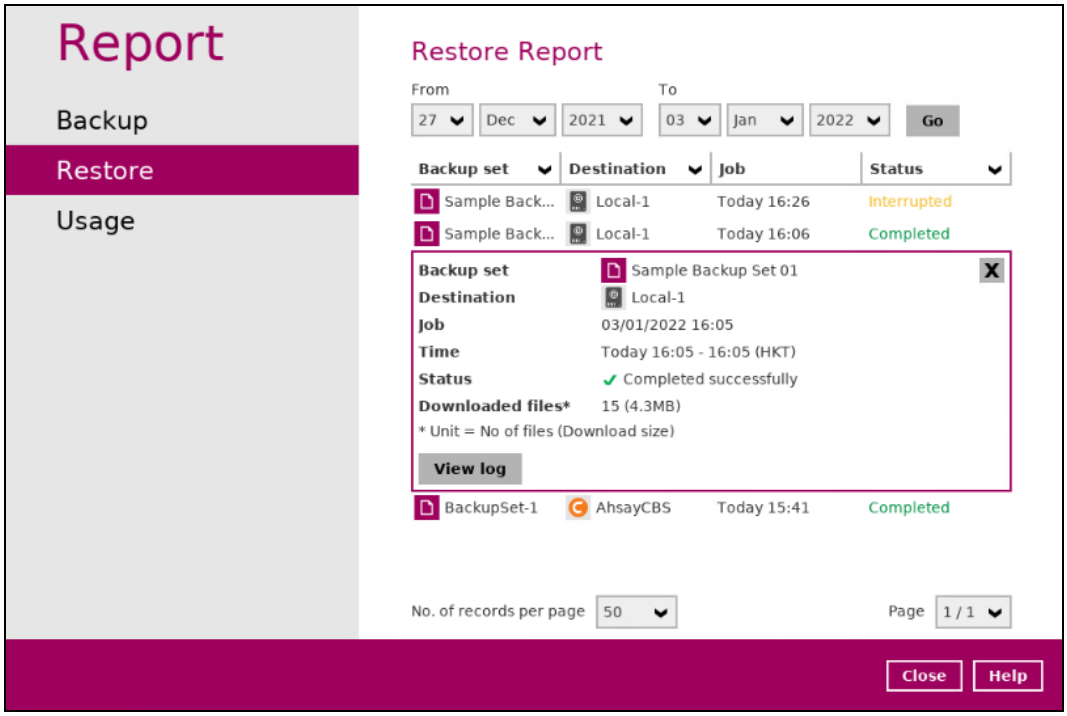


You can filter and view the restore report with the same status using the Status filter.



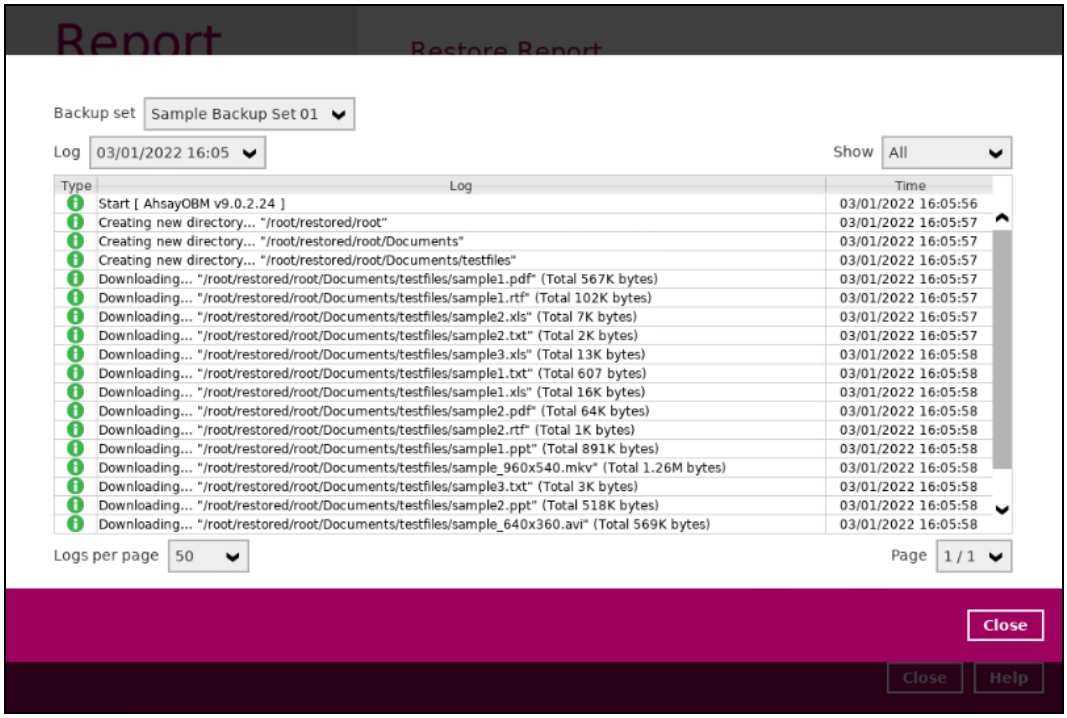
To view the restore log, follow the instructions below:

1. Select and click the restore report.



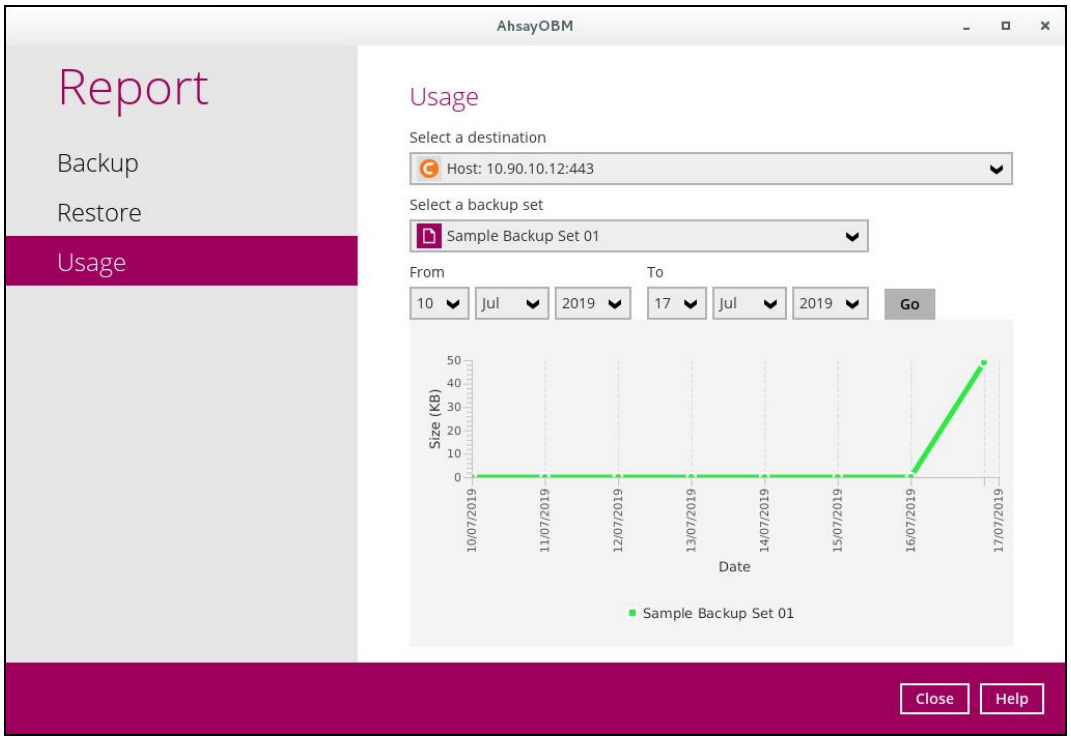
2. Click the **View log** button.

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



9.6.3 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

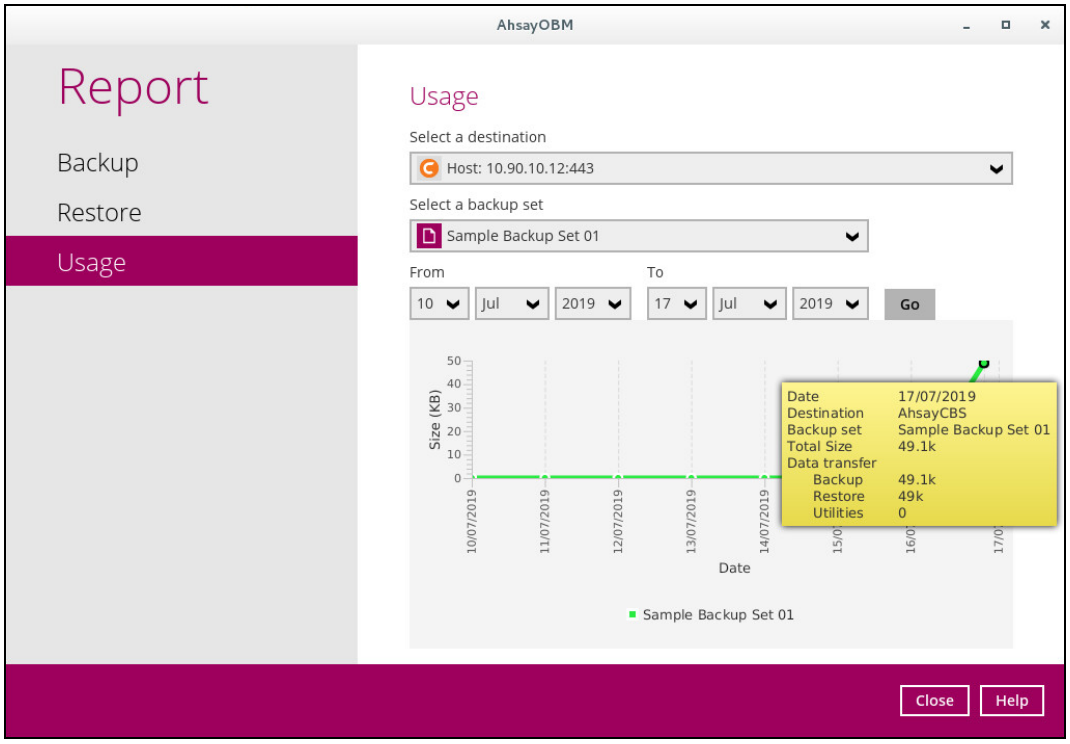
  Total Size: displays the total amount of backed up data on the backup destination

  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

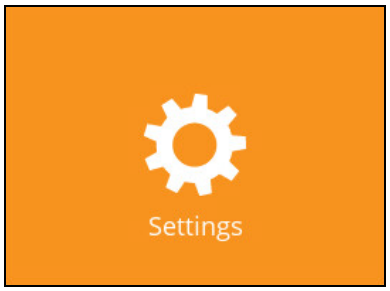
9.7 Restore

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

To restore backed-up files, follow the instructions on Chapter 11: Restoring Data.

9.8 Settings

This allows the User to enable the Proxy Settings.



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

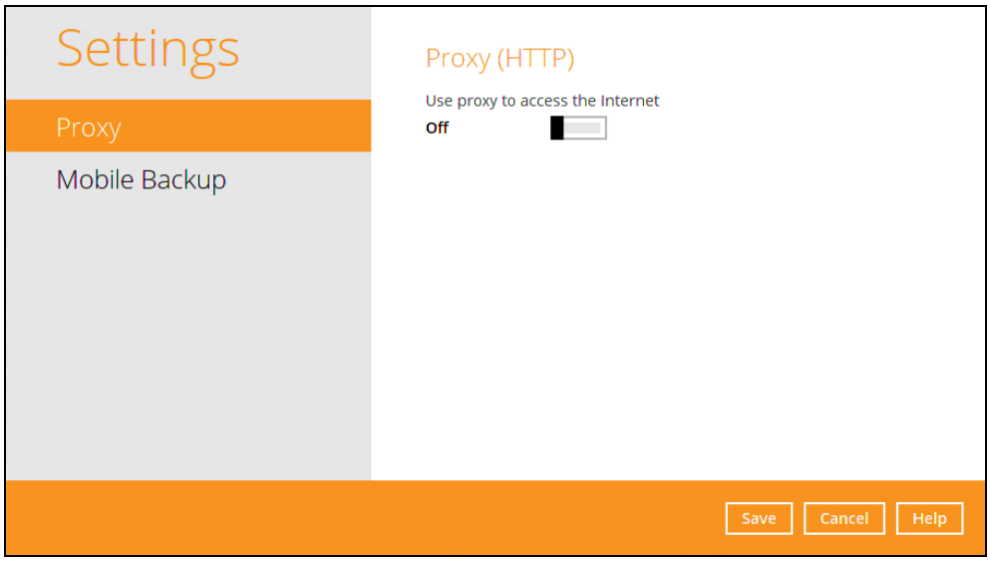
- Proxy
- Mobile Backup

9.8.1 Proxy

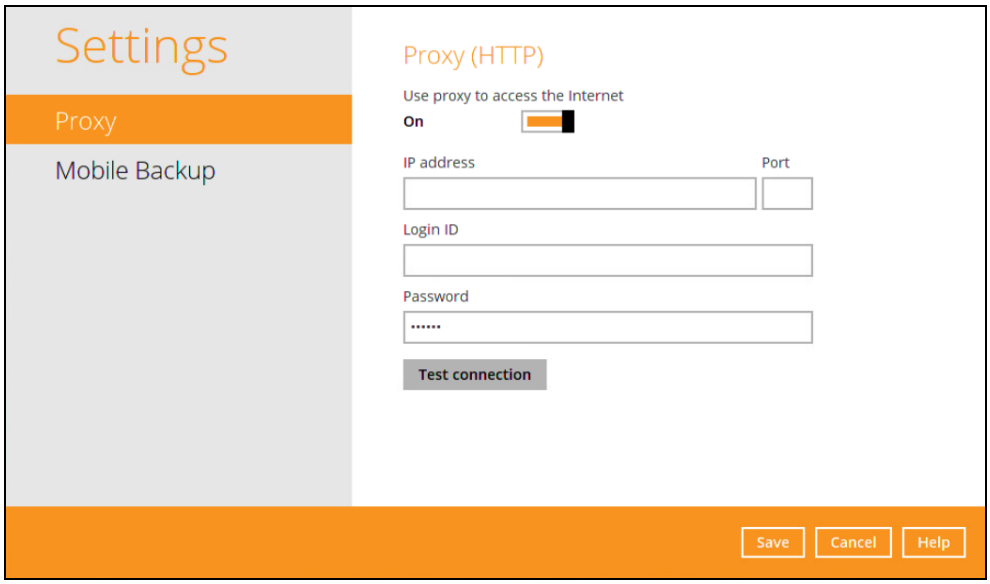
When this feature is on, AhsayOBM will use a proxy to gain access to the internet.

To enable the Proxy Settings, follow the instructions below:

1. Slide the lever on the right to enable the Proxy Settings.



2. Complete the following fields:
    - IP Address
    - Port
    - Login ID
    - Password



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.

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

9.8.2 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

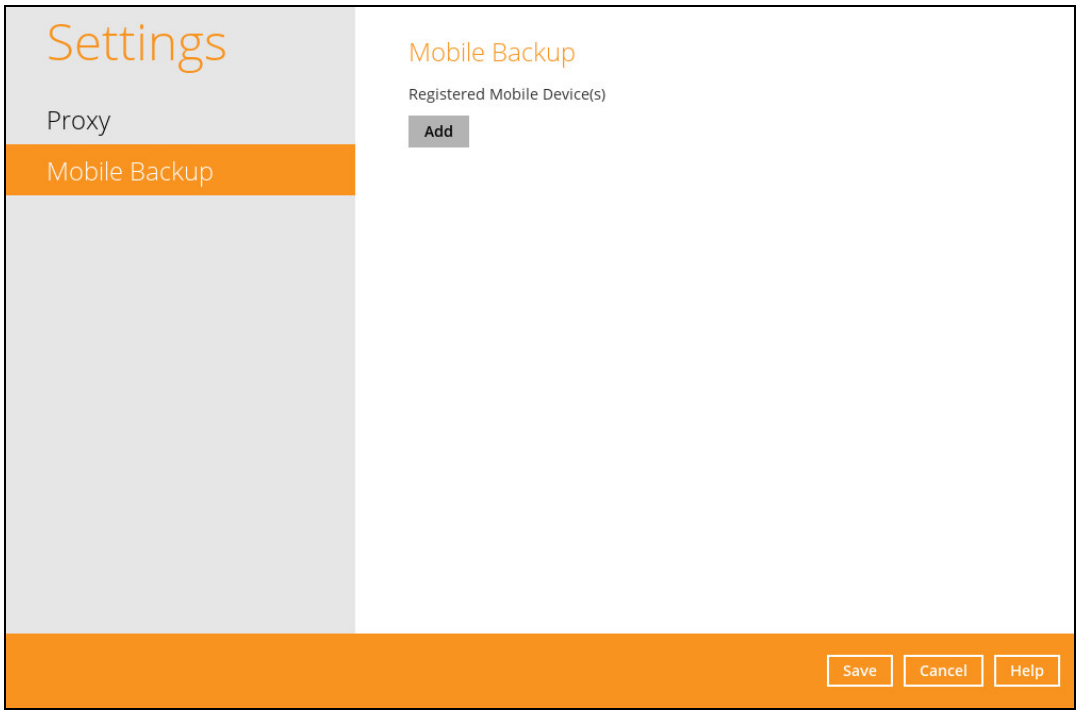
  Please refer to the Ahsay Mobile User Guide for Android and iOS – Chapter 7 for the detailed step-by-step procedure.

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

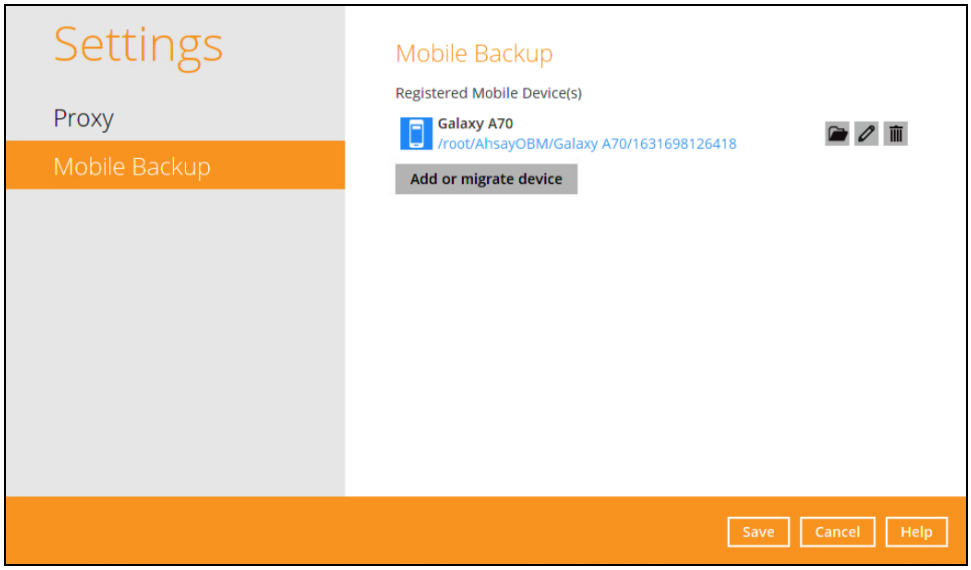
- Restore to a different mobile device on the same operating system.
- Restore to a different mobile device on another operating system, i.e., Android to iOS or iOS to Android.



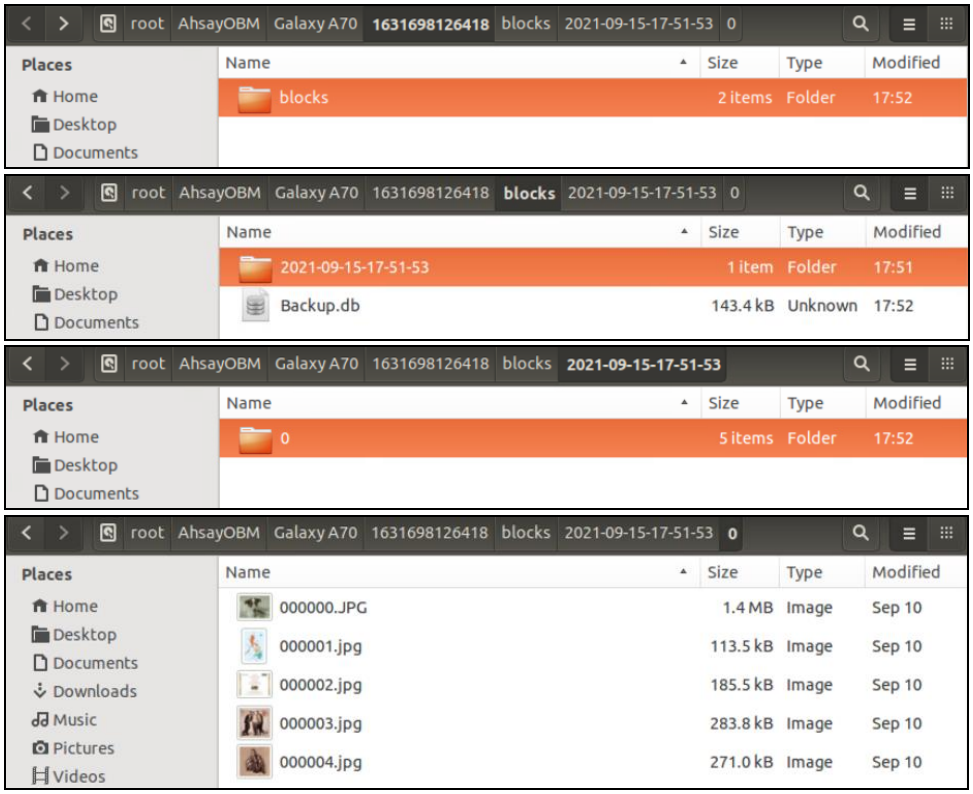
View backed up photos, videos and documents saved in the mobile backup destination

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

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



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



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

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

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

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

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

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

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

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

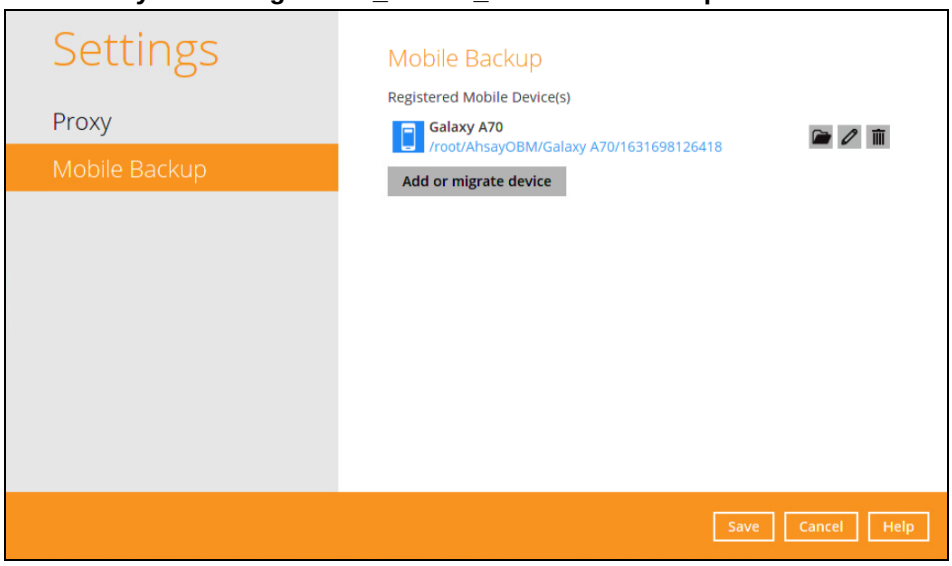
In case the previously backed-up photos, videos, documents and 2FA accounts were not copied to the new location, the backup will re-upload all the photos, videos, documents and 2FA accounts again from the mobile device.

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

Example: Change backup destination from **/root/AhsayOBM/%registered_mobile_device%/%backupsetID%** to **/root/MobileBackup**

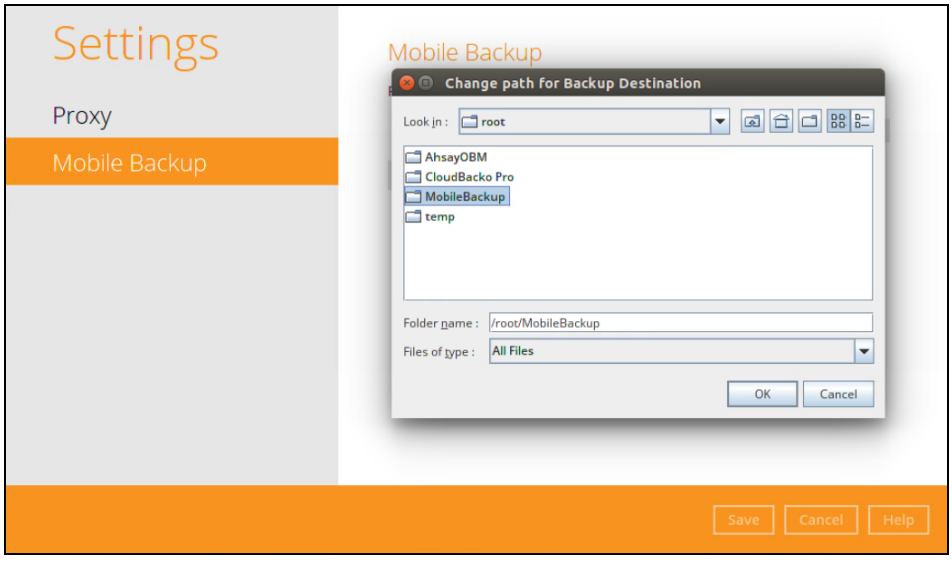
1. From the old location, secure a copy of the previously backed-up photos, videos and 2FA accounts.
2. Copy the previously backed-up photos, videos, documents and 2FA accounts from the original location to the new mobile backup destination (if applicable).
3. Go to **Settings** > **Mobile Backup**.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

   In this example, the old mobile backup destination is **/root/AhsayOBM/%registered_mobile_device%/%backupsetID%**.



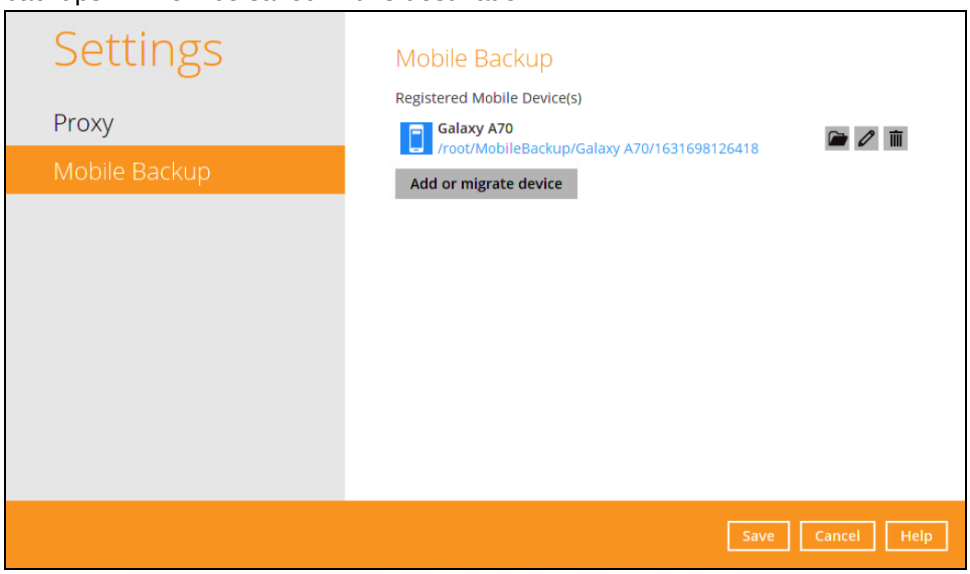
4. **Change path for Backup Destination** screen will be displayed. Select a new mobile backup destination then click **OK**.

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



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

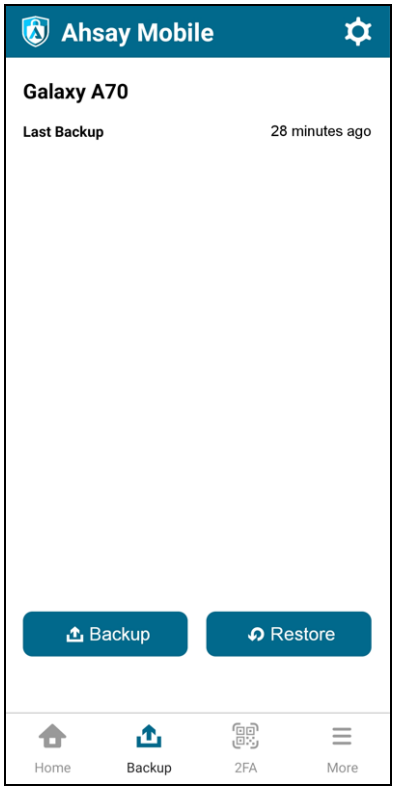
   Mobile backup destination is successfully changed to **/root/MobileBackup**. All mobile backups will now be saved in this destination.



NOTE

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

6. Resume backup of photos, videos and 2FA accounts.



Change mobile backup destination location to new machine

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

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

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

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

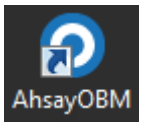
NOTE

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

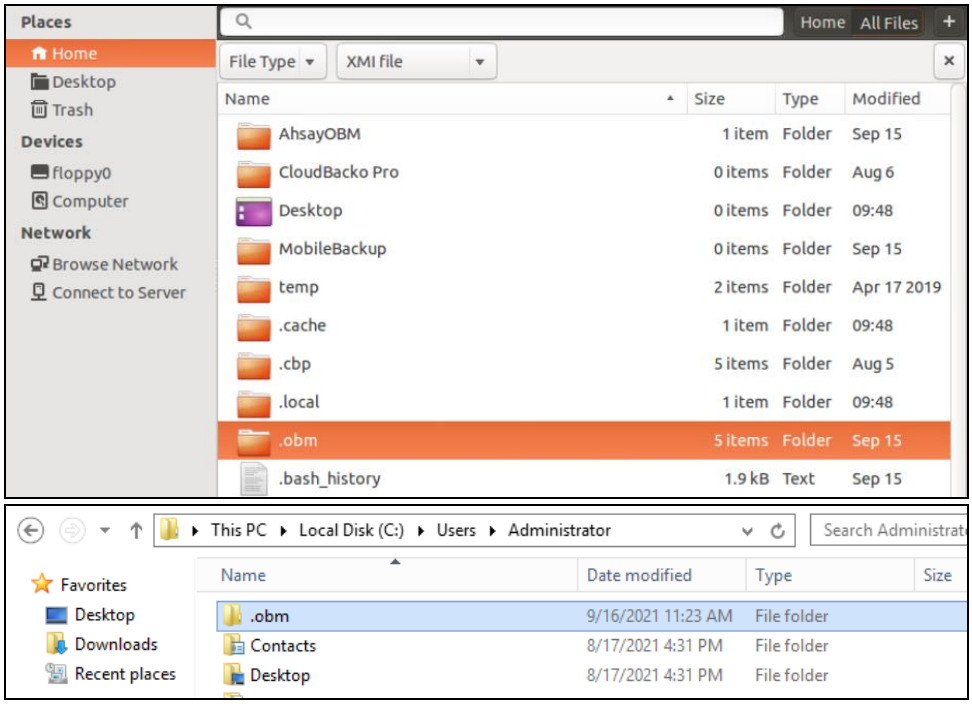
To change the mobile backup destination to a new machine, follow the instructions below:

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

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



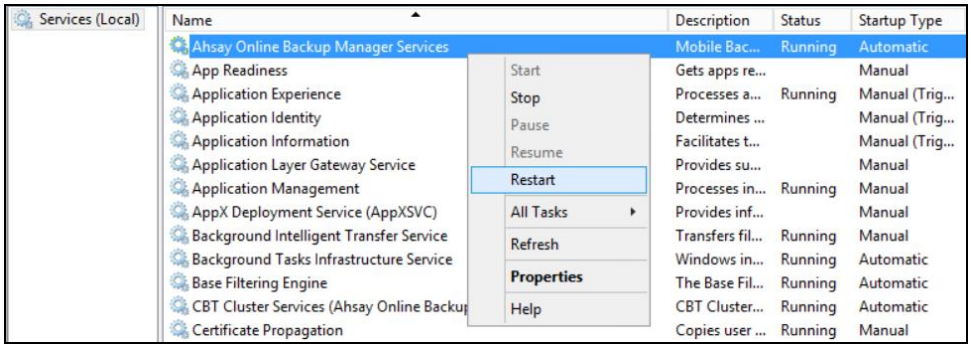
2. Copy the **.obm** folder from the old Linux machine to the new Windows machine.



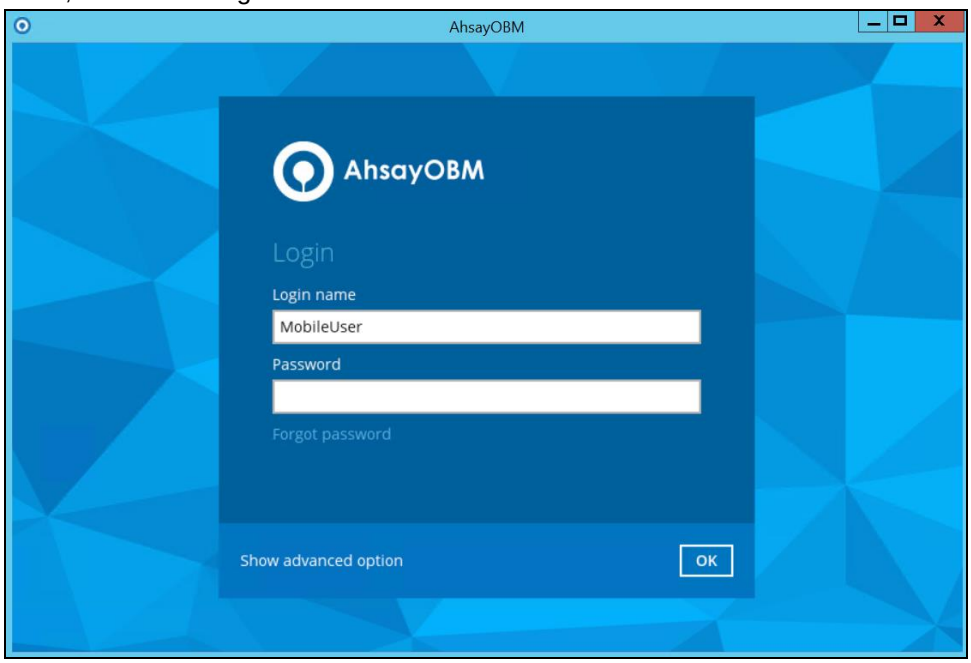
3. Copy the previously backed-up photos, videos, documents and 2FA accounts from the original location to the new mobile backup destination.

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

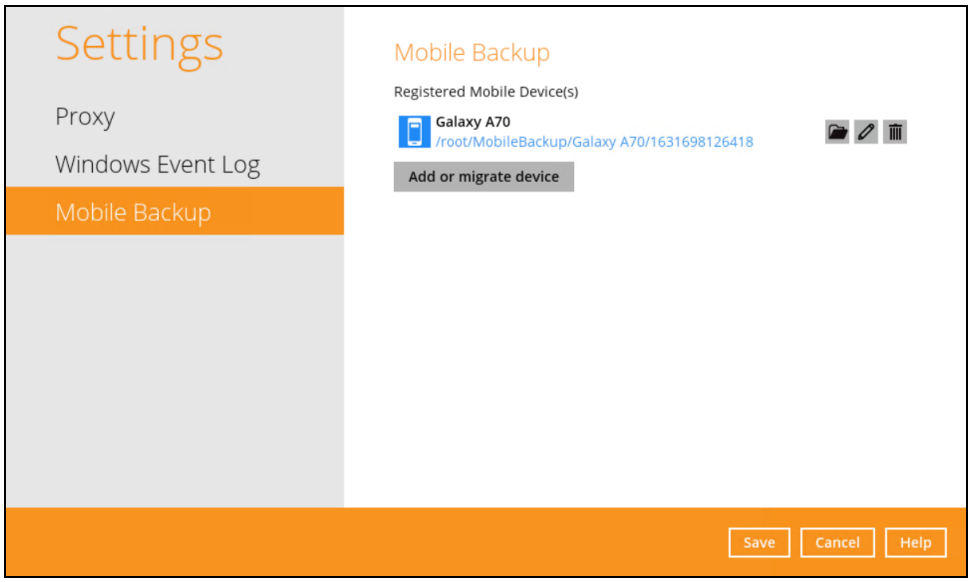
4. Restart the **AhsayOBM Services** because copying the **.obm** folder on a newly installed AhsayOBM will not trigger the MBS.



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

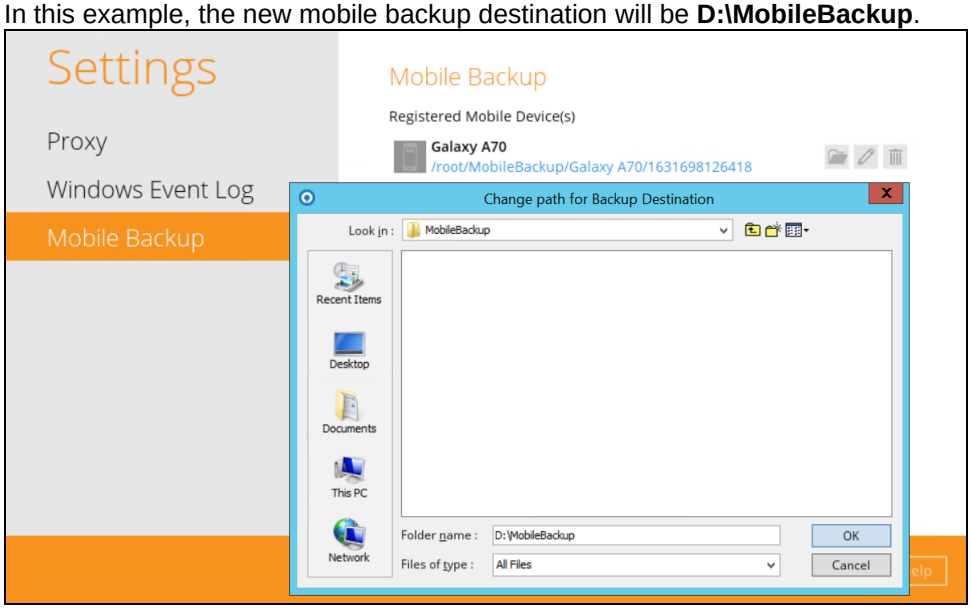


6. Go to **Settings** > **Mobile Backup**. Click the **Edit** icon on the right side of the registered mobile device.



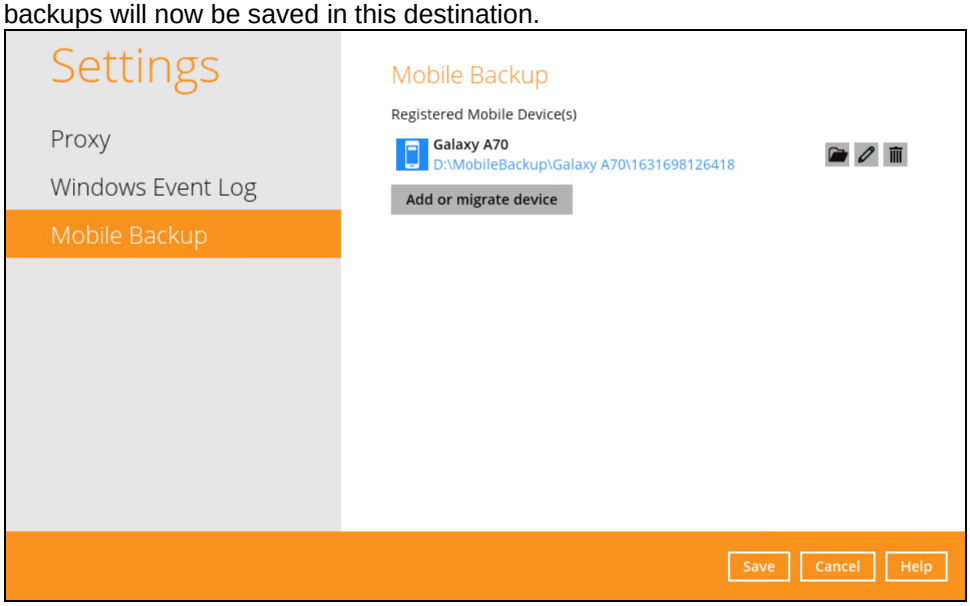
7. **Change path for Backup Destination** screen will be displayed, select the new mobile backup destination then click **OK**.

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



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

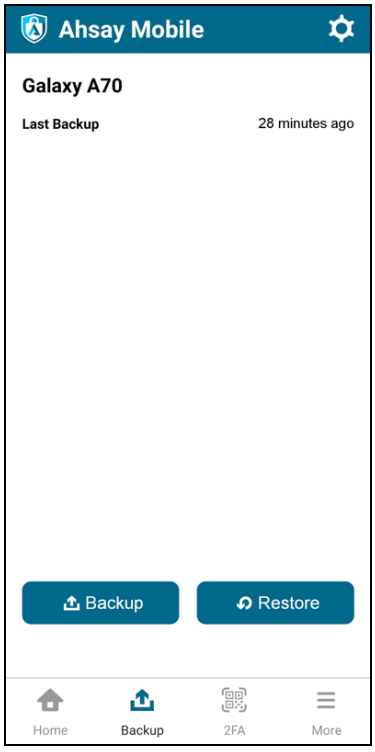
Mobile backup destination is successfully changed to **D:\MobileBackup**. All mobile backups will now be saved in this destination.



NOTE

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

9. Resume backup of photos, videos and 2FA accounts.



NOTE

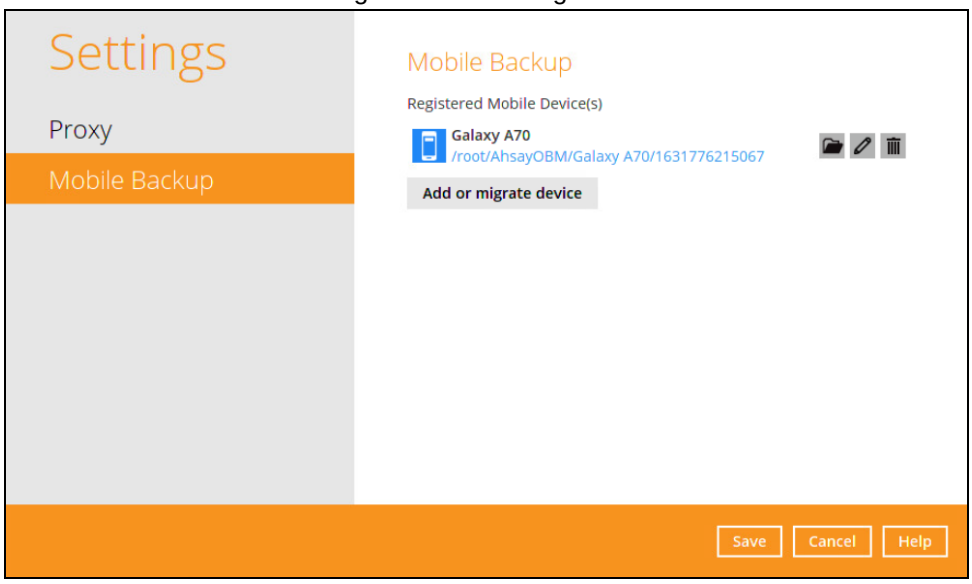
For instructions on changing the mobile backup destination of:

- a macOS machine to a Windows machine please refer to Ch.9.8.2 of the AhsayOBM v9 Quick Start Guide for Mac.
- a Windows machine to a macOS machine please refer to Ch. 10.8.3 of the AhsayOBM v9 Quick Start Guide for Windows.

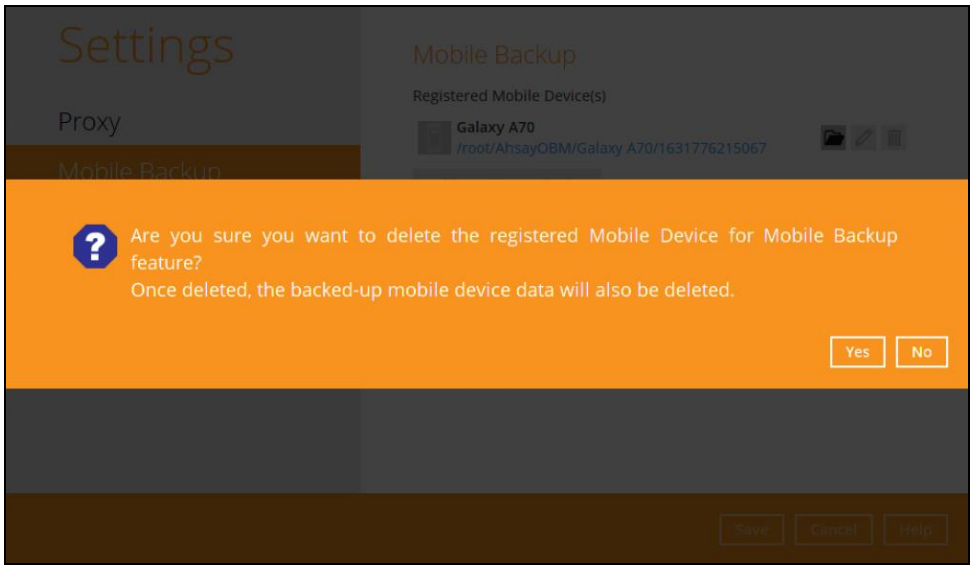
Remove one or more device(s) registered for Mobile Backup

To remove a mobile device, follow the instructions below:

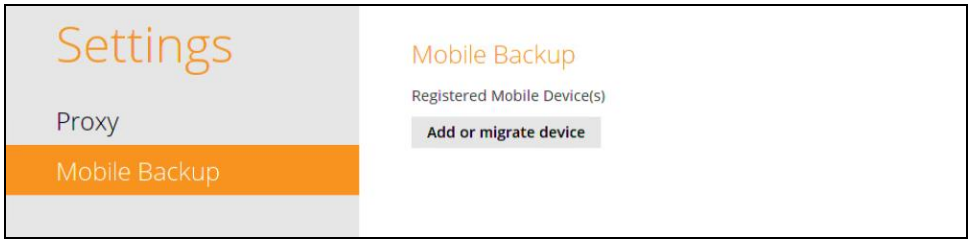
1. Click the **Delete** icon on the right side of the registered mobile device.



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

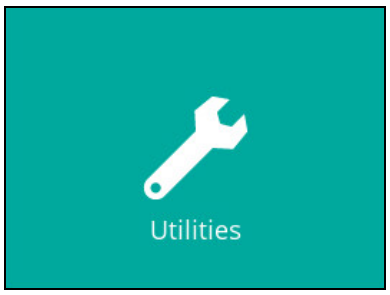


3. Mobile device is successfully removed along with any photos, videos, documents and 2FA accounts backed up in the mobile backup destination.



9.9 Utilities

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



These are the four (4) options available for this feature:

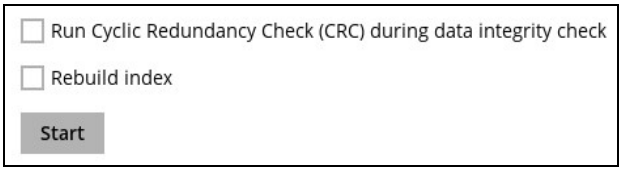
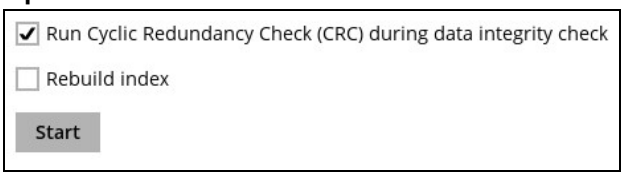
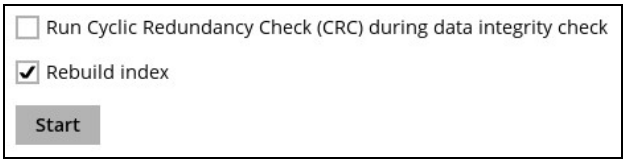
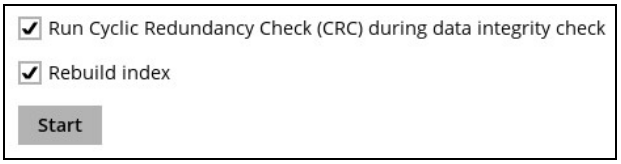
- Data Integrity Check
- Space Freeing Up
- Delete Backup Data
- Decrypt Backup Data

9.9.1 Data Integrity Check

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

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

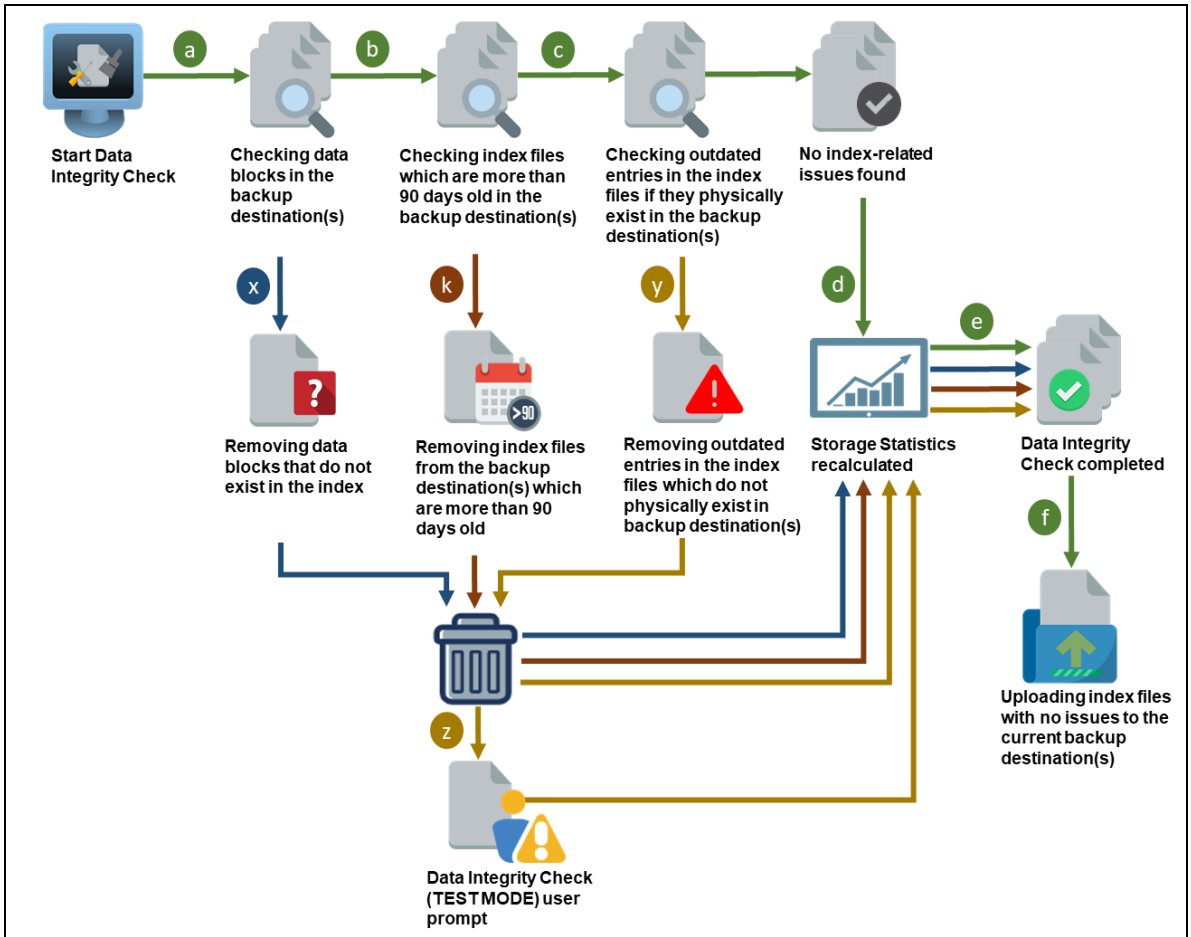
There are four (4) options in performing the Data Integrity Check:

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

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

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

Option 1 - 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).

