

Ahsay Online Backup Manager v9

Quick Start Guide for Linux (GUI)

Ahsay Systems Corporation Limited

27 January 2023

Copyright Notice

© 2023 Ahsay Systems Corporation Limited. All rights reserved.

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

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

Trademarks

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

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

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

Dropbox is a registered trademark of Dropbox Inc.

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

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

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

MariaDB is a registered trademark of MariaDB Corporation AB.

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

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

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

OpenJDK is a registered trademark of Oracle America, Inc.

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

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

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

Ubuntu is a registered trademark of Canonical Ltd.

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

Rocky is a registered trademark of Rocky Brands.

ShadowProtect is a registered trademark of StorageCraft Technology Corporation.

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

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

Disclaimer

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

Revision History

Date	Descriptions	Version
25 January 2022	▪ Ch. 9.5 – added Deduplication	9.1.0.0
7 March 2022	▪ Ch. 12.2 – updated note for Migrate Data	9.1.0.0
6 May 2022	▪ Ch. 9.5 – additional note in Command Line Tool	9.1.0.0
8 August 2022	▪ Ch. 3.8 – added non-compressible file list	9.1.0.0
3 November 2022	<ul style="list-style-type: none">▪ Ch. 9.5 – updated Deduplication screenshots and block size choices; added backup schedule priority; added Recycle Bin instructions▪ Ch. 9.9.1 – updated screenshots and added Delete corrupted data blocks permanently description▪ Ch. 13.2 – updated screenshots due to Show backup job(s) outside retention area checkbox	9.5.0.0
22 November 2022	▪ Ch. 9.5 – fixed typo in Recycle Bin	9.5.0.0
27 January 2023	▪ Ch. 13.2 – updated Restore instructions	9.5.2.0

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
3.8	Limitations	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.....	139
9.6.1	Backup	139
9.6.2	Restore	143
9.6.3	Usage	147
9.7	Restore	149
9.8	Settings.....	149
9.8.1	Proxy	149
9.8.2	Mobile Backup	150
9.9	Utilities	160
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