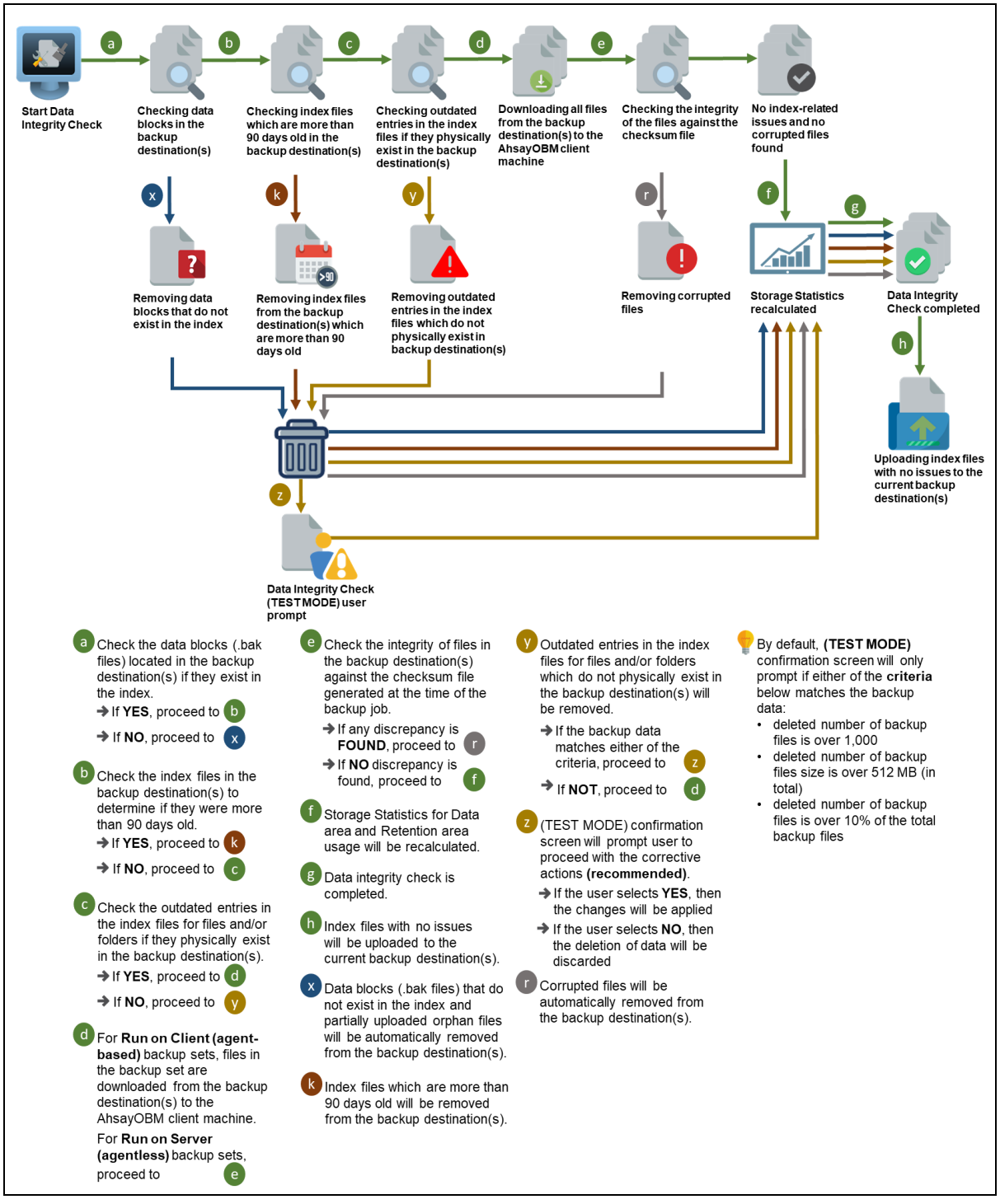
k Index files which are more than 90 days old will be removed from the backup destination(s).

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).

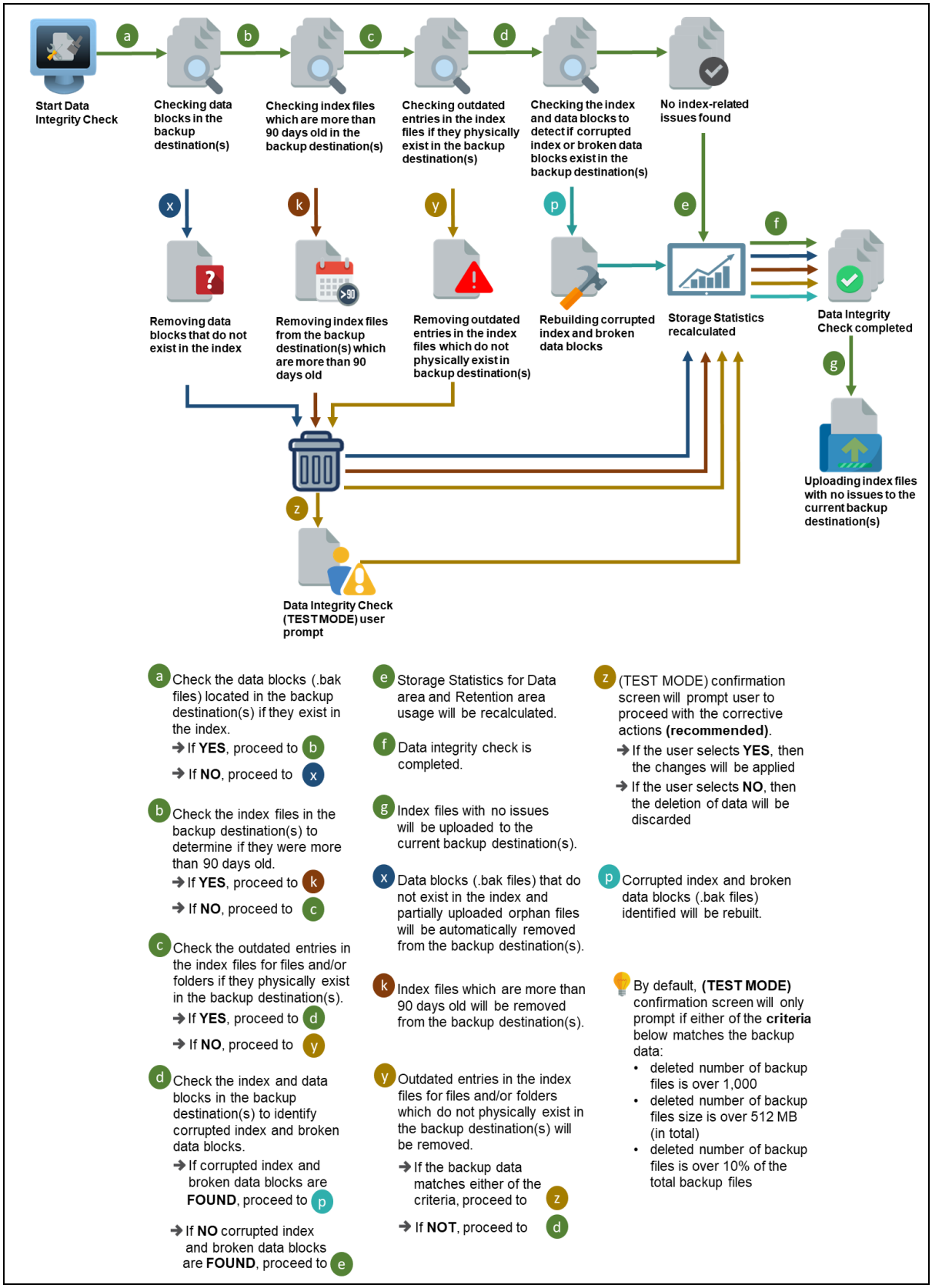
y Outdated entries in the index files for files and/or folders which do not physically exist in the backup destination(s) will be removed.
- If the backup data matches either of the criteria, proceed to z
- If **NOT**, proceed to d

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

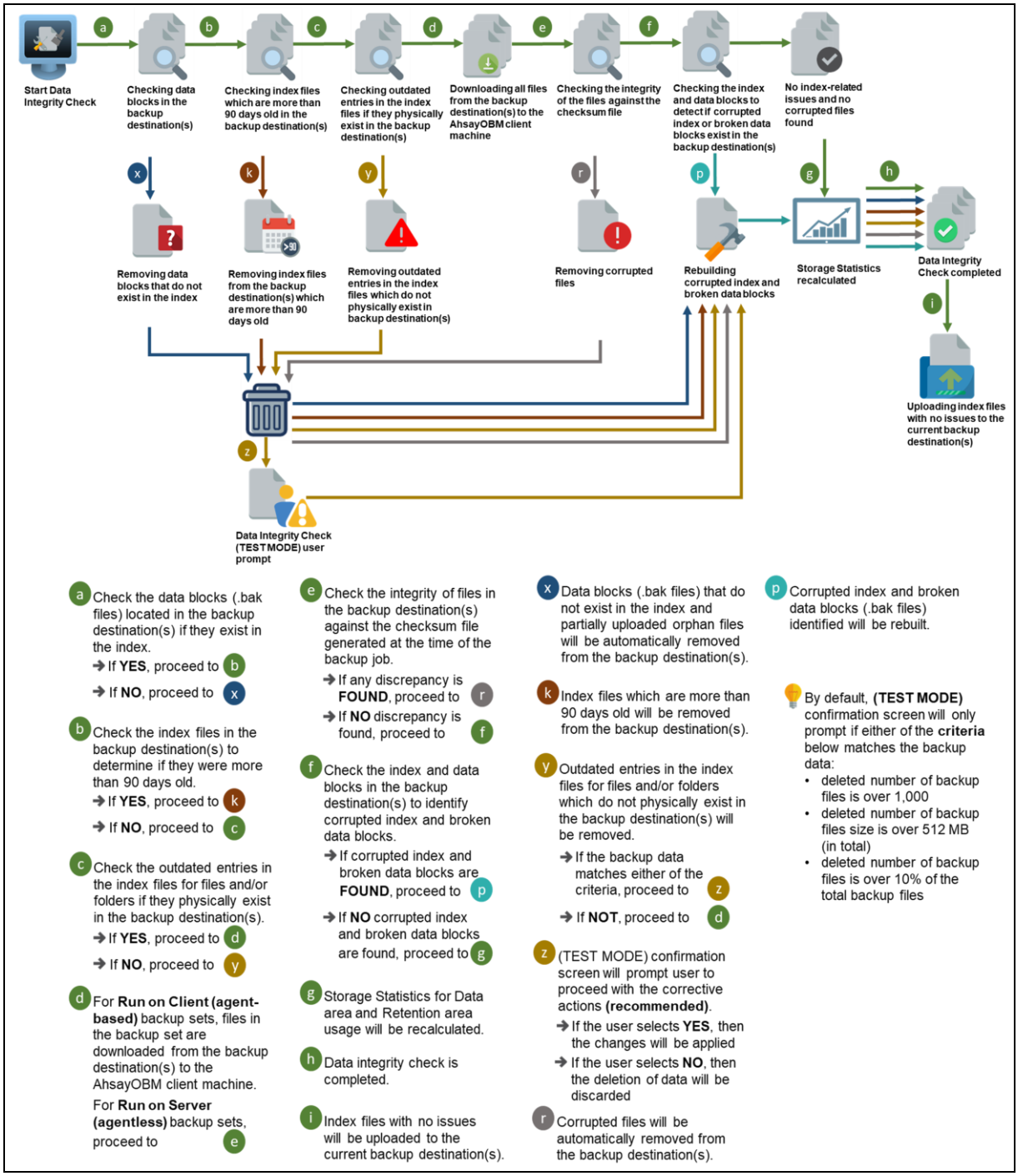
r Corrupted files will be automatically removed from the backup destination(s).

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**



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).

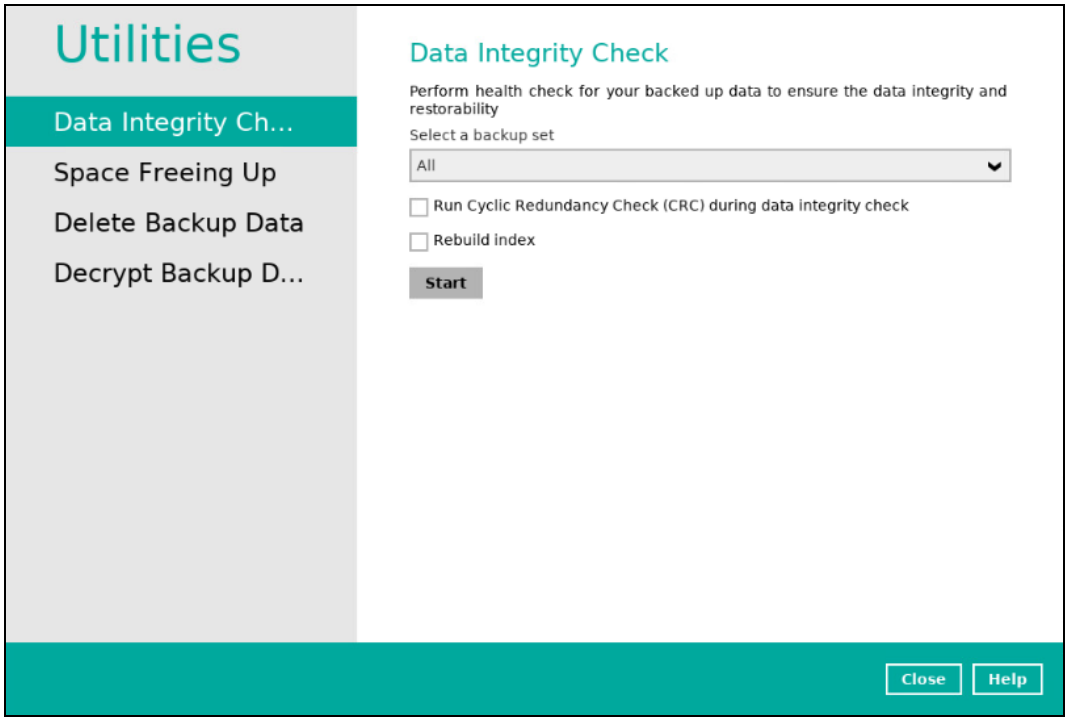
y Outdated entries in the index files for files and/or folders which do not physically exist in the backup destination(s) will be removed.
→ If the backup data matches either of the criteria, proceed to z
→ If **NOT**, proceed to d

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.

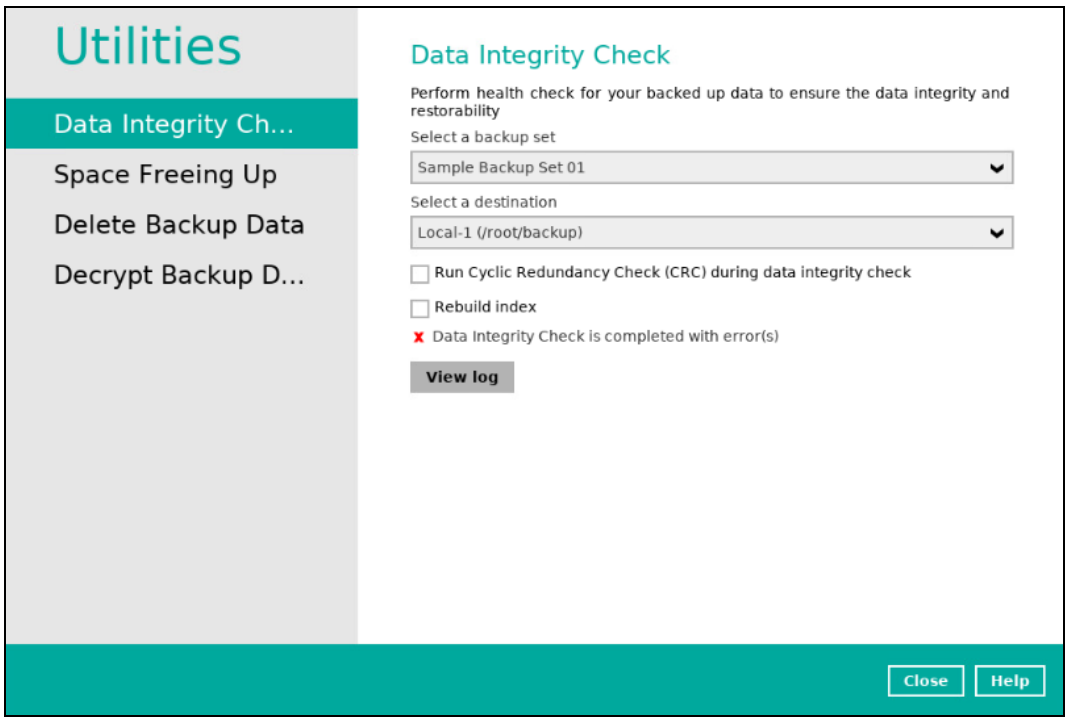
By default, **(TEST MODE)** confirmation screen will only prompt if either of the **criteria** below matches the backup data:
- deleted number of backup files is over 1,000
- deleted number of backup files size is over 512 MB (in total)
- deleted number of backup files is over 10% of the total backup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



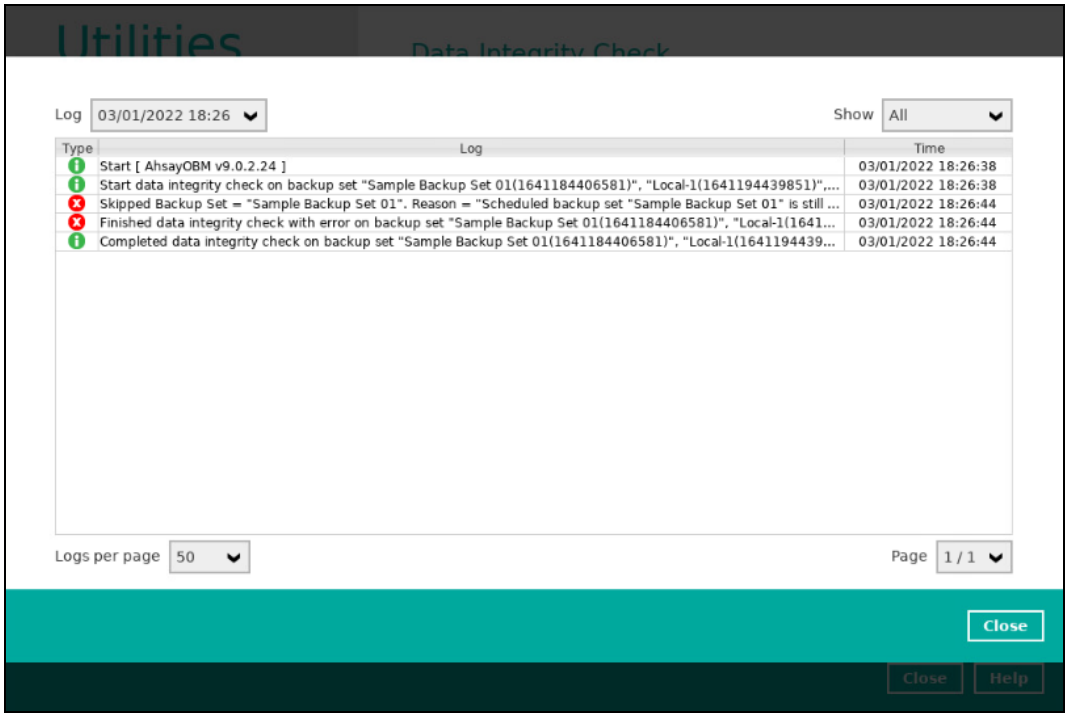
NOTES

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).

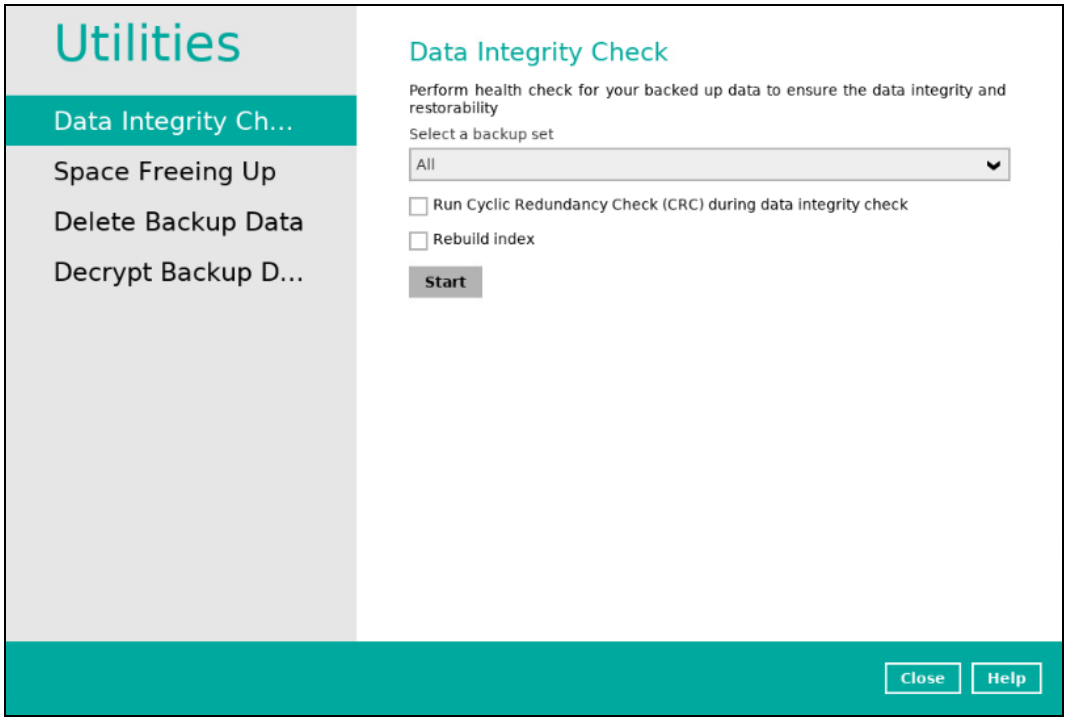


Clicking the **View log** button will display the details of the Data Integrity Check job error(s).

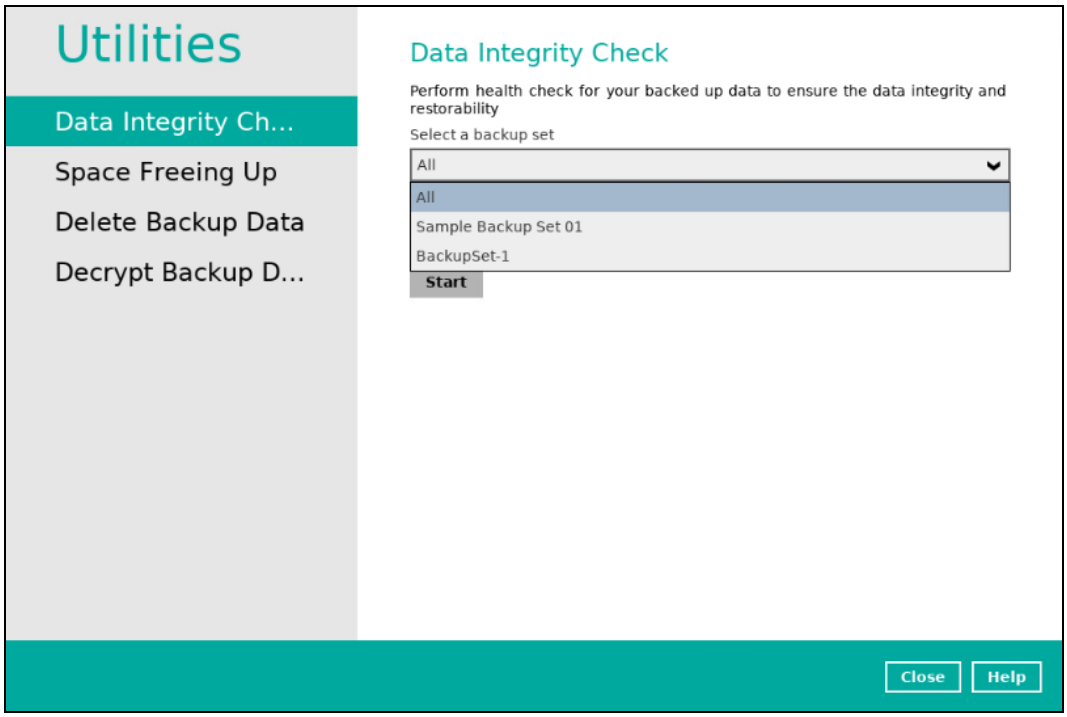


To perform a Data Integrity Check, follow the instructions below:

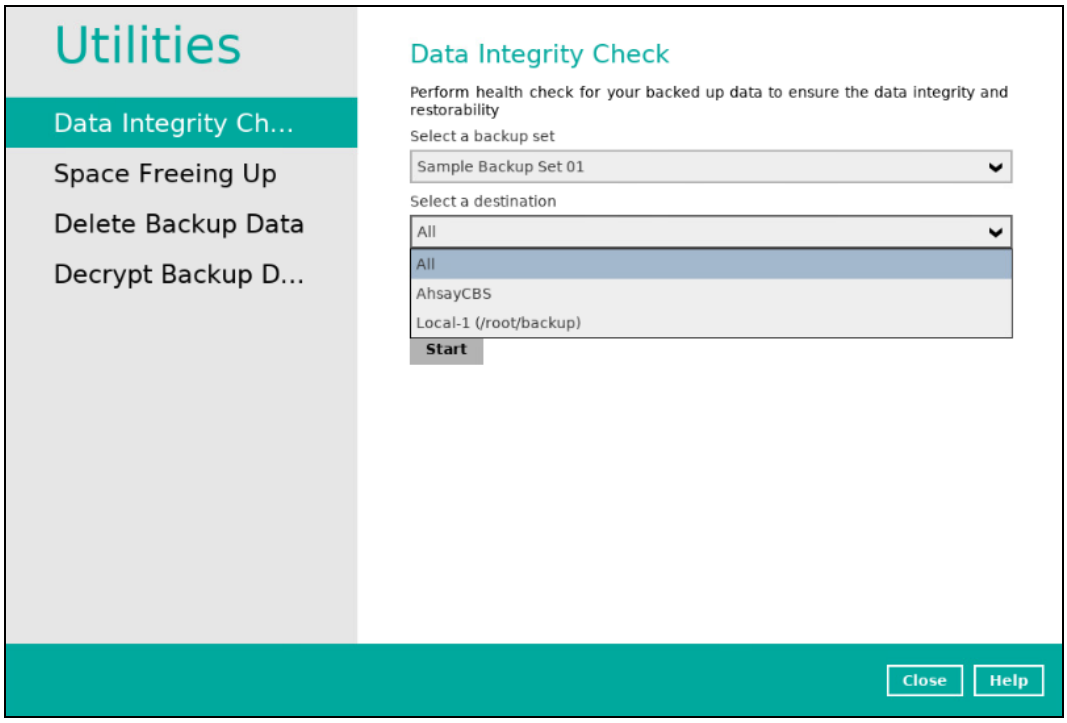
1. Go to the Data Integrity Check tab in the Utilities menu.



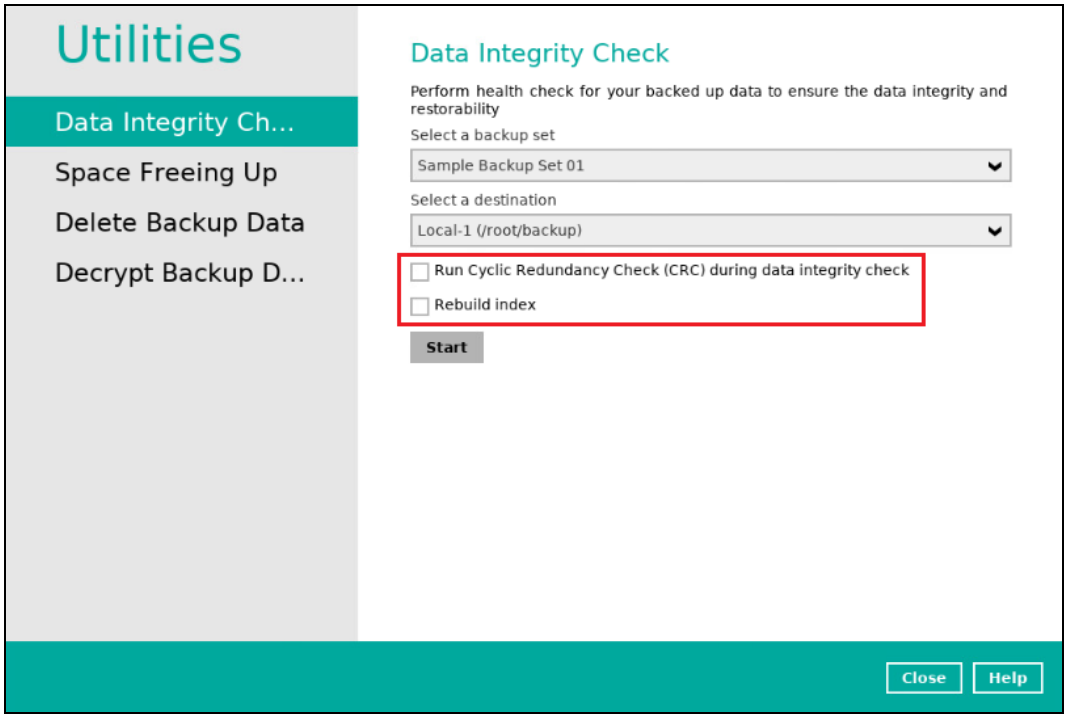
2. Click the drop-down button to select a backup set.



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

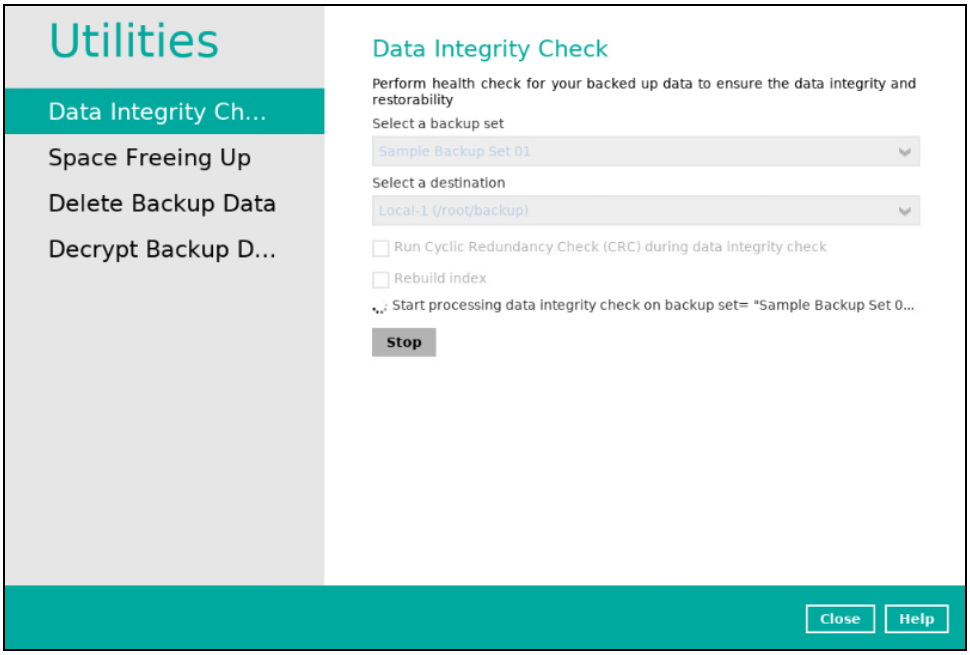
NOTES

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 9.6.3.

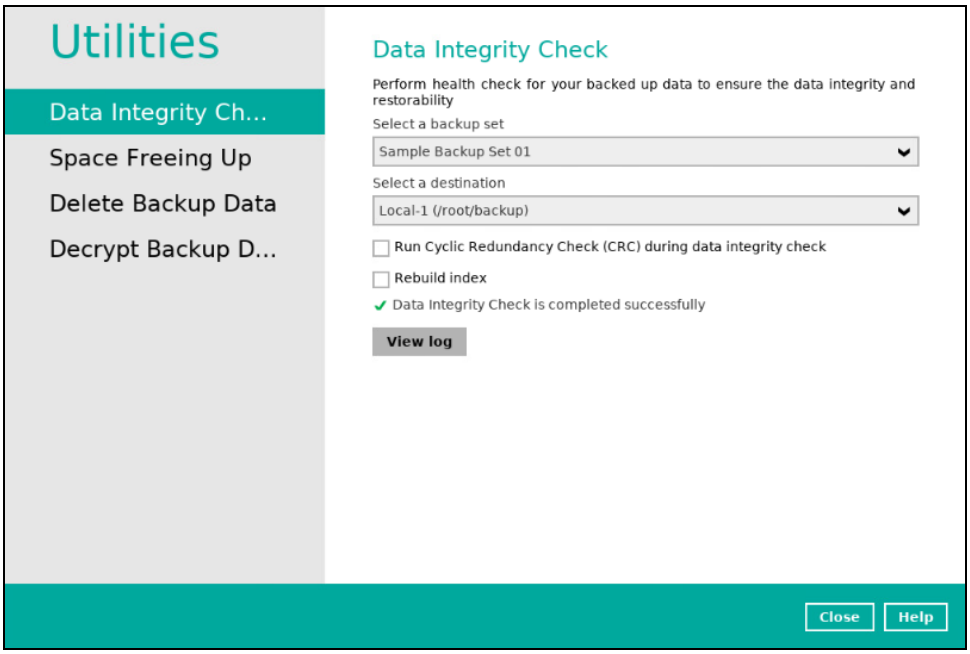
Rebuild index

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

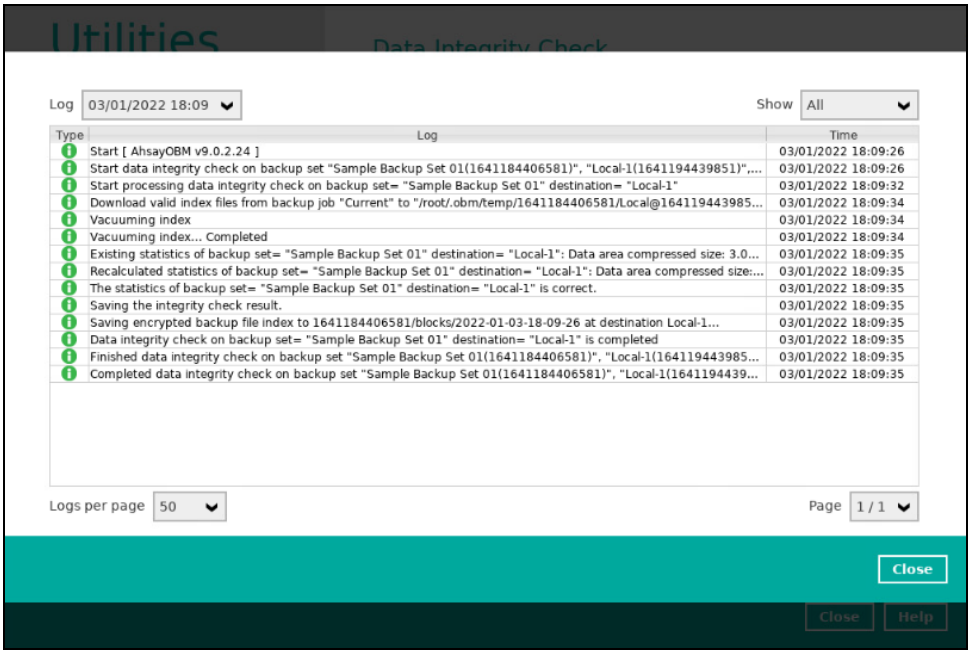
1. Click the **Start** button to begin the Data Integrity Check.
2. Data Integrity Check will start running on the selected backup set(s) and backup destination(s).



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

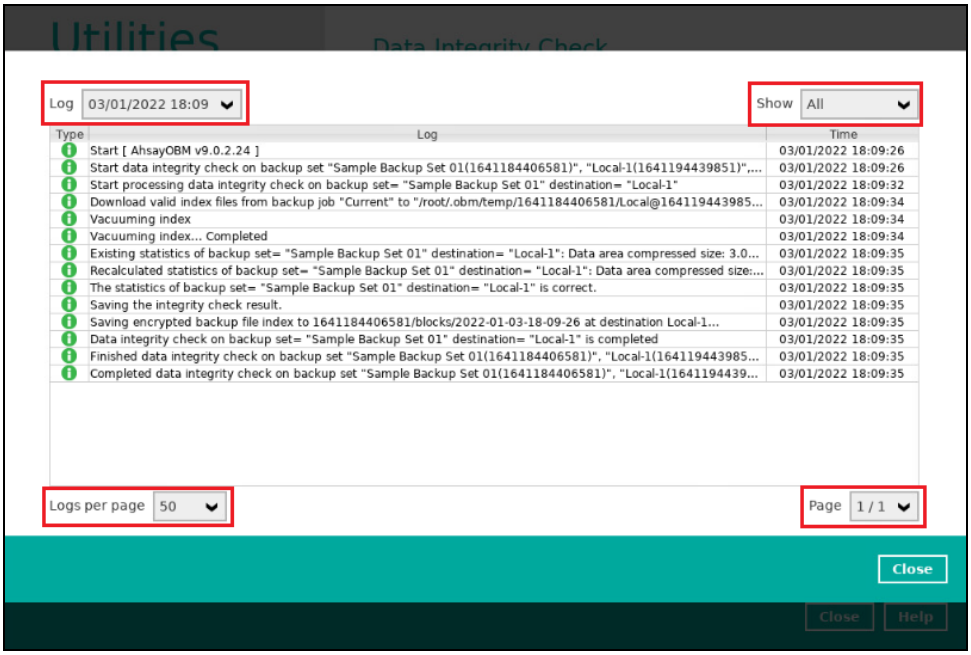


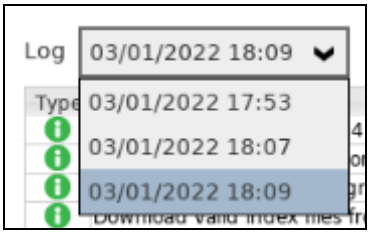
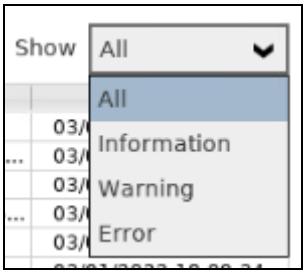
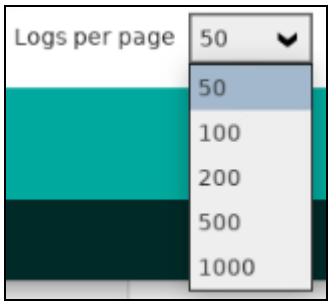
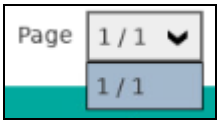
4. The detailed log of data integrity check process will be displayed.



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

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



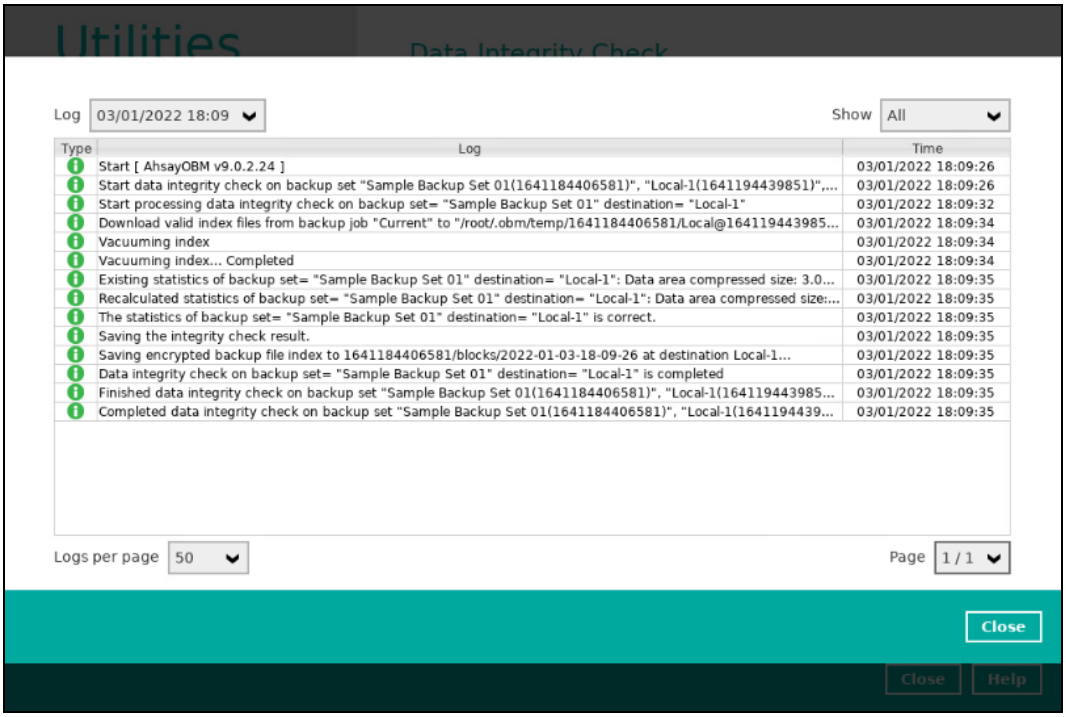
Control	Screenshot	Description
Log filter		This option can be used to display logs of the previous data integrity check jobs.
Show filter		This option can be used to sort the data integrity check log by its status (i.e. All, Information, Warning, and Error). With this filter, it will be easier to sort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

Data Integrity Check Result

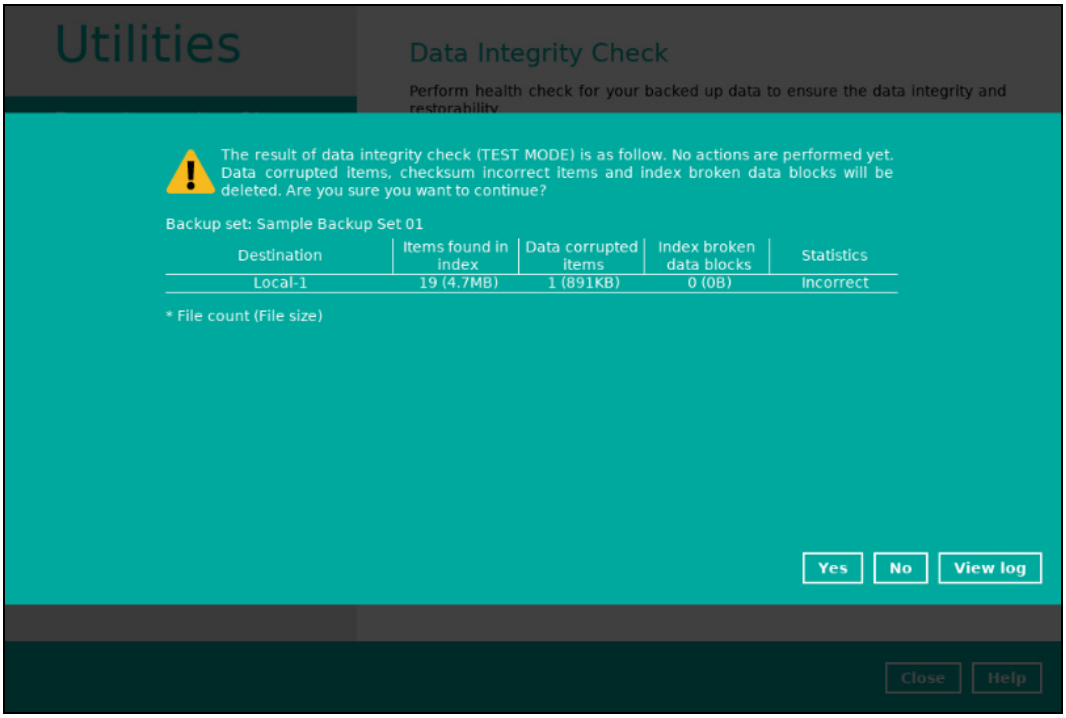
There are two possible outcomes after the completion of a data integrity check:

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

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



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



This is to inform the user of the following details:

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

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:

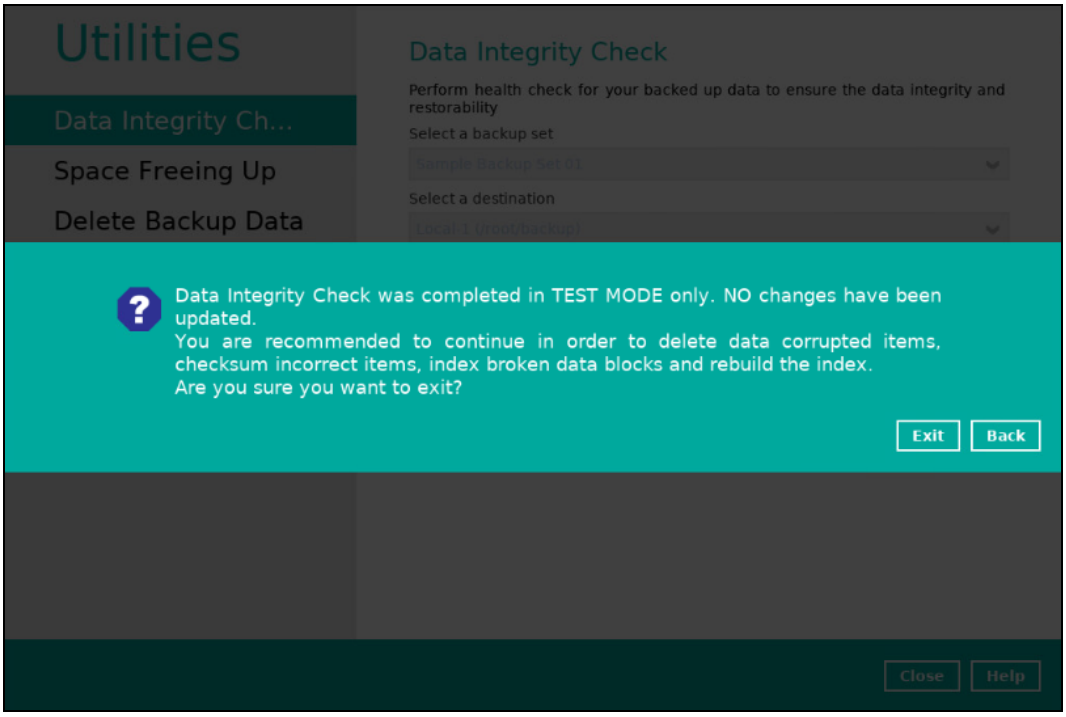
- deleted number of backup files is over 1,000
- deleted number of backup file size is over 512 MB (in total)
- deleted number of backup files is over 10% of total backup files

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.

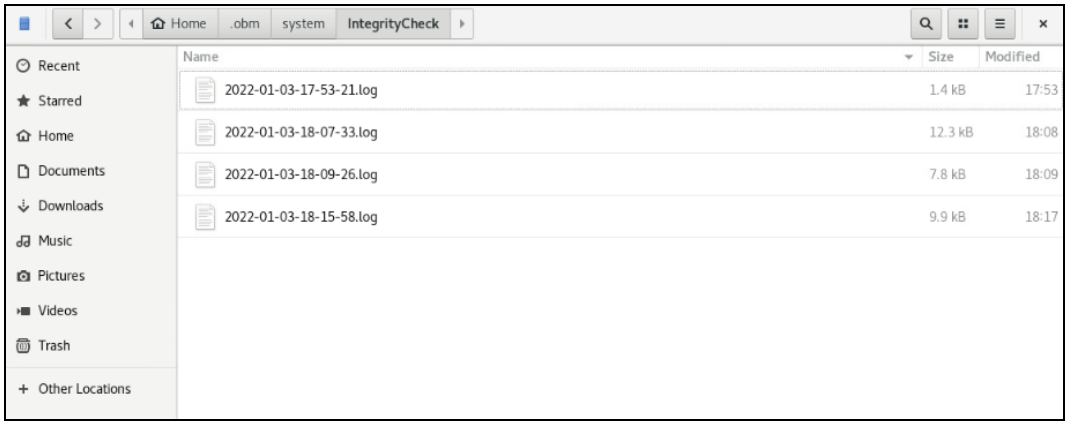
If the **Back** button is clicked, it will go back to the (TEST MODE) confirmation screen.

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 Linux GUI, the DIC logs are located in the following directory:

%UserProfile%\.obm\system\IntegrityCheck

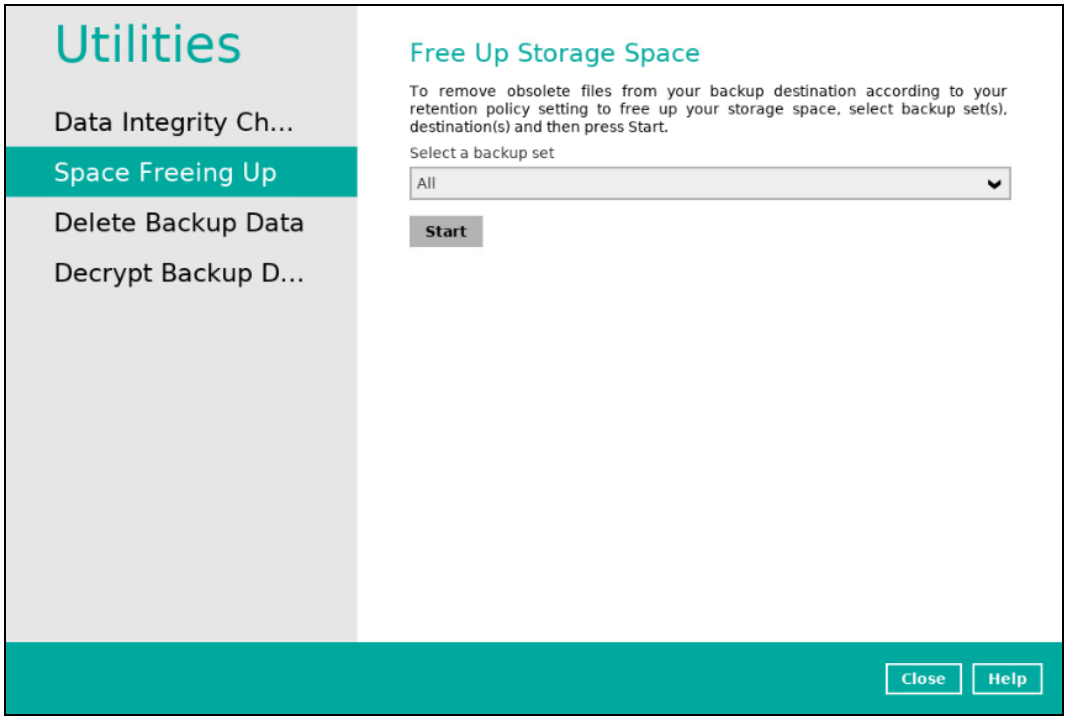


9.9.2 Space Freeing Up

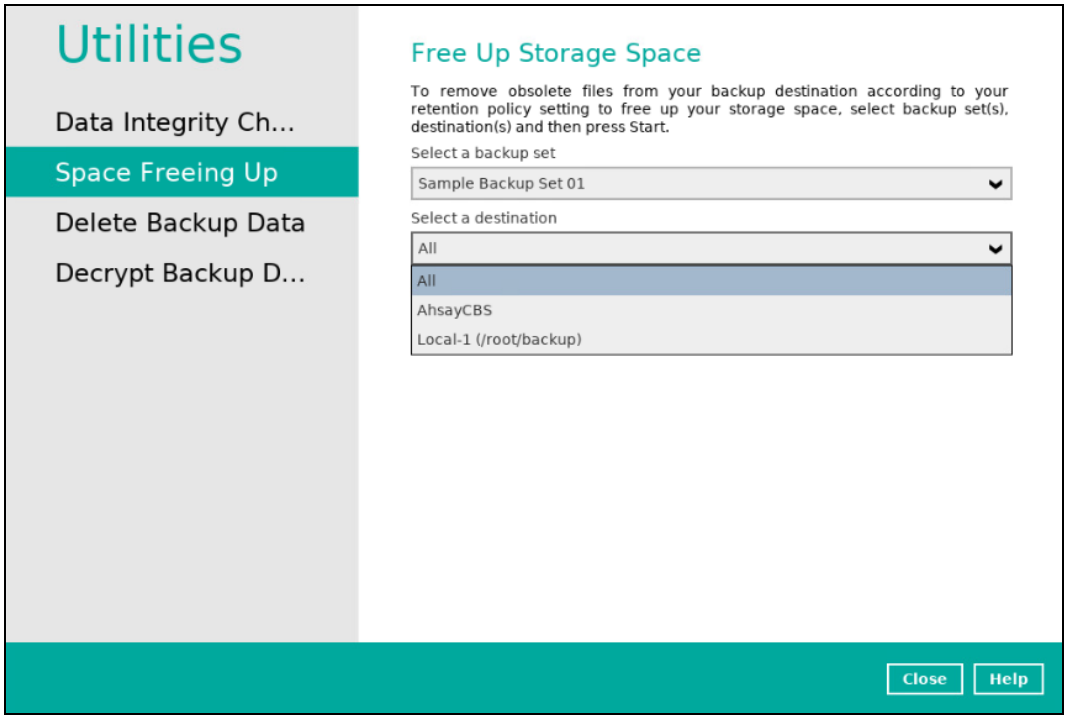
This feature is used to remove obsolete file(s) from your backup set and destination (manually start retention policy). After the Space Freeing Up job is completed, the storage statistics of the backup set(s) are updated.

To perform Space Freeing Up, follow the instructions below:

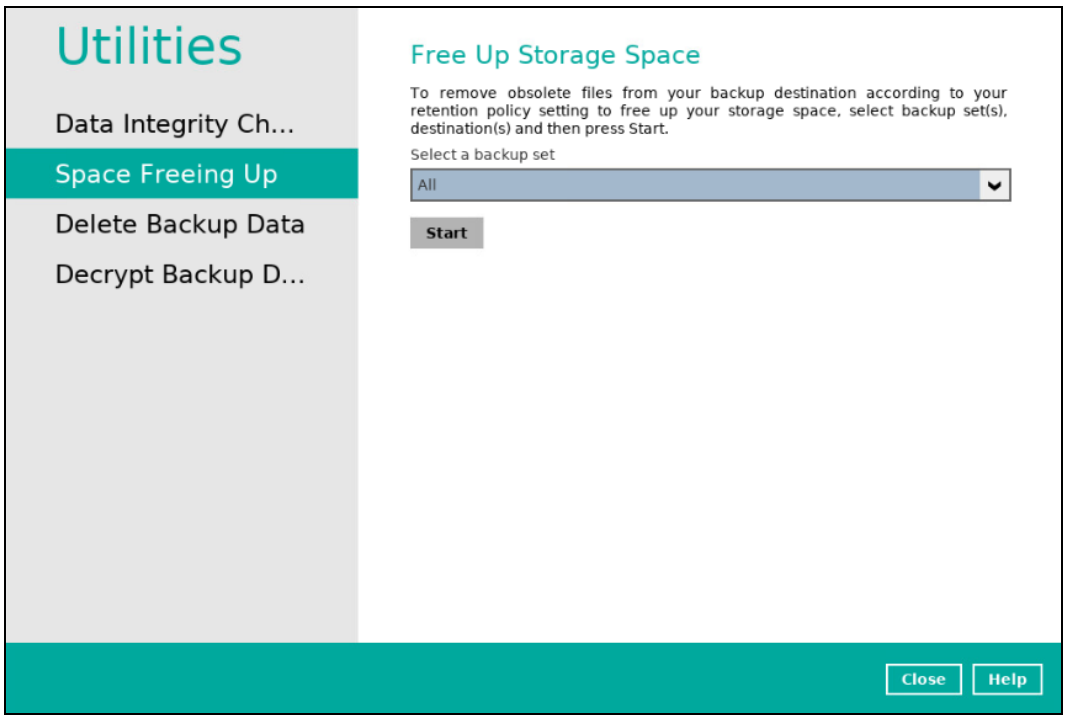
1. Select a backup set from the drop-down list.



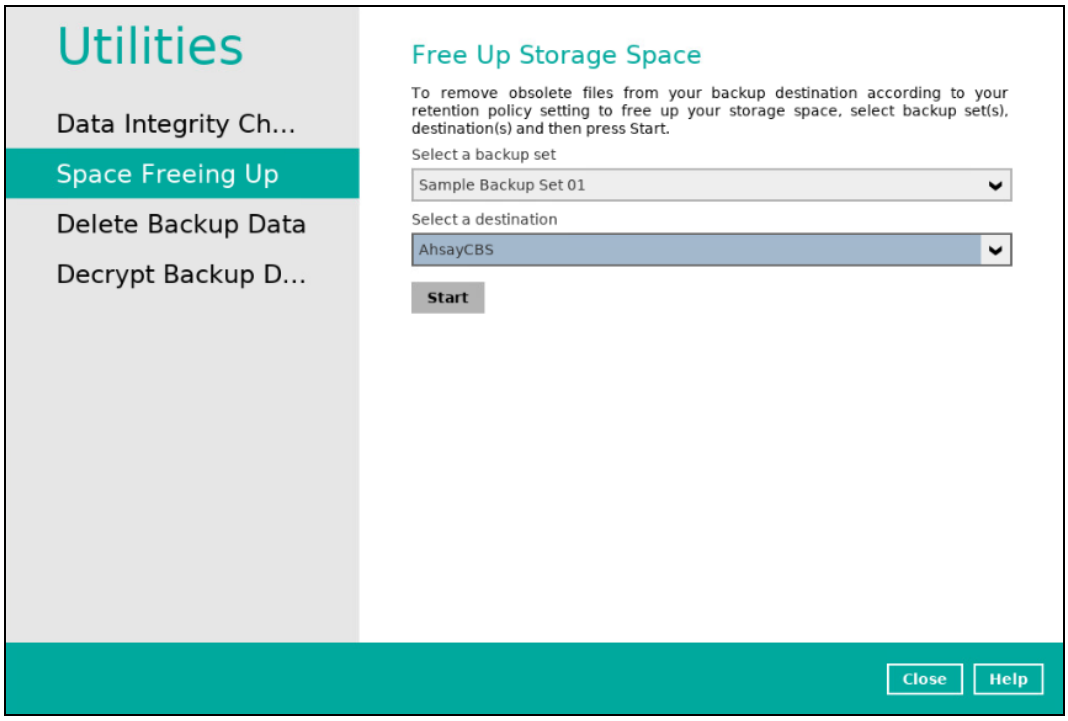
If you select a specific backup set, then you will also have to select a specific destination or all destinations.



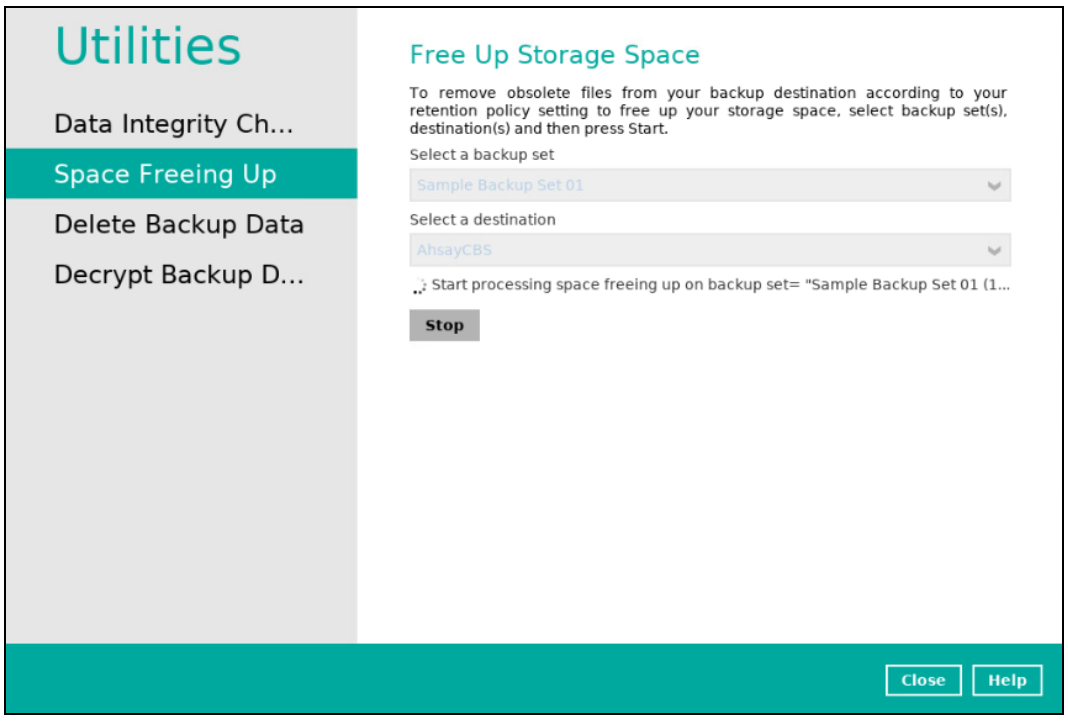
If you select **All** backup sets, then there is no need to select a destination.



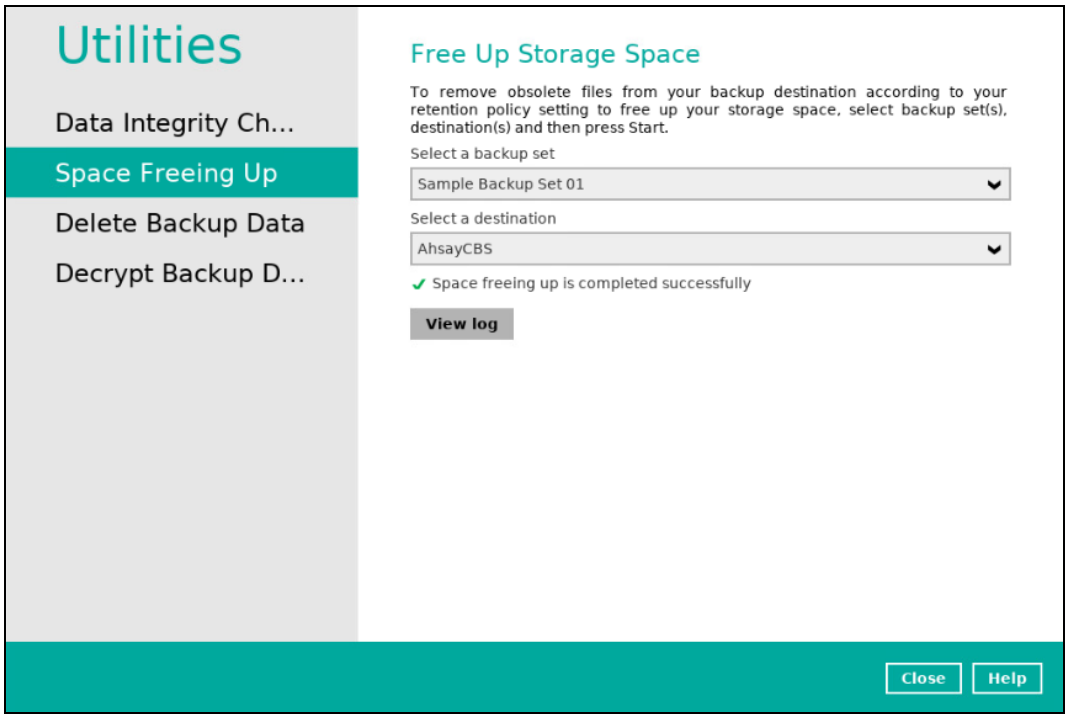
2. Click the **Start** button to perform space free up.

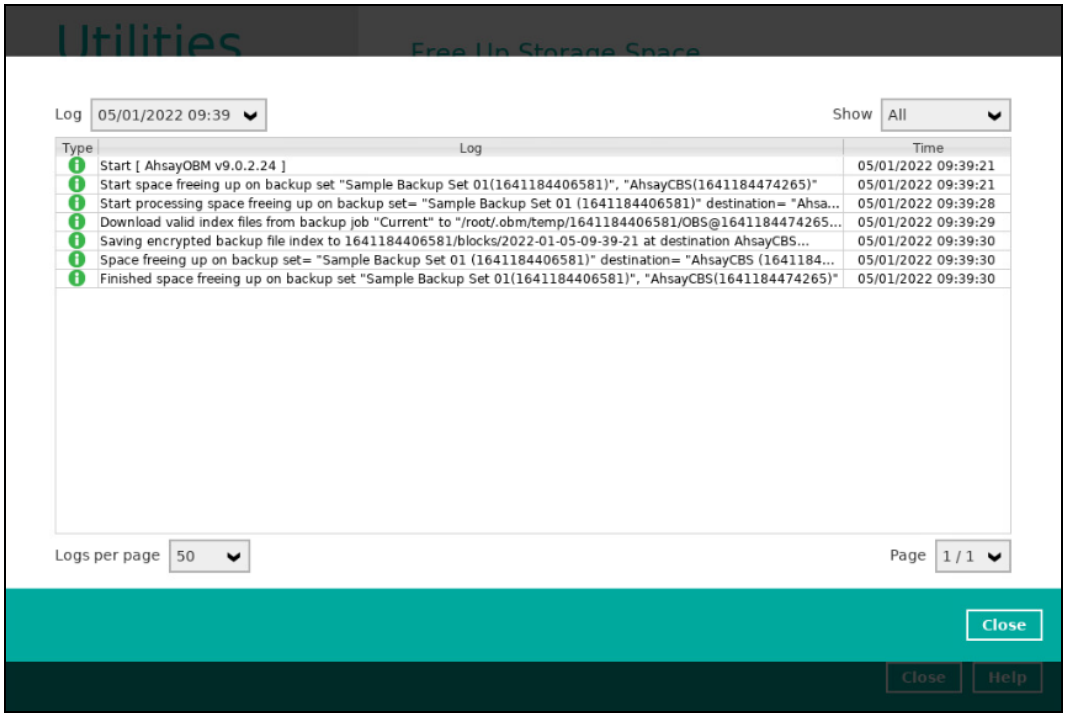


3. Space freeing job will start running on the selected backup set(s) and backup destination(s).



4. The result will be shown once completed. Click the **View Log** to see the event log during the space free up.



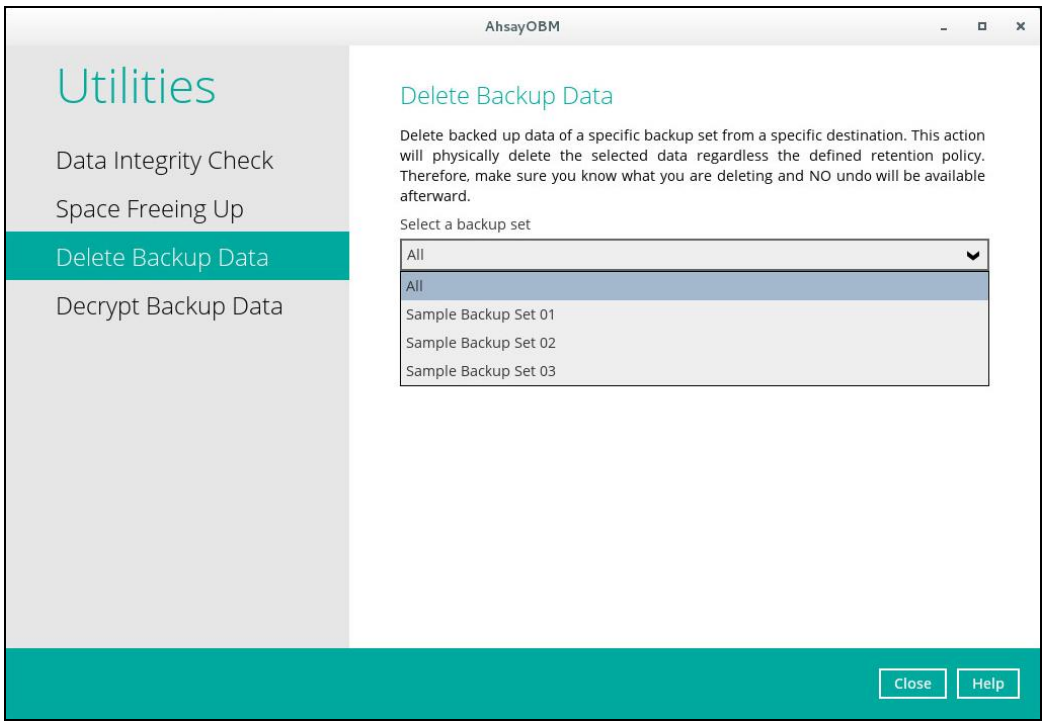


9.9.3 Delete Backup Data

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

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

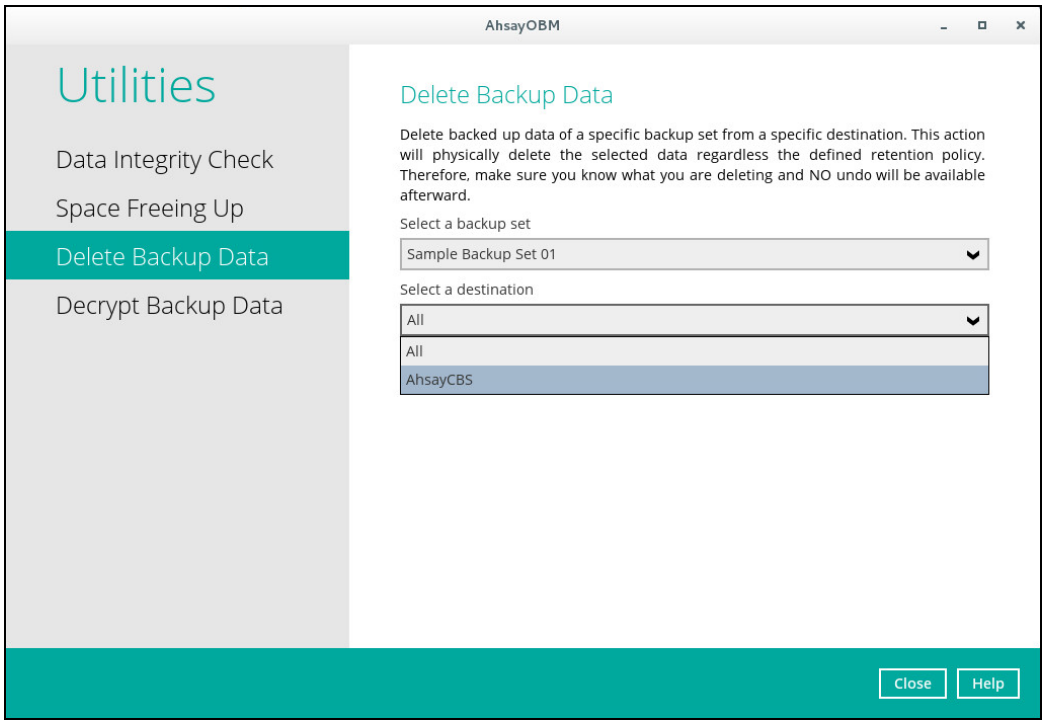
1. Select a backup set from the drop-down list.



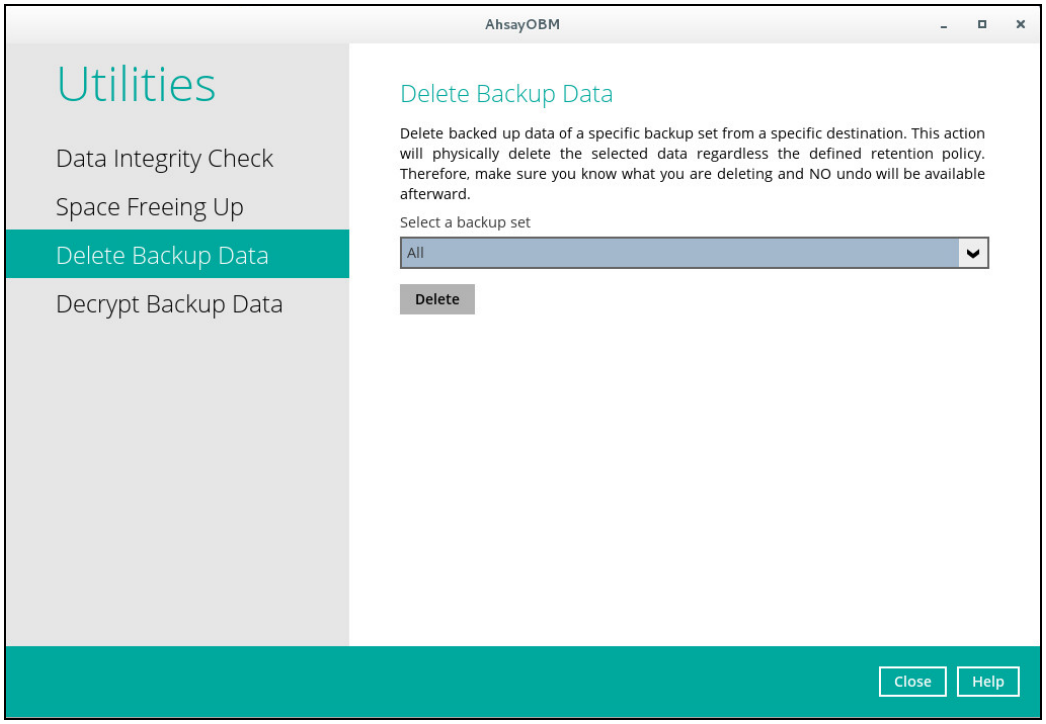
NOTE

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

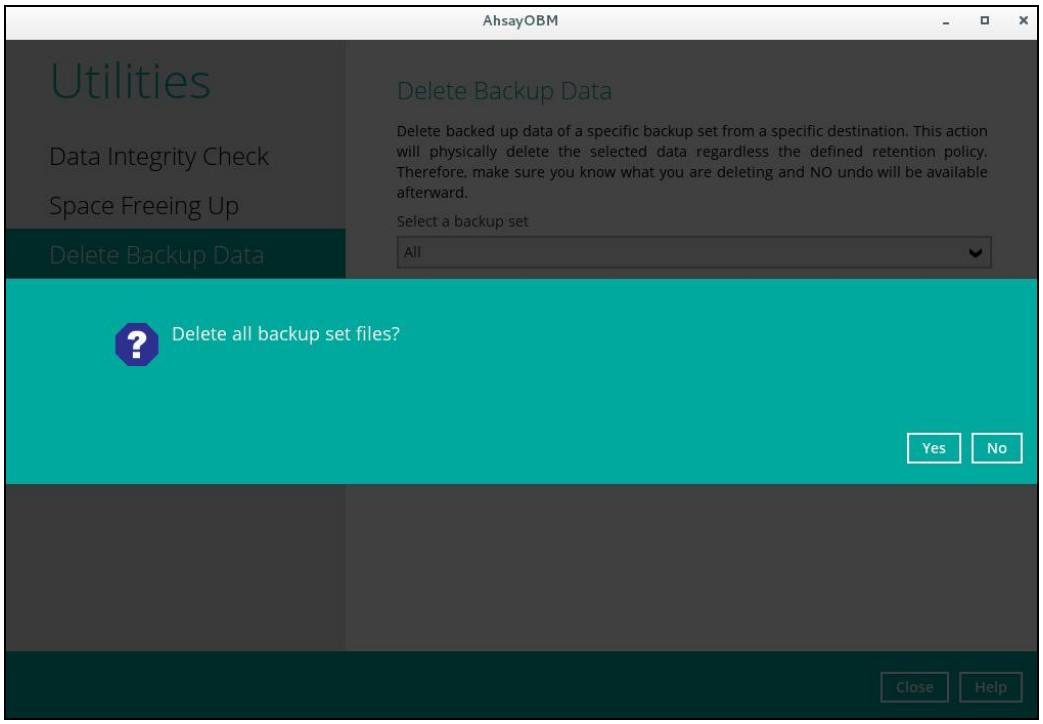
If you select a specific backup set, then you will also have to select a specific destination or all destinations.



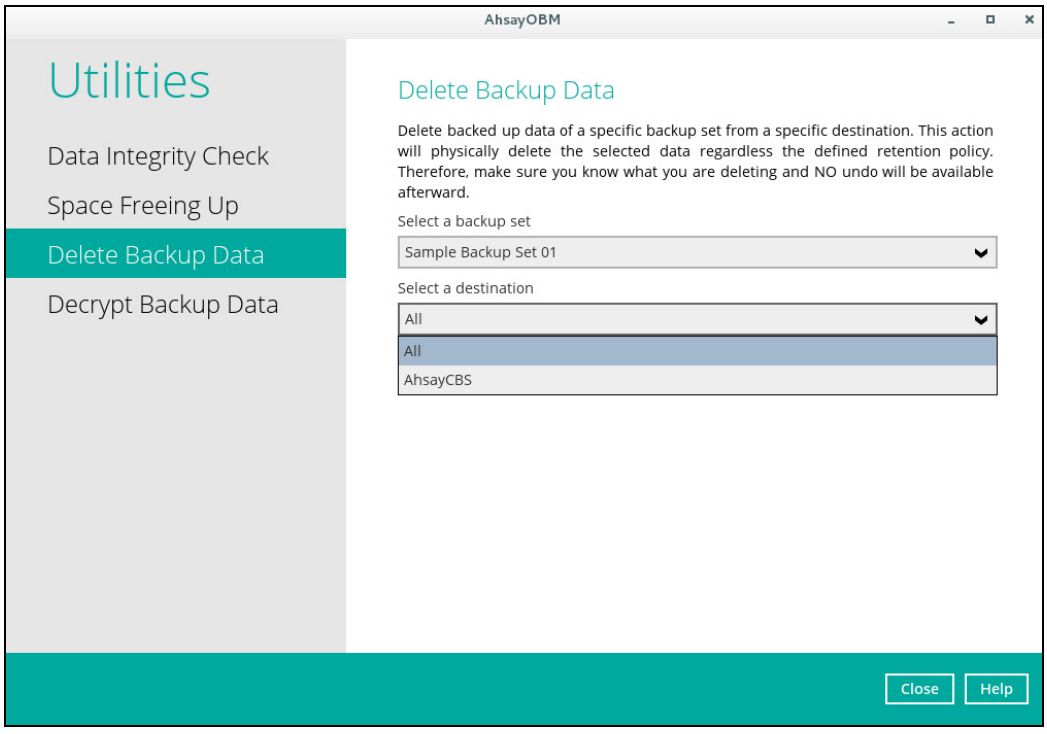
If you select **All** backup sets, then there is no need to select a destination.



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

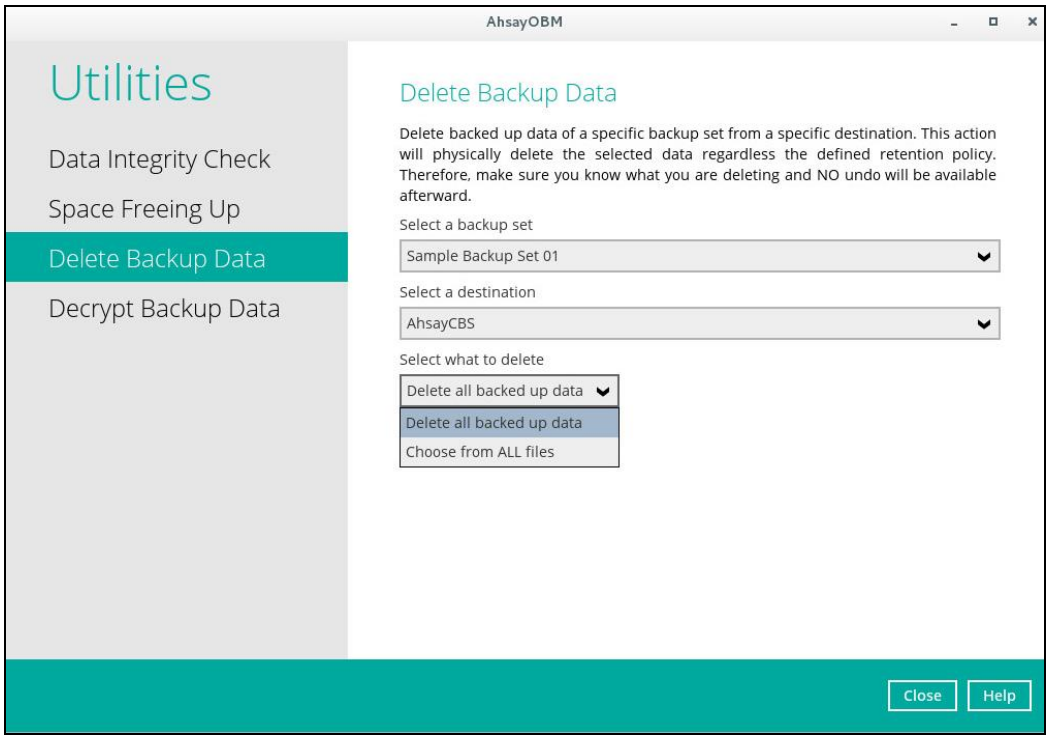


If you select a specific backup set, you will have an option to choose a destination.



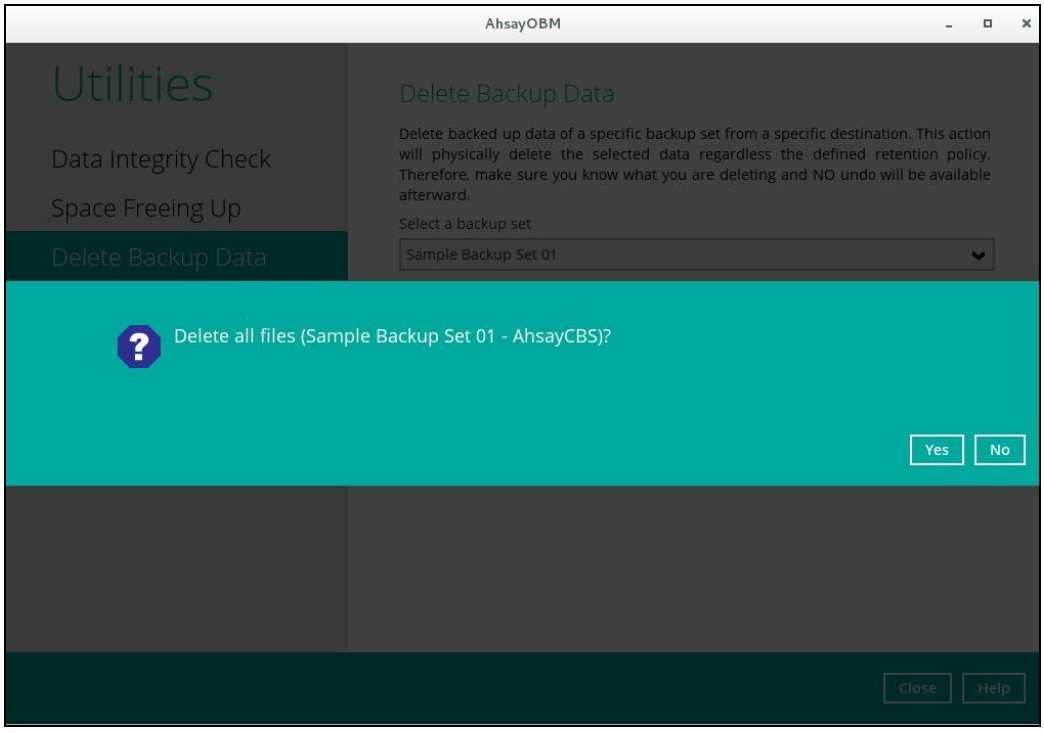
If you select a specific destination, there are two (2) available options for the type of files you wish to delete.

- Delete all backed up data
- Choose from ALL files



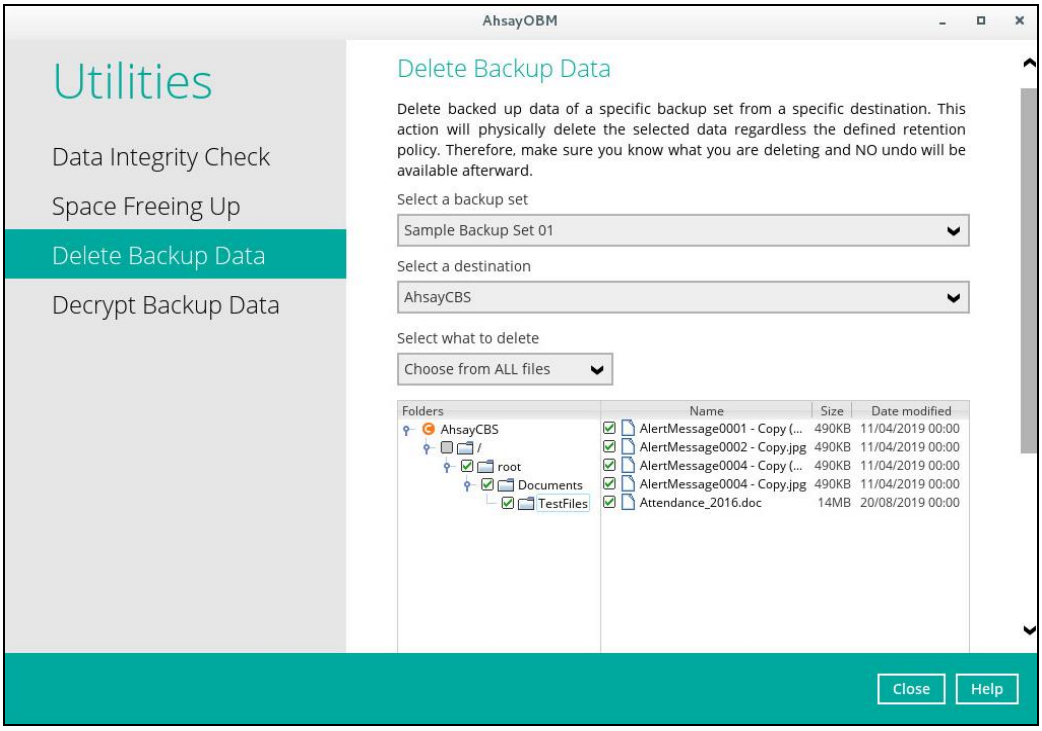
Delete all backed up data

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

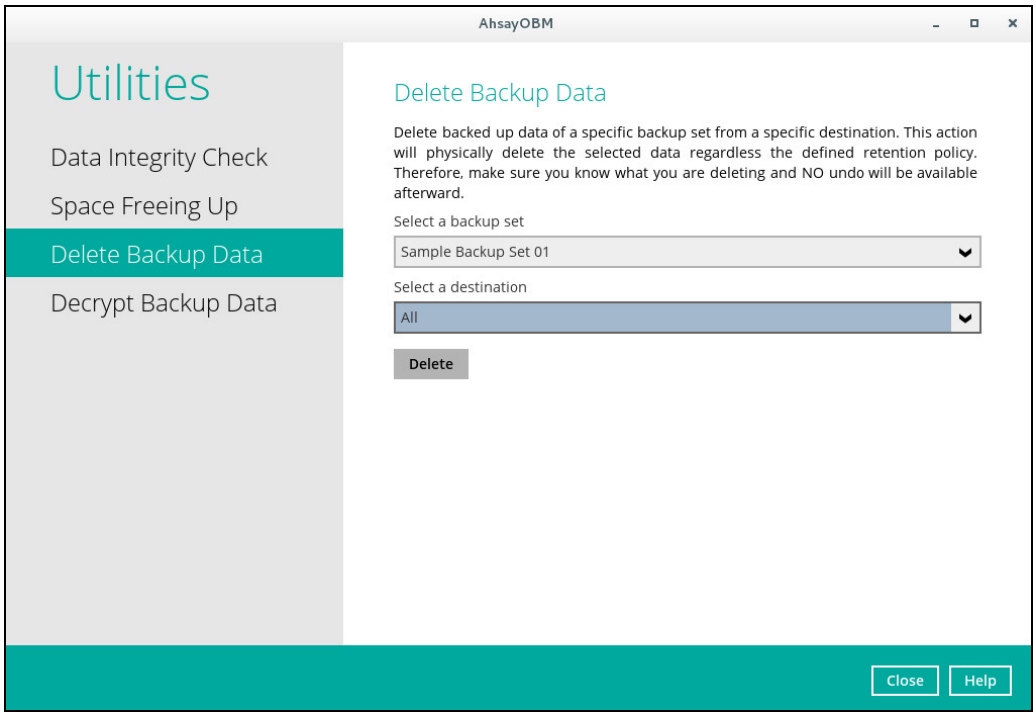


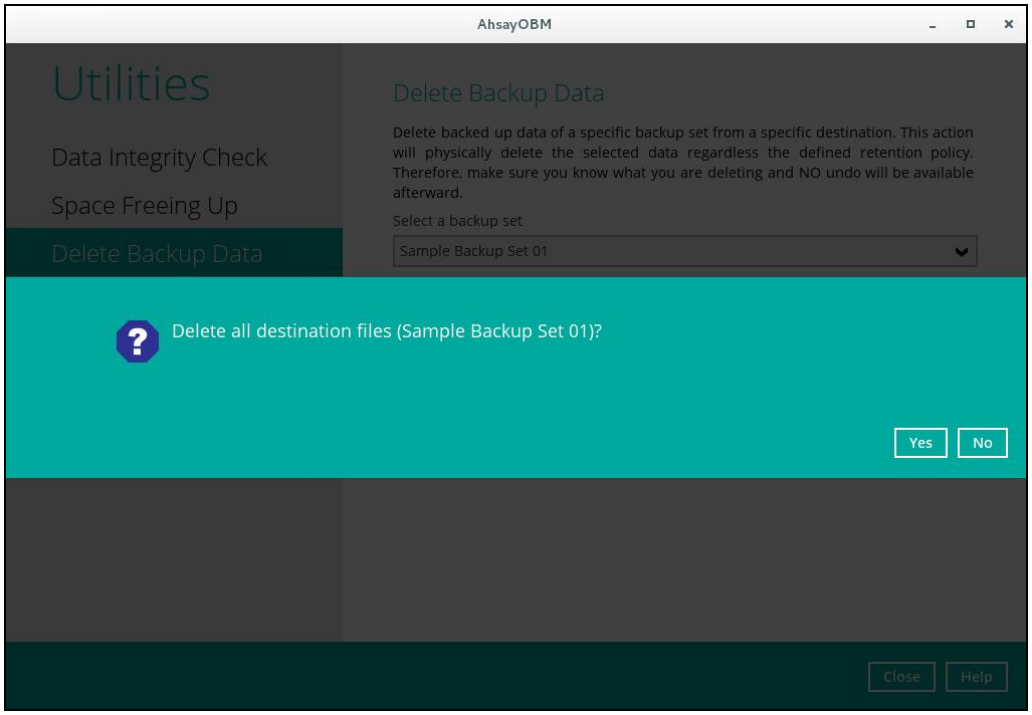
Choose from ALL files

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

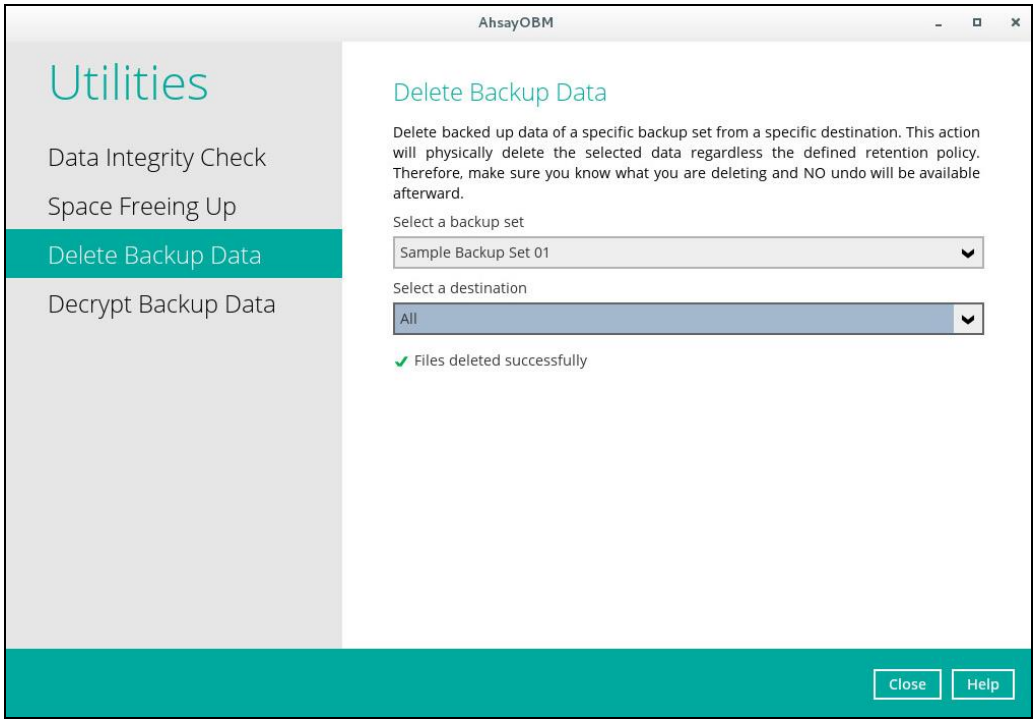


3. Click the **Delete** button, then click **Yes** to start the deletion of files.



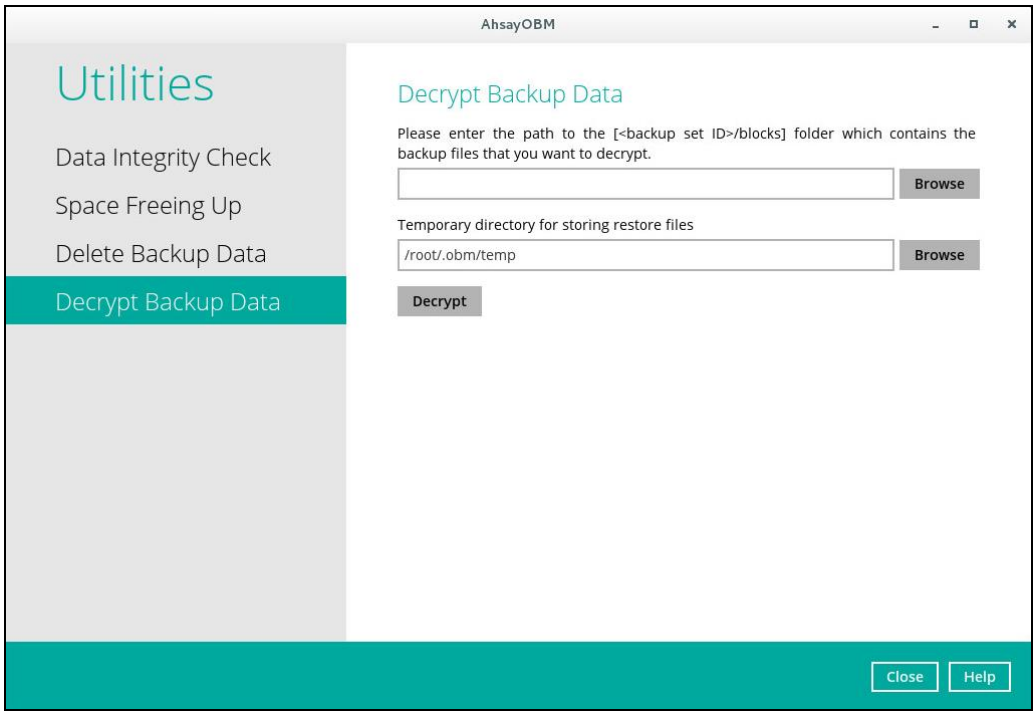


4. Files are successfully deleted.



9.9.4 Decrypt Backup Data

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

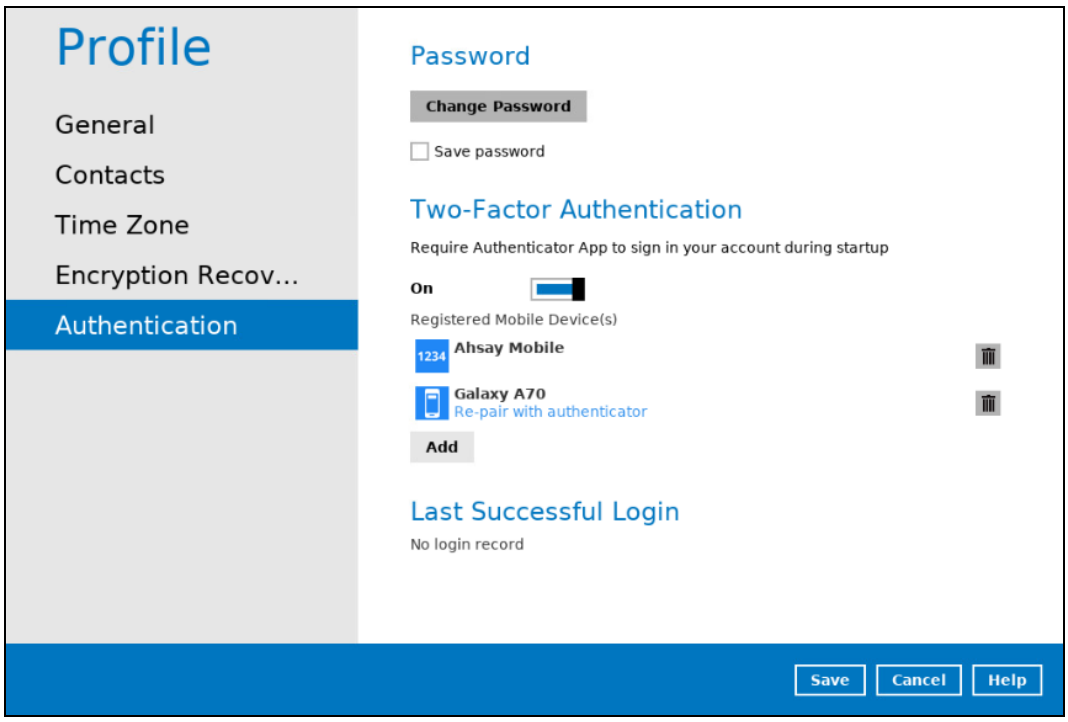


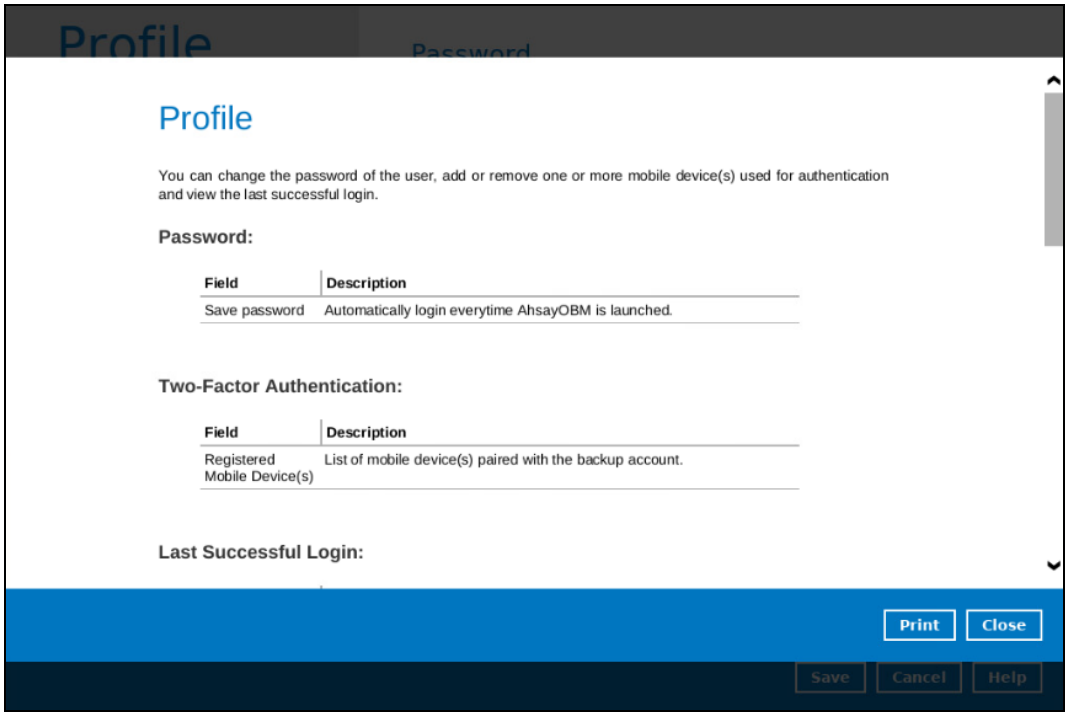
To perform decryption of backup data, follow the instructions below:

1. Click the **Browse** button to locate the path of the backup set ID / blocks folder.
2. Click the **Browse** button to re-select the temporary folder for the decrypt process.
3. Click the **Decrypt** button to begin.

9.10 Online Help

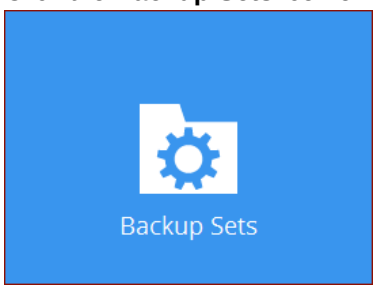
This allows the User to view the summary of information and instructions of each available feature in the AhsayOBM.





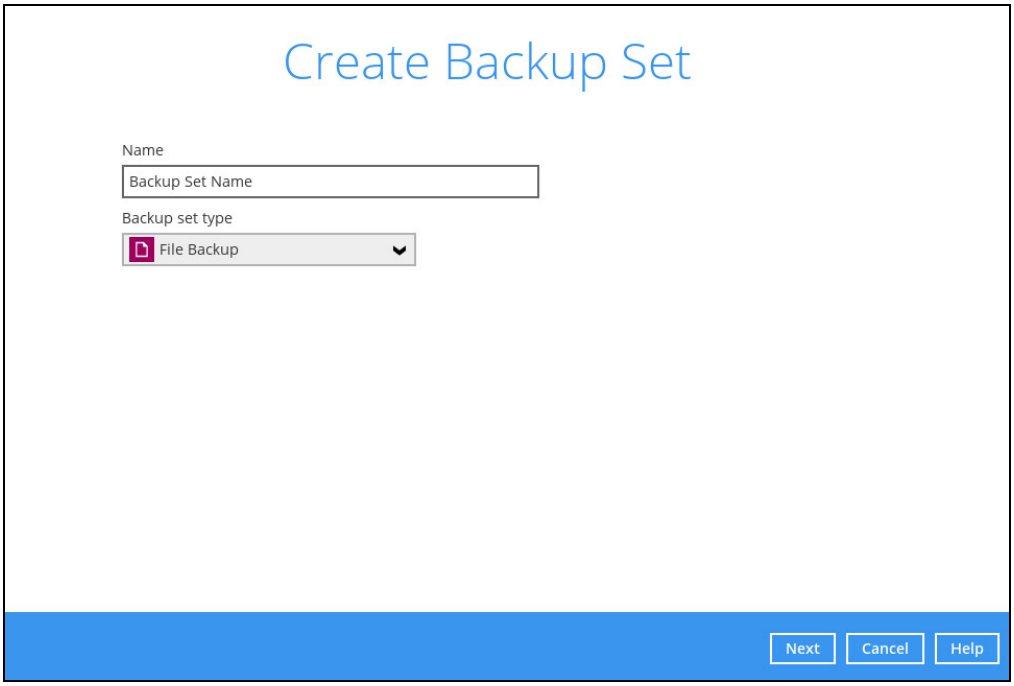
10 Creating a File Backup Set

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

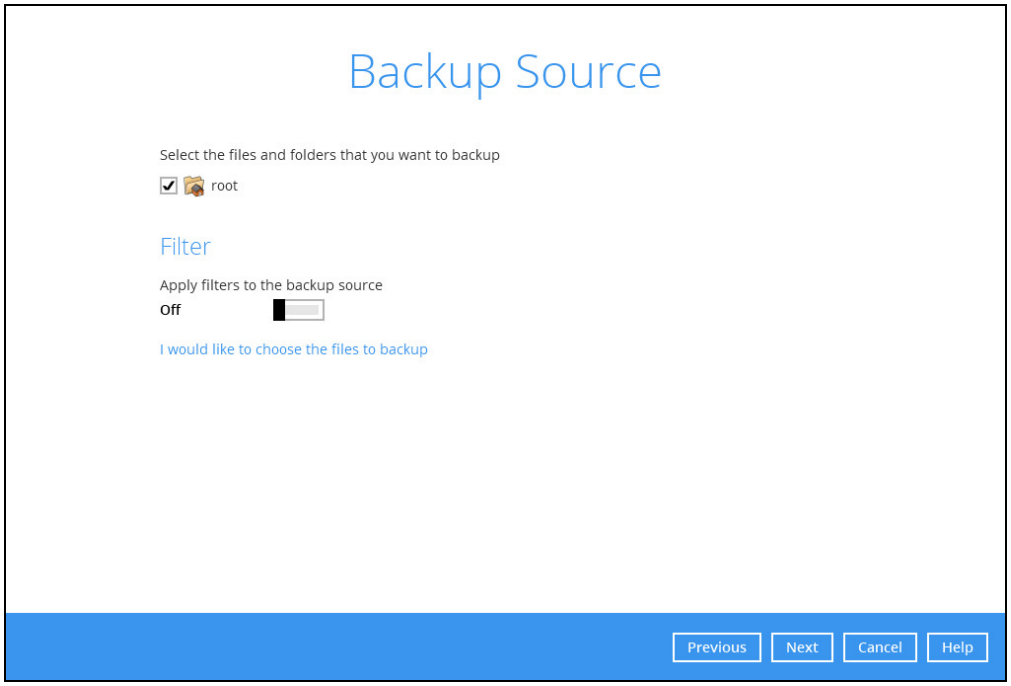


2. Create a new backup set by clicking the "**+**" icon next to **Add new backup set**.

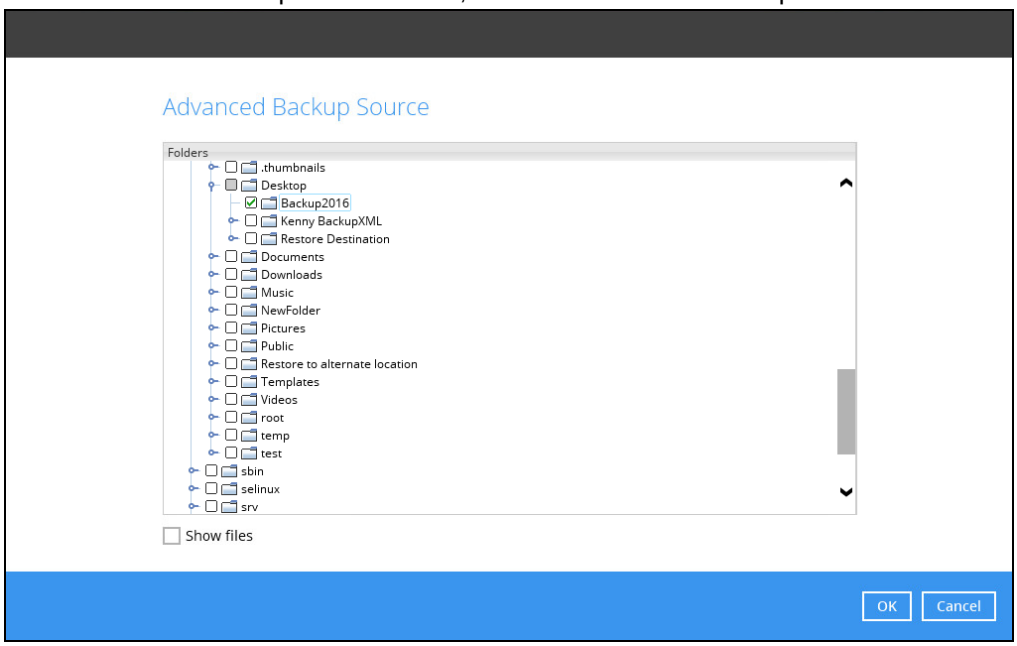
3. Name your new backup set and select the Backup set type. Then, click **Next** to proceed.



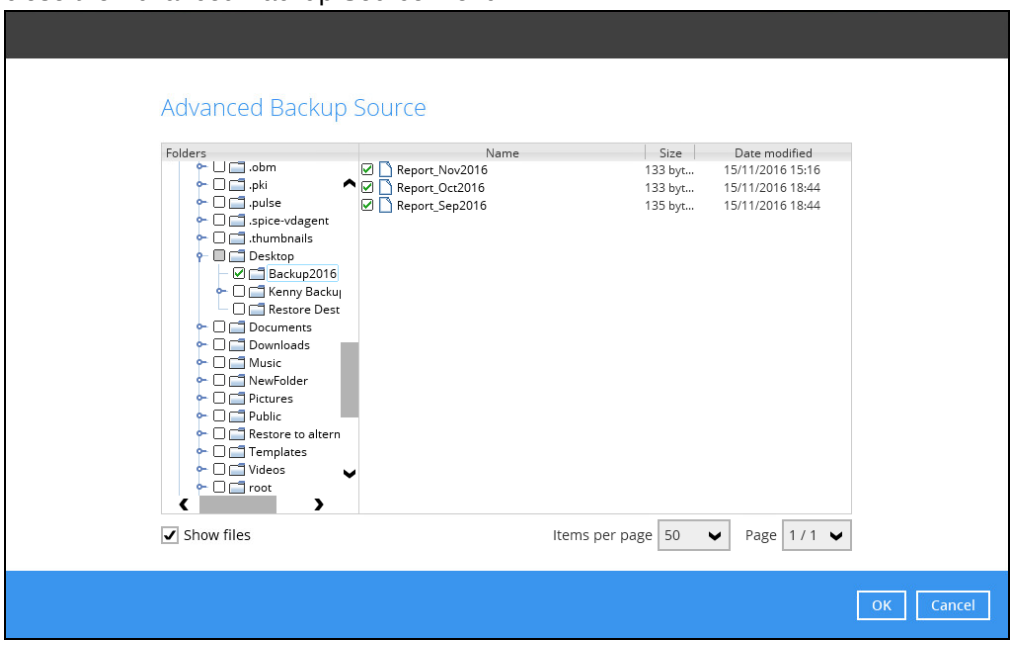
4. In the Backup Source menu, select the files and folder that you would like to backup. Click **I would like to choose the files to backup** to select individual files for backup.