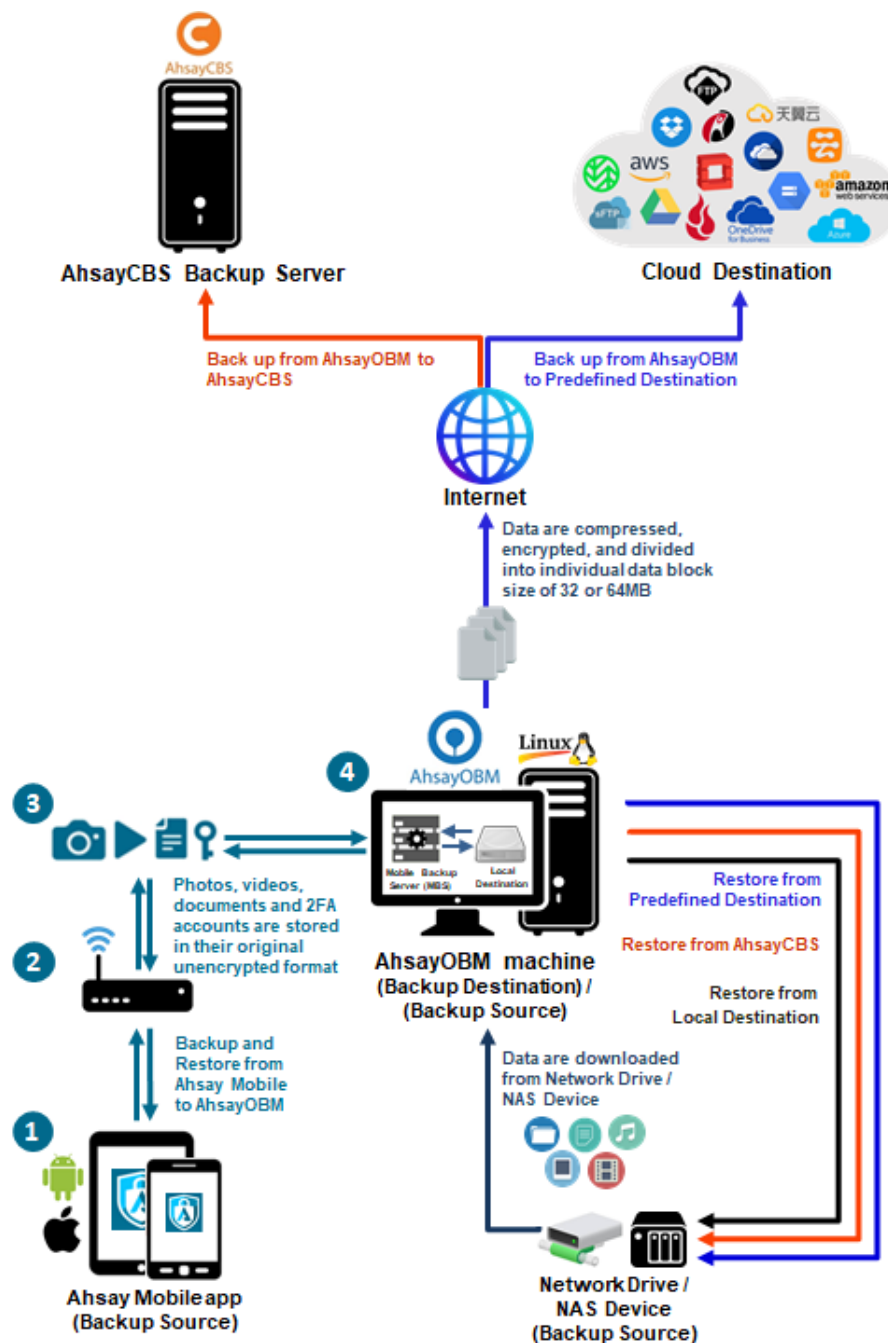
1 Overview

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.

Mobile Backup Setup

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

 Mobile Backup (Add new device for backup without migration)