5. In the Advanced Backup Source menu, select the folder to back up all files in the folder.

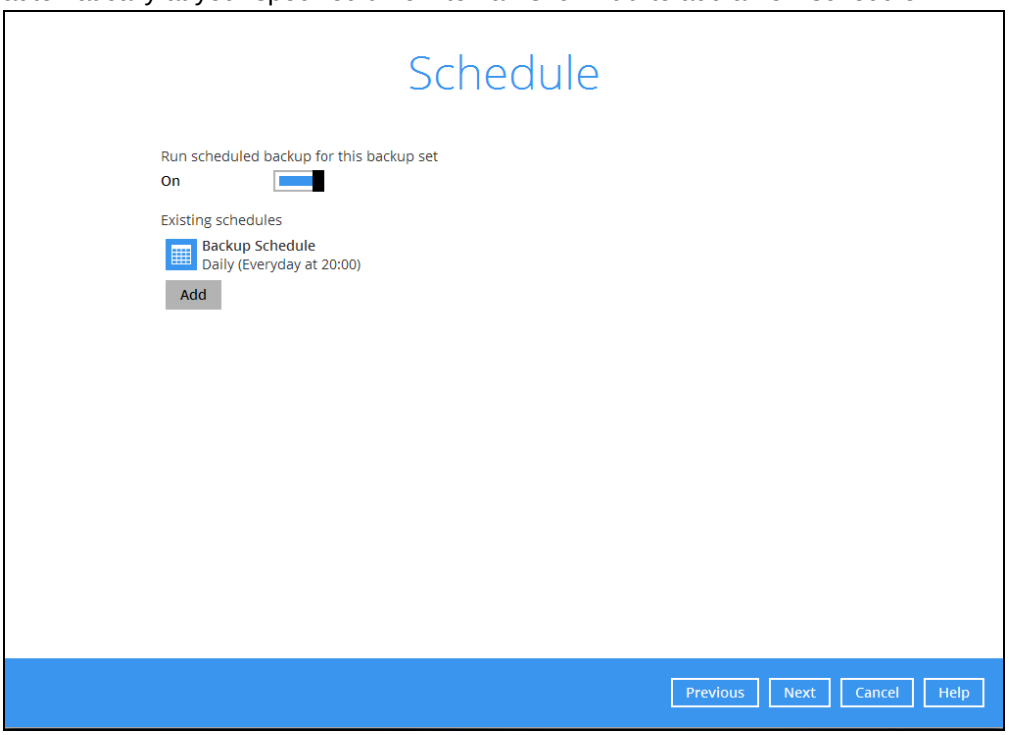


6. Alternatively, if you want to back up a specific file instead of all files in your selected folder, select the **Show files** checkbox at the bottom of the screen. A list of files will appear on the right-hand side. Select the checkbox(es) next to the file(s) to back up. Then, click **OK** to close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

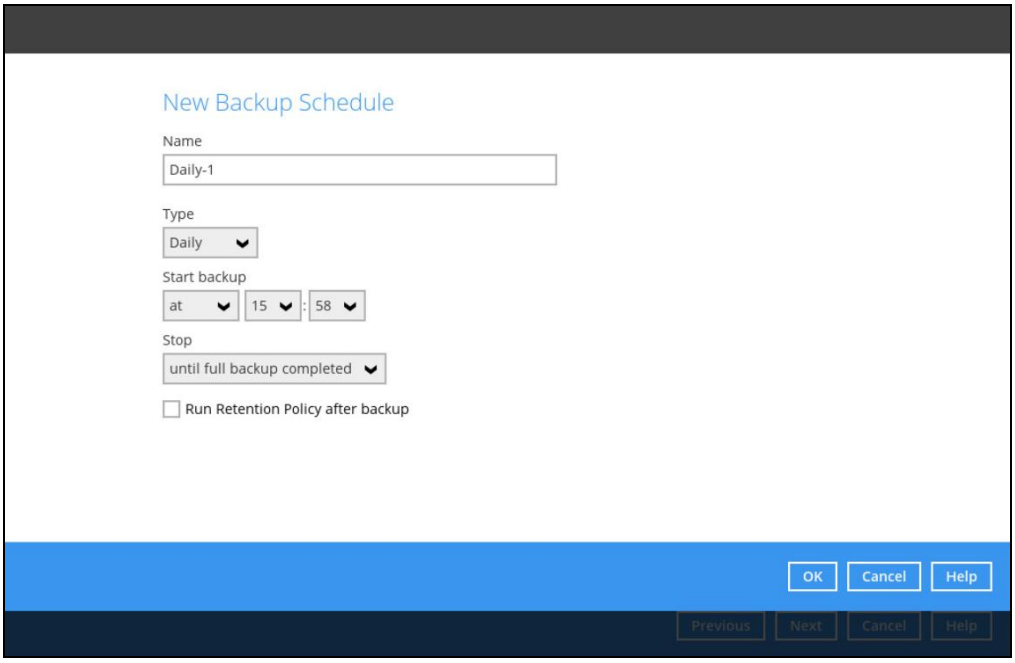


7. In the Backup Source menu, click **Next** to proceed.

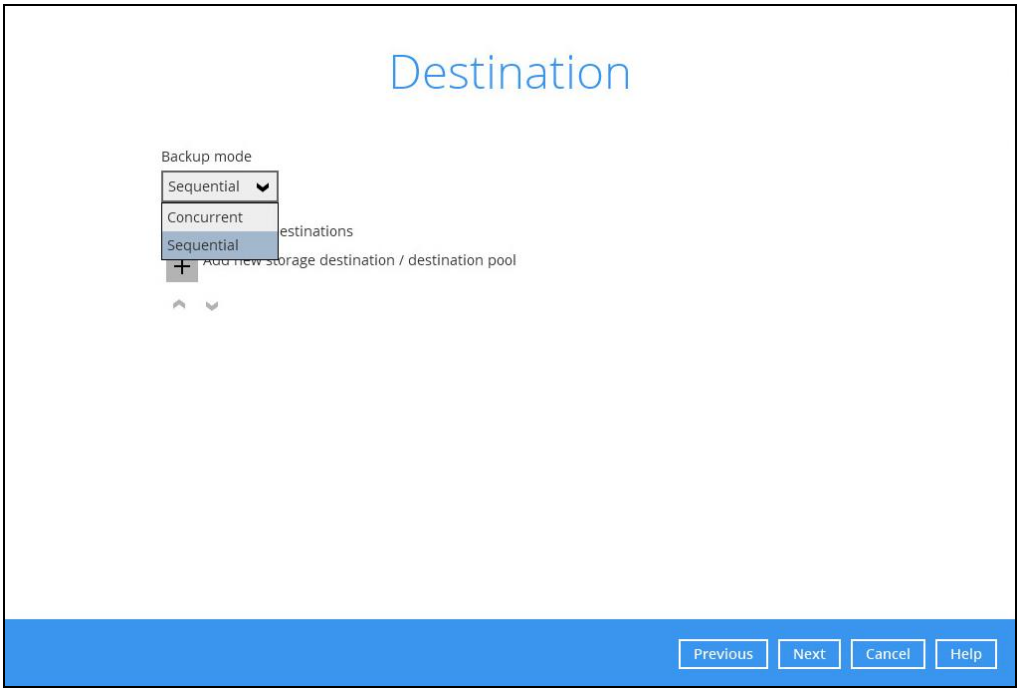
8. In the Schedule menu, you can configure a backup schedule for backup job to run automatically at your specified time interval. Click **Add** to add a new schedule.



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

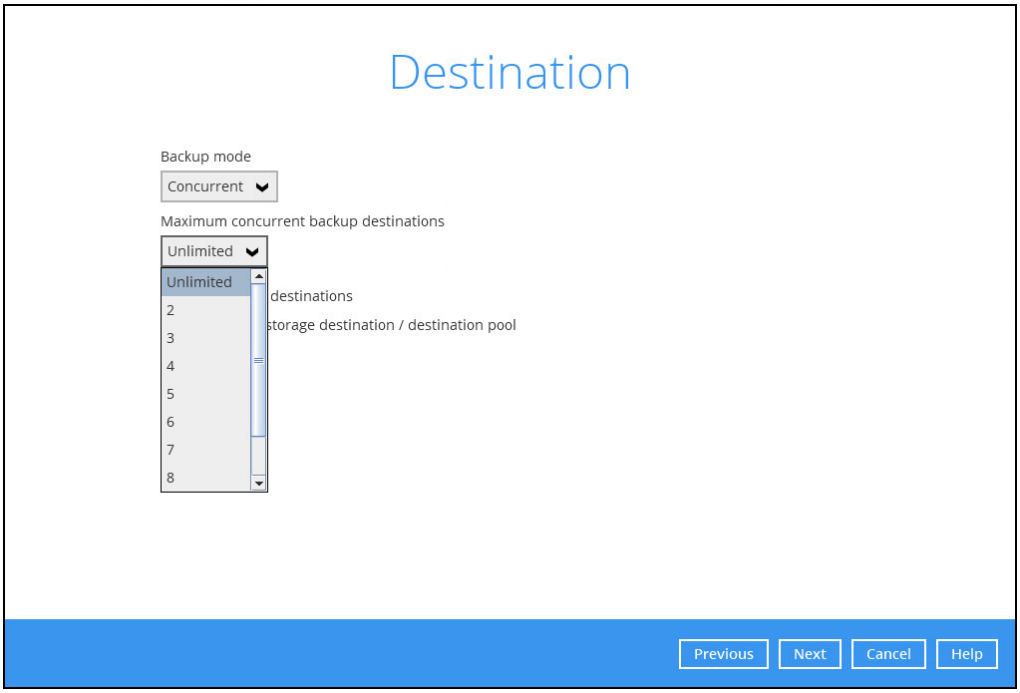


9. In the Destination menu, the default backup mode selected is Sequential since only one backup set is being created.



You can choose from one of the following two Backup mode options:

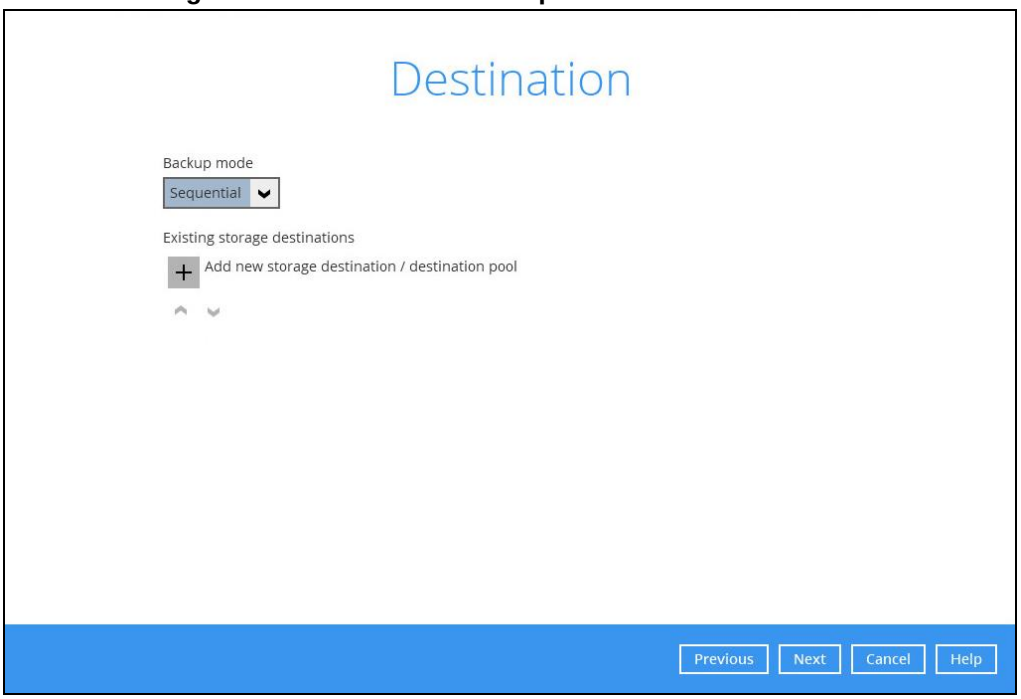
- **Sequential** – if there are multiple destinations configured in the backup set, AhsayOBM will back up to one destination at a time.
- **Concurrent -** if there are multiple destinations configured in the backup set, AhsayOBM will backup to all destinations at the same time or concurrently.



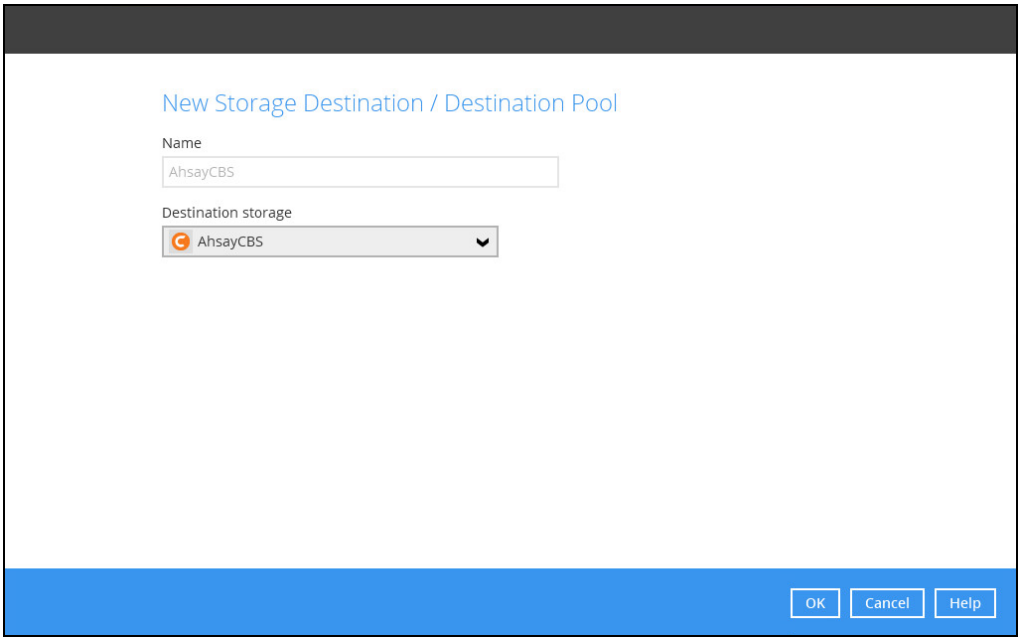
NOTE

For backup sets with multiple destinations, sequential backup mode will take longer compared with concurrent backup mode.

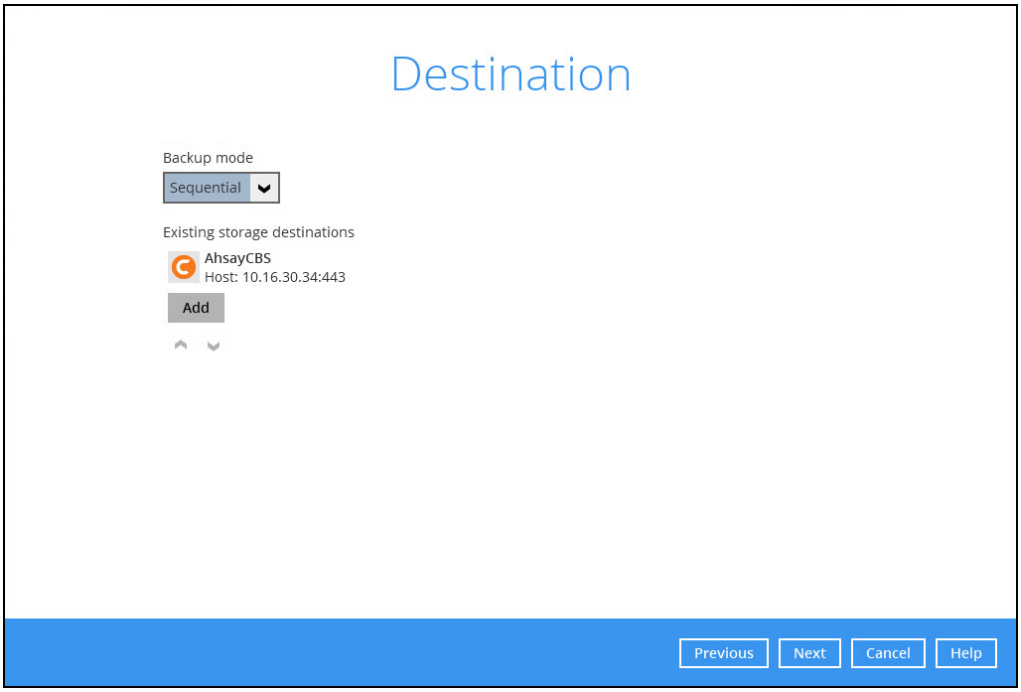
10. Add a backup destination where the backup data will be stored. Click the "**+**" icon next to **Add new storage destination / destination pool**.



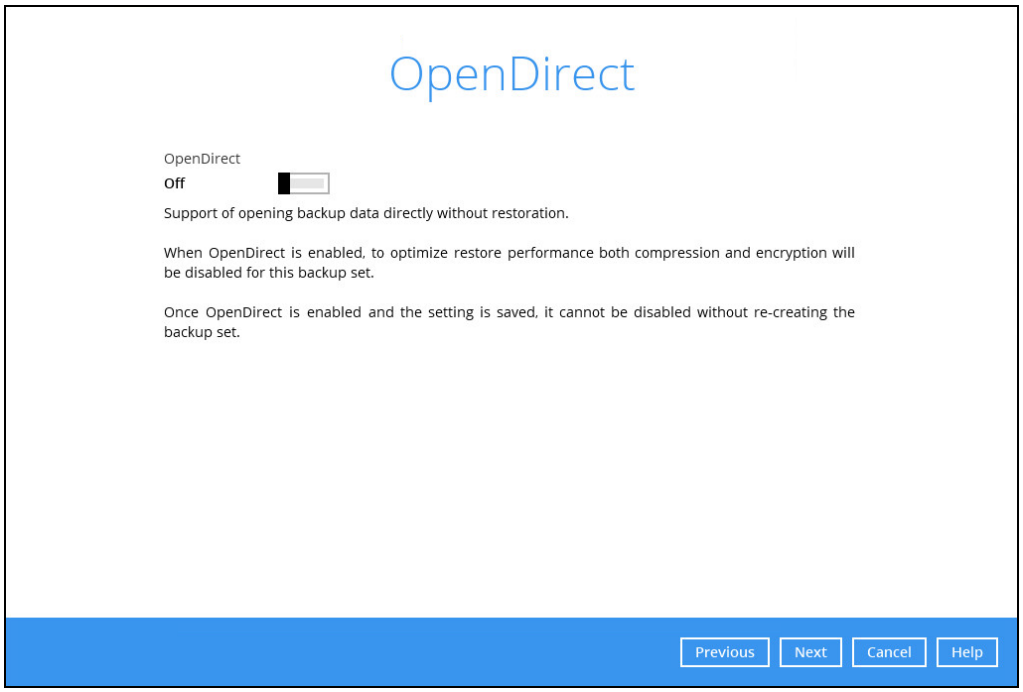
Select the destination storage. Then, click **OK** to proceed.



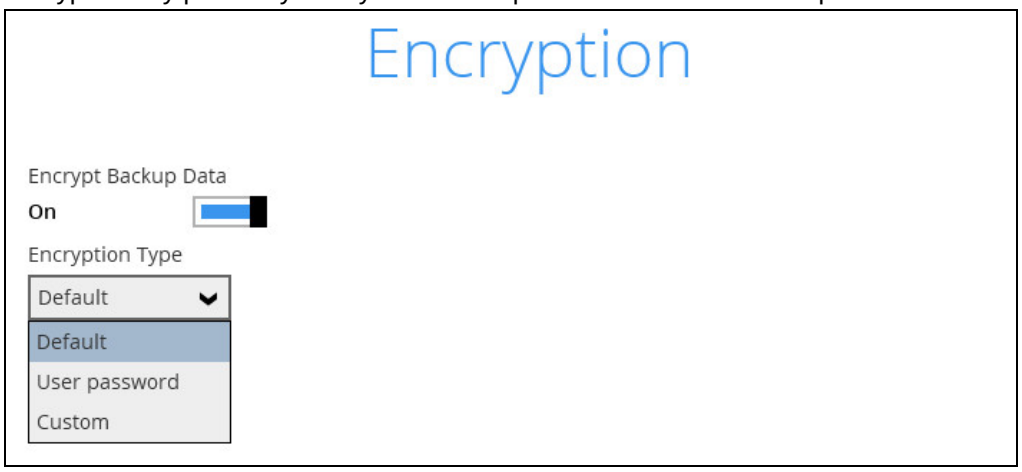
11. Click **Next** on the Destination menu page to proceed.



12. In the OpenDirect window, the default option is disabled. Keep it off since this is not supported in Linux.



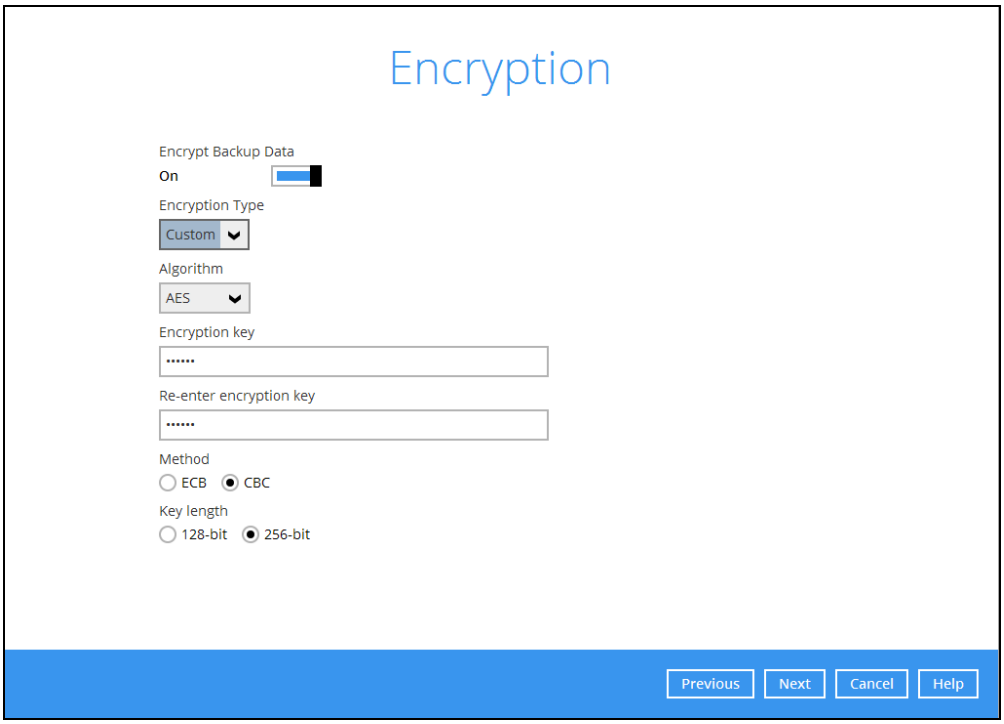
13. In the Encryption window, the default **Encrypt Backup Data** option is enabled with an encryption key preset by the system which provides the most secure protection.



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.

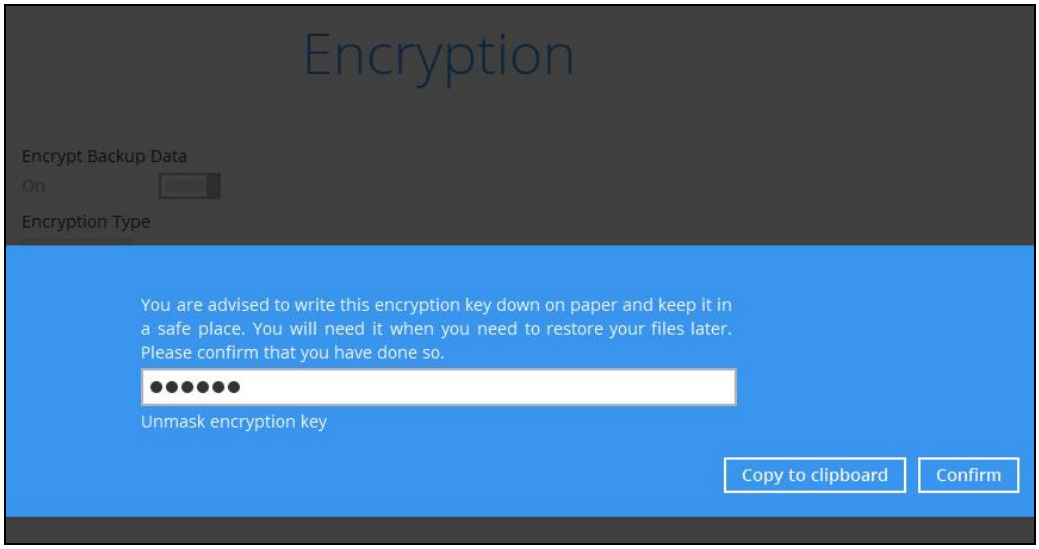


NOTE

For best practice on managing your encryption key, refer to following article:
FAQ: Best practices for managing encryption key on AhsayOBM or AhsayACB

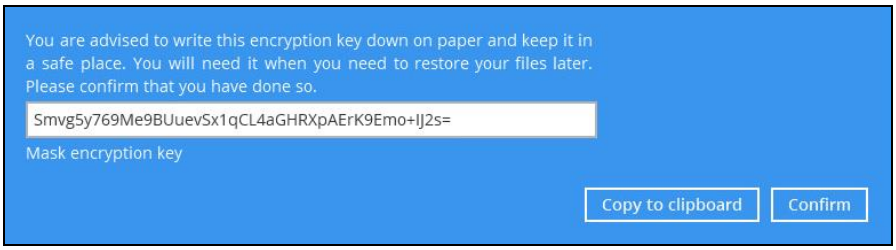
Click **Next** when you are done setting.

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:

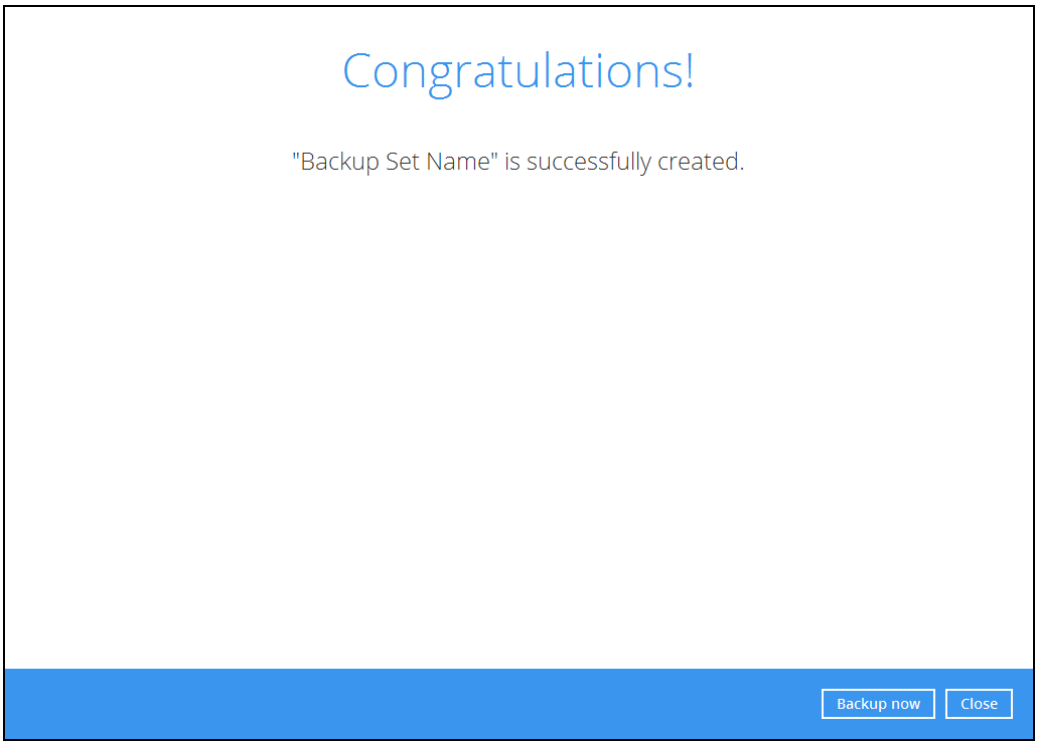
- **Unmask encryption key** – The encryption key is masked by default. Click this option to show the encryption key.



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

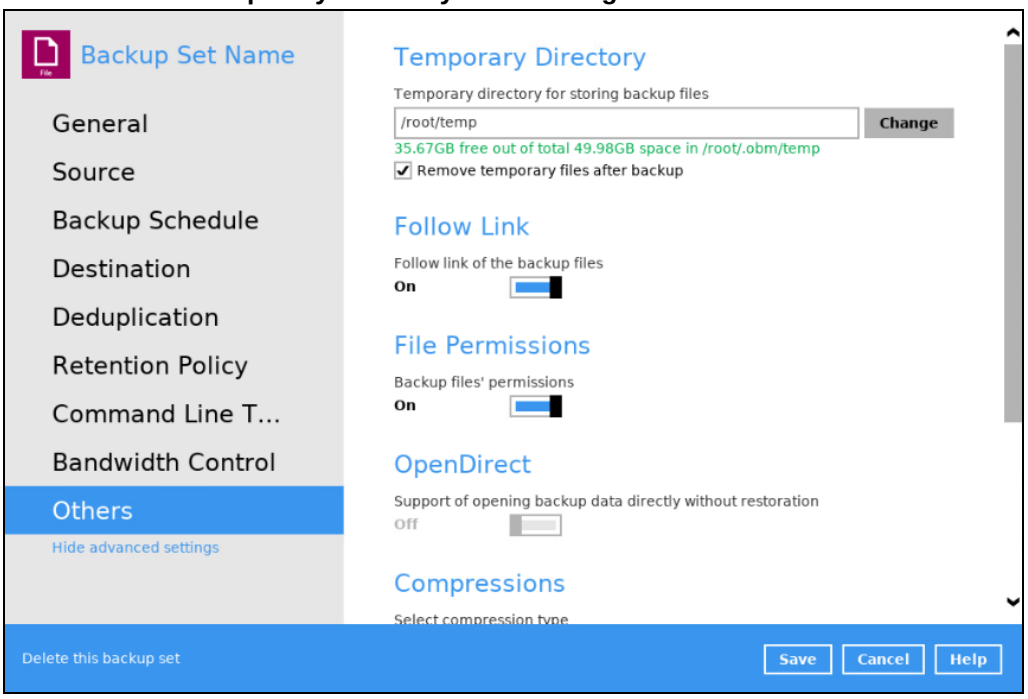
- **Confirm** – Click to exit this pop-up window and proceed to the next step.

15. The following screen shows when the new backup set is created successfully.



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

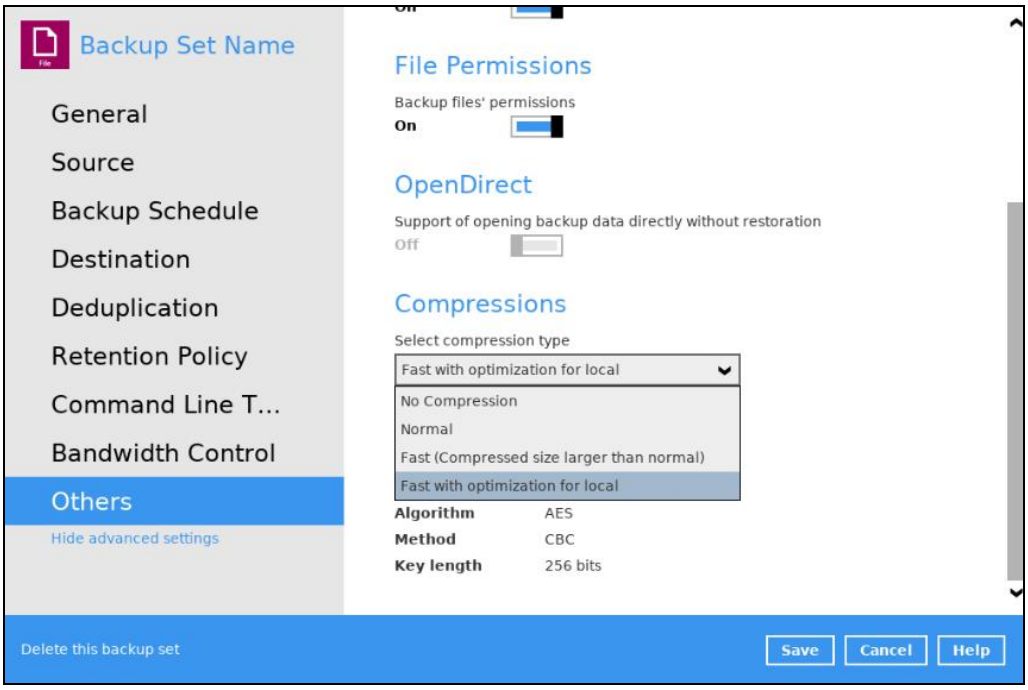
Go to **Others** > **Temporary Directory**. Click **Change** to browse for another location.



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

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

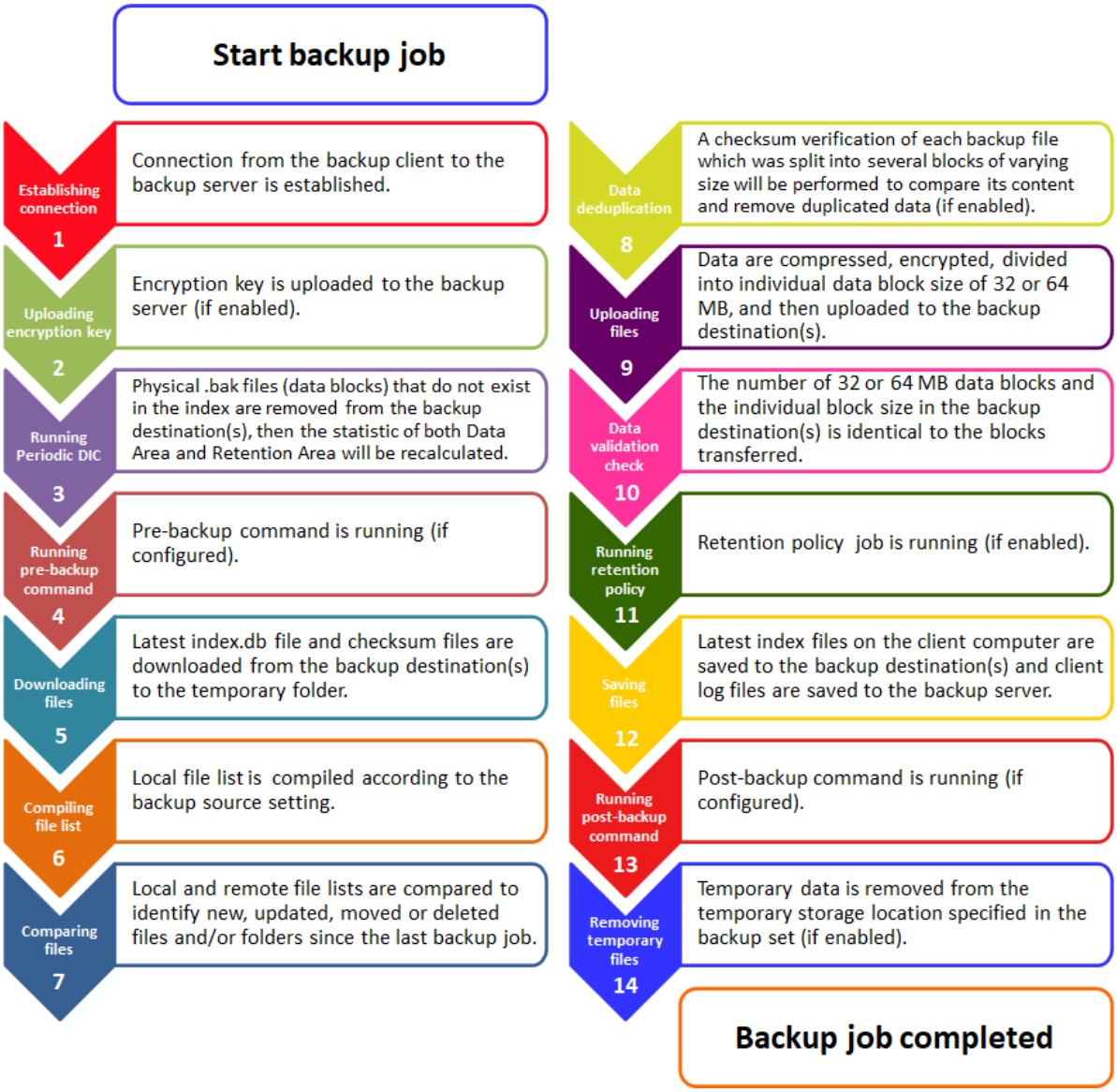
- No Compression
- Normal
- Fast (Compressed size larger than normal)
- Fast with optimization for local



11 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)**



11.1 Periodic Data Integrity Check (PDIC) Process

The PDIC will run on the first backup job that falls on the corresponding day of the week from **Monday to Friday**.

To minimize the impact of the potential load of large number of PDIC jobs running 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:

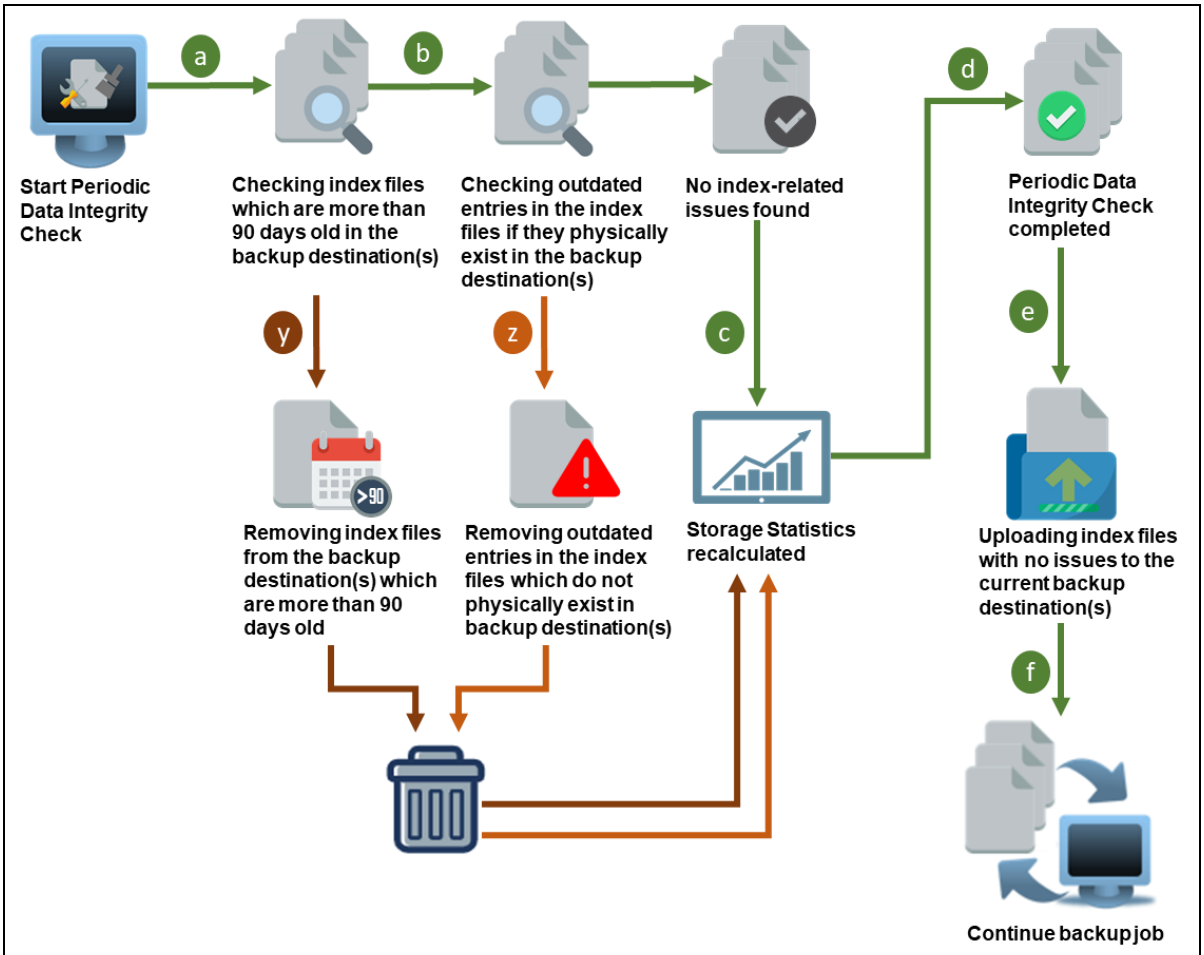
- the PDIC will run on the first backup job that falls on Wednesday; or
- if there is no active backup job(s) running from Monday to Friday, then the PDIC will run on the next available backup job.

NOTE

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

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

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

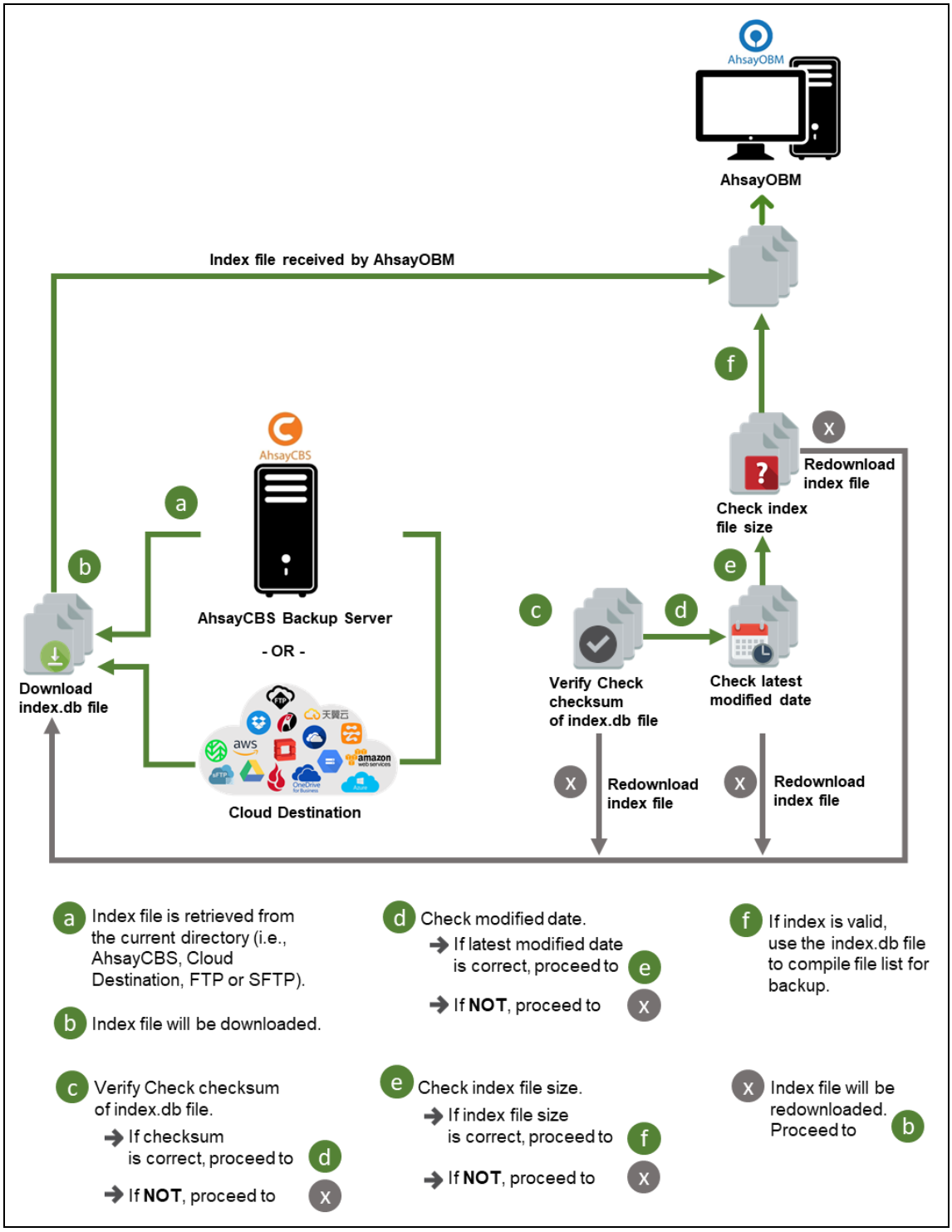
y Index files which are more than 90 days old will be removed from the backup destination(s).

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

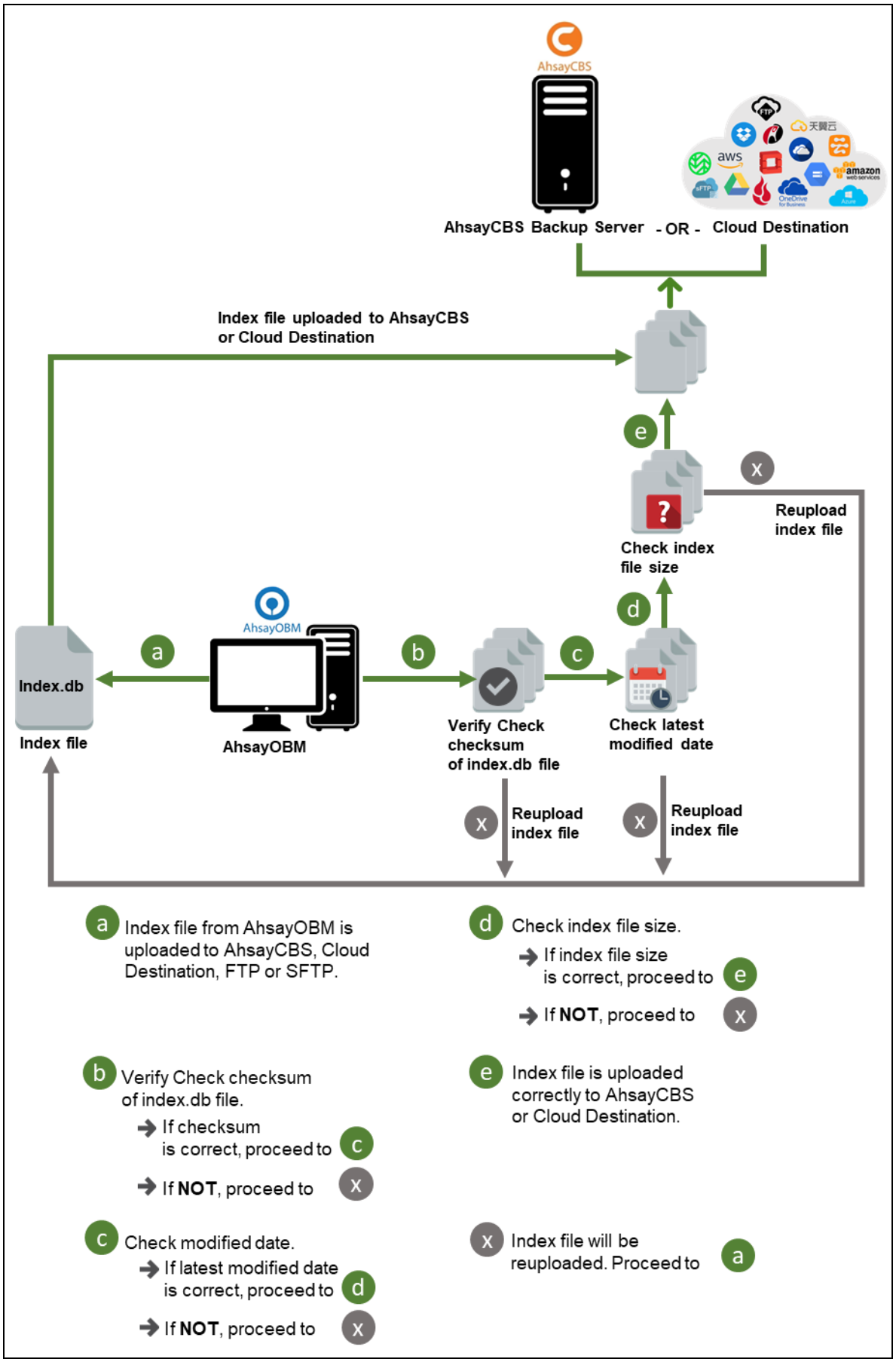
11.2 Backup Set Index Handling Process

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

11.2.1 Start Backup Job

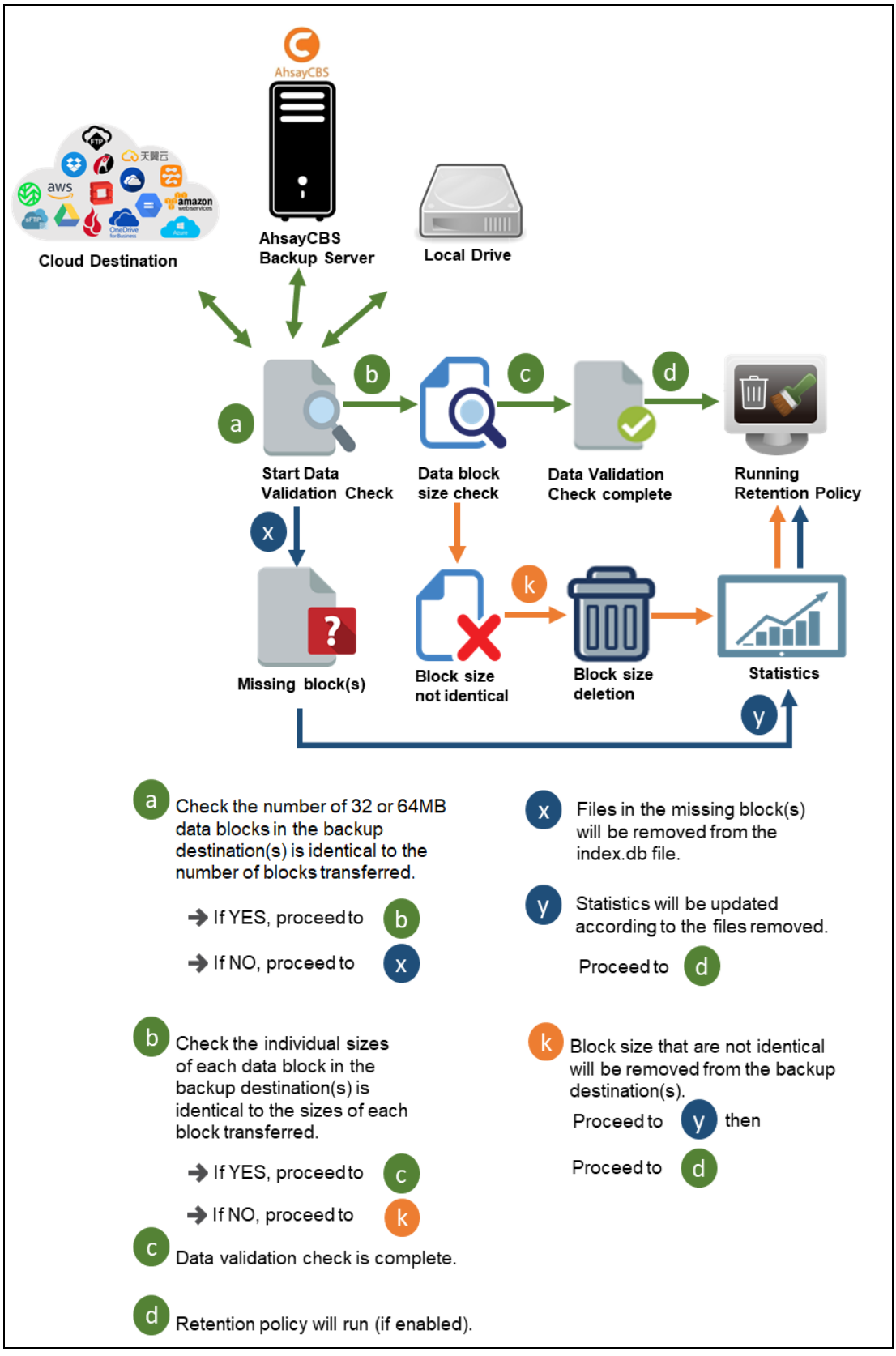


11.2.2 Completed Backup Job



11.3 Data Validation Check Process

As an additional measure to ensure that all files transferred to the backup destination(s) are received and saved correctly, both the number of 32 or 64 MB data block files and the size of each block file are checked again after the files are transferred.