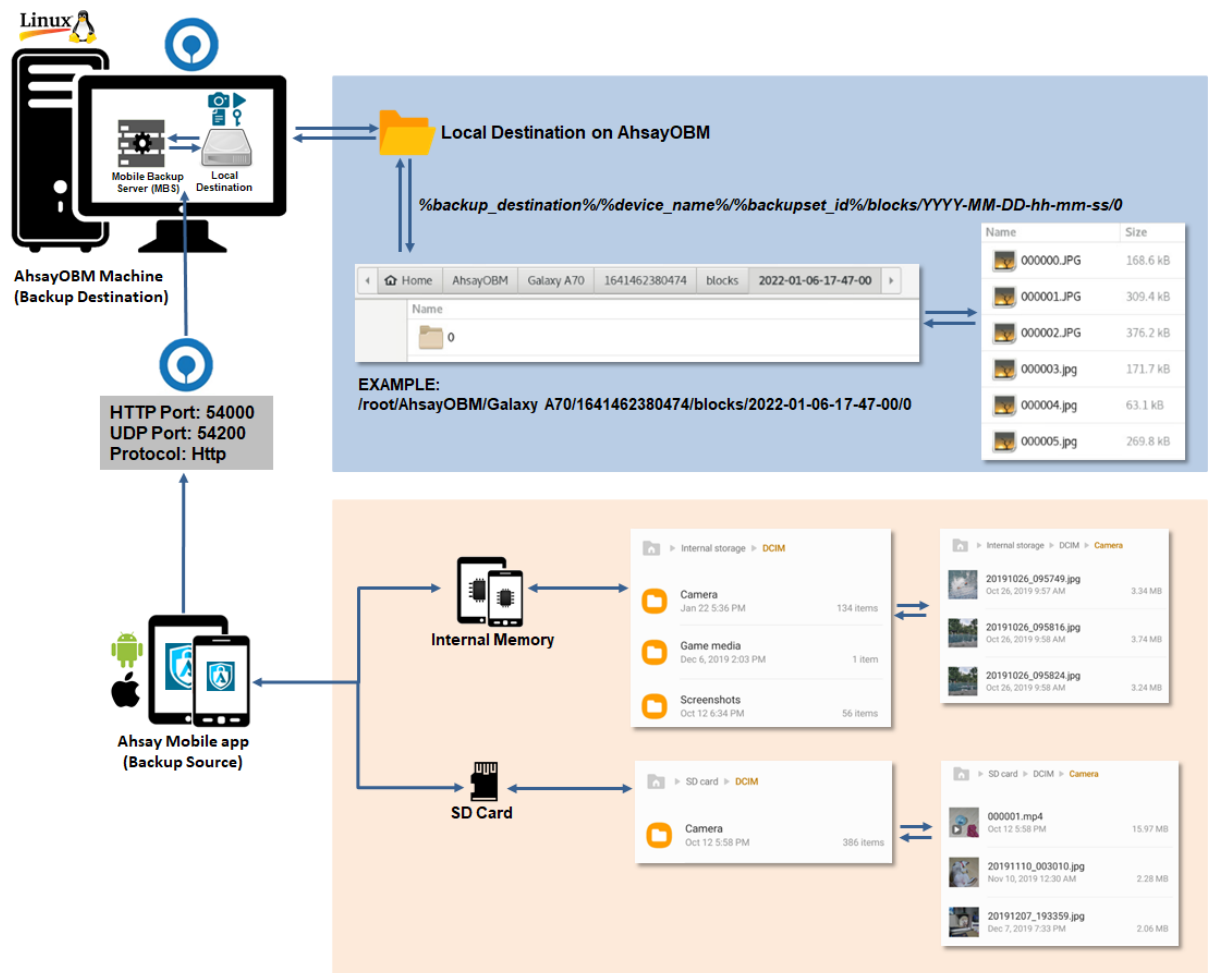


- Please make sure below 2 ports are not blocked by any Firewall settings

TCP Port: 54000

UDP Port: 54200

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

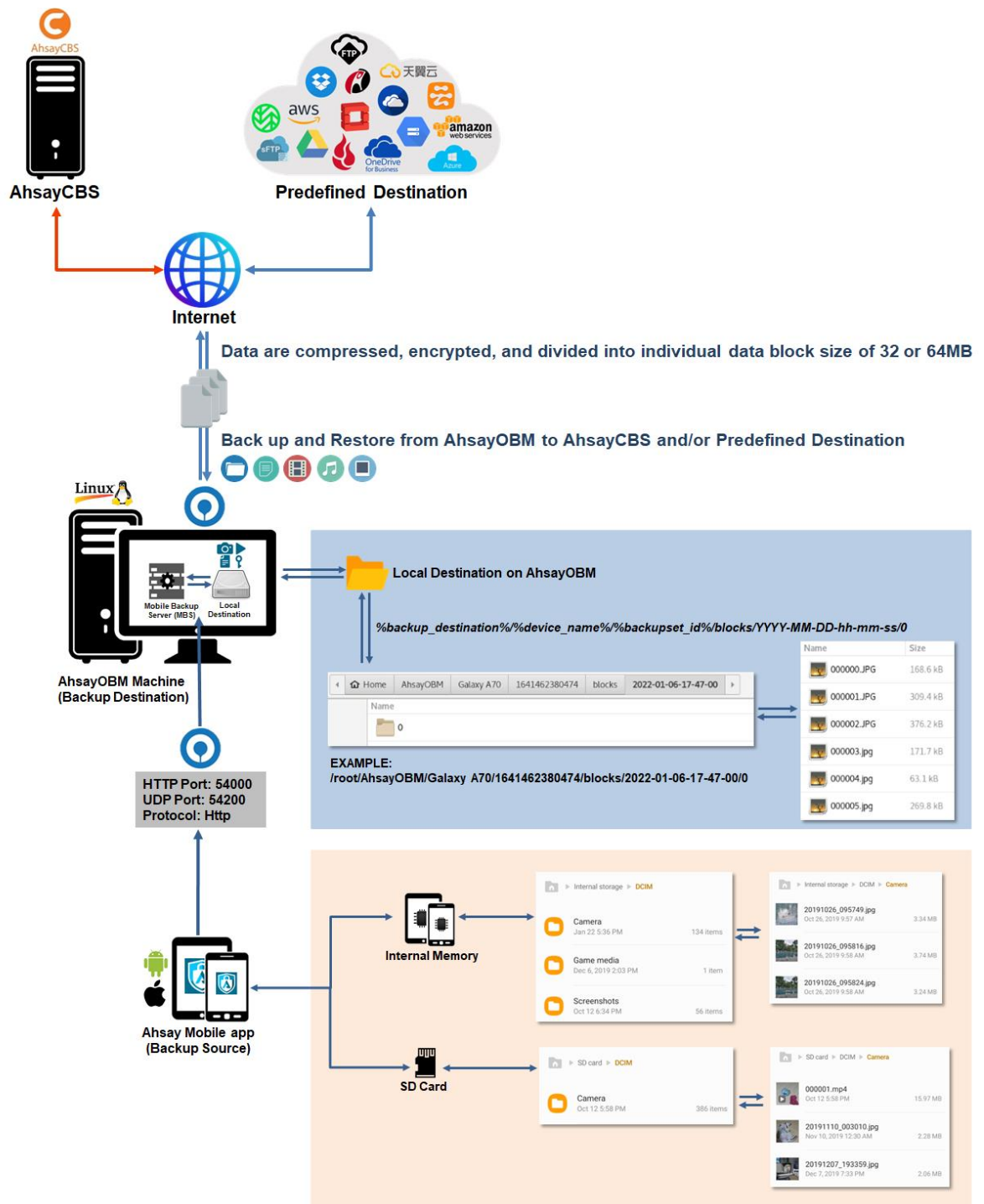


If storage of photos, videos, documents and 2FA accounts to AhsayCBS and/or Predefined Destination is required, then this can be done using AhsayOBM to perform a secondary backup and restore of the photos, videos, documents and 2FA accounts on the local drive to AhsayCBS and/or Predefined Destination.

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

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

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



1.4 Two-Factor Authentication

Two-Factor Authentication (2FA) supports TOTP (Time-based One-time Password) and Push notification 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.

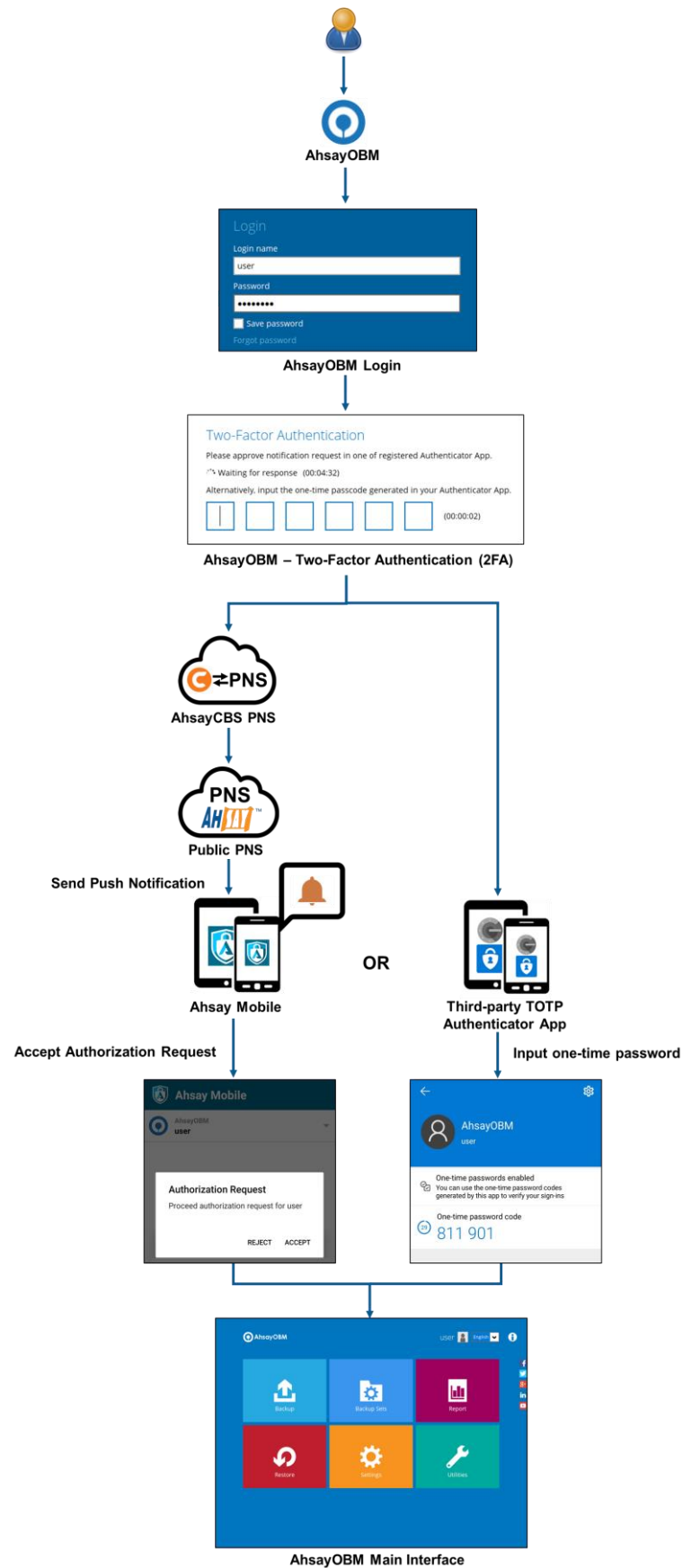
If Ahsay Mobile is used as the authenticator app:

- 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.