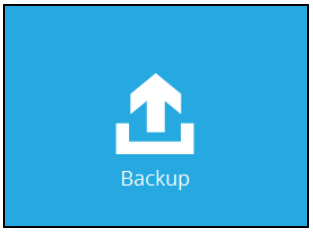
12 Running Backup Jobs

12.1 Login to AhsayOBM

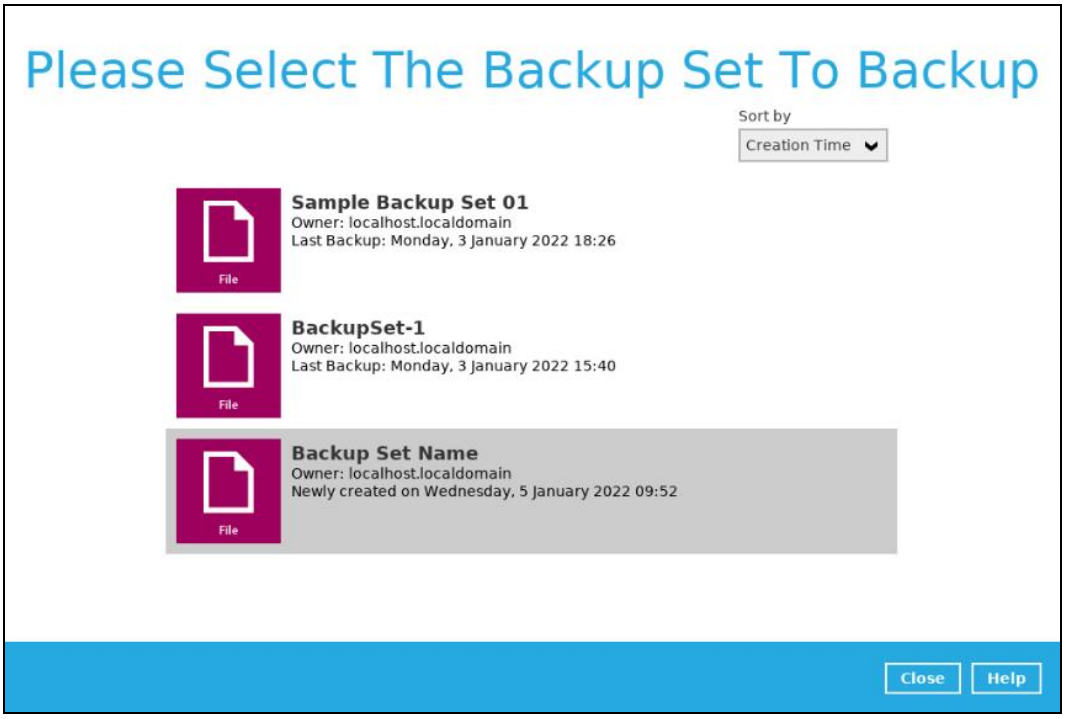
Login to the AhsayOBM application according to the instructions in Chapter 7: Logging in to AhsayOBM.

12.2 Start a Manual Backup

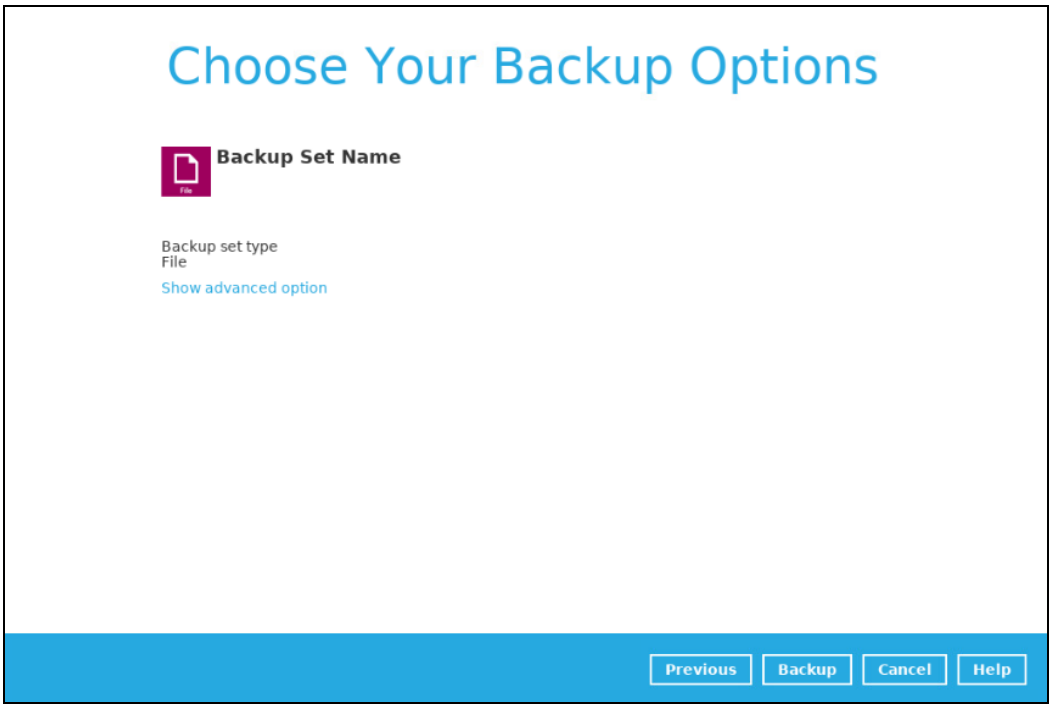
1. Click **Backup** on the main interface of AhsayOBM.



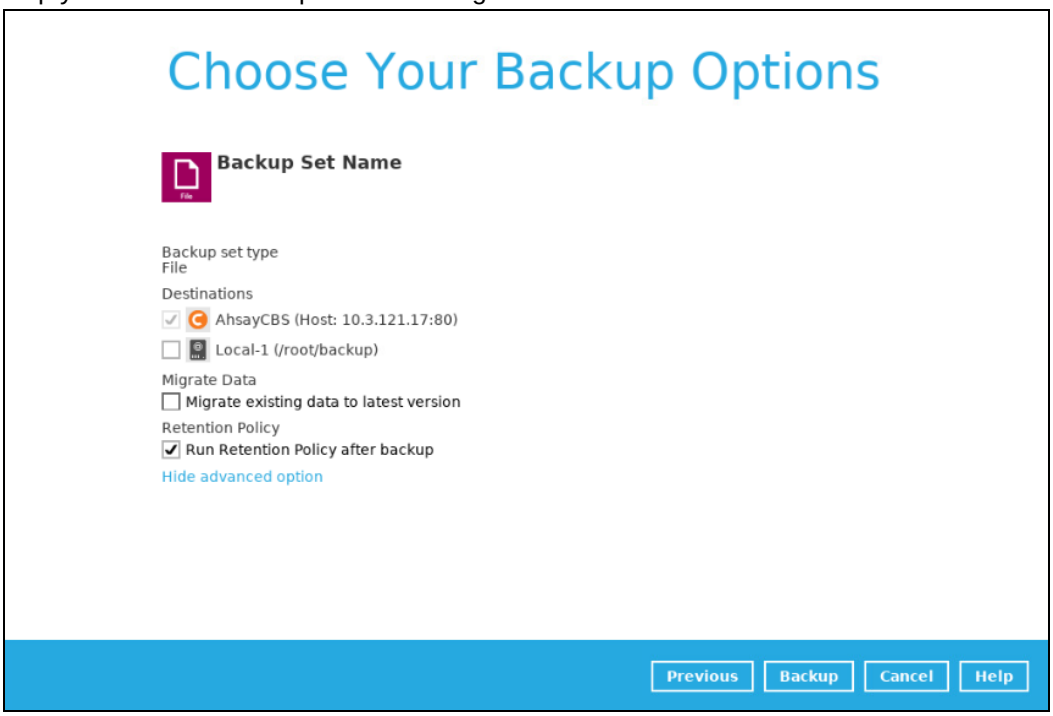
2. Select the backup set which you would like to start a backup for.



3. In case you want to modify the Destinations, Migrate Data and Retention Policy settings, click **Show advanced option**.



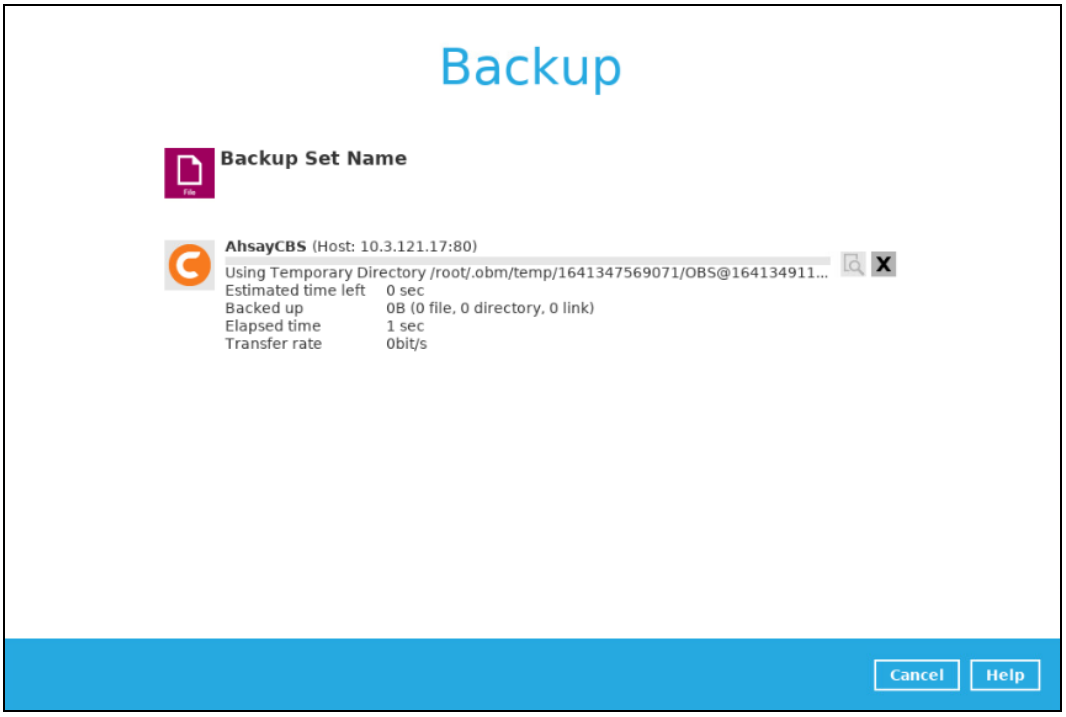
4. When advanced options are shown, it is recommended that you tick the checkbox next to **Run Retention Policy after backup** in the Retention Policy section at the bottom. This will help you save hard disk quota in the long run.



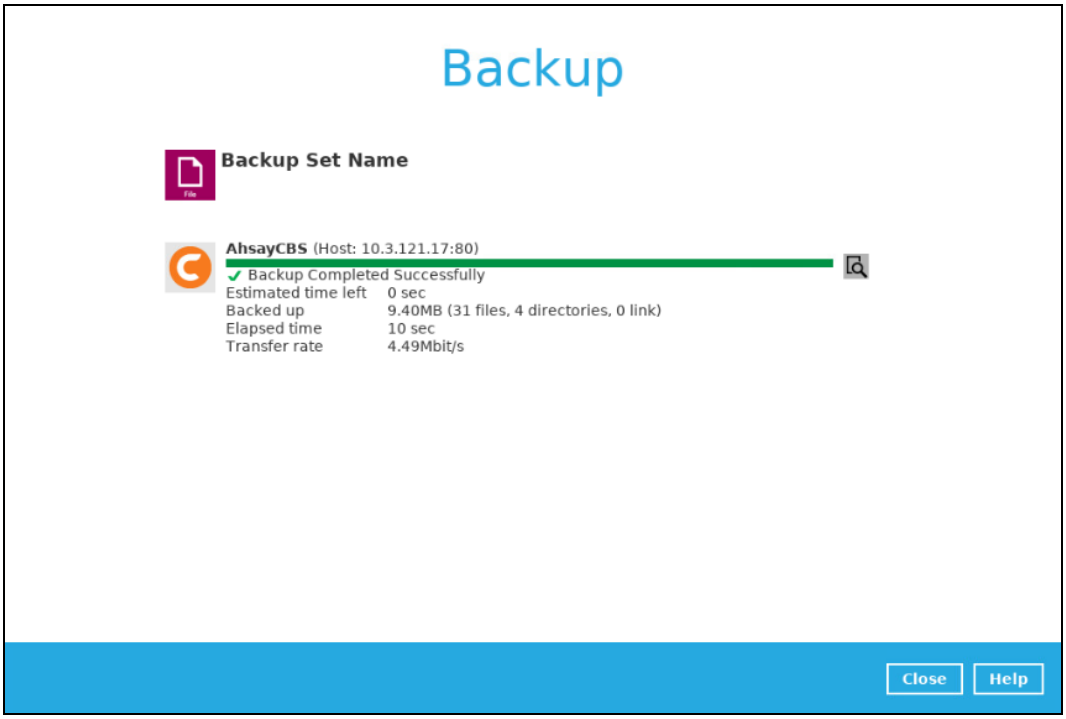
NOTE

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

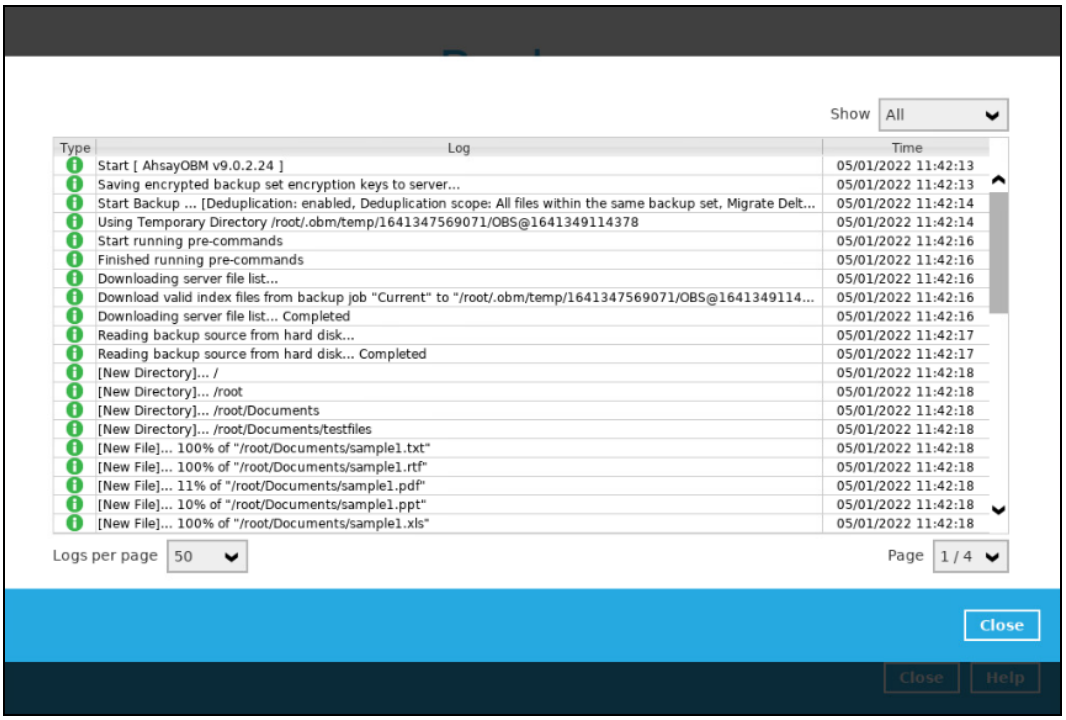
5. Click **Backup** to start the backup. The status will be displayed.



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



7. 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.



13 Restoring Data

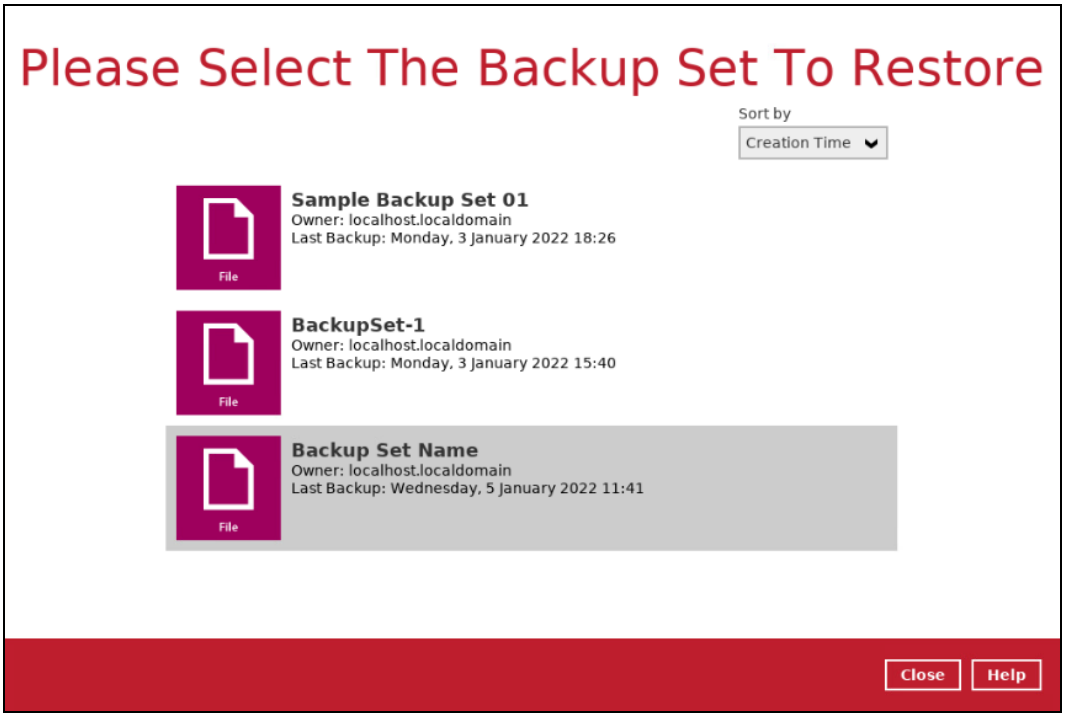
13.1 Login to AhsayOBM

Login to the AhsayOBM application according to the instructions in Chapter 7: Logging in to AhsayOBM.

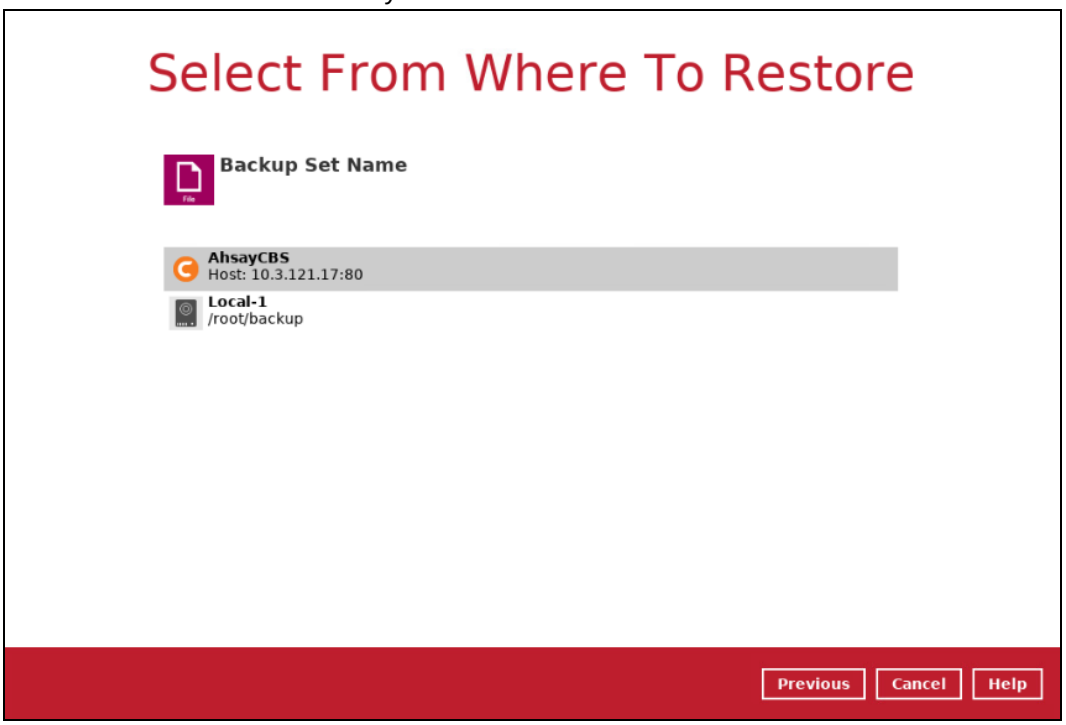
13.2 Restore Data

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

2. After logging in to your backup account successfully, you should see a screen showing all the available backup sets for restore. Double click on the one you would like to restore.



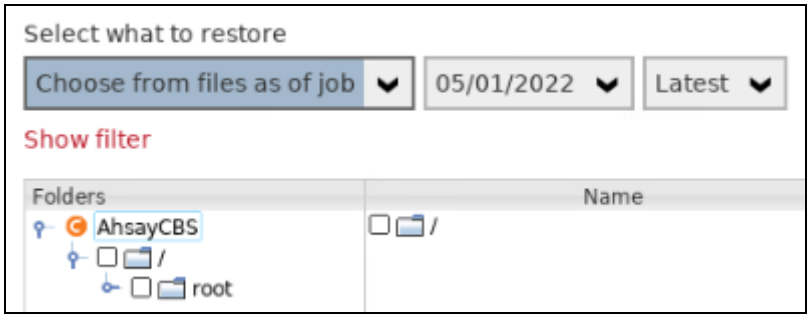
3. Click on the location from which you would like to restore the data from.

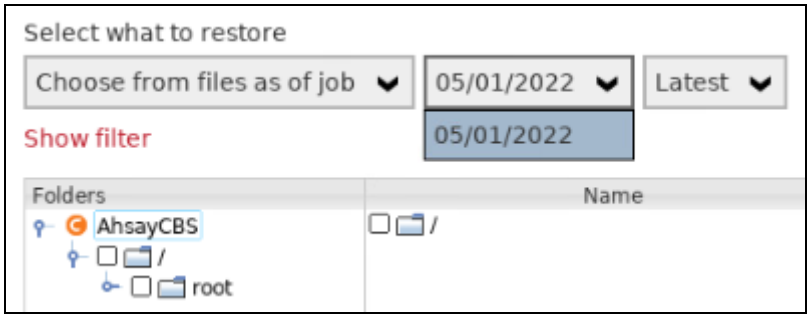


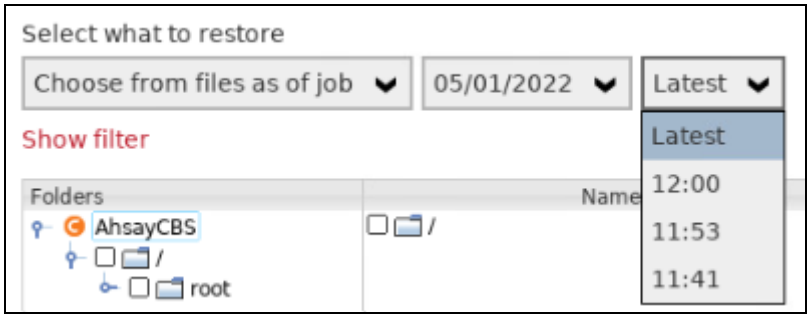
4. Select to restore files from a specific backup job, or from all files available, then select the files or folders that you would like to restore.

There are two options from the **Select what to restore** drop-down menu:

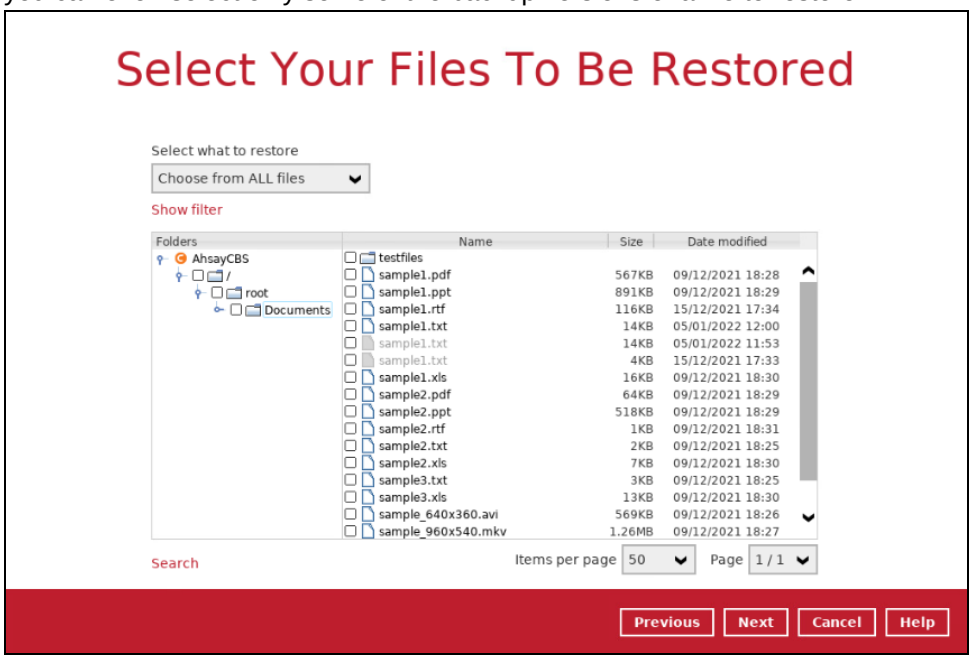
- **Choose from files as of job** – this option allows you to select a backup version from a specific date and time to restore.



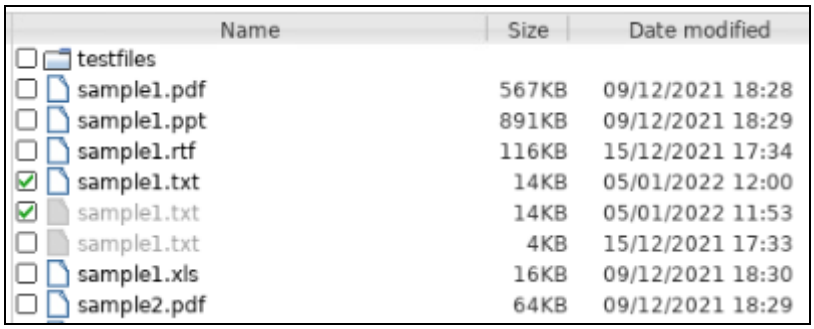




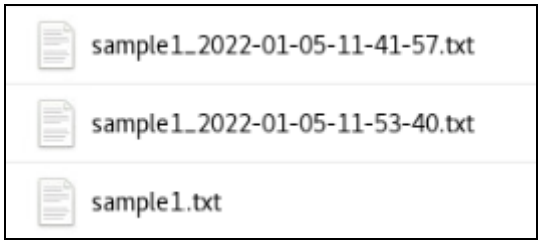
- **Choose from ALL files** – this option allows you to restore all the available backup versions for this backup set. Among all the available backup versions, you can even select only some of the backup versions of a file to restore.



Below is an example showing all the available backup versions of the file **sample1.txt**. The latest version is shown in solid black color and all the previous versions are shown in grey color. You can identify the file version from the **Date modified** column.



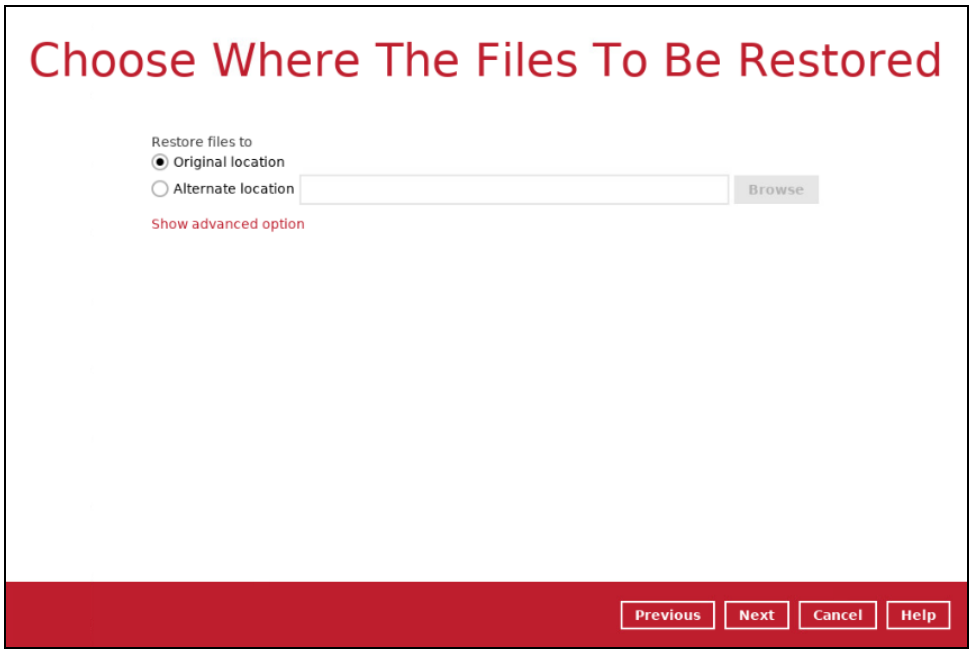
When the restore is done, you will see all the selected backup versions in the restore destination. The latest backup version has the file name as the original file, while the previous versions have the time stamps added to their file names for easy identification.



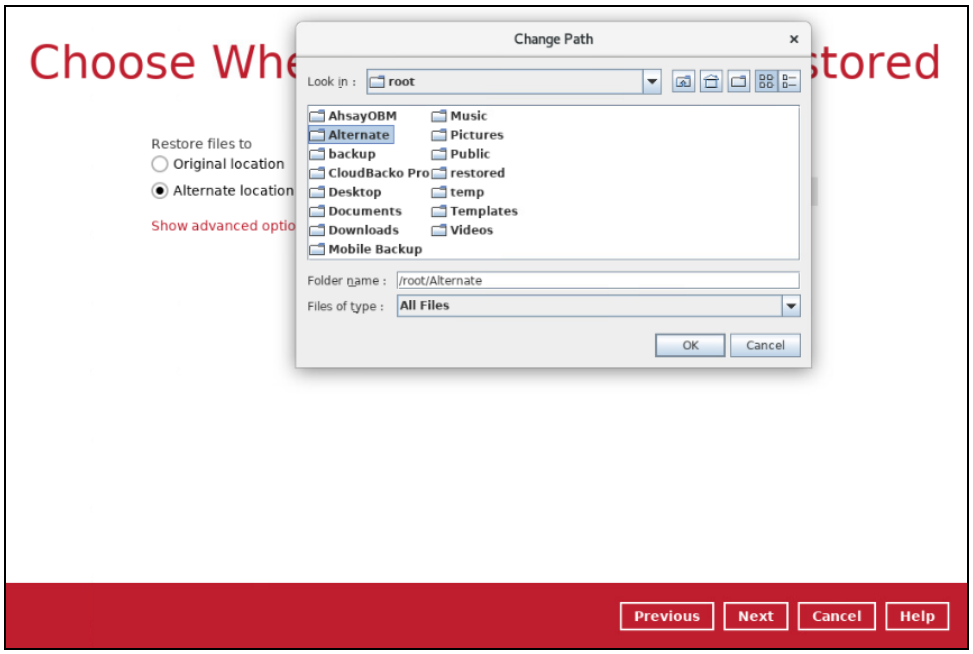
Click **Next** to proceed when you are done with the selections.

5. Select to restore the files to their **Original location**, or to an **Alternate location**.

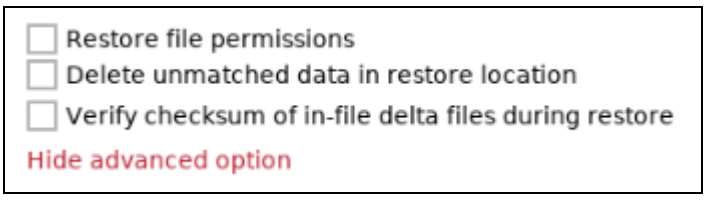
- **Original location** – the backed-up data will be restored to the computer running the AhsayOBM under the same directory path as on the machine storing the backup source. For example, if the backup source files are stored under **root/Downloads** folder, the data will be restored to **root/Downloads** as well on the computer running the AhsayOBM.



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



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



- **Restore file permissions**

  By enabling this option, file permissions of the operating system files will be restored. File permission defines, for example, the right to view or change a file by the system owner/group/individual. If file permission is not restored properly, there is a potential risk that the restored data could be viewed by group/individual who is not supposed to have the access to.

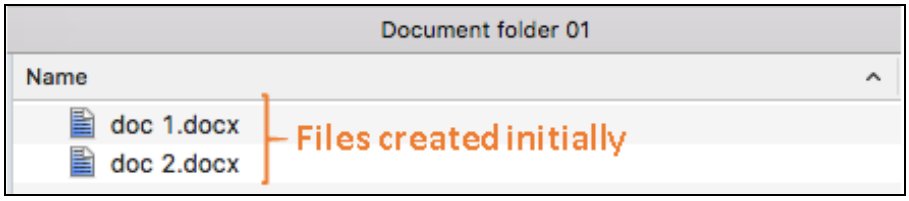
- **Delete unmatched data in restore location**

  By enabling this option, the restore process will attempt to synchronize the selected restore source with the restore destination, making sure the data in the restore destination is exactly the same as the restore source. Any data created

after backup will be treated as “unmatched data” and will be deleted from the restore source if this feature is enabled.

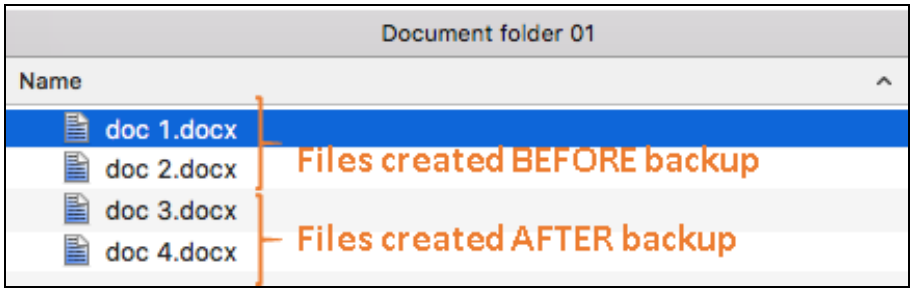
Example:

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



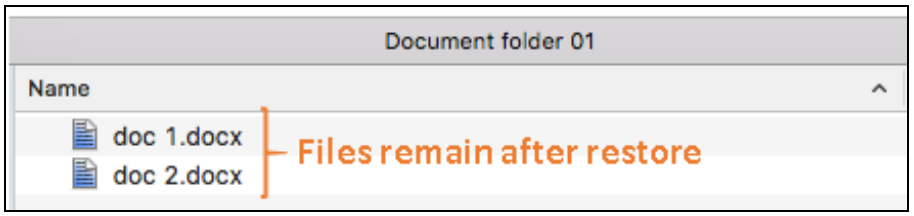
ii) A backup is performed for folder **Document folder 01**.

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.

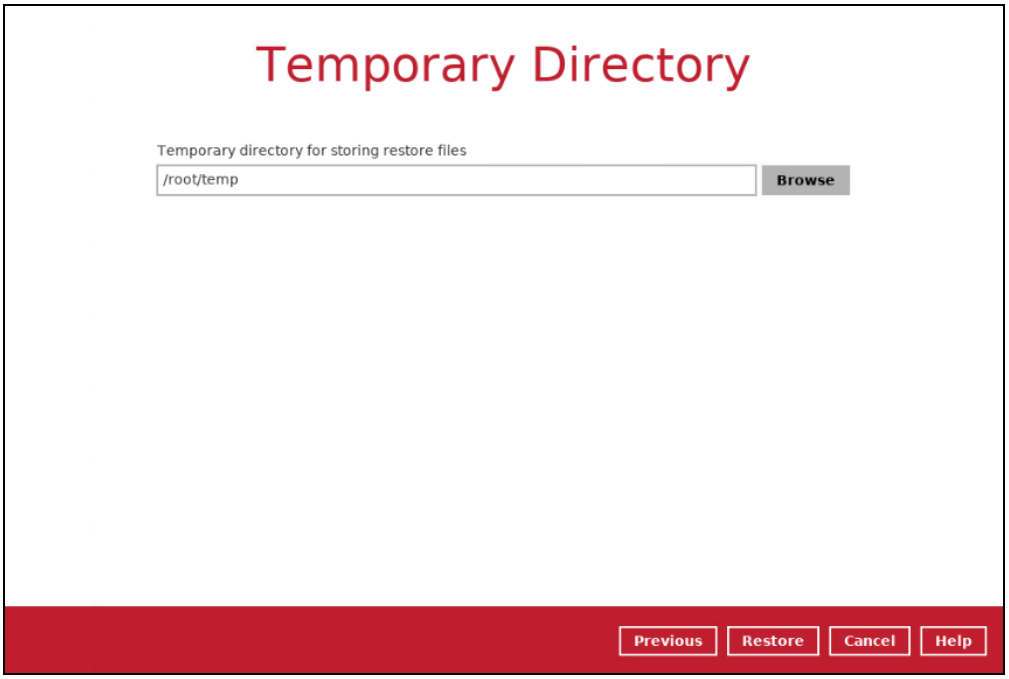
Prior to the data restore and synchronization, a warning message will be displayed. Only clicking **Yes** will the “unmatched data” be deleted. You can click **Apply to all** to confirm deleting all the “unmatched data” at one time.

- **Verify checksum of in-file delta files during restore**
  By enabling this option, the checksum of in-file delta files will be verified during the restore process. This will check the data for errors during the restore process and create a data summary of the in-file delta files which will be included in the report.

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

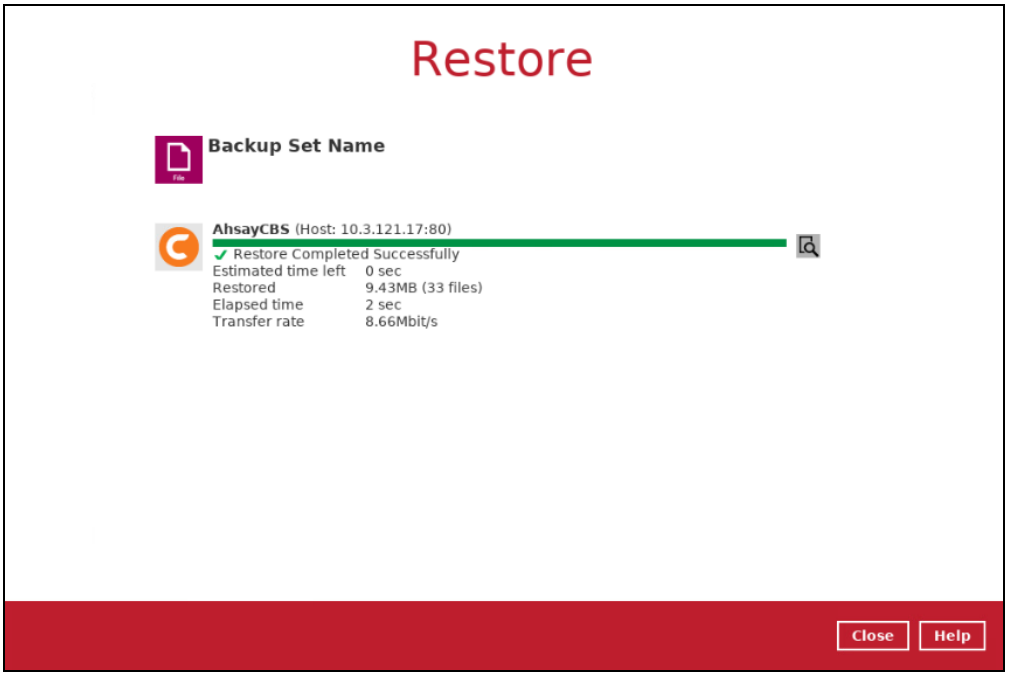
6. Select the temporary directory for storing temporary files, such as delta files when they are being merged.

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



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

8. The progress bar shows **Restore Completed Successfully** when the restore is done. Click **Close** to exit.



13.3 Restore Filter

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

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

- **Contains**

  These are Directories, Files, and Folders with the name **containing** the specific letter or word.

- **Exact**

  These are Directories, Files, and Folders with the **exact** or **accurate** name.

- **Start With**

  These are Directories, Files, and Folders with the name **starting** with a specific letter or word.

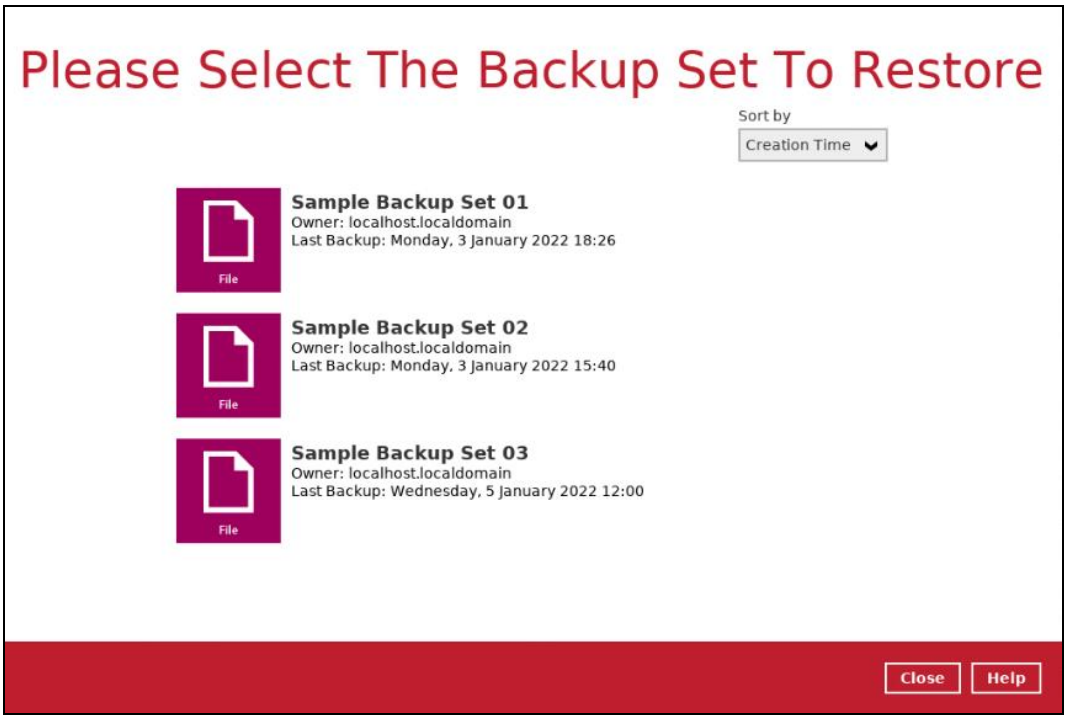
- **Ends With**

  These are Directories, Files, and Folders with the name **ending** with a specific letter or word.

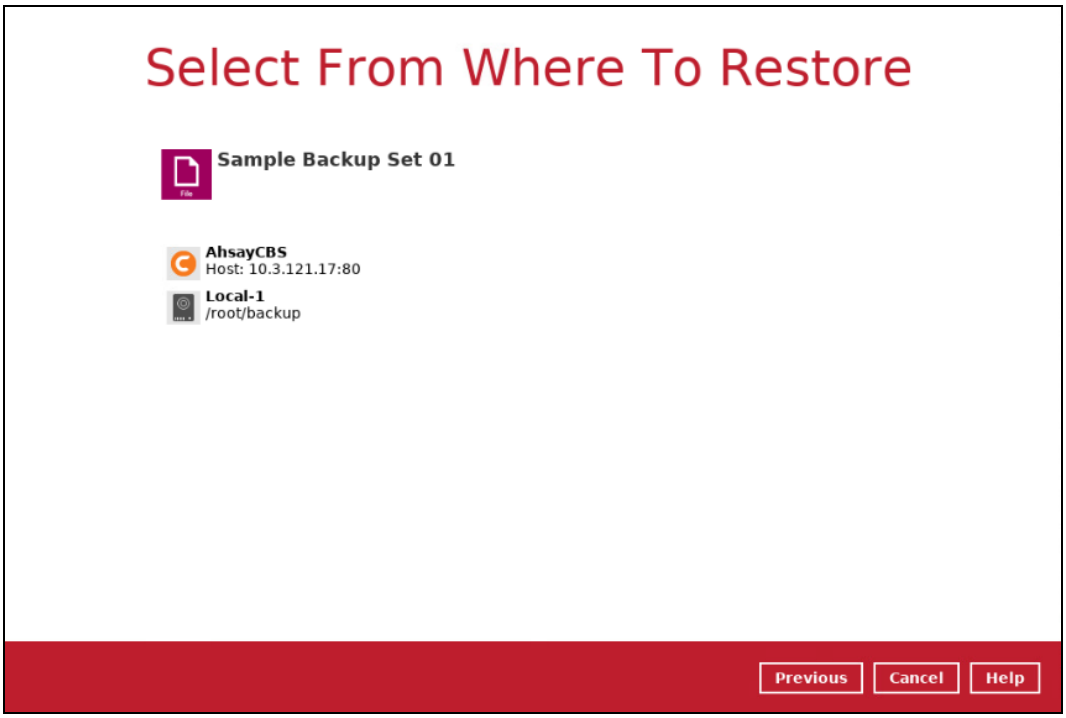
It also has the **Match Case** function, which serves as an additional accuracy when searching for any specific directories, files, folders, and mails.

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

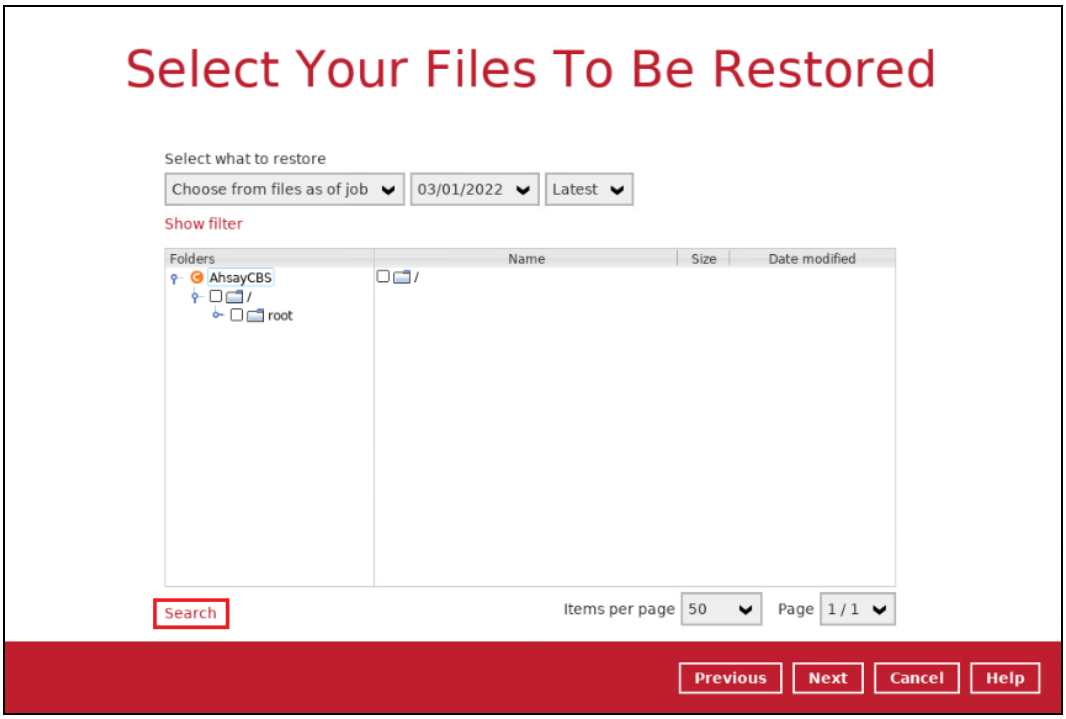
1. Login to AhsayOBM according to the instructions in Logging in to AhsayOBM.
2. Click the **Restore** icon on the main interface of AhsayOBM.
3. Select the backup set that you would like to restore.



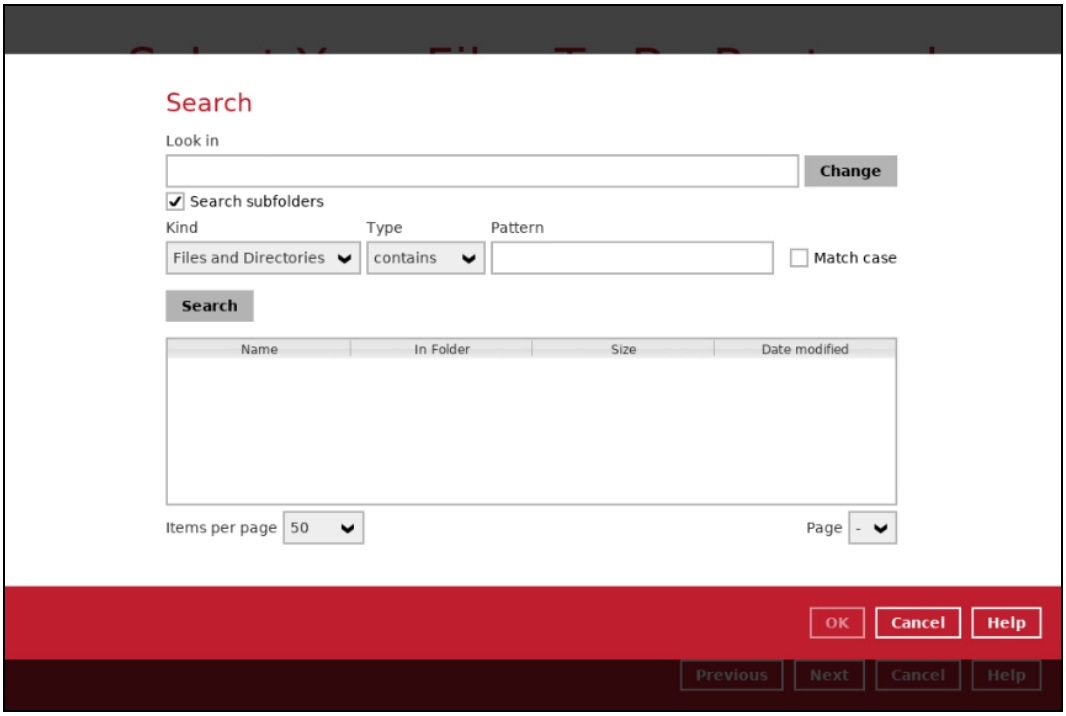
4. Select the backup destination that you would like to restore backed-up items to.

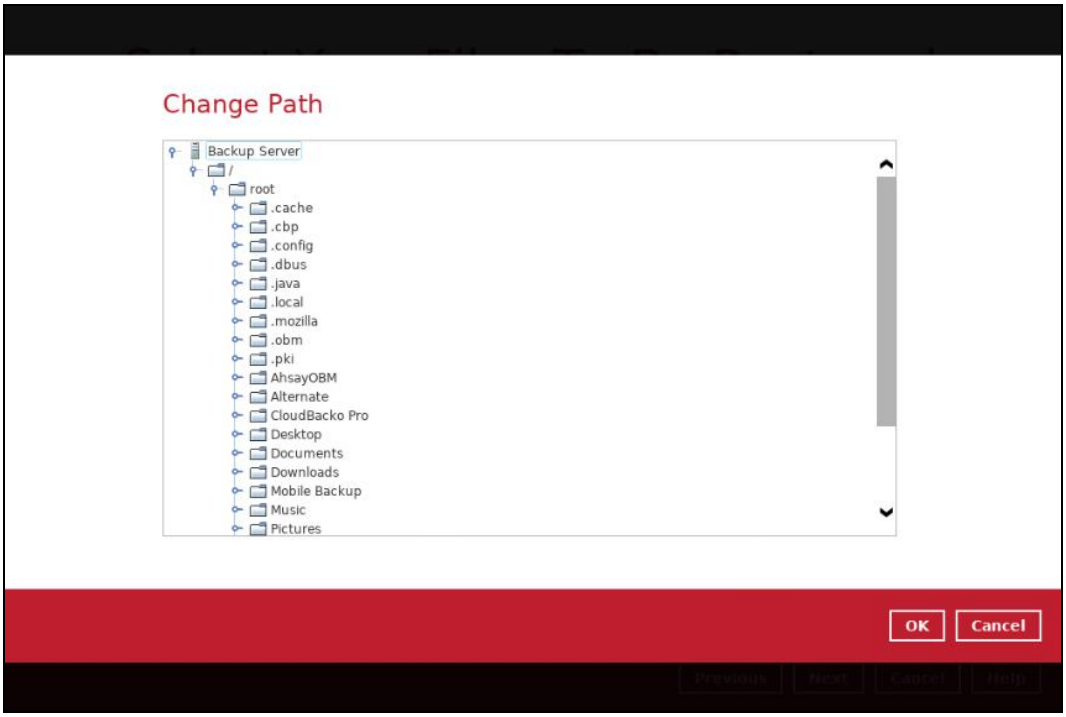


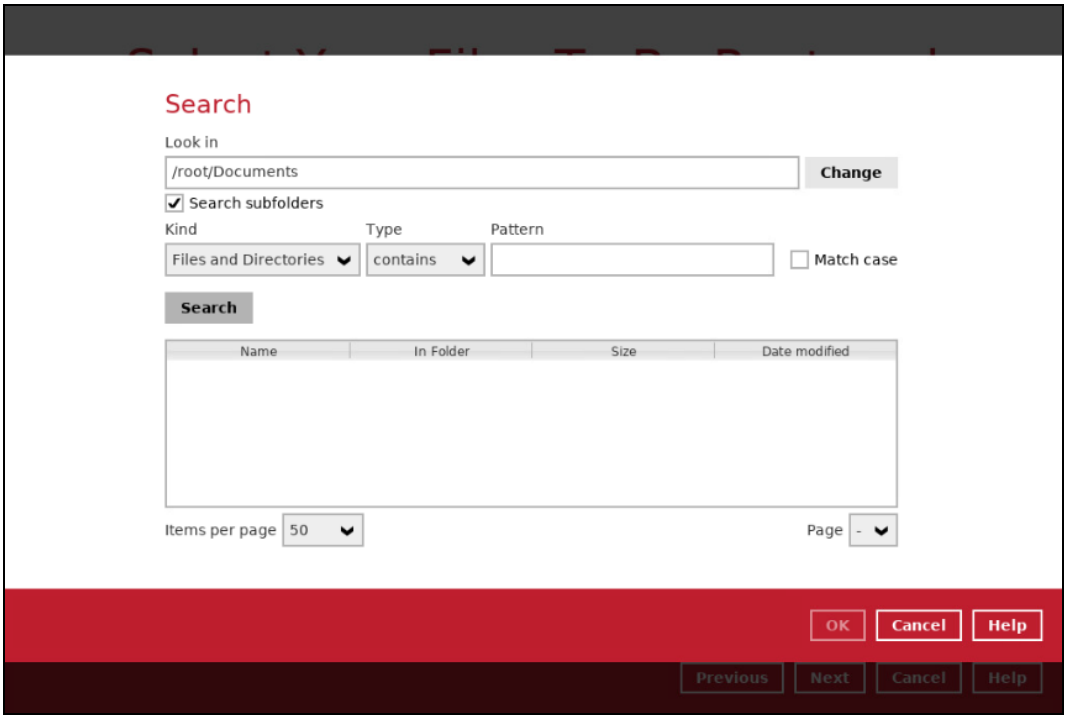
5. Click **Search** located on the lower left side of the screen.