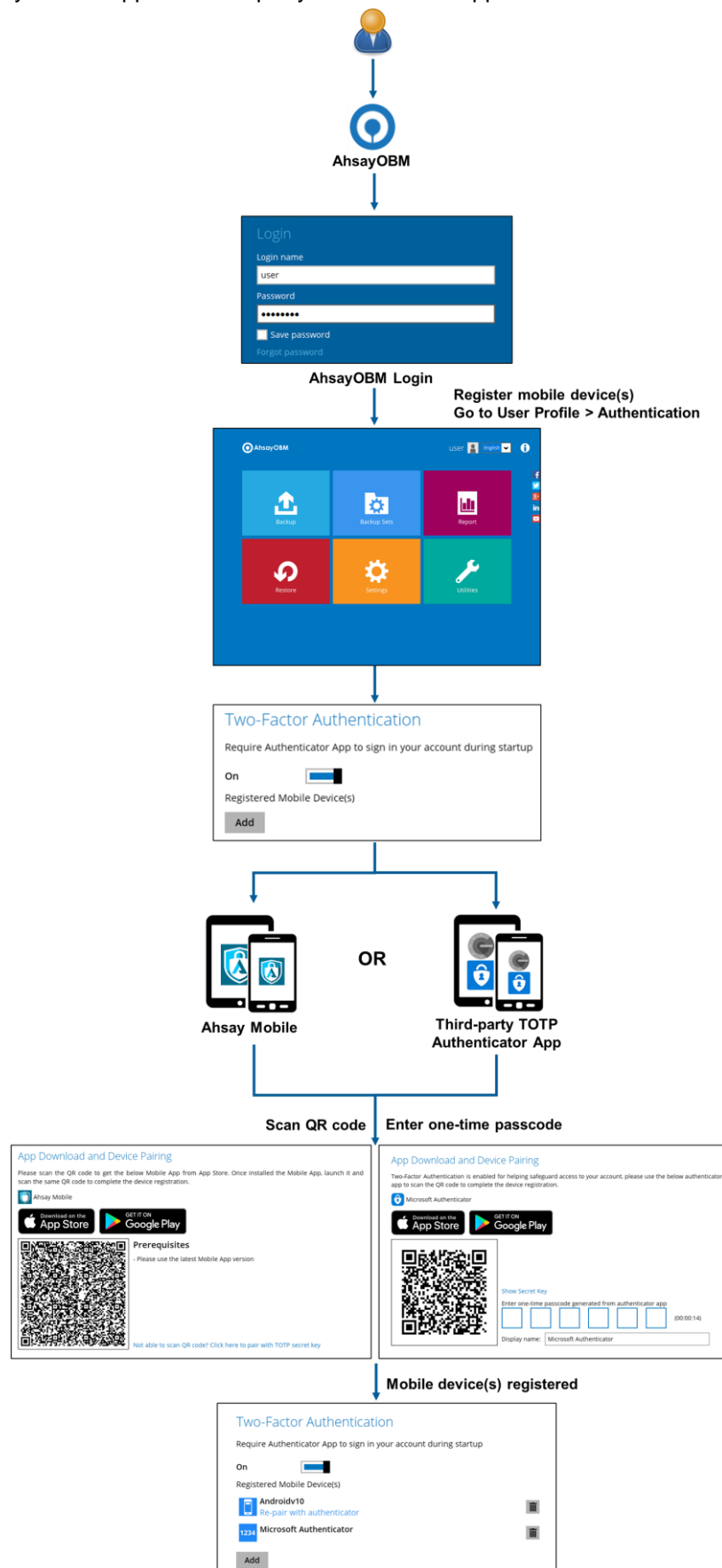
If a third-party authenticator app is used:

- 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.

3.8 Limitations

The following is a list of non-compressible files:

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

4 Getting Started

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

Download and Install

Download and Install AhsayOBM on your Linux machine

Launch AhsayOBM

Launch and log in to AhsayOBM

Set up 2FA and/or Mobile Backup

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

Create a Backup Set

Create a backup set according to your preference

Run Backup Jobs

Run the backup job to back up data

Restore Data

Restore backed up data to your system

5 Download and Install AhsayOBM

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

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

NOTE

The following platforms only support online installation:

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

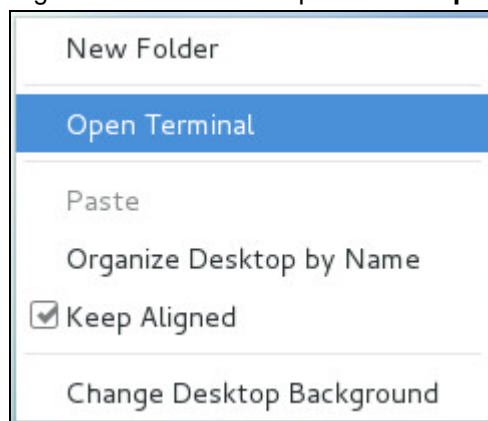
5.1 Online Installation

5.1.1 SH online installer

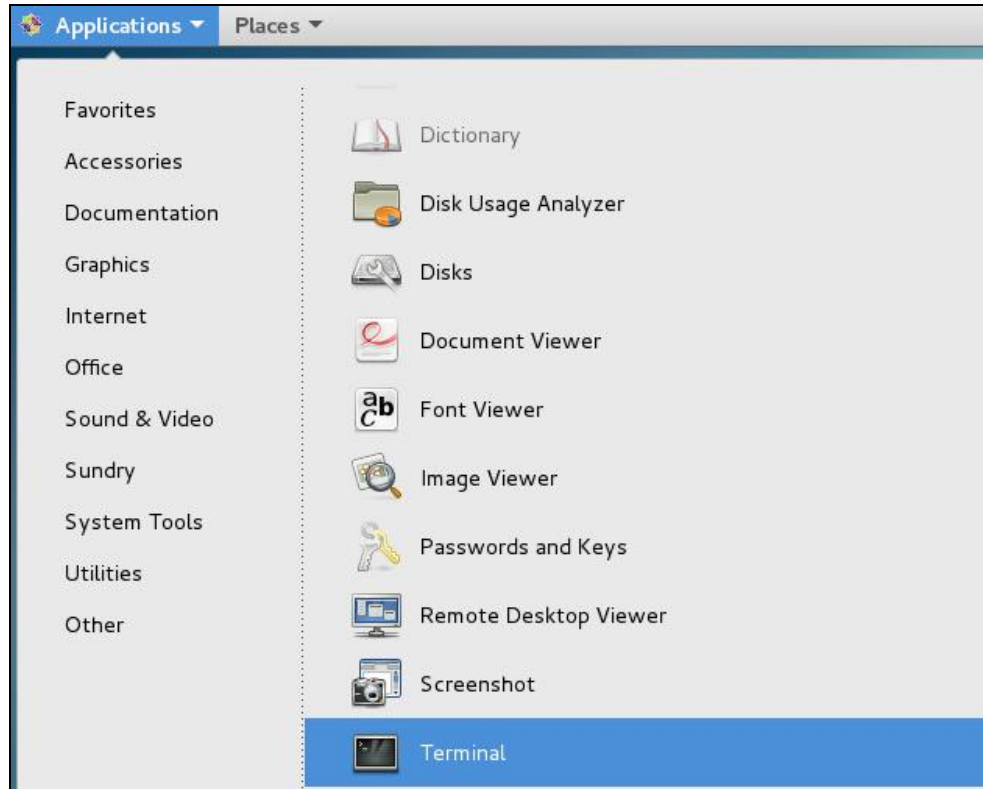
1. Log in to a Linux machine using the root account. (Alternatively, you can remotely invoke the GUI of another Linux machine using SSH client.)



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



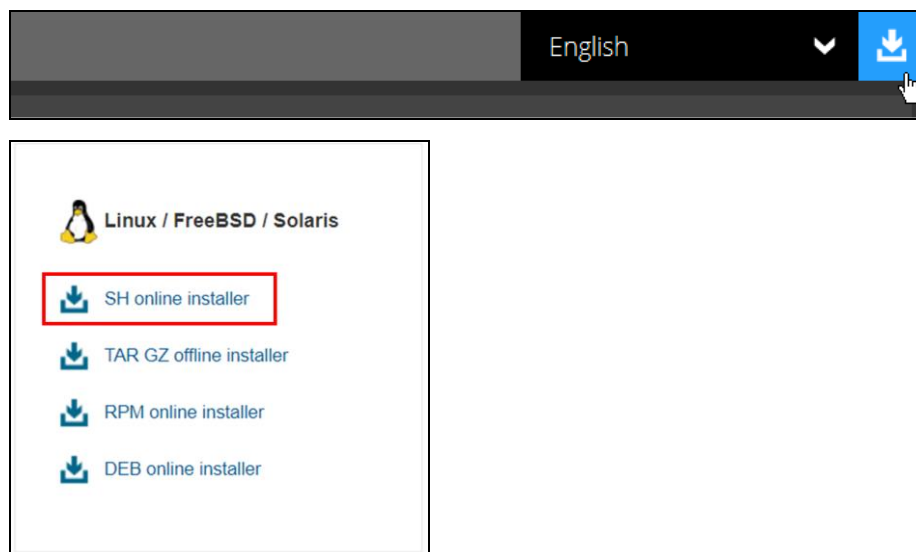
Alternatively, you can also click the **Applications** menu bar then select **Utilities > Terminal**.