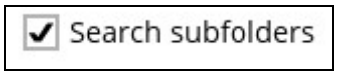
6. Click the **Change** button to change the path of the restore items to other location.



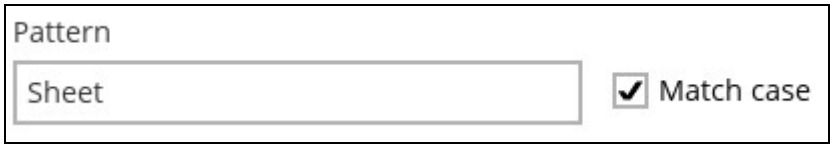

Change Path
Backup Server
/
root
.cache
.cbp
.config
.dbus
.java
.local
.mozilla
.obm
.pki
AhsayOBM
Alternate
CloudBacko Pro
Desktop
Documents
Downloads
Mobile Backup
Music
Pictures
OK
Cancel


Search
Look in
/root/Documents
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
Previous
Next
Cancel
Help

7. Tick “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.

14 Contacting Ahsay

14.1 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/

14.2 Documentation

Documentations for all Ahsay products are available at:
https://www.ahsay.com/jsp/en/home/index.jsp?pageContentKey=ahsay_downloads_documentation_guides

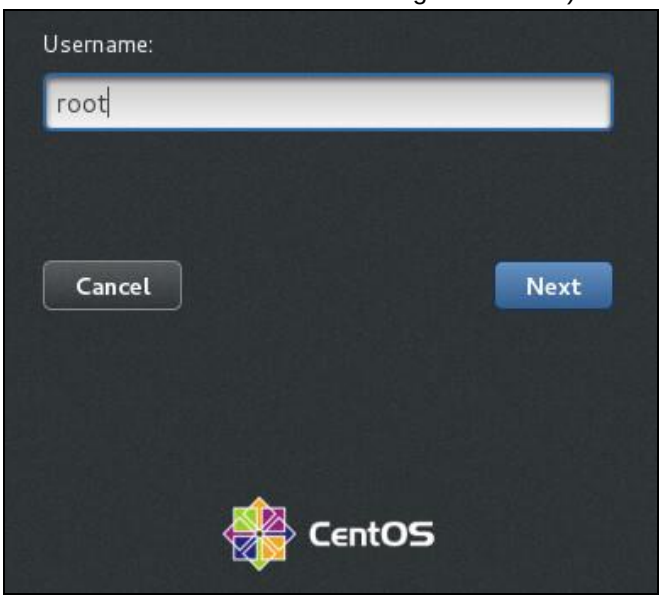
You can send us suggestions for improvements or report on issues in the documentation, by contacting us at:
https://www.ahsay.com/partners/

Please specify the specific document title as well as the change required/suggestion when contacting us.

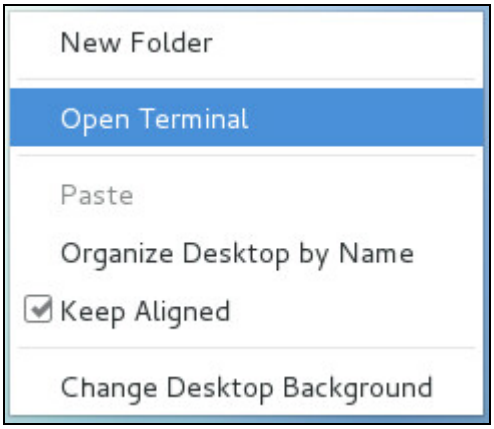
Appendix

Appendix A: Uninstall AhsayOBM (SH online installer)

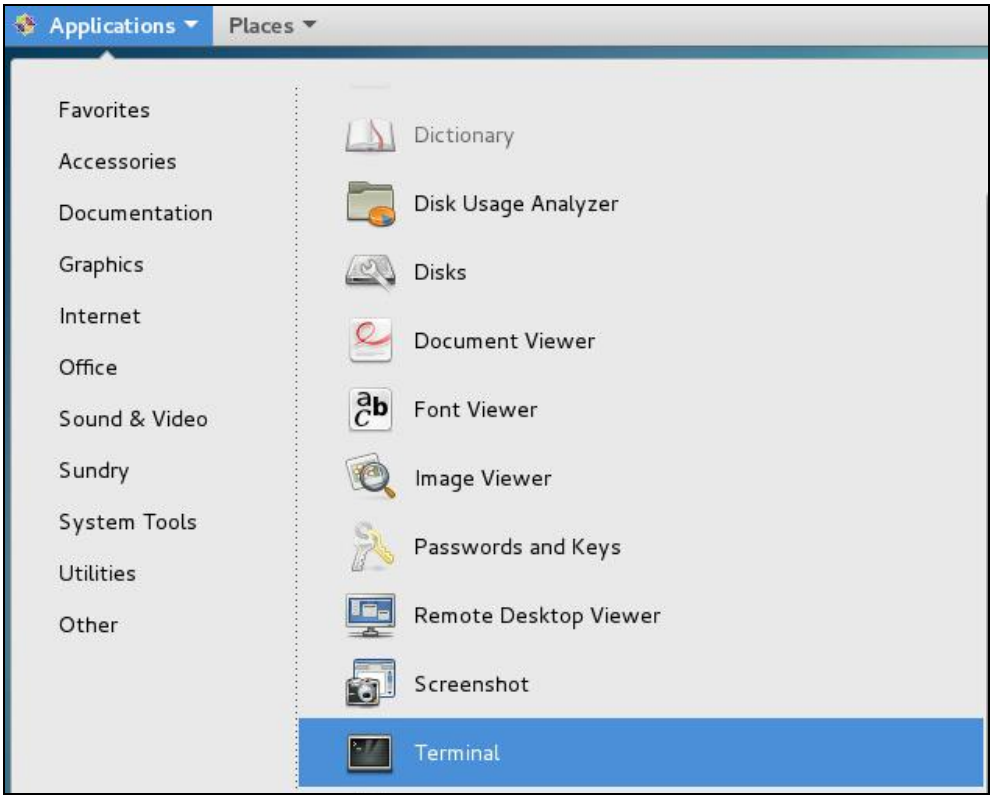
1. Log in to a Linux machine using the root account. (Alternatively, you can remotely invoke the GUI of another Linux machine using SSH client.)



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



Alternatively, you can also click the **Applications** menu bar then select **Utilities > Terminal**.



3. Go to the **/usr/local/obm/bin** directory.

```
# cd /usr/local/obm/bin
```

4. Use the **uninstall.sh** script, then run the **rm** command to remove the remaining AhsayOBM files from the Linux machine.

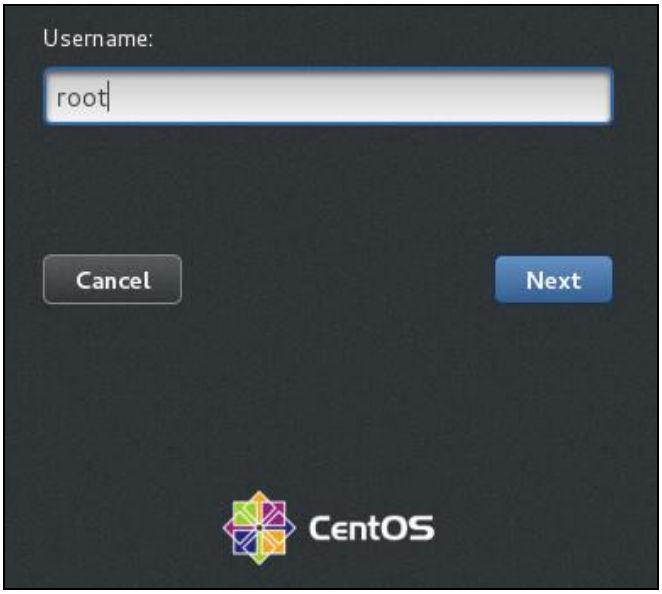
```
# sh uninstall.sh
Log Time: Mon Dec 27 16:43:07 HKT 2021

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

Uninstall Ahsay Online Backup Manager from /usr/local/obm

Shutting down Scheduler
Wait 5 seconds before Scheduler exits
Kill running Ahsay Online Backup Manager
Kill Process by Image Name: /usr/local/obm/jvm/bin/bJW
Ignore Process by Image Name:
Kill Process by Image Name: /usr/local/obm/jvm/bin/bschJW
Ignore Process by Image Name:
Kill Process by Image Name: /usr/local/obm/jvm/bin/java
Ignore Process by Image Name:
Removing Scheduler script obmscheduler from service
Uninstall Service for NIX type OS
Using init script path /etc/init.d
Using run level script path /etc/rc.d
Removing symbolic link from run levels
```

```
Removing script file obmscheduler from /etc/init.d
Remove shortcut /usr/share/applications/obm.desktop
Remove shortcut /root/Desktop/obm.desktop
Ahsay Online Backup Manager uninstall procedure is complete!
It is now safe to remove files from /usr/local/obm
# rm -fr /usr/local/obm
```

5. After successful uninstallation, AhsayOBM will be removed from the **Applications**.

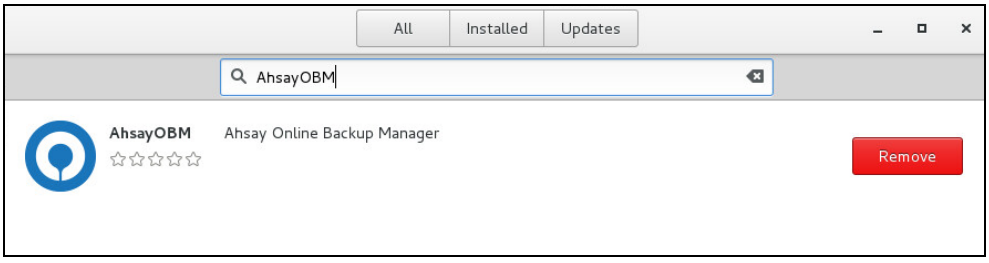
Appendix B: Uninstall AhsayOBM (RPM online installer)

1. Log in to a Linux machine using the root account. (Alternatively, you can remotely invoke the GUI of another Linux machine using SSH client.)



2. Under the **Applications** menu bar, select **System Tools > Application Installer**.

3. Search for “AhsayOBM” on the search bar, then click the **Remove** button to proceed.

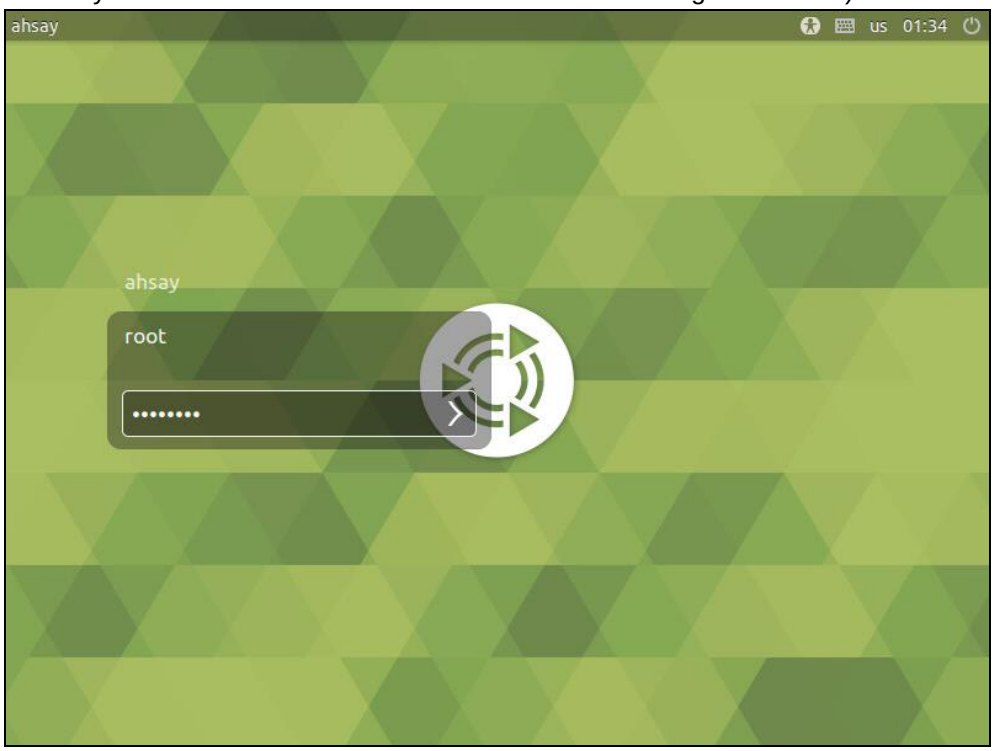


4. Click **Remove** to uninstall AhsayOBM.

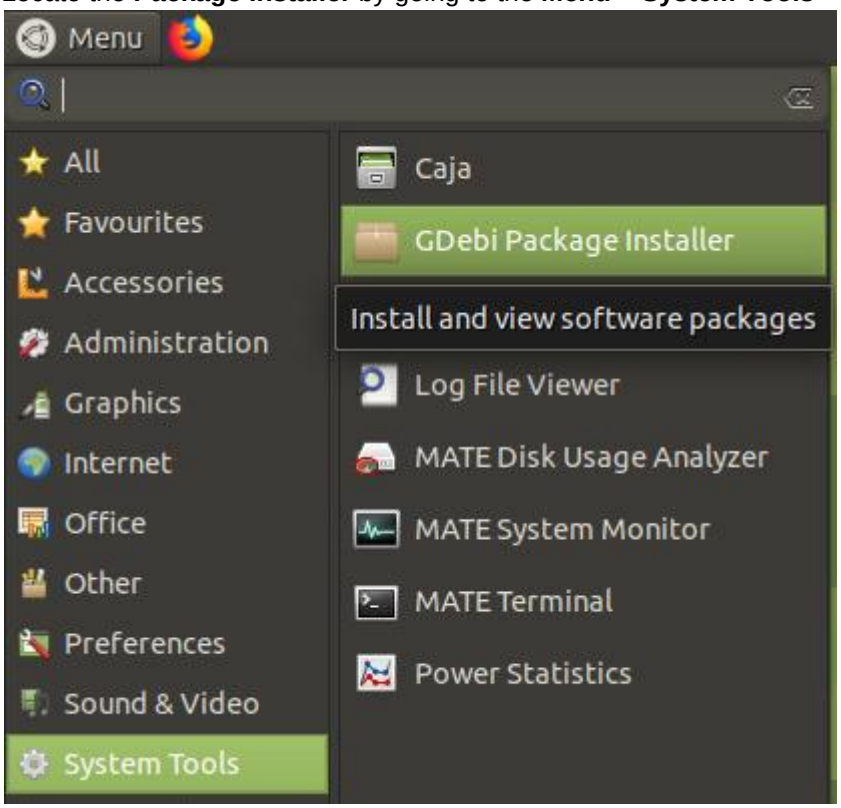
5. After successful uninstallation, AhsayOBM will be removed from the **Applications**.

Appendix C: Uninstall AhsayOBM (DEB online installer)

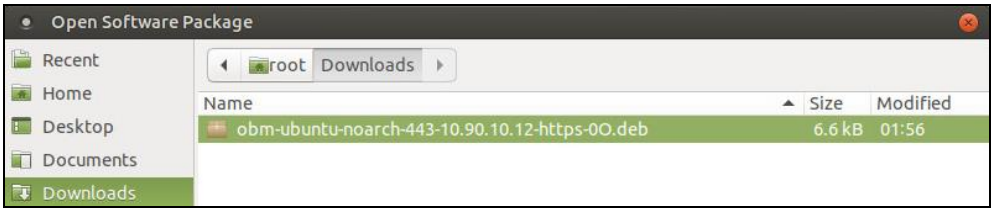
1. Log in to a Debian or Ubuntu machine using the root account. (Alternatively, you can remotely invoke the GUI of another Debian or Ubuntu using SSH client.)



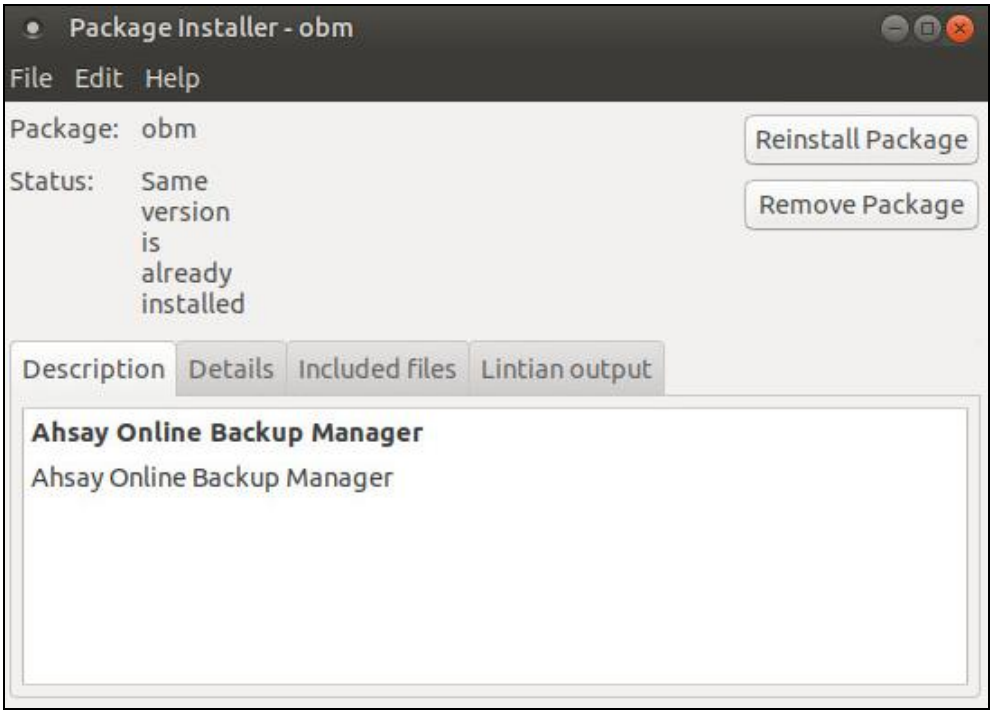
2. Locate the **Package Installer** by going to the **Menu > System Tools > Package Installer**.



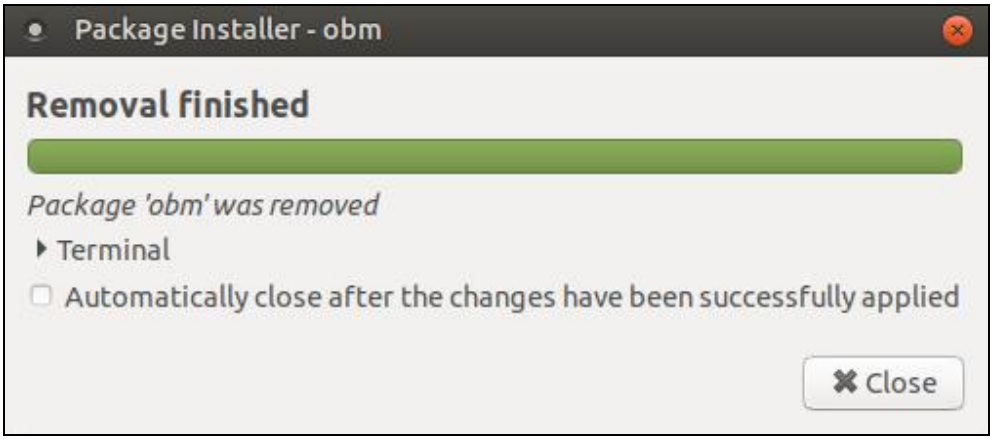
3. Go to **Downloads** and select the AhsayOBM **DEB** installation package file.



4. When the following screen is displayed, click **Remove Package** to proceed.



5. Once the uninstallation is completed, the following screen will be displayed. AhsayOBM is now removed from the **Applications**.



Appendix D: Handling of Non-regular Files

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

Example:
/proc
/dev
/sys
/run

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

Appendix E: Script Files

RunConfigurator.sh

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

```
# vi RunConfigurator.sh
```

Configure the following parameters:

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

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

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

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

```
# vi RunConfigurator.sh



#!/bin/sh



############################## RunConfigurator.sh
###############################

# You can use this shell to run the application
#

#######################################################################
########



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



# ------------------------------- SETTING_HOME -------------------------
--------

# | Directory to your setting home.
|

# | Default to ${HOME}/.obm when not set.
|

# | e.g. SETTING_HOME="${HOME}/.obm"
|
```

```
# ------------------------------------------------------------------------
--------

SETTING_HOME=""


# --------------------------------- DEBUG_MODE -------------------------
--------

# | Enable/Disable debug mode
|

# | e.g. DEBUG_MODE="--debug"
|

# |  or  DEBUG_MODE=""
|

# ------------------------------------------------------------------------
--------

DEBUG_MODE=""


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




################################################################################
########

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

################################################################################
########



EXE_DIR=`pwd`

SCRIPT_HOME=`dirname "$0"`

cd "$SCRIPT_HOME"

APP_BIN=`pwd`

APP_HOME=`dirname "$APP_BIN"`



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

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

#############################################################################
########


if [ "Darwin" = `uname` ]; then

    JAVA_HOME="/System/Library/Frameworks/JavaVM.framework/Home"

fi


if [ ! -x "$APP_HOME/jvm" ];

then

    echo "'$APP_HOME/jvm' does not exist!"

    if [ ! -n "$JAVA_HOME" ]; then

        echo "Please set JAVA_HOME!"

        exit 0

    else

        ln -sf "$JAVA_HOME" "$APP_HOME/jvm"

        echo "Created JAVA_HOME symbolic link at '$APP_HOME/jvm'"

    fi

fi


if [ ! -x "$APP_HOME/jvm" ];

then

    echo "Please create symbolic link for '$JAVA_HOME' to
'$APP_HOME/jvm'"

    exit 0

fi


JAVA_HOME="$APP_HOME/jvm"


# Use alternative executable name to define the GUI execution
```

```
if [ "Darwin" = `uname` ]; then

    JAVA_EXE="$JAVA_HOME/bin/java"

else

    JAVA_EXE="$JAVA_HOME/bin/bJW"

fi



# Verify the JAVA_EXE whether it is a valid JAVA Executable or not.

STRING_JAVA_VERSION="java version,openjdk version"

OUTPUT_JAVA_VERSION=`"${JAVA_EXE}" -version 2>&1`

OUTPUT_JVM_SUPPORT=0

BACKUP_IFS=$IFS

IFS=","

for word in $STRING_JAVA_VERSION; do

    if [ `echo "${OUTPUT_JAVA_VERSION}" | grep "${word}" | grep -cv
"grep ${word}"` -le 0 ]

    then

      #echo "The Java Executable \"${JAVA_EXE}\" is not a valid Java
Executable. Exit \""`basename "$0"`"\" now."

      continue;

    else

      OUTPUT_JVM_SUPPORT=1

      break;

    fi

done

IFS=$BACKUP_IFS

if [ $OUTPUT_JVM_SUPPORT -eq 0 ]

then

    echo "The Java Executable \"${JAVA_EXE}\" is not a valid Java
Executable. Exit \""`basename "$0"`"\" now."

    exit 1

fi
```

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

#                              S T A R T - U P
#

##########################################################################
########




# Set LD_LIBRARY_PATH for Lotus Notes on Linux

if [ "Linux" = `uname` ]; then

    NOTES_PROGRAM=`cat "$APP_HOME/bin/notesenv"`

    LD_LIBRARY_PATH="$APP_HOME/bin:$NOTES_PROGRAM:$LD_LIBRARY_PATH"

    export NOTES_PROGRAM

else

    LD_LIBRARY_PATH="$APP_HOME/bin:$LD_LIBRARY_PATH"

fi


DEP_LIB_PATH="X64"

case "`uname -m`" in

    i[3-6]86)

        DEP_LIB_PATH="X86"

    ;;

esac

LD_LIBRARY_PATH="${APP_BIN}/${DEP_LIB_PATH}":".":"${LD_LIBRARY_PATH}"


SHLIB_PATH="$LD_LIBRARY_PATH"

export LD_LIBRARY_PATH SHLIB_PATH


# Change to APP_BIN for JAVA execution

cd "${APP_BIN}"
```

```
# Reference path will be used to avoid empty space in the parent
directory

LIB_HOME=.

JAVA_OPTS="-Xrs -Xms128m -Xmx768m -client -
Dsun.nio.PageAlignDirectMemory=true"

JNI_PATH="-Djava.library.path=$LIB_HOME"

CLASSPATH="$LIB_HOME:$LIB_HOME/cb.jar"

MAIN_CLASS=Gui



# Execute Java VM Runtime for BackupManager

echo "Startup Ahsay Online Backup Manager ... "

"${JAVA_EXE}" $JAVA_OPTS $JNI_PATH -cp $CLASSPATH $MAIN_CLASS --config
"${DEBUG_MODE}" "${APP_HOME}" "${SETTING_HOME}"



##########################################################################
########

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

##########################################################################
########



cd "${EXE_DIR}"

exit 0
```

Once you have configured the parameters, save the changes. Use the **sh** command to run the script. The AhsayOBM Login Menu will be displayed.

```
# sh RunConfigurator.sh

Startup Ahsay Online Backup Manager ...

Config file found


Login Menu

----------

  (1). Login

  (2). Change Network Settings

  (3). Forgot Password

  (4). Quit

----------

Your Choice:
```

ListBackupSet.sh

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

```
# vi ListBackupSet.sh
```

Configure the following parameters:

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

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

```
# vi ListBackupSet.sh




#!/bin/sh



##############################  ListBackupSet.sh
##############################

# You can use this shell script to list all backup sets available under
#

# your backup account.
#

#########################################################################
########



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



# ------------------------------  SETTING_HOME  -----------------------
--------

# | Directory to your setting home.
|

# | Default to ${HOME}/.obm when not set.
|

# | e.g. SETTING_HOME="${HOME}/.obm"
|

# -------------------------------------------------------------------
--------

SETTING_HOME=""
```

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


#############################################################################
########

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

#############################################################################
########


EXE_DIR=`pwd`

SCRIPT_HOME=`dirname "$0"`

cd "$SCRIPT_HOME"

APP_BIN=`pwd`

APP_HOME=`dirname "$APP_BIN"`


#############################################################################
########

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

#############################################################################
########


if [ "Darwin" = `uname` ]; then

    JAVA_HOME="/System/Library/Frameworks/JavaVM.framework/Home"

fi


if [ ! -x "$APP_HOME/jvm" ];

then

    echo "'$APP_HOME/jvm' does not exist!"

    if [ ! -n "$JAVA_HOME" ]; then

        echo "Please set JAVA_HOME!"

        exit 0
```

```
    else
        ln -sf "$JAVA_HOME" "$APP_HOME/jvm"
        echo "Created JAVA_HOME symbolic link at '$APP_HOME/jvm'"
    fi
fi


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


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


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


# Verify the JAVA_EXE whether it is a valid JAVA Executable or not.
STRING_JAVA_VERSION="java version,openjdk version"
OUTPUT_JAVA_VERSION=`"${JAVA_EXE}" -version 2>&1`
OUTPUT_JVM_SUPPORT=0
BACKUP_IFS=$IFS
IFS=","
for word in $STRING_JAVA_VERSION; do
```

```
    if [ `echo "${OUTPUT_JAVA_VERSION}" | grep "${word}" | grep -cv
"grep ${word}"` -le 0 ]

    then

      #echo "The Java Executable \"${JAVA_EXE}\" is not a valid Java
Executable. Exit \""`basename "$0"`"\" now."

      continue;

    else

      OUTPUT_JVM_SUPPORT=1

      break;

    fi

done

IFS=$BACKUP_IFS

if [ $OUTPUT_JVM_SUPPORT -eq 0 ]

then

    echo "The Java Executable \"${JAVA_EXE}\" is not a valid Java
Executable. Exit \""`basename "$0"`"\" now."

    exit 1

fi



################################################################################
########

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

################################################################################
########



# Change to APP_BIN for JAVA execution

cd "${APP_BIN}"



# Reference path will be used to avoid empty space in the parent
directory

LIB_HOME=.

JAVA_OPTS="-Xrs -Xms128m -Xmx768m -client -
Dsun.nio.PageAlignDirectMemory=true"
```

```
JNI_PATH="-Djava.library.path=$LIB_HOME"

CLASSPATH="$LIB_HOME:$LIB_HOME/cb.jar"

MAIN_CLASS=ListBackupSet



echo "Using APP_HOME     : ${APP_HOME}"

echo "Using SETTING_HOME : ${SETTING_HOME}"

# API Arguments: ListBackupSet [APP_HOME] [SETTING_HOME]

# Do not include double-quote for java options, jni path, classpath and
main class

# Only apply double-quote for path to java executable and execution
arguments

"${JAVA_EXE}" $JAVA_OPTS $JNI_PATH -cp $CLASSPATH $MAIN_CLASS
"${APP_HOME}" "${SETTING_HOME}"



##########################################################################
########

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

##########################################################################
########



cd "${EXE_DIR}"

exit 0
```

Once you have configured the parameters, save the changes. Use the **sh** command to run the script. The list of backup sets will be displayed.

```
# sh ListBackupSet.sh

Using APP_HOME     : /usr/local/obm

Using SETTING_HOME :

BackupSet Name= Sample Backup Set 01, ID= 1641184406581

BackupSet Name= Sample Backup Set 02, ID= 1641195290716

BackupSet Name= Sample Backup Set 03, ID= 1641347569071
```

ListBackupJob.sh

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

```
# vi ListBackupJob.sh
```

Configure the following parameters:

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

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

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

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

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

  e.g. BACKUP_DEST="1119083740107" or BACKUP_DEST="CBS"

```
# vi ListBackupJob.sh




#!/bin/sh



##############################  ListBackupJob.sh
##############################

# You can use this shell script to list all backup job which ran under
#

# this backup set.
#

#########################################################################
########



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



# ----------------------------  SETTING_HOME  ------------------------
--------
```

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


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


# ------------------------------  BACKUP_DEST  ------------------------
--------
# | The name or ID of the destination that you want to run
|
# | If destination name is not in English, please use DestinationID
|
# | e.g. BACKUP_DEST="1119083740107"
|
# | or  BACKUP_DEST="CBS"
|
```

```
# |
|

# | You can leave this parameter blank if you have only 1 destination.
|

# ------------------------------------------------------------------------
--------

BACKUP_DEST=""



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



#############################################################################
########

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

#############################################################################
########



# Input Arguments will overwrite the above settings

# defined in 'User Defined Section'.

if [ $# -ge 1 ]; then



    if [ -n "$1" ]; then

        BACKUP_SET="$1"

    fi



    if [ -n "$2" ]; then

        BACKUP_DEST="$2"

    fi



fi



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

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

#############################################################################
########


EXE_DIR=`pwd`

SCRIPT_HOME=`dirname "$0"`

cd "$SCRIPT_HOME"

APP_BIN=`pwd`

APP_HOME=`dirname "$APP_BIN"`



#############################################################################
########

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

#############################################################################
########



if [ "Darwin" = `uname` ]; then

    JAVA_HOME="/System/Library/Frameworks/JavaVM.framework/Home"

fi



if [ ! -x "$APP_HOME/jvm" ];

then

    echo "'$APP_HOME/jvm' does not exist!"

    if [ ! -n "$JAVA_HOME" ]; then

        echo "Please set JAVA_HOME!"

        exit 0

    else

        ln -sf "$JAVA_HOME" "$APP_HOME/jvm"

        echo "Created JAVA_HOME symbolic link at '$APP_HOME/jvm'"

    fi

fi
```

```
if [ ! -x "$APP_HOME/jvm" ];

then

    echo "Please create symbolic link for '$JAVA_HOME' to
'$APP_HOME/jvm'"

    exit 0

fi



JAVA_HOME="$APP_HOME/jvm"

JAVA_EXE="$JAVA_HOME/bin/java"



# Verify the JAVA_EXE whether it can be executed or not.

if [ ! -x "${JAVA_EXE}" ]

then

    echo "The Java Executable file \"${JAVA_EXE}\" cannot be executed.
Exit \""`basename "$0"`"\" now."

    exit 1

fi



# Verify the JAVA_EXE whether it is a valid JAVA Executable or not.

STRING_JAVA_VERSION="java version,openjdk version"

OUTPUT_JAVA_VERSION=`"${JAVA_EXE}" -version 2>&1`

OUTPUT_JVM_SUPPORT=0

BACKUP_IFS=$IFS

IFS=","

for word in $STRING_JAVA_VERSION; do

    if [ `echo "${OUTPUT_JAVA_VERSION}" | grep "${word}" | grep -cv
"grep ${word}"` -le 0 ]

    then

      #echo "The Java Executable \"${JAVA_EXE}\" is not a valid Java
Executable. Exit \""`basename "$0"`"\" now."

      continue;
```

```
    else

      OUTPUT_JVM_SUPPORT=1

      break;

    fi

done

IFS=$BACKUP_IFS

if [ $OUTPUT_JVM_SUPPORT -eq 0 ]

then

    echo "The Java Executable \"${JAVA_EXE}\" is not a valid Java
Executable. Exit \""`basename "$0"`"\" now."

    exit 1

fi



################################################################################
########

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

################################################################################
########



# Change to APP_BIN for JAVA execution

cd "${APP_BIN}"



# Reference path will be used to avoid empty space in the parent
directory

LIB_HOME=.

JAVA_OPTS="-Xrs -Xms128m -Xmx768m -client -
Dsun.nio.PageAlignDirectMemory=true"

JNI_PATH="-Djava.library.path=$LIB_HOME"

CLASSPATH="$LIB_HOME:$LIB_HOME/cb.jar"

MAIN_CLASS=ListBackupJob



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

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

echo "Using BACKUP_SET   : ${BACKUP_SET}"



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



# Do not include double-quote for java options, jni path, classpath and

# main class.

# Only apply double-quote for path to java executable and execution
arguments

"${JAVA_EXE}" $JAVA_OPTS $JNI_PATH -cp $CLASSPATH $MAIN_CLASS "--app-
home=${APP_HOME}" "--backup-set=${BACKUP_SET}" "--backup-
dest=${BACKUP_DEST}" "--setting-home=${SETTING_HOME}"



################################################################################
########

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

################################################################################
########



cd "${EXE_DIR}"

exit 0
```

Once you have configured the parameters, save the changes. Use the **sh** command to run the script. The list of backup jobs of a specific backup set will be displayed.

```
# sh ListBackupJob.sh

Using APP_HOME     : /usr/local/obm

Using SETTING_HOME :

Using BACKUP_SET   : Sample Backup Set 03

Sample Backup Set 03 [1641347569071]

2022-01-05-15-47-41
```

RunBackupSet.sh

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

```
# vi RunBackupSet.sh
```

Configure the following parameters:

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

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

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

  e.g. BACKUP_DESTS=”1119083740107” or BACKUP_DEST=”CBS”

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

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

  BACKUP_TYPE=”DATABASE” for full database backup

  BACKUP_TYPE=”DIFFERENTIAL” for differential database backup

  BACKUP_TYPE=”LOG” for log database backup

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

  e.g. SETTING_HOME=”/root/.obm”

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

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

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

  DELTA_MODE=”F” for full file backup

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

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

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

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

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

```
# vi RunBackupSet.sh

#!/bin/sh



##############################  RunBackupSet.sh
################################

# You can use this shell script to run any of your backup sets from the
#

# command line. Just customize the "User Defined Section" below with
your      #

# values for your backup action.
#

#########################################################################
########



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



# ---------------------------------- BACKUP_SET -------------------------
--------

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

# | If backup set name is not in English, please use ID instead.
|

# | e.g. BACKUP_SET="1119083740107"
|

# |  or  BACKUP_SET="FileBackupSet-1"
|

# |
|

# | You can leave this parameter blank if you have only 1 backup set.
|

# -------------------------------------------------------------------------
--------

BACKUP_SET=""



# ---------------------------------- BACKUP_DESTS -----------------------
--------
```

```
# | The list of name or ID of the backup destinations that you want to
run.    |

# | If backup destination name is not in English, please use ID instead.
|

# | e.g. BACKUP_DESTS="1740107119083"
|

# |  or  BACKUP_DESTS="Destination-1,Destination-2"
|

# |  or  BACKUP_DESTS="ALL"
|

# |
|

# | You can specify multiple destinations in comma-separated format,
|

# | or use "ALL" to run backup for all destinations.
|

# ------------------------------------------------------------------------
--------

BACKUP_DESTS="ALL"



# -------------------------------- BACKUP_TYPE -------------------------
--------

# | Set backup type. You don't need to change this if you are backing up
a     |

# | file backup set.
|

# | Options available: FILE/DATABASE/DIFFERENTIAL/LOG
|

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

# |  or  BACKUP_TYPE="DATABASE"      for Full database backup
|

# |  or  BACKUP_TYPE="DIFFERENTIAL"  for Differential database backup
|

# |  or  BACKUP_TYPE="LOG"           for Log database backup
|

# ------------------------------------------------------------------------
--------

BACKUP_TYPE="FILE"
```

```
# ------------------------------- SETTING_HOME -----------------------
--------

# | Directory to your setting home.
|

# | Default to ${HOME}/.obm when not set.
|

# | e.g. SETTING_HOME="${HOME}/.obm"
|

# ------------------------------------------------------------------
--------

SETTING_HOME=""



# ------------------------------- DELTA_MODE -----------------------
--------

# | Set In-File Delta mode.
|

# | Options available: Incremental/Differential/Full (I/D/F)
|

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

# |  or  DELTA_MODE="D"   for Differential In-file delta backup
|

# |  or  DELTA_MODE="F"   for Full File backup
|

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

# ------------------------------------------------------------------
--------

DELTA_MODE=""



# ------------------------------- CLEANUP_MODE -----------------------
--------

# | You can enable Cleanup mode to remove obsolete files from your
backup      |

# | destinations after backup.
|

# | Options available: ENABLE-CLEANUP/DISABLE-CLEANUP
|
```

```
# | e.g. CLEANUP_MODE="ENABLE-CLEANUP"
|

# |  or  CLEANUP_MODE="DISABLE-CLEANUP"
|

# ---------------------------------------------------------------------
--------

CLEANUP_MODE="DISABLE-CLEANUP"



# -------------------------------- DEBUG_MODE -------------------------
--------

# | Set Debug mode.
|

# | Options available: ENABLE-DEBUG/DISABLE-DEBUG
|

# | e.g. DEBUG_MODE="ENABLE-DEBUG"
|

# |  or  DEBUG_MODE="DISABLE-DEBUG"
|

# ---------------------------------------------------------------------
--------

DEBUG_MODE="DISABLE-DEBUG"



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




#######################################################################
########

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

#######################################################################
########



# Input Arguments will overwrite the above settings

# defined in 'User Defined Section'.

if [ $# -ge 1 ]; then
```

```
    if [ -n "$1" ]; then

        BACKUP_SET="$1"

    fi


fi


#############################################################################
########

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

#############################################################################
########


EXE_DIR=`pwd`

SCRIPT_HOME=`dirname "$0"`

cd "$SCRIPT_HOME"

APP_BIN=`pwd`

APP_HOME=`dirname "$APP_BIN"`


#############################################################################
########

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

#############################################################################
########


if [ "Darwin" = `uname` ]; then

    JAVA_HOME="/System/Library/Frameworks/JavaVM.framework/Home"

fi


if [ ! -x "$APP_HOME/jvm" ];

then

    echo "'$APP_HOME/jvm' does not exist!"
```

```
    if [ ! -n "$JAVA_HOME" ]; then
        echo "Please set JAVA_HOME!"
        exit 0
    else
        ln -sf "$JAVA_HOME" "$APP_HOME/jvm"
        if [ ! -x "$APP_HOME/jvm" ];
        then
            echo "Please create symbolic link for '$JAVA_HOME' to
'$APP_HOME/jvm'"
            exit 0
        else
            echo "Created JAVA_HOME symbolic link at '$APP_HOME/jvm'"
        fi
    fi
fi


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


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


# Verify the JAVA_EXE whether it is a valid JAVA Executable or not.
STRING_JAVA_VERSION="java version,openjdk version"
OUTPUT_JAVA_VERSION=`"${JAVA_EXE}" -version 2>&1`
OUTPUT_JVM_SUPPORT=0
```

```
BACKUP_IFS=$IFS

IFS=","

for word in $STRING_JAVA_VERSION; do

    if [ `echo "${OUTPUT_JAVA_VERSION}" | grep "${word}" | grep -cv
"grep ${word}"` -le 0 ]

    then

      #echo "The Java Executable \"${JAVA_EXE}\" is not a valid Java
Executable. Exit \""`basename "$0"`"\" now."

      continue;

    else

      OUTPUT_JVM_SUPPORT=1

      break;

    fi

done

IFS=$BACKUP_IFS

if [ $OUTPUT_JVM_SUPPORT -eq 0 ]

then

    echo "The Java Executable \"${JAVA_EXE}\" is not a valid Java
Executable. Exit \""`basename "$0"`"\" now."

    exit 1

fi



################################################################################
########

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

################################################################################
########



# Set LD_LIBRARY_PATH for Lotus Notes on Linux

if [ "Linux" = `uname` ];

then

    NOTES_PROGRAM=`cat "$APP_HOME/bin/notesenv"`
```

```
    LD_LIBRARY_PATH="$APP_HOME/bin:$NOTES_PROGRAM:$LD_LIBRARY_PATH"

    export NOTES_PROGRAM

else

    LD_LIBRARY_PATH="$APP_HOME/bin:$LD_LIBRARY_PATH"

fi



DEP_LIB_PATH="X64"

case "`uname -m`" in

    i[3-6]86)

        DEP_LIB_PATH="X86"

    ;;

esac

LD_LIBRARY_PATH="${APP_BIN}/${DEP_LIB_PATH}":".":"${LD_LIBRARY_PATH}"



SHLIB_PATH="$LD_LIBRARY_PATH"

export LD_LIBRARY_PATH SHLIB_PATH



##########################################################################
########

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

##########################################################################
########



# Change to APP_BIN for JAVA execution

cd "${APP_BIN}"



# Reference path will be used to avoid empty space in the parent
directory

LIB_HOME=.

JAVA_OPTS="-Xrs -Xms128m -Xmx768m -XX:MaxDirectMemorySize=512m -client -
Dsun.nio.PageAlignDirectMemory=true"

JNI_PATH="-Djava.library.path=$LIB_HOME"
```

```
CLASSPATH="$LIB_HOME:$LIB_HOME/cb.jar"

MAIN_CLASS=RunBackupSet


echo "-"

echo "Using APP_HOME      : $APP_HOME"

echo "Using SETTING_HOME  : $SETTING_HOME"

echo "Using JAVA_HOME     : $JAVA_HOME"

echo "Using JAVA_EXE      : $JAVA_EXE"

echo "Using JAVA_OPTS     : $JAVA_OPTS"

echo "Using JNI_PATH      : $JNI_PATH"

echo "Using CLASSPATH     : $CLASSPATH"

echo "-"


echo "Running Backup Set - '$BACKUP_SET' ..."


# API Arguments: RunBackupSet [APP_HOME] [BACKUP_SET] [BACKUP_DESTS]
[BACKUP_TYPE] [SETTING_HOME] [DELTA_MODE] [CLEANUP_MODE] [DEBUG_MODE]


# Do not include double-quote for java options, jni path, classpath and

# main class.

# Only apply double-quote for path to java executable and execution
arguments

"${JAVA_EXE}" $JNI_PATH -cp $CLASSPATH $JAVA_OPTS $MAIN_CLASS
"${APP_HOME}" "${BACKUP_SET}" "${BACKUP_DESTS}" "${BACKUP_TYPE}"
"${SETTING_HOME}" "${DELTA_MODE}" "${CLEANUP_MODE}" "${DEBUG_MODE}"

################################################################################
########

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

################################################################################
########

cd "${EXE_DIR}"

exit 0
```

Once you have configured the parameters, save the changes. Use the **sh** command to run the script. The backup will be run manually.

```
# sh RunBackupSet.sh

Using APP_HOME      : /usr/local/obm

Using SETTING_HOME  :

Using JAVA_HOME     : /usr/local/obm/jvm

Using JAVA_EXE      : /usr/local/obm/jvm/bin/java

Using JAVA_OPTS     : -Xrs -Xms128m -Xmx2048m -
XX:MaxDirectMemorySize=512m -client -Dsun.nio.PageAlignDirectMemory=true

Using JNI_PATH      : -Djava.library.path=.:./LinX64

Using CLASSPATH     : .:./cb.jar

-

Running Backup Set - 'Sample Backup Set 03' ...

[2022/01/05 15:47:57] [info] [-] Start [ AhsayOBM v9.0.2.24 ]

[2022/01/05 15:47:57] [info] [-] Saving encrypted backup set encryption
keys to server...

[2022/01/05 15:47:58] [info] [1641349114378] Start Backup ...
[Deduplication: enabled, Deduplication scope: All files within the same
backup set, Migrate Delta: enabled]

[2022/01/05 15:47:58] [info] [1641349114378] Using Temporary Directory
/root/.obm/temp/1641347569071/OBS@1641349114378

[2022/01/05 15:48:00] [info] [1641349114378] Start Periodic Data
Integrity Check on backup set = "Sample Backup Set 03" destination =
"AhsayCBS"

[2022/01/05 15:48:00] [info] [1641349114378] Start data integrity check
on backup set "Sample Backup Set 03(1641347569071)",
"AhsayCBS(1641349114378)", crc disabled, rebuild index disabled

[2022/01/05 15:48:00] [info] [1641349114378] Start processing data
integrity check on backup set= "Sample Backup Set 03" destination=
"AhsayCBS"

[2022/01/05 15:48:02] [info] [1641349114378] Download valid index files
from backup job "Current" to
"/root/.obm/temp/1641347569071/OBS@1641349114378/index".

[2022/01/05 15:48:02] [info] [1641349114378] Skipped to run Data
Integrity Check for backup set "Sample Backup Set 03" in destination
"AhsayCBS" because no data is in index.

[2022/01/05 15:48:03] [info] [1641349114378] Data integrity check on
backup set= "Sample Backup Set 03" destination= "AhsayCBS" is completed
```

```
[2022/01/05 15:48:03] [info] [1641349114378] Finished data integrity
check on backup set "Sample Backup Set 03(1641347569071)",
"AhsayCBS(1641349114378)", crc disabled, rebuild index disabled

[2022/01/05 15:48:03] [info] [1641349114378] Completed data integrity
check on backup set "Sample Backup Set 03(1641347569071)",
"AhsayCBS(1641349114378)", crc disabled, rebuild index disabled

[2022/01/05 15:48:03] [info] [-] Start running pre-commands

[2022/01/05 15:48:03] [info] [-] Finished running pre-commands

[2022/01/05 15:48:03] [info] [1641349114378] Downloading server file
list...

[2022/01/05 15:48:03] [info] [1641349114378] Download valid index files
from backup job "Current" to
"/root/.obm/temp/1641347569071/OBS@1641349114378/index".

[2022/01/05 15:48:03] [info] [1641349114378] Downloading server file
list... Completed

[2022/01/05 15:48:04] [info] [1641349114378] Reading backup source from
hard disk...

[2022/01/05 15:48:04] [info] [1641349114378] Reading backup source from
hard disk... Completed

[2022/01/05 15:48:04] [info] [1641349114378] [New Directory]... /

[2022/01/05 15:48:04] [info] [1641349114378] [New Directory]... /root

[2022/01/05 15:48:05] [info] [1641349114378] [New Directory]...
/root/Documents

[2022/01/05 15:48:05] [info] [1641349114378] [New Directory]...
/root/Documents/testfiles

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 100% of
"/root/Documents/sample1.rtf"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 10% of
"/root/Documents/sample1.ppt"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 21% of
"/root/Documents/sample1.ppt"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 11% of
"/root/Documents/sample1.pdf"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 25% of
"/root/Documents/sample1.pdf"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 36% of
"/root/Documents/sample1.pdf"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 32% of
"/root/Documents/sample1.ppt"
```

```
[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 47% of
"/root/Documents/sample1.pdf"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 59% of
"/root/Documents/sample1.pdf"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 43% of
"/root/Documents/sample1.ppt"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 70% of
"/root/Documents/sample1.pdf"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 53% of
"/root/Documents/sample1.ppt"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 81% of
"/root/Documents/sample1.pdf"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 100% of
"/root/Documents/sample1.txt"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 92% of
"/root/Documents/sample1.pdf"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 64% of
"/root/Documents/sample1.ppt"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 100% of
"/root/Documents/sample1.pdf"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 100% of
"/root/Documents/sample1.xls"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 75% of
"/root/Documents/sample1.ppt"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 49% of
"/root/Documents/sample2.pdf"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 74% of
"/root/Documents/sample2.pdf"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 99% of
"/root/Documents/sample2.pdf"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 100% of
"/root/Documents/sample2.pdf"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 12% of
"/root/Documents/sample2.ppt"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 100% of
"/root/Documents/sample2.rtf"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 89% of
"/root/Documents/sample1.ppt"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 24% of
"/root/Documents/sample2.ppt"
```

```
[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 100% of
"/root/Documents/sample1.ppt"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 37% of
"/root/Documents/sample2.ppt"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 100% of
"/root/Documents/sample2.txt"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 49% of
"/root/Documents/sample2.ppt"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 100% of
"/root/Documents/sample3.xls"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 61% of
"/root/Documents/sample2.ppt"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 100% of
"/root/Documents/sample3.txt"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 100% of
"/root/Documents/sample2.xls"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 71% of
"/root/Documents/sample2.ppt"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 100% of
"/root/Documents/sample2.ppt"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 10% of
"/root/Documents/sample_640x360.avi"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 20% of
"/root/Documents/sample_640x360.avi"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 10% of
"/root/Documents/sample_960x540.mpg"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 30% of
"/root/Documents/sample_640x360.avi"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 20% of
"/root/Documents/sample_960x540.mpg"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 10% of
"/root/Documents/sample_960x540.mkv"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 40% of
"/root/Documents/sample_640x360.avi"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 30% of
"/root/Documents/sample_960x540.mpg"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 50% of
"/root/Documents/sample_640x360.avi"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 20% of
"/root/Documents/sample_960x540.mkv"
```

```
[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 60% of
"/root/Documents/sample_640x360.avi"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 40% of
"/root/Documents/sample_960x540.mpg"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 70% of
"/root/Documents/sample_640x360.avi"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 50% of
"/root/Documents/sample_960x540.mpg"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 30% of
"/root/Documents/sample_960x540.mkv"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 60% of
"/root/Documents/sample_960x540.mpg"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 70% of
"/root/Documents/sample_960x540.mpg"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 80% of
"/root/Documents/sample_960x540.mpg"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 80% of
"/root/Documents/sample_640x360.avi"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 40% of
"/root/Documents/sample_960x540.mkv"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 90% of
"/root/Documents/sample_960x540.mpg"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 90% of
"/root/Documents/sample_640x360.avi"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 100% of
"/root/Documents/sample_960x540.mpg"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 100% of
"/root/Documents/sample_640x360.avi"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 50% of
"/root/Documents/sample_960x540.mkv"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 60% of
"/root/Documents/sample_960x540.mkv"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 70% of
"/root/Documents/sample_960x540.mkv"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 72% of
"/root/Documents/settings.sys"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 80% of
"/root/Documents/sample_960x540.mkv"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 100% of
"/root/Documents/settings.sys"
```

```
[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 90% of
"/root/Documents/sample_960x540.mkv"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 11% of
"/root/Documents/testfiles/sample1.pdf"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 100% of
"/root/Documents/sample_960x540.mkv"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 25% of
"/root/Documents/testfiles/sample1.pdf"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 36% of
"/root/Documents/testfiles/sample1.pdf"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 10% of
"/root/Documents/testfiles/sample1.ppt"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 47% of
"/root/Documents/testfiles/sample1.pdf"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 100% of
"/root/Documents/testfiles/sample1.rtf"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 59% of
"/root/Documents/testfiles/sample1.pdf"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 100% of
"/root/Documents/testfiles/sample1.txt"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 70% of
"/root/Documents/testfiles/sample1.pdf"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 21% of
"/root/Documents/testfiles/sample1.ppt"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 81% of
"/root/Documents/testfiles/sample1.pdf"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 32% of
"/root/Documents/testfiles/sample1.ppt"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 49% of
"/root/Documents/testfiles/sample2.pdf"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 43% of
"/root/Documents/testfiles/sample1.ppt"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 74% of
"/root/Documents/testfiles/sample2.pdf"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 99% of
"/root/Documents/testfiles/sample2.pdf"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 100% of
"/root/Documents/testfiles/sample2.pdf"

[2022/01/05 15:48:05] [info] [1641349114378]
com.ahsay.afc.event.d@6ce6b6a1
```

```
[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 53% of
"/root/Documents/testfiles/sample1.ppt"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 100% of
"/root/Documents/testfiles/sample1.xls"

[2022/01/05 15:48:05] [info] [1641349114378]
com.ahsay.afc.event.d@5d640301

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 64% of
"/root/Documents/testfiles/sample1.ppt"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 92% of
"/root/Documents/testfiles/sample1.pdf"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 100% of
"/root/Documents/testfiles/sample1.pdf"

[2022/01/05 15:48:05] [info] [1641349114378]
com.ahsay.afc.event.d@701eac98

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 75% of
"/root/Documents/testfiles/sample1.ppt"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 12% of
"/root/Documents/testfiles/sample2.ppt"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 24% of
"/root/Documents/testfiles/sample2.ppt"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 37% of
"/root/Documents/testfiles/sample2.ppt"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 89% of
"/root/Documents/testfiles/sample1.ppt"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 49% of
"/root/Documents/testfiles/sample2.ppt"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 100% of
"/root/Documents/testfiles/sample1.ppt"

[2022/01/05 15:48:05] [info] [1641349114378]
com.ahsay.afc.event.d@2380b5c0

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 61% of
"/root/Documents/testfiles/sample2.ppt"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 100% of
"/root/Documents/testfiles/sample2.rtf"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 71% of
"/root/Documents/testfiles/sample2.ppt"

[2022/01/05 15:48:05] [info] [1641349114378]
com.ahsay.afc.event.d@27bf3568

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 100% of
"/root/Documents/testfiles/sample2.xls"
```

```
[2022/01/05 15:48:05] [info] [1641349114378]
com.ahsay.afc.event.d@53a3e6dd

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 100% of
"/root/Documents/testfiles/sample3.txt"

[2022/01/05 15:48:05] [info] [1641349114378]
com.ahsay.afc.event.d@579c6871

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 100% of
"/root/Documents/testfiles/sample2.txt"

[2022/01/05 15:48:05] [info] [1641349114378]
com.ahsay.afc.event.d@62bdbffb

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 100% of
"/root/Documents/testfiles/sample3.xls"

[2022/01/05 15:48:05] [info] [1641349114378]
com.ahsay.afc.event.d@26ecf4e9

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 100% of
"/root/Documents/testfiles/sample2.ppt"

[2022/01/05 15:48:05] [info] [1641349114378]
com.ahsay.afc.event.d@3bad0936

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 10% of
"/root/Documents/testfiles/sample_640x360.avi"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 20% of
"/root/Documents/testfiles/sample_640x360.avi"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 30% of
"/root/Documents/testfiles/sample_640x360.avi"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 40% of
"/root/Documents/testfiles/sample_640x360.avi"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 50% of
"/root/Documents/testfiles/sample_640x360.avi"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 60% of
"/root/Documents/testfiles/sample_640x360.avi"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 70% of
"/root/Documents/testfiles/sample_640x360.avi"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 80% of
"/root/Documents/testfiles/sample_640x360.avi"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 90% of
"/root/Documents/testfiles/sample_640x360.avi"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 100% of
"/root/Documents/testfiles/sample_640x360.avi"

[2022/01/05 15:48:05] [info] [1641349114378]
com.ahsay.afc.event.d@6d2dd184
```

```
[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 10% of
"/root/Documents/testfiles/sample_960x540.mkv"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 20% of
"/root/Documents/testfiles/sample_960x540.mkv"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 30% of
"/root/Documents/testfiles/sample_960x540.mkv"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 40% of
"/root/Documents/testfiles/sample_960x540.mkv"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 50% of
"/root/Documents/testfiles/sample_960x540.mkv"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 10% of
"/root/Documents/testfiles/sample_960x540.mpg"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 20% of
"/root/Documents/testfiles/sample_960x540.mpg"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 30% of
"/root/Documents/testfiles/sample_960x540.mpg"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 40% of
"/root/Documents/testfiles/sample_960x540.mpg"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 50% of
"/root/Documents/testfiles/sample_960x540.mpg"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 60% of
"/root/Documents/testfiles/sample_960x540.mpg"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 70% of
"/root/Documents/testfiles/sample_960x540.mpg"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 80% of
"/root/Documents/testfiles/sample_960x540.mpg"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 90% of
"/root/Documents/testfiles/sample_960x540.mpg"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 100% of
"/root/Documents/testfiles/sample_960x540.mpg"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 60% of
"/root/Documents/testfiles/sample_960x540.mkv"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 70% of
"/root/Documents/testfiles/sample_960x540.mkv"

[2022/01/05 15:48:05] [info] [1641349114378]
com.ahsay.afc.event.d@759d9a2a

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 80% of
"/root/Documents/testfiles/sample_960x540.mkv"

[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 90% of
"/root/Documents/testfiles/sample_960x540.mkv"
```

```
[2022/01/05 15:48:05] [info] [1641349114378] [New File]... 100% of
"/root/Documents/testfiles/sample_960x540.mkv"

[2022/01/05 15:48:05] [info] [1641349114378]
com.ahsay.afc.event.d@19ea1c7

[2022/01/05 15:48:06] [info] [1641349114378] Start validating the
presence and size of backup data in destination "AhsayCBS"...