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.

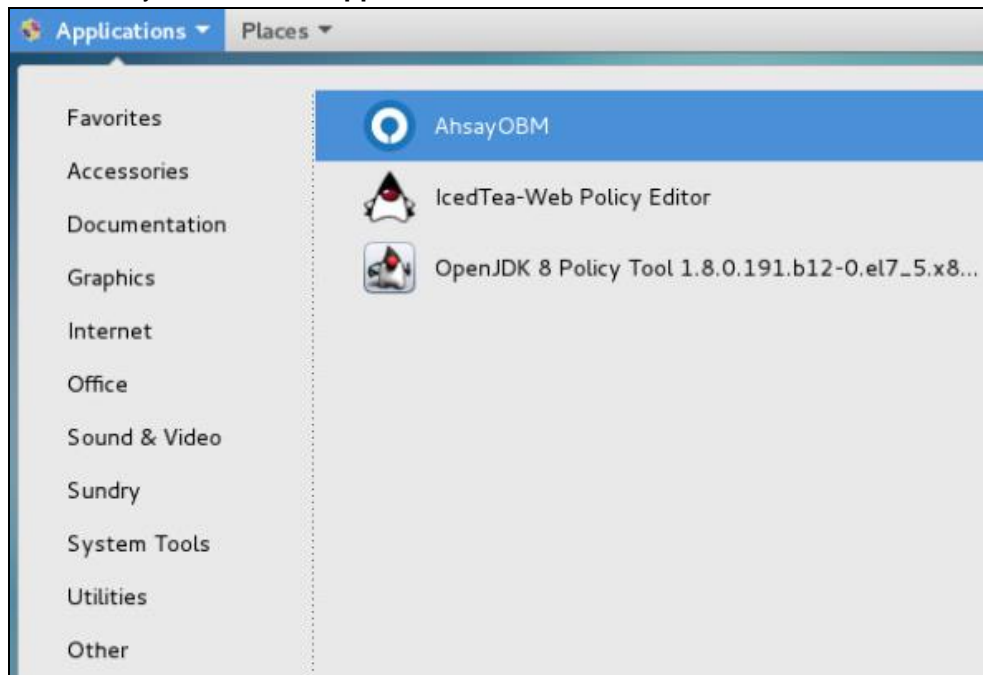
NOTE: The .sh script file should be copied and run under the directory path where you want the AhsayOBM application to be installed, i.e., /usr/local/obm

```
# ./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**.

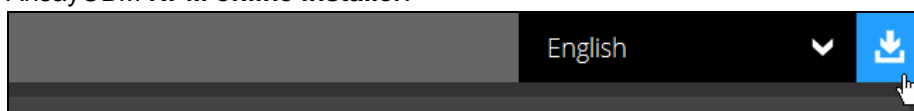


5.1.2 RPM online installer

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.)

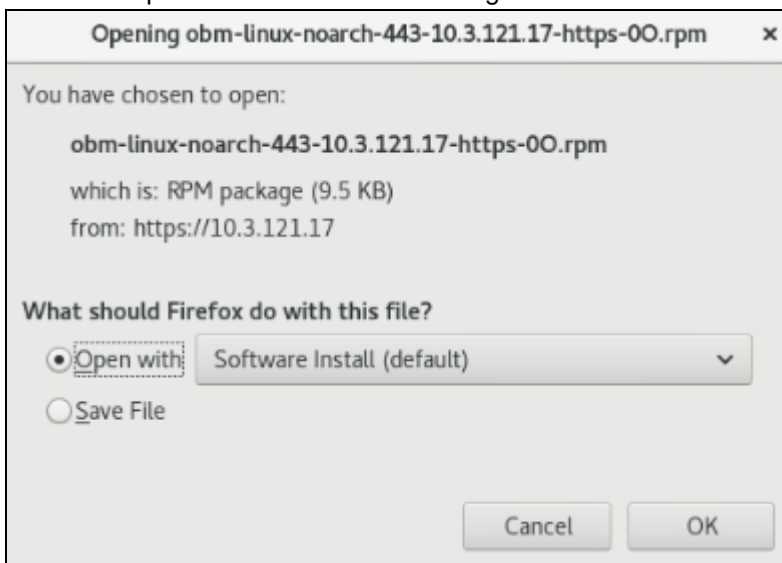