[2022/01/05 15:48:06] [info] [1641349114378] File:
"1641347569071/blocks/2022-01-05-15-47-41/0/000000.bak", Size:
1,335,776, OK

[2022/01/05 15:48:06] [info] [1641349114378] File:
"1641347569071/blocks/2022-01-05-15-47-41/0/000001.bak", Size:
1,307,600, OK

[2022/01/05 15:48:06] [info] [1641349114378] File:
"1641347569071/blocks/2022-01-05-15-47-41/0/000002.bak", Size:
1,754,864, OK

[2022/01/05 15:48:06] [info] [1641349114378] File:
"1641347569071/blocks/2022-01-05-15-47-41/0/000003.bak", Size: 45,440,
OK

[2022/01/05 15:48:06] [info] [1641349114378] Finished validating the
presence and size of backup data in destination "AhsayCBS"

[2022/01/05 15:48:06] [info] [1641349114378] Total New Files = 31

[2022/01/05 15:48:06] [info] [1641349114378] Total New Directories = 4

[2022/01/05 15:48:06] [info] [1641349114378] Total New Links = 0

[2022/01/05 15:48:06] [info] [1641349114378] Total Updated Files = 0

[2022/01/05 15:48:06] [info] [1641349114378] Total Attributes Changed
Files = 0

[2022/01/05 15:48:06] [info] [1641349114378] Total Deleted Files = 0

[2022/01/05 15:48:06] [info] [1641349114378] Total Deleted Directories =
0

[2022/01/05 15:48:06] [info] [1641349114378] Total Deleted Links = 0

[2022/01/05 15:48:06] [info] [1641349114378] Total Moved Files = 0

[2022/01/05 15:48:06] [info] [1641349114378] Total Dedupe Saving for
this job = 4.57MB

[2022/01/05 15:48:06] [info] [1641349114378] Total Backup Data Size for
this job = 9.41MB

[2022/01/05 15:48:06] [info] [1641349114378] Total Dedupe Saving for
destination = 4.57MB

[2022/01/05 15:48:06] [info] [1641349114378] Total Backup Data Size for
destination = 9.41MB
```

```
[2022/01/05 15:48:06] [info] [-] Saving server information to
destination.

[2022/01/05 15:48:07] [info] [1641349114378] Saving encrypted backup
file index to 1641347569071/blocks/2022-01-05-15-47-41 at destination
AhsayCBS...

[2022/01/05 15:48:07] [info] [-] Start running post-commands

[2022/01/05 15:48:07] [info] [-] Finished running post-commands

[2022/01/05 15:48:10] [info] [1641349114378] Deleting temporary file
/root/.obm/temp/1641347569071/OBS@1641349114378

[2022/01/05 15:48:10] [info] [1641349114378] Backup Completed
Successfully
```

Restore.sh

This script file is used to restore backup files to its original or alternate location. To configure the parameters, open the script file in a text editor like vi.

```
# vi Restore.sh
```

Configure the following parameters:

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

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

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

  e.g. DESTINATION="1119083740107" or DESTINATION="CBS"

- **RESTORE_TO** – this is the directory where you want to restore the backup file. You do not need to change this if you want the backup file to be restored to its original location.

  e.g. RESTORE_TO="" or RESTORE_TO-"/tmp"

- **RESTORE_FROM** – this is the file or directory that you would like to restore.

  e.g. RESTORE_FROM="/Data"

- **POINT_IN_TIME** – this is the specific successful backup that you want to restore. You can use *Current* if you want to use the latest backup snapshot. You can see the point in time snapshot by using the *ListBackupJob.sh* script file.

  e.g. POINT_IN_TIME="Current" or POINT_IN_TIME="2006-10-04-12-57-13"

- **RESTORE_PERMISSION** – you can set the file permission here.

  e.g. RESTORE_PERMISSION="N" or RESTORE_PERMISSION="Y"

- **SKIP_INVALID_KEY** – you can set here if you want to skip restoring the backup file with an invalid key. There are two (2) options for this: *Y* or *N*.

  e.g. SKIP_INVALID_KEY="N"

- **SYNC_OPTION** – this is the sync options if you want to delete extra files.

  e.g. SYNC_OPTIONS="Y" if you want to enable sync options

  SYNC_OPTIONS="N" if you do not want to enable sync options

  SYNC_OPTIONS="" if you want to prompt for selection

- **REPLACE_EXISTING_FILE** – you can set here if you want files with the same filename to be replaced. There are three (3) options for this: *--all, --none* or blank.

  e.g. REPLACE_EXISTING_FILE="—all" if you want to replace existing files with the same filename

REPLACE_EXISTING_FILE="—none" if you want to keep all existing files with the same filename

REPLACE_EXISTING_FILE="" if you want to be prompted for selection

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

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

- **FILTER** – you can filter the files that you want to be restored. You can use this format to set the filter *-Pattern=xxx-Type=yyy-Target=zzz.*

  xxx is the filter pattern

  yyy is the filter type, you have eight (8) options available for this: *exact, exactMatchCase, contains, containsMatchCase, startWith*, *startWithMatchCase*, *endWith* and *endWithMatchCase*.

  zzz is the filter target, you have three (3) options available for this: *toFile, toFileDir* and *toDir*.

  e.g. FILTER="-Pattern=.txt-Type=exact-Target=toFile"

- **TEMP_DIR** – this is the directory where the restore files will be stored temporarily. If set to "" the temporary directory in the backup set will be used.

  e.g. TEMP_DIR="/tmp"

- **VERIFY_CHKSUM** – you can set here if you want the in-file delta file checksum to be verified during restore. There are two (2) options available for this: *Y* or *N*.

  e.g. VERIFY_CHKSUM="N" or VERIFY_CHKSUM="Y"

```
# vi Restore.sh




#!/bin/sh



##################################  Restore.sh
##################################

# You can use this shell script to restore backup files using command-
line.    #

# Just customize the "User Define Section" below with values for your
restore  #

# action.
#

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

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


# ------------------------------  BACKUP_SET  -------------------------
--------

# | The name or ID of the backup set that you want to restore.
|

# | If backup set name is not in English, please use ID instead.
|

# | e.g. BACKUP_SET="1119083740107"
|

# |  or  BACKUP_SET="FileBackupSet-1"
|

# |
|

# | You can leave this parameter blank if you have only 1 backup set.
|

# ------------------------------------------------------------------
--------

BACKUP_SET=""



# ------------------------------  DESTINATION  -------------------------
--------

# | The name or ID of the backup destination that you want to restore
from.    |

# | If backup destination name is not in English, please use ID instead.
|

# | e.g. DESTINATION="1740107119083"
|

# |  or  DESTINATION="Destination-1"
|

# |
|

# | You can leave this parameter blank if you have only 1 destination.
|

# ------------------------------------------------------------------
--------

DESTINATION=""
```

```
# ------------------------------  RESTORE_TO  -------------------------
--------

# | Directory to where you want files to be restored
|

# | set to "" to restore files to original location
|

# | e.g. RESTORE_TO="/tmp"
|

# ------------------------------------------------------------------
--------

RESTORE_TO=""



# ------------------------------  RESTORE_FROM  -------------------------
--------

# | File/Directory on the backup server that you would like to restore
|

# | e.g. RESTORE_FROM="/Data"
|

# ------------------------------------------------------------------
--------

RESTORE_FROM=""



# ------------------------------  POINT_IN_TIME  -------------------------
--------

# | The point-in-time snapshot (successful backup) that you want to
restore    |

# | from the backup server. Use "Current" for the latest backup snapshot
|

# | e.g. POINT_IN_TIME="2006-10-04-12-57-13"
|

# |  or  POINT_IN_TIME="Current"
|

# |
|

# | You can retrieve the point in time by using the ListBackupJob.sh
|

# ------------------------------------------------------------------
--------

POINT_IN_TIME="Current"
```

```
# -------------------------  RESTORE_PERMISSION  ----------------------
--------

# | set to "Y" if you want to restore file permissions
|

# | set to "N" if you do NOT want to restore file permissions
|

# ------------------------------------------------------------------
--------

RESTORE_PERMISSION="N"



# ----------------------------  SKIP_INVALID_KEY  ----------------------
--------

# | set to "Y" if you want to skip restore file with invalid key
|

# | set to "N" if you want to prompt user to input a correct key
|

# ------------------------------------------------------------------
--------

SKIP_INVALID_KEY="N"



# -------------------------------  SYNC_OPTION  -------------------------
--------

# | Delete extra files
|

# | set to "Y" if you want to enable sync option
|

# | set to "N" if you do NOT want to enable sync option
|

# | set to "" to prompt for selection
|

# ------------------------------------------------------------------
--------

SYNC_OPTION="N"



# -------------------------  REPLACE_EXISTING_FILE  --------------------
--------
```

```
# | set to "--all" to replace all existing file(s) of the same filename
|

# | set to "--none" to skip all existing file(s) with the same filename
|

# | set to "" to prompt for selection
|

# ------------------------------------------------------------------------
--------

REPLACE_EXISTING_FILE="--all"



# ------------------------------  SETTING_HOME  -------------------------
--------

# | Directory to your setting home.
|

# | Default to ${HOME}/.obm when not set.
|

# | e.g. SETTING_HOME="${HOME}/.obm"
|

# ------------------------------------------------------------------------
--------

SETTING_HOME=""



# ---------------------------------  FILTER  ----------------------------
--------

# | Filter out what files you want to restore
|

# | -Pattern=xxx-Type=yyy-Target=zzz
|

# | where xxx is the filter pattern,
|

# |       yyy is the filter type, whice can be one of the following:
|

# |           [exact | exactMatchCase | contains | containsMatchCase|
|

# |            startWith | startWithMatchCase | endWith |
endWithMatchCase]    |

# |       zzz is the filter target, which can be one of the following:
|
```

```
# |           [toFile | toFileDir | toDir]
|

# |
|

# | e.g. FILTER="-Pattern=.txt-Type=exact-Target=toFile"
|

# ------------------------------------------------------------------------
--------

FILTER=""



# -------------------------------  TEMP_DIR  -------------------------
--------

# | Directory to where you want to store restore files temporarily
|

# | set to "" to use the temporary directory in the backup set
|

# | e.g. TEMP_DIR="/tmp"
|

# ------------------------------------------------------------------------
--------

TEMP_DIR=""



# ----------------------------  VERIFY_CHKSUM  ------------------------
--------

# | set to "Y" if you want to verify in-file delta file checksum during
restore|

# | set to "N" if you do NOT want to verify in-file delta file checksum
during |

# | restore
|

# ------------------------------------------------------------------------
--------

VERIFY_CHKSUM="N"



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

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

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

#############################################################################
########



EXE_DIR=`pwd`

SCRIPT_HOME=`dirname "$0"`

cd "$SCRIPT_HOME"

APP_BIN=`pwd`

APP_HOME=`dirname "$APP_BIN"`



#############################################################################
########

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

#############################################################################
########



if [ "Darwin" = `uname` ]; then

    JAVA_HOME="/System/Library/Frameworks/JavaVM.framework/Home"

fi



if [ ! -x "$APP_HOME/jvm" ];

then

    echo "'$APP_HOME/jvm' does not exist!"

    if [ ! -n "$JAVA_HOME" ]; then

        echo "Please set JAVA_HOME!"

        exit 0

    else

        ln -sf "$JAVA_HOME" "$APP_HOME/jvm"

        echo "Created JAVA_HOME symbolic link at '$APP_HOME/jvm'"
```

```
    fi

fi

if [ ! -x "$APP_HOME/jvm" ];

then

    echo "Please create symbolic link for '$JAVA_HOME' to
'$APP_HOME/jvm'"

    exit 0

fi



JAVA_HOME="$APP_HOME/jvm"

JAVA_EXE="$JAVA_HOME/bin/java"



# Verify the JAVA_EXE whether it can be executed or not.

if [ ! -x "${JAVA_EXE}" ]

then

    echo "The Java Executable file \"${JAVA_EXE}\" cannot be executed.
Exit \""`basename "$0"`"\" now."

    exit 1

fi



# Verify the JAVA_EXE whether it is a valid JAVA Executable or not.

STRING_JAVA_VERSION="java version,openjdk version"

OUTPUT_JAVA_VERSION=`"${JAVA_EXE}" -version 2>&1`

OUTPUT_JVM_SUPPORT=0

BACKUP_IFS=$IFS

IFS=","

for word in $STRING_JAVA_VERSION; do

    if [ `echo "${OUTPUT_JAVA_VERSION}" | grep "${word}" | grep -cv
"grep ${word}"` -le 0 ]

    then

      #echo "The Java Executable \"${JAVA_EXE}\" is not a valid Java
Executable. Exit \""`basename "$0"`"\" now."
```

```
      continue;

    else

      OUTPUT_JVM_SUPPORT=1

      break;

    fi

done

IFS=$BACKUP_IFS

if [ $OUTPUT_JVM_SUPPORT -eq 0 ]

then

    echo "The Java Executable \"${JAVA_EXE}\" is not a valid Java
Executable. Exit \""`basename "$0"`"\" now."

    exit 1

fi




##############################################################################
########

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

##############################################################################
########



# Set LD_LIBRARY_PATH for Lotus Notes on Linux

if [ "Linux" = `uname` ];

then

    NOTES_PROGRAM=`cat "$APP_BIN/notesenv"`

    LD_LIBRARY_PATH="$APP_BIN:$NOTES_PROGRAM:$LD_LIBRARY_PATH"

    export NOTES_PROGRAM

else

    LD_LIBRARY_PATH="$APP_BIN:$LD_LIBRARY_PATH"

fi
```

```
# The Restore Action must be execute at path $APP_HOME/bin

cd "${APP_BIN}"


DEP_LIB_PATH="X64"

case "`uname -m`" in

    i[3-6]86)

        DEP_LIB_PATH="X86"

    ;;

esac

LD_LIBRARY_PATH="${APP_BIN}/${DEP_LIB_PATH}":".":"${LD_LIBRARY_PATH}"


SHLIB_PATH="$LD_LIBRARY_PATH"

export LD_LIBRARY_PATH SHLIB_PATH


# Reference path will be used to avoid empty space in the parent
directory

LIB_HOME=.

JAVA_OPTS="-Xrs -Xms128m -Xmx768m -XX:MaxDirectMemorySize=512m -client -
Dsun.nio.PageAlignDirectMemory=true"

JNI_PATH="-Djava.library.path=$LIB_HOME"

CLASSPATH="$LIB_HOME:$LIB_HOME/cb.jar"

MAIN_CLASS=Restore


echo "Using APP_HOME:          : ${APP_HOME}"

echo "Using BACKUP_SET         : ${BACKUP_SET}"

echo "Using RESTORE_FROM       : ${RESTORE_FROM}"

echo "Using RESTORE_TO         : ${RESTORE_TO}"

echo "Using POINT_IN_TIME      : ${POINT_IN_TIME}"

echo "Using RESTORE_PERMISSION : ${RESTORE_PERMISSION}"

echo "Using TEMP_DIR           : ${TEMP_DIR}"
```

```
# Do not include double-quote for java options, jni path, classpath and

# main class.

# Only apply double-quote for path to java executable and execution
arguments

"${JAVA_EXE}" $JAVA_OPTS $JNI_PATH -cp $CLASSPATH $MAIN_CLASS --
to="${RESTORE_TO}" --from="${RESTORE_FROM}" --backup-set="${BACKUP_SET}"
--backup-dest="${DESTINATION}" "${REPLACE_EXISTING_FILE}" --
date="${POINT_IN_TIME}" --set-permission="${RESTORE_PERMISSION}" --skip-
invalid-key="${SKIP_INVALID_KEY}" --sync="${SYNC_OPTION}" --
filter="${FILTER}" --temp-dir="${TEMP_DIR}" --verify-delta-file-
chksum="${VERIFY_CHKSUM}" --app-home="${APP_HOME}" --setting-
home="${SETTING_HOME}"



################################################################################
########

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

################################################################################
########



cd "${EXE_DIR}"

exit 0
```

Once you have configured the parameters, save the changes. Use the **sh** command to run the script. The restore will be run manually.

```
# sh Restore.sh



Using APP_HOME:           : /usr/local/obm

Using BACKUP_SET          : Sample Backup Set 03

Using RESTORE_FROM        : /root/Documents

Using RESTORE_TO          : /usr/local/alternate

Using POINT_IN_TIME       : Current

Using RESTORE_PERMISSION : N

Using TEMP_DIR            : /root/temp

Filter Pattern not set, filter would not apply to restore
```

```
[2022-01-05 16:03:53] Start [ AhsayOBM v9.0.2.24 ]

[2022-01-05 16:03:53] OS: Linux 4.18.0-240.1.1.el8_3.x86_64
(localhost.localdomain); CPU Model: VMware-Intel(R) Xeon(R) Gold 5218R
CPU @ 2.10GHz,Intel(R) Xeon(R) Gold 5218R CPU @ 2.10GHz,Intel(R) Xeon(R)
Gold 5218R CPU @ 2.10GHz,Intel(R) Xeon(R) Gold 5218R CPU @ 2.10GHz;
Number of Processors: 4; Heap Size: 109.1MB (Current) / 1.8GB (Maximum);
Physical Memory: 565.7MB (Free) / 3.6GB (Total)

[2022-01-05 16:03:53] start,Start [ AhsayOBM v9.0.2.24 ],0,0,0,,0,0



[2022-01-05 16:03:53] Selected job: 2022-01-05-16-03-45

[2022-01-05 16:03:53] Selected source: [/root/Documents]

[2022-01-05 16:03:53] Info: [followLink=false marshalTargetPath=false
deleteForSync=false skipFaultKey=false verifyDeltaFileChecksum=false
ignoreSegmentInfoCorruptedData=true restorePermission=false
[RestoreLocation] type=RAW path=[/usr/local/alternate]]

[2022-01-05 16:03:54] Creating new directory...
"/usr/local/alternate/root"

[2022-01-05 16:03:54] Creating new directory...
"/usr/local/alternate/root/Documents"

[2022-01-05 16:03:54] Creating new directory...
"/usr/local/alternate/root/Documents/testfiles"

[2022-01-05 16:03:54] Downloading...
"/usr/local/alternate/root/Documents/settings.sys" (Total 44K bytes)

[2022-01-05 16:03:54] Downloading...
"/usr/local/alternate/root/Documents/sample1.ppt" (Total 891K bytes)

[2022-01-05 16:03:54] Downloading...
"/usr/local/alternate/root/Documents/testfiles/sample1.ppt" (Total 891K
bytes)

[2022-01-05 16:03:54] Downloading...
"/usr/local/alternate/root/Documents/sample3.xls" (Total 13K bytes)

[2022-01-05 16:03:54] Downloading...
"/usr/local/alternate/root/Documents/testfiles/sample3.xls" (Total 13K
bytes)

[2022-01-05 16:03:54] Downloading...
"/usr/local/alternate/root/Documents/sample2.xls" (Total 7K bytes)

[2022-01-05 16:03:54] Downloading...
"/usr/local/alternate/root/Documents/testfiles/sample2.xls" (Total 7K
bytes)

[2022-01-05 16:03:54] Downloading...
"/usr/local/alternate/root/Documents/sample_640x360.avi" (Total 569K
bytes)
```

```
[2022-01-05 16:03:54] Downloading...
"/usr/local/alternate/root/Documents/testfiles/sample_640x360.avi"
(Total 569K bytes)

[2022-01-05 16:03:54] Downloading...
"/usr/local/alternate/root/Documents/sample1.pdf" (Total 567K bytes)

[2022-01-05 16:03:54] Downloading...
"/usr/local/alternate/root/Documents/testfiles/sample1.pdf" (Total 567K
bytes)

[2022-01-05 16:03:54] Downloading...
"/usr/local/alternate/root/Documents/sample2.pdf" (Total 64K bytes)

[2022-01-05 16:03:54] Downloading...
"/usr/local/alternate/root/Documents/testfiles/sample2.pdf" (Total 64K
bytes)

[2022-01-05 16:03:54] Downloading...
"/usr/local/alternate/root/Documents/sample2.rtf" (Total 1K bytes)

[2022-01-05 16:03:54] Downloading...
"/usr/local/alternate/root/Documents/testfiles/sample2.rtf" (Total 1K
bytes)

[2022-01-05 16:03:54] Downloading...
"/usr/local/alternate/root/Documents/sample2.txt" (Total 2K bytes)

[2022-01-05 16:03:54] Downloading...
"/usr/local/alternate/root/Documents/testfiles/sample2.txt" (Total 2K
bytes)

[2022-01-05 16:03:54] Downloading...
"/usr/local/alternate/root/Documents/sample3.txt" (Total 3K bytes)

[2022-01-05 16:03:54] Downloading...
"/usr/local/alternate/root/Documents/testfiles/sample3.txt" (Total 3K
bytes)

[2022-01-05 16:03:54] Downloading...
"/usr/local/alternate/root/Documents/sample_960x540.mpg" (Total 733K
bytes)

[2022-01-05 16:03:54] Downloading...
"/usr/local/alternate/root/Documents/testfiles/sample_960x540.mpg"
(Total 733K bytes)

[2022-01-05 16:03:54] Downloading...
"/usr/local/alternate/root/Documents/testfiles/sample1.rtf" (Total 102K
bytes)

[2022-01-05 16:03:54] Downloading...
"/usr/local/alternate/root/Documents/testfiles/sample1.txt" (Total 607
bytes)

[2022-01-05 16:03:54] Downloading...
"/usr/local/alternate/root/Documents/sample1.rtf" (Total 116K bytes)

[2022-01-05 16:03:54] Downloading...
"/usr/local/alternate/root/Documents/sample1.txt" (Total 14K bytes)
```

```
[2022-01-05 16:03:54] Downloading...
"/usr/local/alternate/root/Documents/sample1.xls" (Total 16K bytes)

[2022-01-05 16:03:54] Downloading...
"/usr/local/alternate/root/Documents/testfiles/sample1.xls" (Total 16K
bytes)

[2022-01-05 16:03:54] Downloading...
"/usr/local/alternate/root/Documents/sample2.ppt" (Total 518K bytes)

[2022-01-05 16:03:54] Downloading...
"/usr/local/alternate/root/Documents/testfiles/sample2.ppt" (Total 518K
bytes)

[2022-01-05 16:03:54] Downloading...
"/usr/local/alternate/root/Documents/sample_960x540.mkv" (Total 1.26M
bytes)

[2022-01-05 16:03:54] Downloading...
"/usr/local/alternate/root/Documents/testfiles/sample_960x540.mkv"
(Total 1.26M bytes)

[2022-01-05 16:03:55] Restore Completed Successfully

[2022-01-05 16:03:55] end,RESTORE_STOP_SUCCESS,0,0,0,,0,0
```

Decrypt.sh

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

```
# vi Decrypt.sh
```

Configure the following parameters:

- **SOURCE_DIR** – this is the path of the folder that contains the backup files that you want to decrypt.

  e.g. SOURCE_DIR="/usr/local/cbs/user/LinuxTest/1563436721634/blocks"

- **ENCRYPT_KEY** – this is the encryption key of the backup set. You can leave this blank if you backup set is not encypted.

  e.g. ENCRYPT_KEY="RU5DUllQVF9LRVk="

- **DECRYPT_TO** – this is the directory where you want to store the decrypted backup file.

  e.g. DECRYPT_TO="/tmp"

- **DECRYPT_FROM** – this is the file or directory that you would like to decrypt.

  e.g. DECRYPT_FROM="/Data"

- **POINT_IN_TIME** – this is the specific successful backup that you want to decrypt. You can use *Current* if you want to use the latest backup snapshot. You can see the point in time snapshot by using the *ListBackupJob.sh* script file.

  e.g. POINT_IN_TIME="Current" or POINT_IN_TIME="2006-10-04-12-57-13"

- **RESTORE_PERMISSION** – you can set the file permission here.

  e.g. RESTORE_PERMISSION="N" or RESTORE_PERMISSION="Y"

- **SKIP_INVALID_KEY** – you can set here if you want to skip decrypting the backup file with an invalid key. There are two (2) options for this: *Y* or *N*.

  e.g. SKIP_INVALID_KEY="N"

- **SYNC_OPTION** – this is the sync options if you want to delete extra files.

  e.g. SYNC_OPTIONS="Y" if you want to enable sync options

  SYNC_OPTIONS="N" if you do not want to enable sync options

  SYNC_OPTIONS="" if you want to prompt for selection

- **REPLACE_EXISTING_FILE** – you can set here if you want files with the same filename to be replaced. There are three (3) options for this: *--all, --none* or blank.

  e.g. REPLACE_EXISTING_FILE="—all" if you want to replace existing files with the same filename

  REPLACE_EXISTING_FILE="—none" if you want to keep all existing files with the same filename

  REPLACE_EXISTING_FILE="" if you want to be prompted for selection

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

  e.g. SETTING_HOME=”/root/.obm”

- **FILTER** – you can filter the files that you want to be restored. You can use this format to set the filter *-Pattern=xxx-Type=yyy-Target=zzz.*

  xxx is the filter pattern

  yyy is the filter type, you have eight (8) options available for this: *exact, exactMatchCase, contains, containsMatchCase, startWith*, *startWithMatchCase*, *endWith* and *endWithMatchCase*.

  zzz is the filter target, you have three (3) options available for this: *toFile, toFileDir* and *toDir*.

  e.g. FILTER=”-Pattern=.txt-Type=exact-Target=toFile”

- **TEMP_DIR** – this is the directory where the restore files will be stored temporarily. If set to “” the temporary directory in the backup set will be used.

  e.g. TEMP_DIR=”/tmp”

- **VERIFY_CHKSUM** – you can set here if you want the in-file delta file checksum to be verified during restore. There are two (2) options available for this: *Y* or *N*.

  e.g. VERIFY_CHKSUM=”N” or VERIFY_CHKSUM=”Y”

```
# vi Decrypt.sh



#!/bin/sh



################################  Decrypt.sh
################################

# You can use this shell script to decrypt backup files using command-
line.    #

# Just customize the "User Define Section" below with values for your
decrypt  #

# action.
#

##########################################################################
########



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



# ------------------------------  SOURCE_DIR  -------------------------
--------
```

```
# | The path to the [<backup set ID>/blocks] folder which contains
|

# | the backup files that you want to decrypt.
|

# | This folder should located under backup destination physically.
|

# | e.g. SET SOURCE_DIR="/Users/john/backupdata/1498444438340/blocks"
|

# |      where directory "/Users/john/backupdata" is path of local
destination |

# ------------------------------------------------------------------
--------

SOURCE_DIR=""



# -------------------------------  ENCRYPT_KEY  ---------------------
--------

# | The encrypting key of the backup data.
|

# | e.g. SET ENCRYPT_KEY="RU5DUllQVF9LRVk="
|

# |
|

# | You can leave this parameter blank if backup data is not encrypted.
|

# ------------------------------------------------------------------
--------

ENCRYPT_KEY=""



# -------------------------------  DECRYPT_TO  ----------------------
--------

# | Directory to where you want files to be decrypted
|

# | e.g. DECRYPT_TO="/tmp"
|

# ------------------------------------------------------------------
--------

DECRYPT_TO=""
```

```
# ------------------------------  DECRYPT_FROM  ------------------------
--------

# | File/Directory on the backup data that you would like to decrypt
|

# | e.g. DECRYPT_FROM="/Data"
|

# ------------------------------------------------------------------------
--------

DECRYPT_FROM=""



# ------------------------------  POINT_IN_TIME  ------------------------
--------

# | The point-in-time snapshot (successful backup) that you want to
decrypt    |

# | from the backup data. Use "Current" for the latest backup snapshot
|

# | e.g. POINT_IN_TIME="2006-10-04-12-57-13"
|

# |  or  POINT_IN_TIME="Current"
|

# |
|

# | You can retrieve the point in time by using the ListBackupJob.sh
|

# ------------------------------------------------------------------------
--------

POINT_IN_TIME="Current"



# --------------------------  RESTORE_PERMISSION  ----------------------
--------

# | set to "Y" if you want to restore file permissions
|

# | set to "N" if you do NOT want to restore file permissions
|

# ------------------------------------------------------------------------
--------

RESTORE_PERMISSION="N"
```

```
# ----------------------------  SKIP_INVALID_KEY  ----------------------
--------

# | set to "Y" if you want to skip decrypt file with invalid key
|

# | set to "N" if you want to prompt to input a correct key
|

# ------------------------------------------------------------------------
--------

SKIP_INVALID_KEY="N"



# -----------------------------  SYNC_OPTION  -------------------------
--------

# | Delete extra files
|

# | set to "Y" if you want to enable sync option
|

# | set to "N" if you do NOT want to enable sync option
|

# | set to "" to prompt for selection
|

# ------------------------------------------------------------------------
--------

SYNC_OPTION="N"



# -------------------------  REPLACE_EXISTING_FILE  --------------------
--------

# | set to "--all" to replace all existing file(s) of the same filename
|

# | set to "--none" to skip all existing file(s) with the same filename
|

# | set to "" to prompt for selection
|

# ------------------------------------------------------------------------
--------

REPLACE_EXISTING_FILE="--all"



# ------------------------------  SETTING_HOME  ------------------------
--------
```

```
# | Directory to your setting home. Log files will be located inside.
|

# | Default to ${HOME}/.obm when not set.                        |

# | e.g. SETTING_HOME="/Users/john/.obm"                         |

# ------------------------------------------------------------------
--------

SETTING_HOME=""



# ---------------------------------  FILTER  -------------------------
--------

# | Filter out what files you want to decrypt
|

# | -Pattern=xxx-Type=yyy-Target=zzz
|

# | where xxx is the filter pattern,
|

# |       yyy is the filter type, whice can be one of the following:
|

# |           [exact | exactMatchCase | contains | containsMatchCase|
|

# |            startWith | startWithMatchCase | endWith |
endWithMatchCase]    |

# |       zzz is the filter target, which can be one of the following:
|

# |           [toFile | toFileDir | toDir]
|

# |
|

# | e.g. FILTER="-Pattern=.txt-Type=exact-Target=toFile"
|

# ------------------------------------------------------------------
--------

FILTER=""



# ---------------------------------  TEMP_DIR  -------------------------
--------

# | Directory to where you want to store decrypt files temporarily
|
```

```
# | e.g. TEMP_DIR="/tmp"
|

# ------------------------------------------------------------------------
--------

TEMP_DIR=""



# ----------------------------  VERIFY_CHKSUM  -------------------------
--------

# | set to "Y" if you want to verify in-file delta file checksum during
decrypt|

# | set to "N" if you do NOT want to verify in-file delta file checksum
during |

# | decrypt
|

# ------------------------------------------------------------------------
--------

VERIFY_CHKSUM="N"



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



#############################################################################
########

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

#############################################################################
########



EXE_DIR=`pwd`

SCRIPT_HOME=`dirname "$0"`

cd "$SCRIPT_HOME"

APP_BIN=`pwd`

APP_HOME=`dirname "$APP_BIN"`



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

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

##############################################################################
########


if [ "Darwin" = `uname` ]; then

    JAVA_HOME="/System/Library/Frameworks/JavaVM.framework/Home"

fi


if [ ! -x "$APP_HOME/jvm" ];

then

    echo "'$APP_HOME/jvm' does not exist!"

    if [ ! -n "$JAVA_HOME" ]; then

        echo "Please set JAVA_HOME!"

        exit 0

    else

        ln -sf "$JAVA_HOME" "$APP_HOME/jvm"

        echo "Created JAVA_HOME symbolic link at '$APP_HOME/jvm'"

    fi

fi


if [ ! -x "$APP_HOME/jvm" ];

then

    echo "Please create symbolic link for '$JAVA_HOME' to
'$APP_HOME/jvm'"

    exit 0

fi


JAVA_HOME="$APP_HOME/jvm"

JAVA_EXE="$JAVA_HOME/bin/java"
```

```
# Verify the JAVA_EXE whether it can be executed or not.

if [ ! -x "${JAVA_EXE}" ]

then

    echo "The Java Executable file \"${JAVA_EXE}\" cannot be executed.
Exit \""`basename "$0"`"\" now."

    exit 1

fi



# Verify the JAVA_EXE whether it is a valid JAVA Executable or not.

STRING_JAVA_VERSION="java version,openjdk version"

OUTPUT_JAVA_VERSION=`"${JAVA_EXE}" -version 2>&1`

OUTPUT_JVM_SUPPORT=0

BACKUP_IFS=$IFS

IFS=","

for word in $STRING_JAVA_VERSION; do

    if [ `echo "${OUTPUT_JAVA_VERSION}" | grep "${word}" | grep -cv
"grep ${word}"` -le 0 ]

    then

      #echo "The Java Executable \"${JAVA_EXE}\" is not a valid Java
Executable. Exit \""`basename "$0"`"\" now."

      continue;

    else

      OUTPUT_JVM_SUPPORT=1

      break;

    fi

done

IFS=$BACKUP_IFS

if [ $OUTPUT_JVM_SUPPORT -eq 0 ]

then

    echo "The Java Executable \"${JAVA_EXE}\" is not a valid Java
Executable. Exit \""`basename "$0"`"\" now."

    exit 1
```

```
fi


################################################################################
########

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

################################################################################
########


# Set LD_LIBRARY_PATH for Lotus Notes on Linux

if [ "Linux" = `uname` ];

then

    NOTES_PROGRAM=`cat "$APP_BIN/notesenv"`

    LD_LIBRARY_PATH="$APP_BIN:$NOTES_PROGRAM:$LD_LIBRARY_PATH"

    export NOTES_PROGRAM

else

    LD_LIBRARY_PATH="$APP_BIN:$LD_LIBRARY_PATH"

fi


# The Decrypt Action must be execute at path $APP_HOME/bin

cd "${APP_BIN}"


DEP_LIB_PATH="X64"

case "`uname -m`" in

    i[3-6]86)

        DEP_LIB_PATH="X86"

    ;;

esac

LD_LIBRARY_PATH="${APP_BIN}/${DEP_LIB_PATH}":".":"${LD_LIBRARY_PATH}"


SHLIB_PATH="$LD_LIBRARY_PATH"
```

```
export LD_LIBRARY_PATH SHLIB_PATH



# Reference path will be used to avoid empty space in the parent
directory

LIB_HOME=.

JAVA_OPTS="-Xrs -Xms128m -Xmx768m -XX:MaxDirectMemorySize=512m -client -
Dsun.nio.PageAlignDirectMemory=true"

JNI_PATH="-Djava.library.path=$LIB_HOME"

CLASSPATH="$LIB_HOME:$LIB_HOME/cb.jar"

MAIN_CLASS=Decrypt



echo "Using APP_HOME:          : ${APP_HOME}"

echo "Using SETTING_HOME:      : ${SETTING_HOME}"

echo "Using SOURCE_DIR         : ${SOURCE_DIR}"

echo "Using DECRYPT_FROM       : ${DECRYPT_FROM}"

echo "Using DECRYPT_TO         : ${DECRYPT_TO}"

echo "Using POINT_IN_TIME      : ${POINT_IN_TIME}"

echo "Using RESTORE_PERMISSION : ${RESTORE_PERMISSION}"

echo "Using TEMP_DIR           : ${TEMP_DIR}"



# Do not include double-quote for java options, jni path, classpath and

# main class.

# Only apply double-quote for path to java executable and execution
arguments

"${JAVA_EXE}" $JAVA_OPTS $JNI_PATH -cp $CLASSPATH $MAIN_CLASS --
to="${DECRYPT_TO}" --from="${DECRYPT_FROM}" --source-dir="${SOURCE_DIR}"
--key="${ENCRYPT_KEY}" "${REPLACE_EXISTING_FILE}" --
date="${POINT_IN_TIME}" --set-permission="${RESTORE_PERMISSION}" --skip-
invalid-key="${SKIP_INVALID_KEY}" --sync="${SYNC_OPTION}" --
filter="${FILTER}" --temp-dir="${TEMP_DIR}" --verify-delta-file-
chksum="${VERIFY_CHKSUM}" --app-home="${APP_HOME}" --setting-
home="${SETTING_HOME}"



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

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

#########################################################################
########


cd "${EXE_DIR}"

exit 0
```

Once you have configured the parameters, save the changes. Use the **sh** command to run the script. The decryption will be run manually.

```
# sh Decrypt.sh

Using APP_HOME:           : /usr/local/obm

Using SETTING_HOME:       :

Using SOURCE_DIR          : /root/backup/1641347569071/blocks

Using DECRYPT_FROM        : /root/Documents

Using DECRYPT_TO          : /tmp

Using POINT_IN_TIME       : Current

Using RESTORE_PERMISSION : N

Using TEMP_DIR            : /root/temp

Filter Pattern not set, filter would not apply to decrypt

[2022-01-05 16:45:14] Start [ AhsayOBM v9.0.2.24 ]

[2022-01-05 16:45:14] OS: Linux 4.18.0-240.1.1.el8_3.x86_64
(localhost.localdomain); CPU Model: VMware-Intel(R) Xeon(R) Gold 5218R
CPU @ 2.10GHz,Intel(R) Xeon(R) Gold 5218R CPU @ 2.10GHz,Intel(R) Xeon(R)
Gold 5218R CPU @ 2.10GHz,Intel(R) Xeon(R) Gold 5218R CPU @ 2.10GHz;
Number of Processors: 4; Heap Size: 30.5MB (Current) / 1.8GB (Maximum);
Physical Memory: 457.2MB (Free) / 3.6GB (Total)

[2022-01-05 16:45:14] start,Start [ AhsayOBM v9.0.2.24 ],0,0,0,,0,0



[2022-01-05 16:45:14] Selected job: 2022-01-05-16-45-06

[2022-01-05 16:45:14] Selected source: [/root/Documents]

[2022-01-05 16:45:14] Info: [followLink=false marshalTargetPath=false
deleteForSync=false skipFaultKey=false verifyDeltaFileChecksum=false
ignoreSegmentInfoCorruptedData=true restorePermission=false
[RestoreLocation] type=RAW path=[/tmp]]

[2022-01-05 16:45:16] Creating new directory... "/tmp/root"

[2022-01-05 16:45:16] Creating new directory... "/tmp/root/Documents"
```

```
[2022-01-05 16:45:16] Creating new directory...
"/tmp/root/Documents/testfiles"

[2022-01-05 16:45:16] Downloading... "/tmp/root/Documents/sample1.rtf"
(Total 116K bytes)

[2022-01-05 16:45:16] Downloading... "/tmp/root/Documents/sample1.txt"
(Total 14K bytes)

[2022-01-05 16:45:16] Downloading... "/tmp/root/Documents/sample1.xls"
(Total 16K bytes)

[2022-01-05 16:45:16] Downloading... "/tmp/root/Documents/sample1.pdf"
(Total 567K bytes)

[2022-01-05 16:45:16] Downloading...
"/tmp/root/Documents/testfiles/sample1.xls" (Total 16K bytes)

[2022-01-05 16:45:16] Downloading... "/tmp/root/Documents/sample2.pdf"
(Total 64K bytes)

[2022-01-05 16:45:16] Downloading...
"/tmp/root/Documents/testfiles/sample1.pdf" (Total 567K bytes)

[2022-01-05 16:45:16] Downloading... "/tmp/root/Documents/sample1.ppt"
(Total 891K bytes)

[2022-01-05 16:45:16] Downloading... "/tmp/root/Documents/sample2.txt"
(Total 2K bytes)

[2022-01-05 16:45:16] Downloading...
"/tmp/root/Documents/testfiles/sample1.ppt" (Total 891K bytes)

[2022-01-05 16:45:16] Downloading...
"/tmp/root/Documents/testfiles/sample2.txt" (Total 2K bytes)

[2022-01-05 16:45:16] Downloading... "/tmp/root/Documents/sample2.ppt"
(Total 518K bytes)

[2022-01-05 16:45:16] Downloading... "/tmp/root/Documents/sample3.txt"
(Total 3K bytes)

[2022-01-05 16:45:16] Downloading...
"/tmp/root/Documents/testfiles/sample3.txt" (Total 3K bytes)

[2022-01-05 16:45:16] Downloading... "/tmp/root/Documents/sample2.xls"
(Total 7K bytes)

[2022-01-05 16:45:16] Downloading...
"/tmp/root/Documents/testfiles/sample2.xls" (Total 7K bytes)

[2022-01-05 16:45:16] Downloading... "/tmp/root/Documents/sample3.xls"
(Total 13K bytes)

[2022-01-05 16:45:16] Downloading...
"/tmp/root/Documents/testfiles/sample3.xls" (Total 13K bytes)

[2022-01-05 16:45:16] Downloading...
"/tmp/root/Documents/sample_640x360.avi" (Total 569K bytes)
```

```
[2022-01-05 16:45:16] Downloading...
"/tmp/root/Documents/testfiles/sample_640x360.avi" (Total 569K bytes)

[2022-01-05 16:45:16] Downloading...
"/tmp/root/Documents/testfiles/sample2.ppt" (Total 518K bytes)

[2022-01-05 16:45:16] Downloading...
"/tmp/root/Documents/testfiles/sample2.pdf" (Total 64K bytes)

[2022-01-05 16:45:16] Downloading...
"/tmp/root/Documents/testfiles/sample1.rtf" (Total 102K bytes)

[2022-01-05 16:45:16] Downloading... "/tmp/root/Documents/sample2.rtf"
(Total 1K bytes)

[2022-01-05 16:45:16] Downloading...
"/tmp/root/Documents/testfiles/sample2.rtf" (Total 1K bytes)

[2022-01-05 16:45:16] Downloading...
"/tmp/root/Documents/testfiles/sample1.txt" (Total 607 bytes)

[2022-01-05 16:45:16] Downloading... "/tmp/root/Documents/settings.sys"
(Total 44K bytes)

[2022-01-05 16:45:16] Downloading...
"/tmp/root/Documents/sample_960x540.mkv" (Total 1.26M bytes)

[2022-01-05 16:45:16] Downloading...
"/tmp/root/Documents/testfiles/sample_960x540.mkv" (Total 1.26M bytes)

[2022-01-05 16:45:16] Downloading...
"/tmp/root/Documents/sample_960x540.mpg" (Total 733K bytes)

[2022-01-05 16:45:16] Downloading...
"/tmp/root/Documents/testfiles/sample_960x540.mpg" (Total 733K bytes)

[2022-01-05 16:45:17] Restore Completed Successfully

[2022-01-05 16:45:17] end,RESTORE_STOP_SUCCESS,0,0,0,,0,0
```

RunDataIntegrityCheck.sh

This script file is used to run data integrity check on your backup set. To configure the parameters, open the script file in a text editor like vi.

```
# vi RunDataIntegrityCheck.sh
```

Configure the following parameters:

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

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

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

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

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

  e.g. DESTINATION="1119083740107" or DESTINATION="CBS"

- **CRC_MODE** – you can set here if you want to run cyclic redundancy check while doing the data integrity check. There are two (2) options available: *ENABLE-CRC* or *DISABLE-CRC*

  e.g. CRC_MODE="DISABLE-CRC" or CRC_MODE="ENABLE-CRC"

```
# vi RunDataIntegrityCheck.sh



#!/bin/sh



##########################  RunDataIntegrityCheck.sh
##########################

# You can use this shell script to run any of your backup sets from the
#

# command line. Just customize the "User Defined Section" below with
your      #

# values for your backup action.
#

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

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


# -------------------------- SETTING_HOME (Optional) -------------------
--------

# | Directory to your setting home.
|

# | Default to ${HOME}/.obm when not set.
|

# | e.g. SETTING_HOME="${HOME}/.obm"
|

# ----------------------------------------------------------------------
--------

SETTING_HOME=""


# --------------------------------- BACKUP_SET -------------------------
--------

# | The name or ID of the backup set that you want to run.
|

# | If backup set name is not in English, please use ID instead.
|

# | e.g. BACKUP_SET="1119083740107"
|

# |  or  BACKUP_SET="FileBackupSet-1"
|

# | You can use "ALL" to run data integrity check for all backup sets.
|

# | i.e. BACKUP_SET="ALL"
|

# |
|

# | You can leave this parameter blank if you have only 1 backup set.
|

# ----------------------------------------------------------------------
--------

BACKUP_SET="ALL"
```

```
# ---------------------------------- BACKUP_DEST -------------------------
--------

# | The name or ID of the backup destination that you want to run.
|

# | If backup destination name is not in English, please use ID instead.
|

# | e.g. BACKUP_DEST="1740107119083"
|

# |  or  BACKUP_DEST="Destination-1"
|

# | You can use "ALL" to run data integrity check for all destinations.
|

# | i.e. BACKUP_DEST="ALL"
|

# |
|

# | You can leave this parameter blank if you have only 1 destination.
|

# | Remark: This option is ignored if BACKUP_SET="ALL"
|

# ------------------------------------------------------------------------
--------

BACKUP_DEST="ALL"



# ---------------------------------- CRC_MODE ----------------------------
--------

# | You can run Cyclic Redundancy Check (CRC) during data integrity
check      |

# | Options available: ENABLE-CRC/DISABLE-CRC
|

# | i.e. CRC_MODE="ENABLE-CRC"
|

# |  or  CRC_MODE="DISABLE-CRC"
|

# ------------------------------------------------------------------------
--------

CRC_MODE="DISABLE-CRC"
```

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

#############################################################################
########

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

#############################################################################
########



# Input Arguments will overwrite the above settings

# defined in 'User Defined Section'.

if [ $# -ge 1 ]; then



    if [ -n "$1" ]; then

        BACKUP_SET="$1"

    fi



fi



#############################################################################
########

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

#############################################################################
########



EXE_DIR=`pwd`

SCRIPT_HOME=`dirname "$0"`

cd "$SCRIPT_HOME"

APP_BIN=`pwd`

APP_HOME=`dirname "$APP_BIN"`



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

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

#############################################################################
########


if [ "Darwin" = `uname` ]; then

    JAVA_HOME="/System/Library/Frameworks/JavaVM.framework/Home"

fi


if [ ! -x "$APP_HOME/jvm" ];

then

    echo "'$APP_HOME/jvm' does not exist!"

    if [ ! -n "$JAVA_HOME" ]; then

        echo "Please set JAVA_HOME!"

        exit 0

    else

        ln -sf "$JAVA_HOME" "$APP_HOME/jvm"

        if [ ! -x "$APP_HOME/jvm" ];

        then

            echo "Please create symbolic link for '$JAVA_HOME' to
'$APP_HOME/jvm'"

            exit 0

        else

            echo "Created JAVA_HOME symbolic link at '$APP_HOME/jvm'"

        fi

    fi

fi


JAVA_HOME="$APP_HOME/jvm"

JAVA_EXE="$JAVA_HOME/bin/java"
```

```
# Verify the JAVA_EXE whether it can be executed or not.

if [ ! -x "${JAVA_EXE}" ]

then

    echo "The Java Executable file \"${JAVA_EXE}\" cannot be executed.
Exit \""`basename "$0"`"\" now."

    exit 1

fi



# Verify the JAVA_EXE whether it is a valid JAVA Executable or not.

STRING_JAVA_VERSION="java version,openjdk version"

OUTPUT_JAVA_VERSION=`"${JAVA_EXE}" -version 2>&1`

OUTPUT_JVM_SUPPORT=0

BACKUP_IFS=$IFS

IFS=","

for word in $STRING_JAVA_VERSION; do

    if [ `echo "${OUTPUT_JAVA_VERSION}" | grep "${word}" | grep -cv
"grep ${word}"` -le 0 ]

    then

      #echo "The Java Executable \"${JAVA_EXE}\" is not a valid Java
Executable. Exit \""`basename "$0"`"\" now."

      continue;

else

      OUTPUT_JVM_SUPPORT=1

      break;

    fi

done

IFS=$BACKUP_IFS

if [ $OUTPUT_JVM_SUPPORT -eq 0 ]

then

    echo "The Java Executable \"${JAVA_EXE}\" is not a valid Java
Executable. Exit \""`basename "$0"`"\" now."

    exit 1
```

```
fi


#############################################################################
########

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

#############################################################################
########


# Set LD_LIBRARY_PATH for Lotus Notes on Linux

if [ "Linux" = `uname` ];

then

    NOTES_PROGRAM=`cat "$APP_HOME/bin/notesenv"`

    LD_LIBRARY_PATH="$APP_HOME/bin:$NOTES_PROGRAM:$LD_LIBRARY_PATH"

    export NOTES_PROGRAM

else

    LD_LIBRARY_PATH="$APP_HOME/bin:$LD_LIBRARY_PATH"

fi


DEP_LIB_PATH="X64"

case "`uname -m`" in

    i[3-6]86)

        DEP_LIB_PATH="X86"

    ;;

esac

LD_LIBRARY_PATH="${APP_BIN}/${DEP_LIB_PATH}":".":"${LD_LIBRARY_PATH}"


SHLIB_PATH="$LD_LIBRARY_PATH"

export LD_LIBRARY_PATH SHLIB_PATH


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

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

#############################################################################
########


# Change to APP_BIN for JAVA execution

cd "${APP_BIN}"


# Reference path will be used to avoid empty space in the parent
directory

LIB_HOME=.

JAVA_OPTS="-Xrs -Xms128m -Xmx768m -XX:MaxDirectMemorySize=512m -client -
Dsun.nio.PageAlignDirectMemory=true"

JNI_PATH="-Djava.library.path=$LIB_HOME"

CLASSPATH="$LIB_HOME:$LIB_HOME/cb.jar"

MAIN_CLASS=RunDataIntegrityCheck


echo "-"

echo "Using APP_HOME      : $APP_HOME"

echo "Using SETTING_HOME  : $SETTING_HOME"

echo "Using JAVA_HOME     : $JAVA_HOME"

echo "Using JAVA_EXE      : $JAVA_EXE"

echo "Using JAVA_OPTS     : $JAVA_OPTS"

echo "Using JNI_PATH      : $JNI_PATH"

echo "Using CLASSPATH     : $CLASSPATH"

echo "-"


echo "Running data integrity check for backup set - '$BACKUP_SET',
destination - '$BACKUP_DEST' ..."


# API Arguments: RunDataIntegrityCheck [APP_HOME] [SETTING_HOME]
[BACKUP_SET] [BACKUP_DEST] [CRC_MODE] [REBUILD_MODE]
```

```
# Do not include double-quote for java options, jni path, classpath and

# main class.

# Only apply double-quote for path to java executable and execution
arguments

"${JAVA_EXE}" $JNI_PATH -cp $CLASSPATH $JAVA_OPTS $MAIN_CLASS
"${APP_HOME}" "${SETTING_HOME}" "${BACKUP_SET}" "${BACKUP_DEST}"
"${CRC_MODE}" "${REBUILD_MODE}"

##########################################################################
########

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

##########################################################################
########

cd "${EXE_DIR}"

exit 0
```

Once you have configured the parameters, save the changes. Use the **sh** command to run the script. The data integrity check will be run in the backup set.

```
# sh RunDataIntegrityCheck.sh

-

Using APP_HOME      : /usr/local/obm

Using SETTING_HOME  :

Using JAVA_HOME     : /usr/local/obm/jvm

Using JAVA_EXE      : /usr/local/obm/jvm/bin/java

Using JAVA_OPTS     : -Xrs -Xms128m -Xmx2048m -
XX:MaxDirectMemorySize=512m -client -Dsun.nio.PageAlignDirectMemory=true

Using JNI_PATH      : -Djava.library.path=.:./LinX64

Using CLASSPATH     : .:./cb.jar

-

Running data integrity check for backup set - 'Sample Backup Set 03',
destination - 'Local-1' ...

[doInfo] Start [ AhsayOBM v9.0.2.24 ]

[doStart] Start data integrity check on backup set "Sample Backup Set
03(1641347569071)", "Local-1(1641353833383)", crc disabled, rebuild
index disabled
```

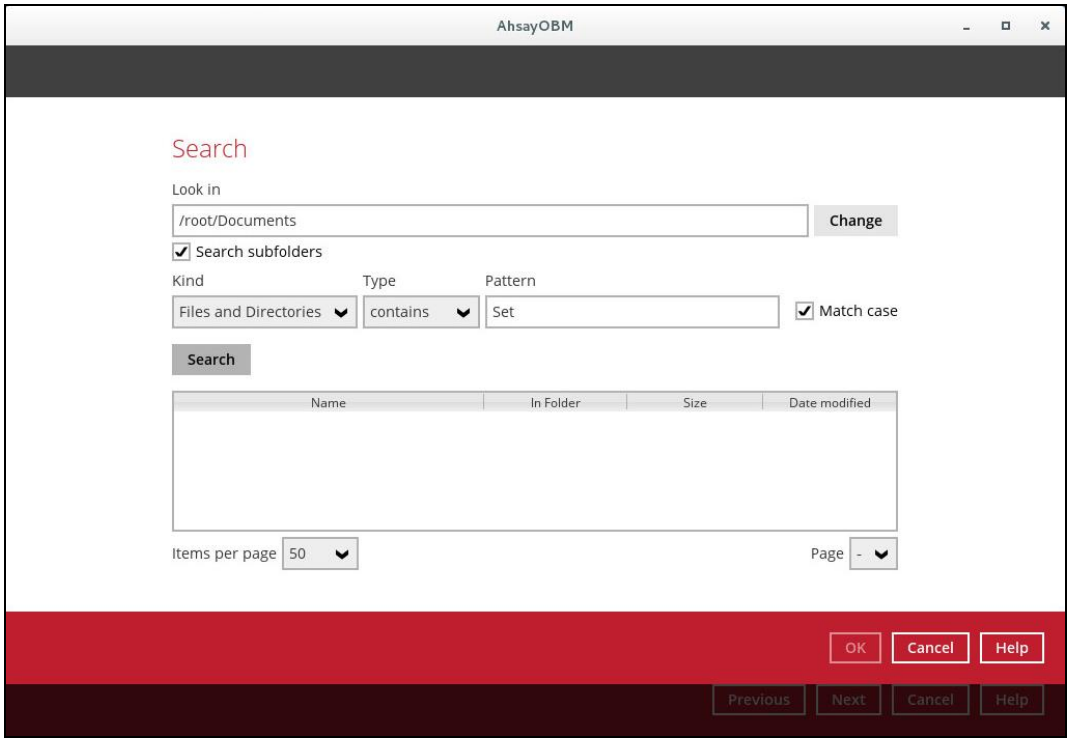
```
[doDetail] Start processing data integrity check on backup set= "Sample
Backup Set 03" destination= "Local-1"

[doLogProgress] Start processing data integrity check on backup set=
"Sample Backup Set 03" destination= "Local-1"

[doLogProgress] Download valid index files from backup job "Current" to
"/root/.obm/temp/1641347569071/Local@1641353833383/index".

[doInfo] Download valid index files from backup job "Current" to
"/root/.obm/temp/1641347569071/Local@1641353833383/index".

[doLogProgress] Browsing "1641347569071/blocks/2022-01-05-16-39-20"

[doLogProgress] Browsing "1641347569071/blocks/2022-01-05-16-39-20/0"

[doLogProgress] Browsing "1641347569071/blocks/2022-01-05-16-51-08"

[doLogProgress] Processing Job "Current", ""

[doInfo] Vacuuming index

[doInfo] Vacuuming index... Completed

[doInfo] Existing statistics of backup set= "Sample Backup Set 03"
destination= "Local-1": Data area compressed size: 8.68MB, Data area
uncompressed size: 9.41MB, Data area file count: 31, Retention area
compressed size: 0B, Retention area uncompressed size: 0B, Retention
area file count: 0, Dedupe saving compressed size: 4.57MB, Dedupe saving
uncompressed size: 9.41MB

[doInfo] Recalculated statistics of backup set= "Sample Backup Set 03"
destination= "Local-1": Data area compressed size: 8.68MB, Data area
uncompressed size: 9.41MB, Data area file count: 31, Retention area
compressed size: 0B, Retention area uncompressed size: 0B, Retention
area file count: 0, Dedupe saving compressed size: 4.84MB, Dedupe saving
uncompressed size: 9.41MB

[doInfo] The statistics of backup set= "Sample Backup Set 03"
destination= "Local-1" is correct.

[doLogProgress] Saving encrypted backup file index to
1641347569071/blocks/2022-01-05-16-52-38 at destination Local-1...

[doInfo] Saving encrypted backup file index to
1641347569071/blocks/2022-01-05-16-52-38 at destination Local-1...

[doDetail] Data integrity check on backup set= "Sample Backup Set 03"
destination= "Local-1" is completed

[doLogProgress] Data integrity check on backup set= "Sample Backup Set
03" destination= "Local-1" is completed

[doEnd][INFO] Finished data integrity check on backup set "Sample Backup
Set 03(1641347569071)", "Local-1(1641353833383)", crc disabled, rebuild
index disabled

[doInfo] Completed data integrity check on backup set "Sample Backup Set
03(1641347569071)", "Local-1(1641353833383)", crc disabled, rebuild
index disabled
```

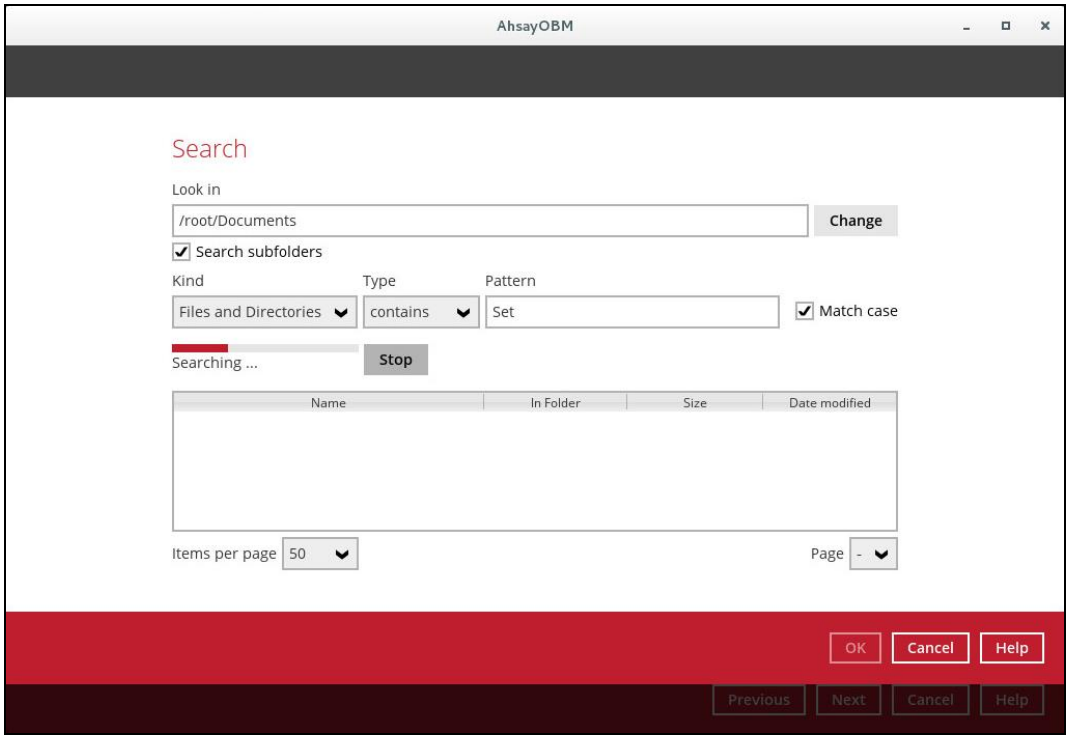
Appendix F: Example Scenarios for Restore Filter

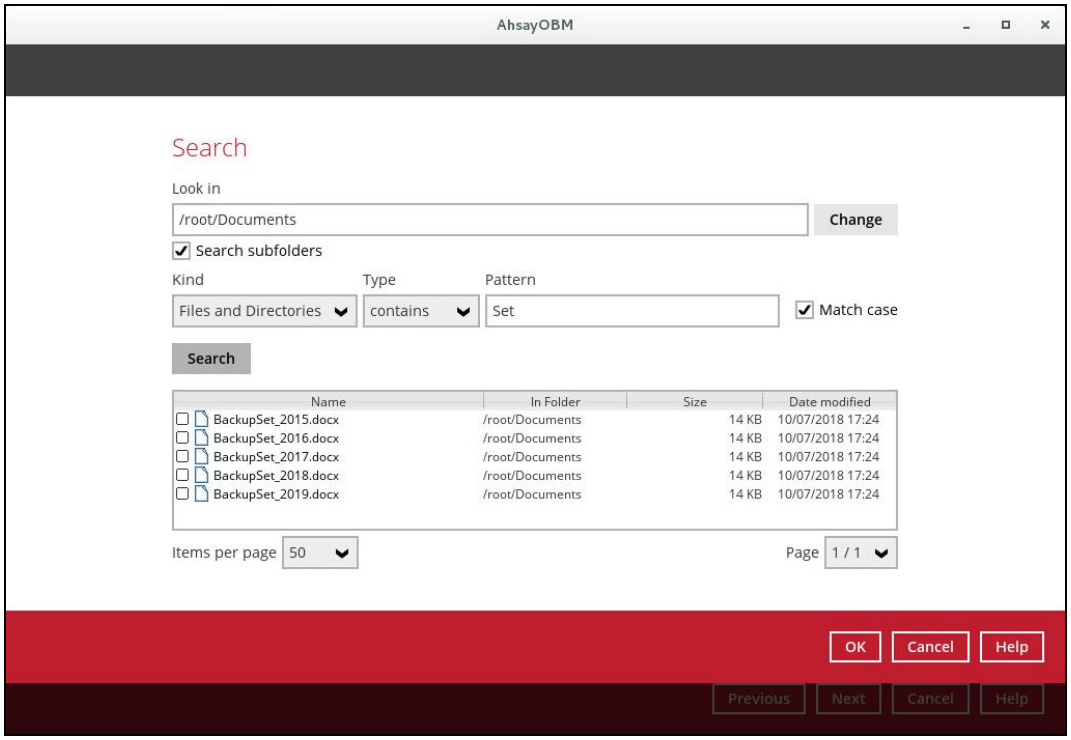
Example No.1: Restore filter setting from /root/Documents with filter type Contains

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

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







Explanation:

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

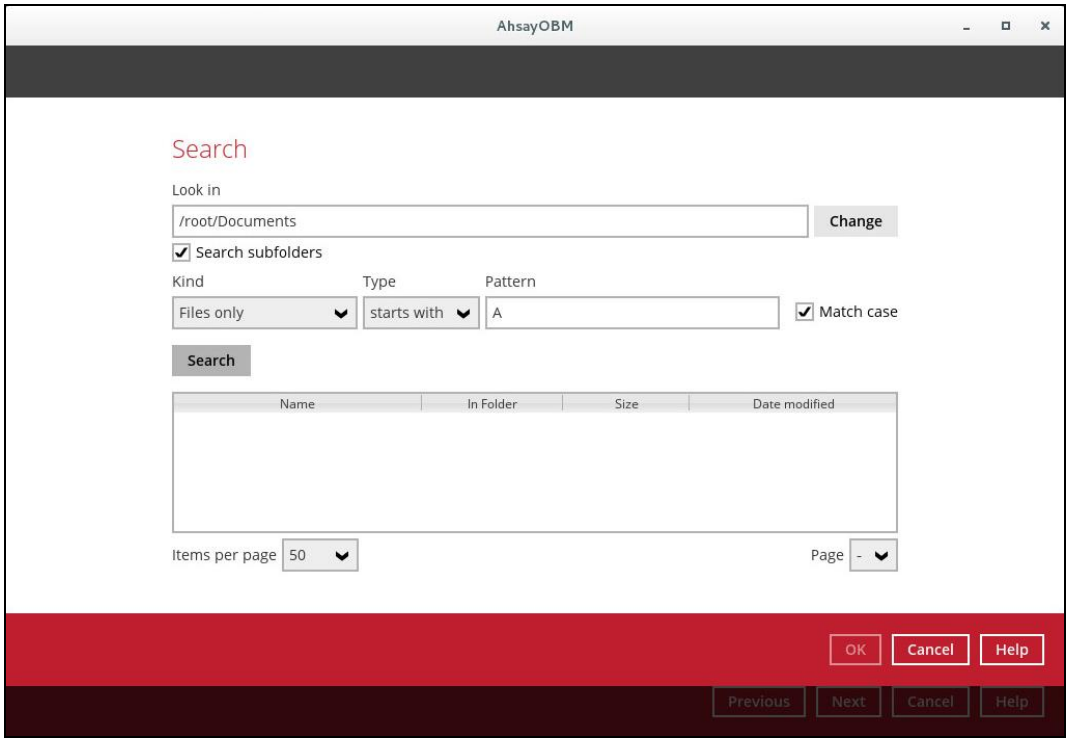
As you can see on the screen shot above, the result panel contains the Name of the file or directory, Directory which are indicated In-Folder column, Size, and Date Modified.

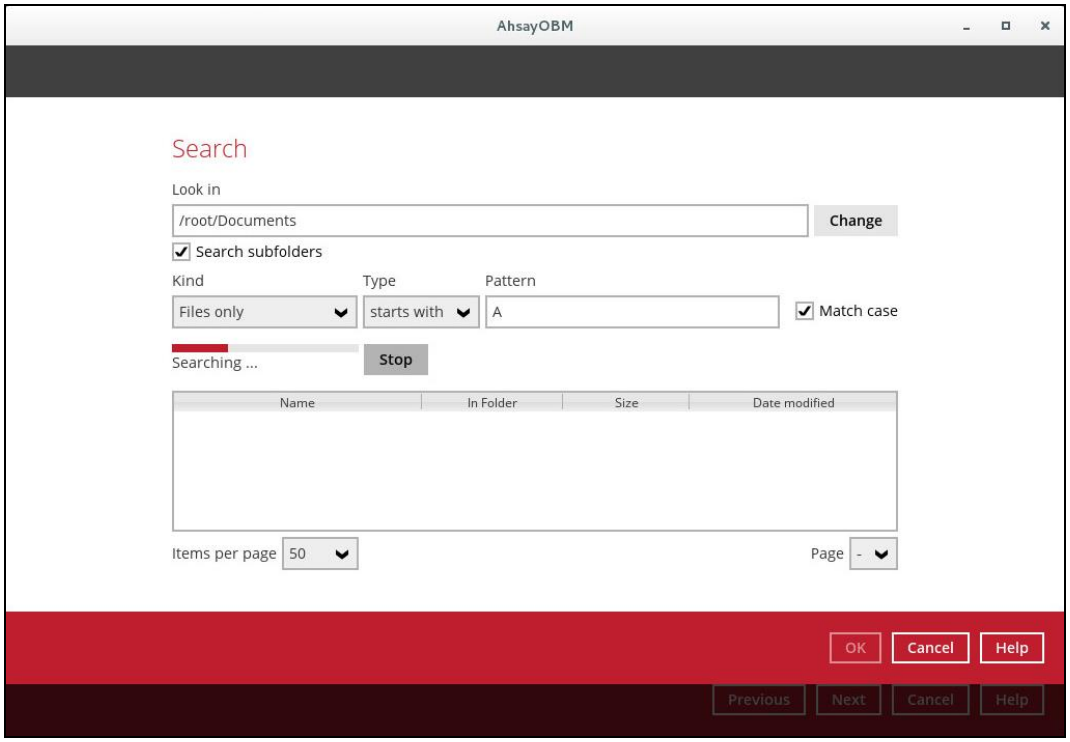
The restore filter setting includes the Search subfolder and Match case set to true. Meaning, the filter will include all available subfolders in \Documents upon searching. And it will strictly search only the specified pattern and case which starts with ‘Set’.

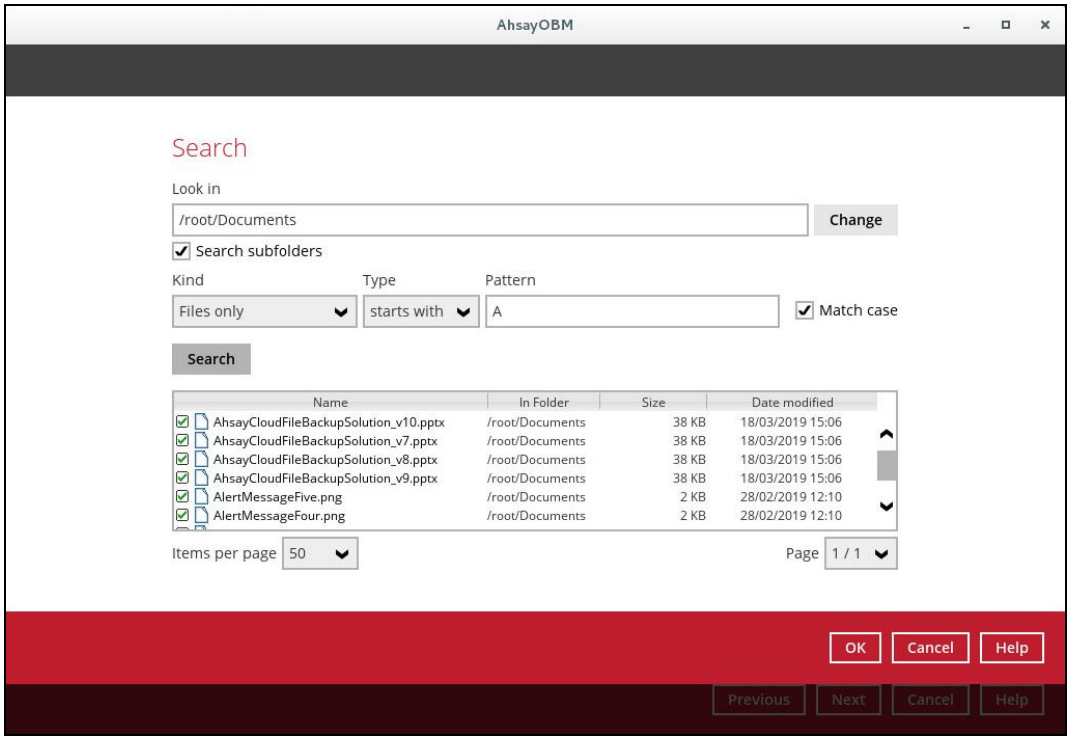
Example No.2: Restore filter setting from /root/Documents with filter type Starts With

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

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







Explanation:

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

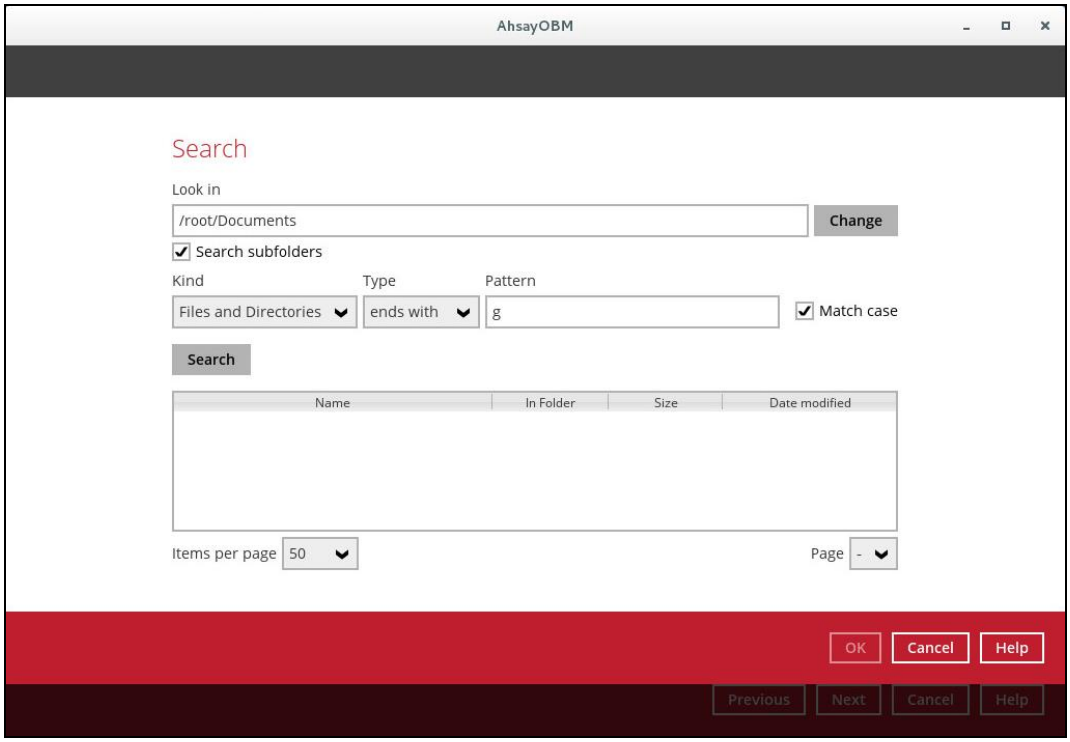
As you can see on the screen shot above, the result panel contains the Name of the file, Directory which are indicated In-Folder column, Size, and Date Modified.

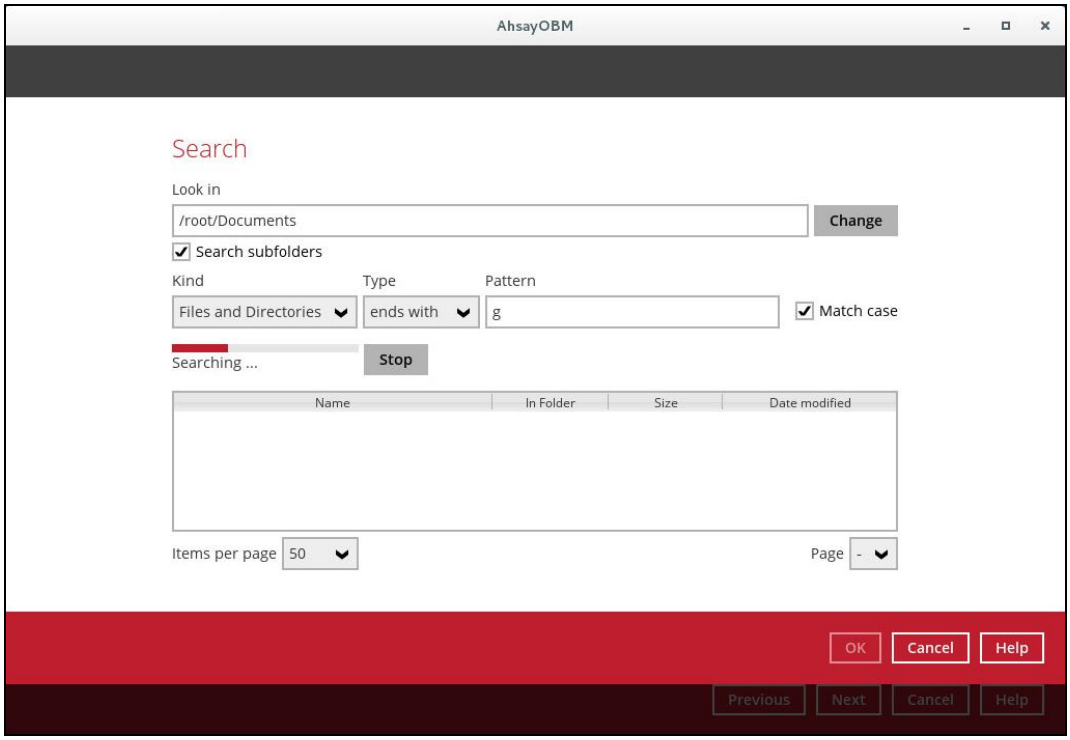
The restore filter setting includes the Search subfolder and Match case set to true. Meaning, the filter will include all available subfolders in \Documents upon searching. And it will strictly search only the specified pattern and case which starts with ‘A’.

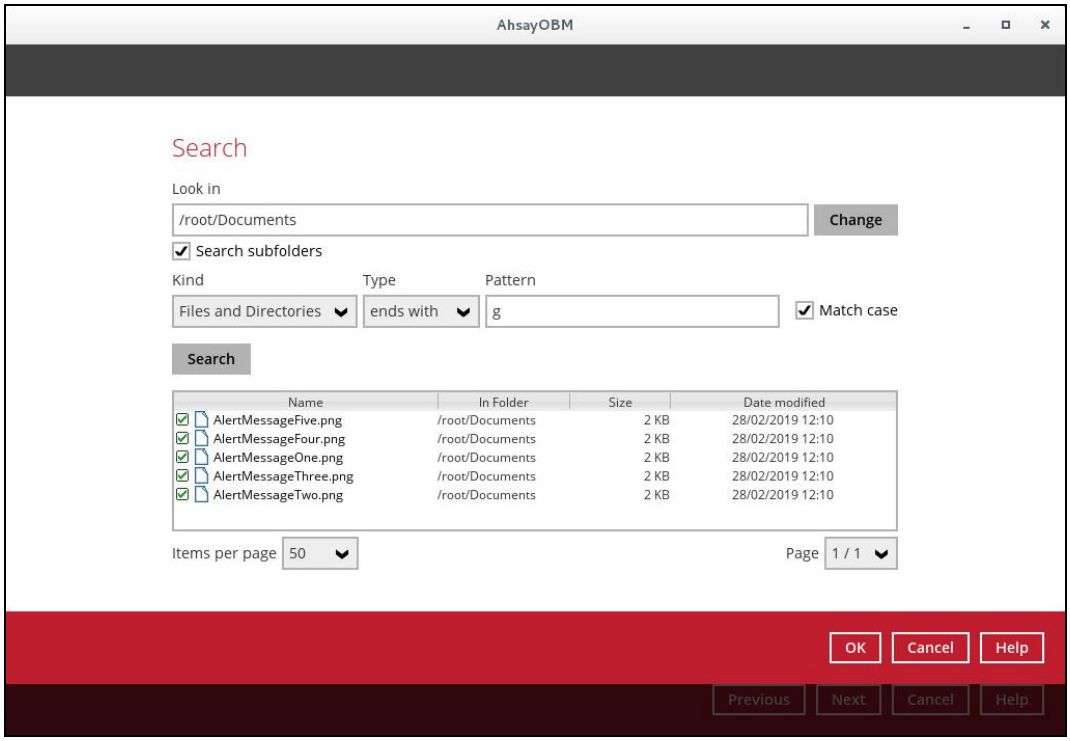
Example No.3: Restore filter setting from /root/Documents with filter type Ends With

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

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







Explanation:

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

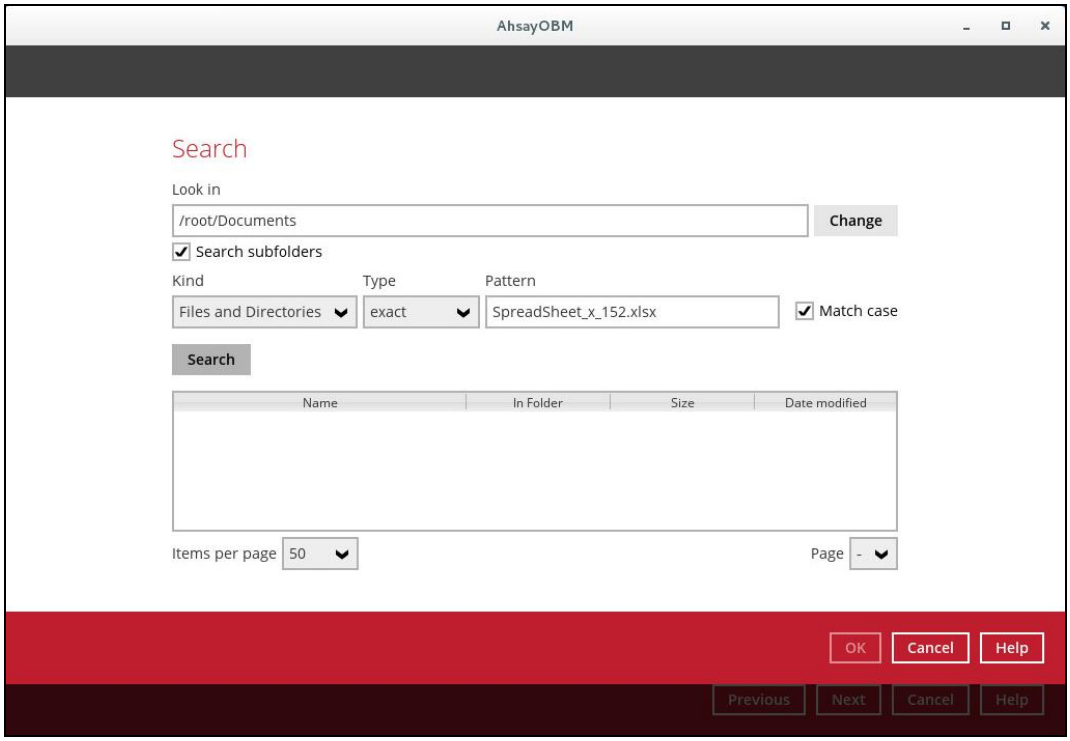
As you can see on the screen shot above, the result panel contains the Name of the files and directories, Directory which are indicated In-Folder column, Size, and Date Modified.

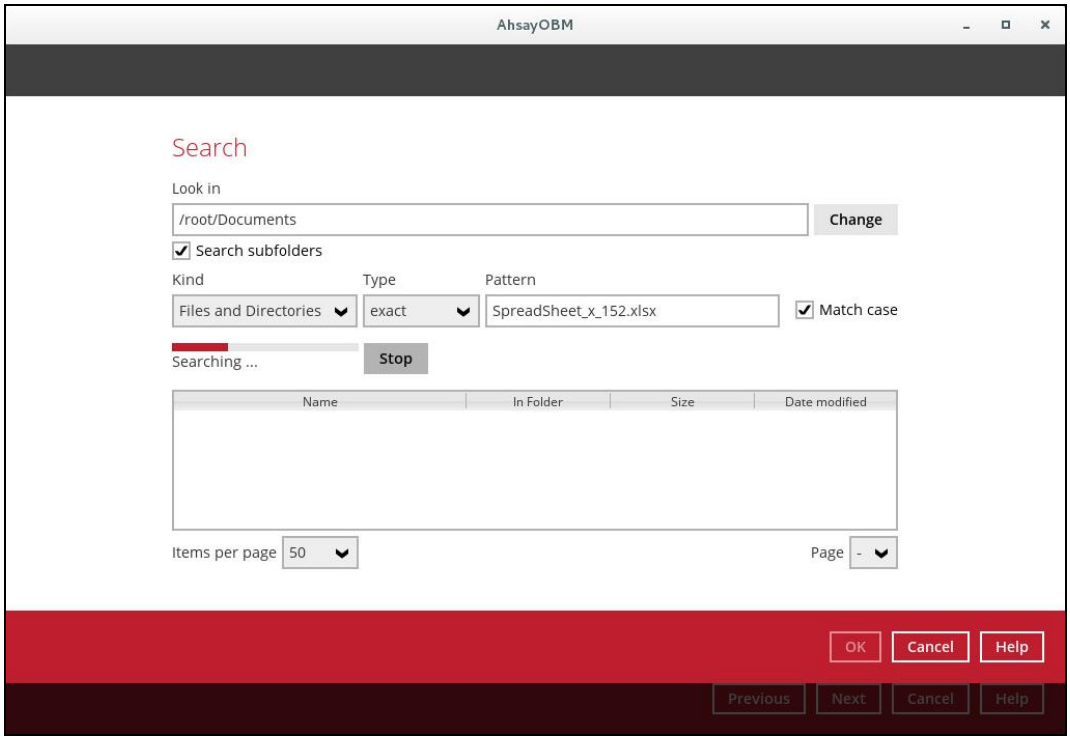
The restore filter setting includes the Search subfolder and Match case set to true. Meaning, the filter will include all available subfolders in \Documents upon searching. And it will strictly search only the specified pattern and case which starts with ‘g’.

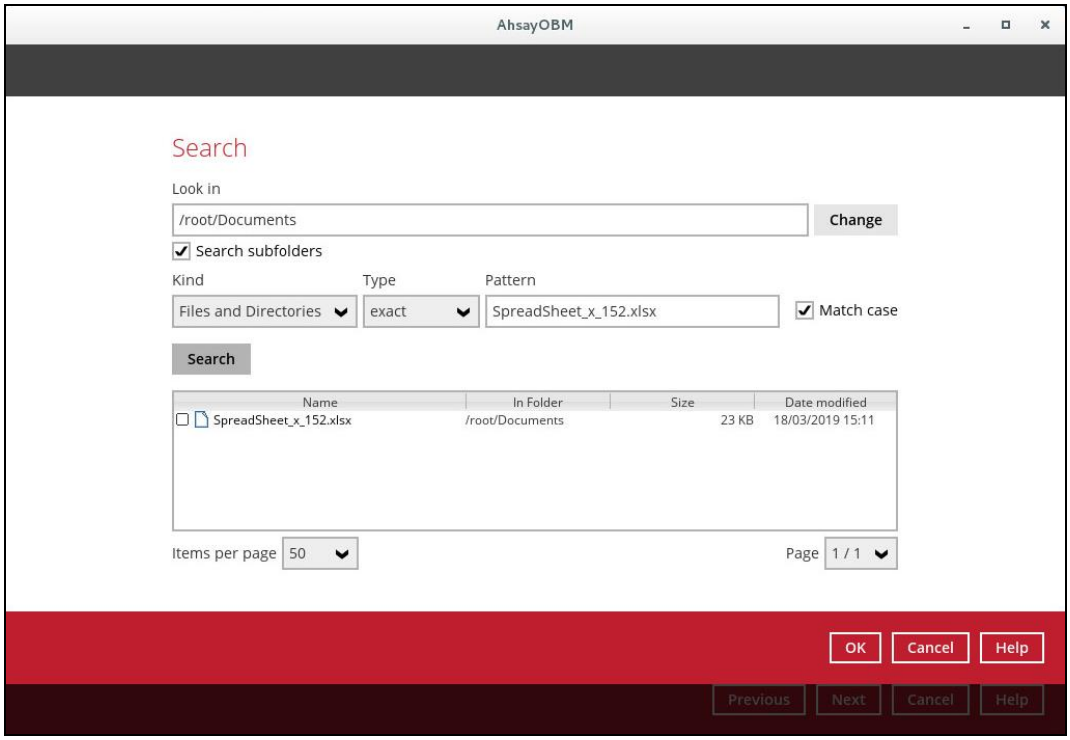
Example No.4: Restore filter setting from /root/Documents with filter type Exact

Location:	/root/Documents
Search subfolders:	True
Kind:	Files and Directories
Type:	Exact
Pattern:	SpreadSheet_x_152.xlsx
Match Case:	True

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







Explanation:

All files and directories under \root\Documents that has the pattern that has the exact pattern 'SpreadSheet_x_152.xlsx' with match case set to true will be included upon performing search.

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

The restore filter setting includes the Search subfolder and Match case set to true. Meaning, the filter will include all available subfolders in \Documents upon searching. And it will strictly search only the specified pattern and case which starts with 'SpreadSheet_x_152.xlsx'.

Appendix G: Create Free Trial Account in AhsayOBM

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

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

While here are the limitations of a trial account:

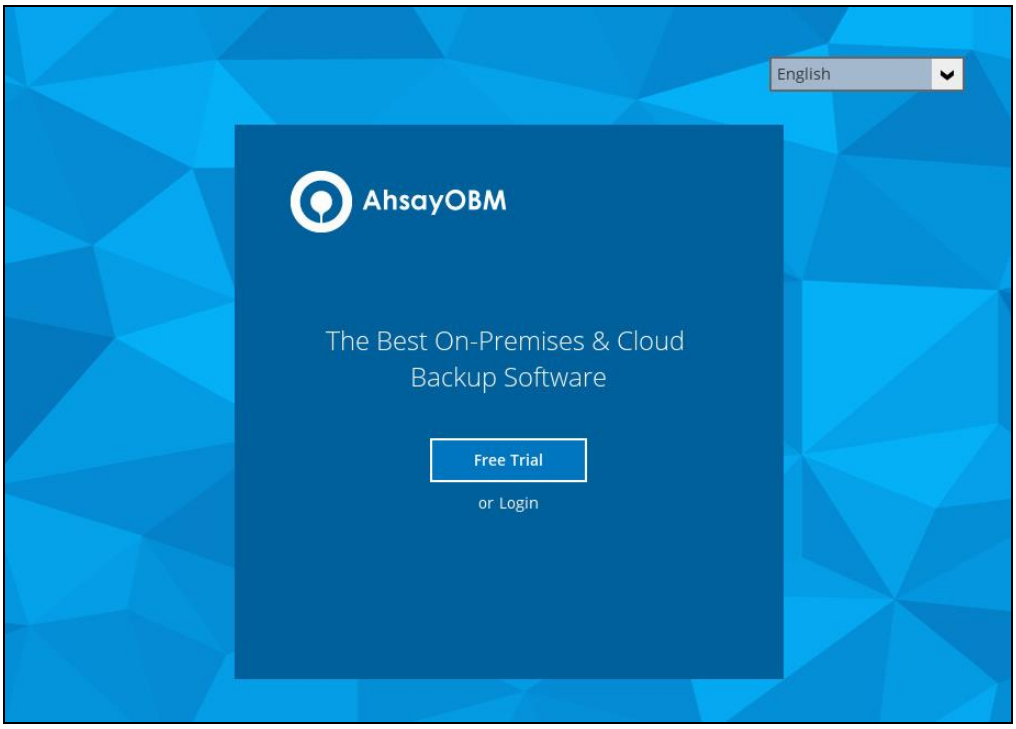
- The Free Trial button will only be displayed once when the user login for the first time. If you cannot create a free trial account kindly contact your backup service provider.
- Only alphanumeric characters and selected special characters, A to Z, 0 to 9, @, - and _, are allowed to be used for the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

NOTE

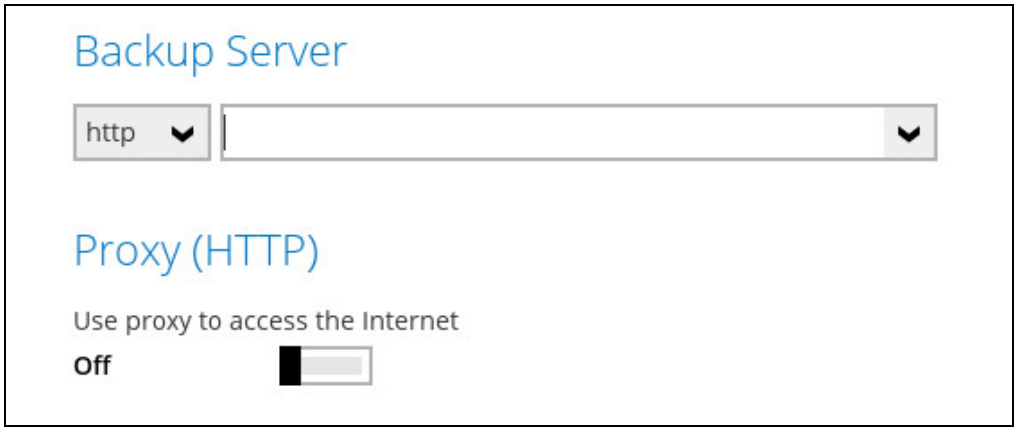
The Free Trial Registration option may not be available. This depends on the settings of your backup service provider. Please contact your backup service provider for more information.

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

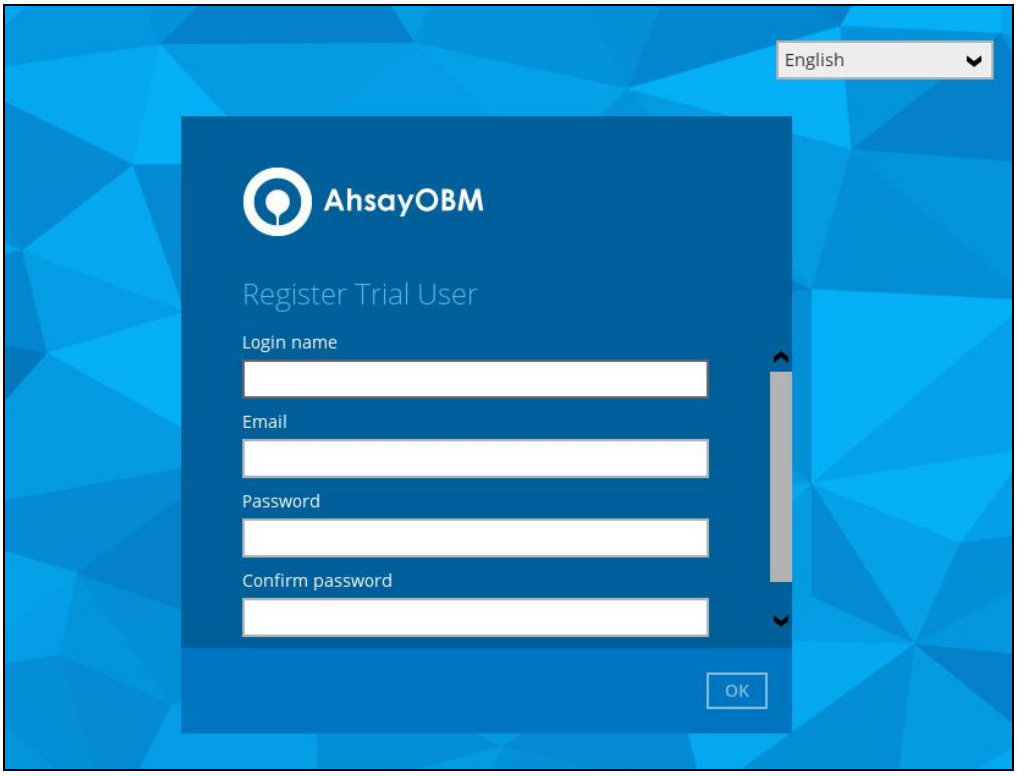
1. Click on **Free Trial**.



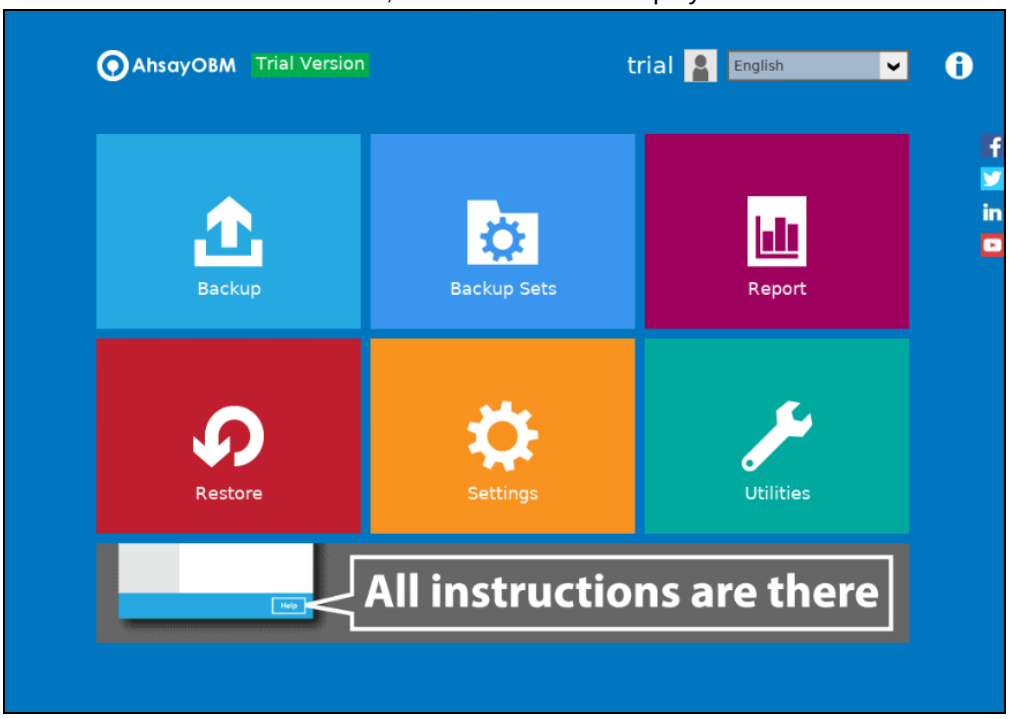
2. Configure your Backup Server settings.



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



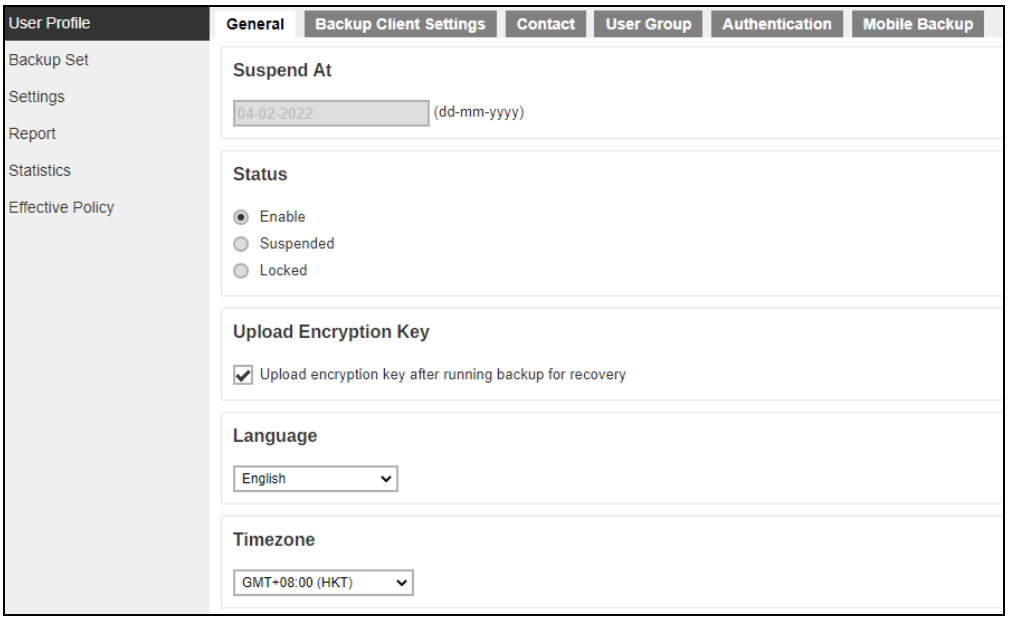
4. Once the trial account is created, this screen will be displayed.



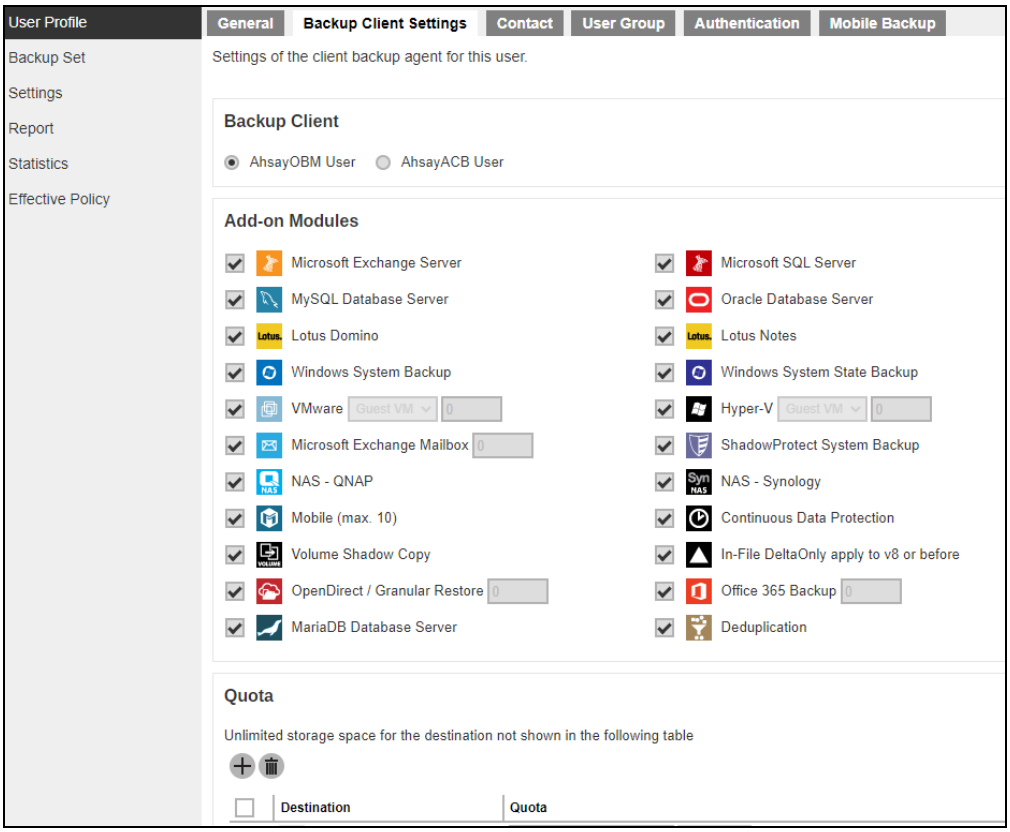
5. After your trial account has been created, you need to check several things:

   - 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.

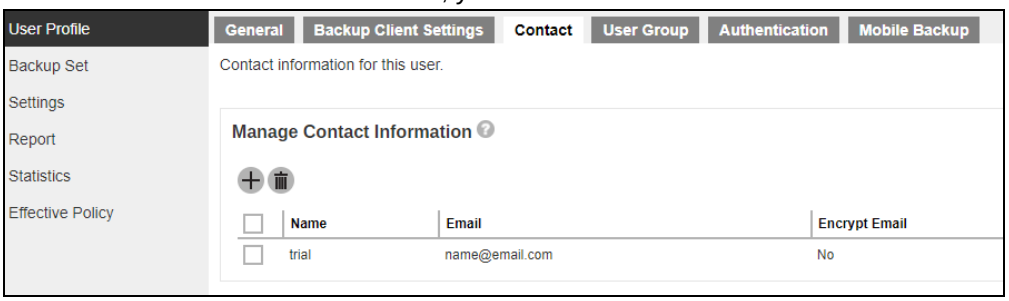
   You can check this by logging in to AhsayCBS, go to **Backup / Restore > User > User Profile > General**. For more information please refer to the AhsayCBS User's Guide.



6. You also need to check the available add-on modules and quota by going to the **Backup Client Settings** tab.



7. 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.

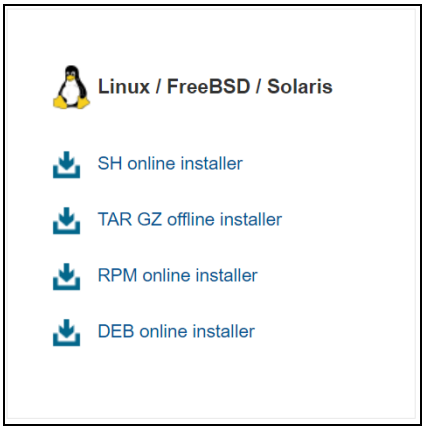


Appendix H: Manually Upgrade AhsayOBM

Before you proceed with upgrading of AhsayOBM to the latest version, make sure that you have read the system requirements especially if upgrading from AhsayOBM v6 or v7.

To upgrade AhsayOBM, follow the instructions below.

1. Uninstall the current AhsayOBM version depending on how AhsayOBM was installed. There are three ways to uninstall AhsayOBM.
   - To uninstall AhsayOBM installed using **SH** online installer, refer to Appendix A
   - To uninstall AhsayOBM installed using **RPM** online installer, refer to Appendix B
   - To uninstall AhsayOBM installed using **DEB** online installer, refer to Appendix C
2. Go to the download page of your backup service provider's website and select which type of installation method you would like to use.



3. Refer to Chapter 5 Download and Install AhsayOBM to download and install the latest version of AhsayOBM.
   - For online installation method using either **SH**, **RPM**, or **DEB** online installer, refer to Ch. 5.1 Online Installation.
   - For offline installation method using **TAR GZ** offline installer, refer to Ch. 5.2 Offline Installation.