2. Go to the download page of your backup service provider's website and download the AhsayOBM **RPM online installer**.

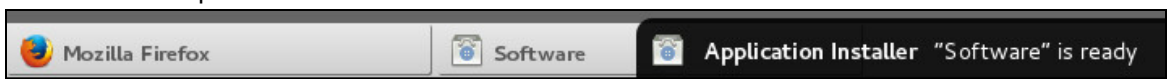




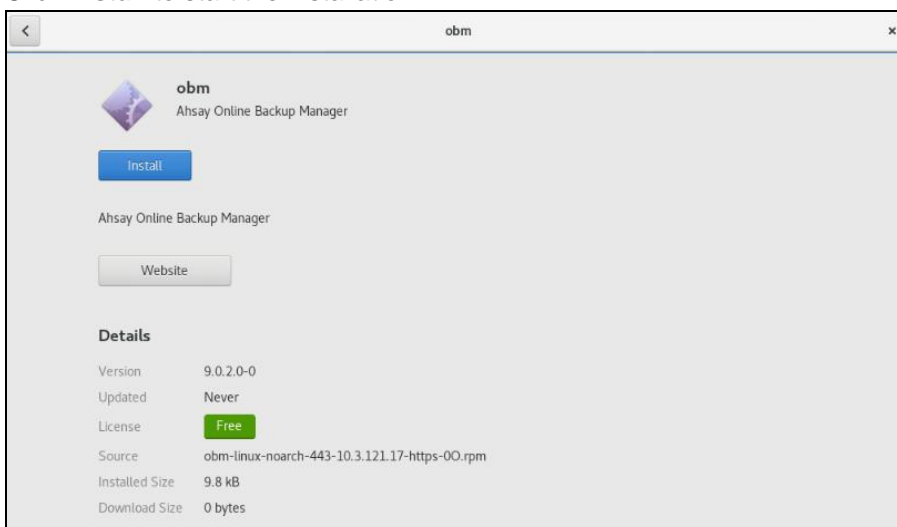
3. Click **OK** to proceed with the downloading of file.



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



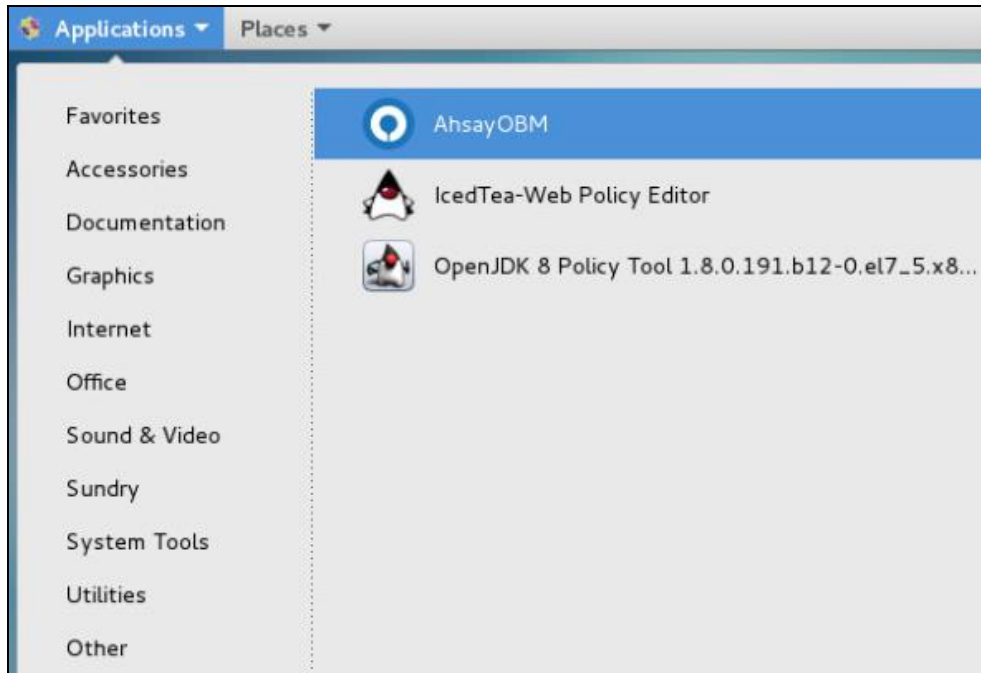
5. Click **Install** to start the installation.



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

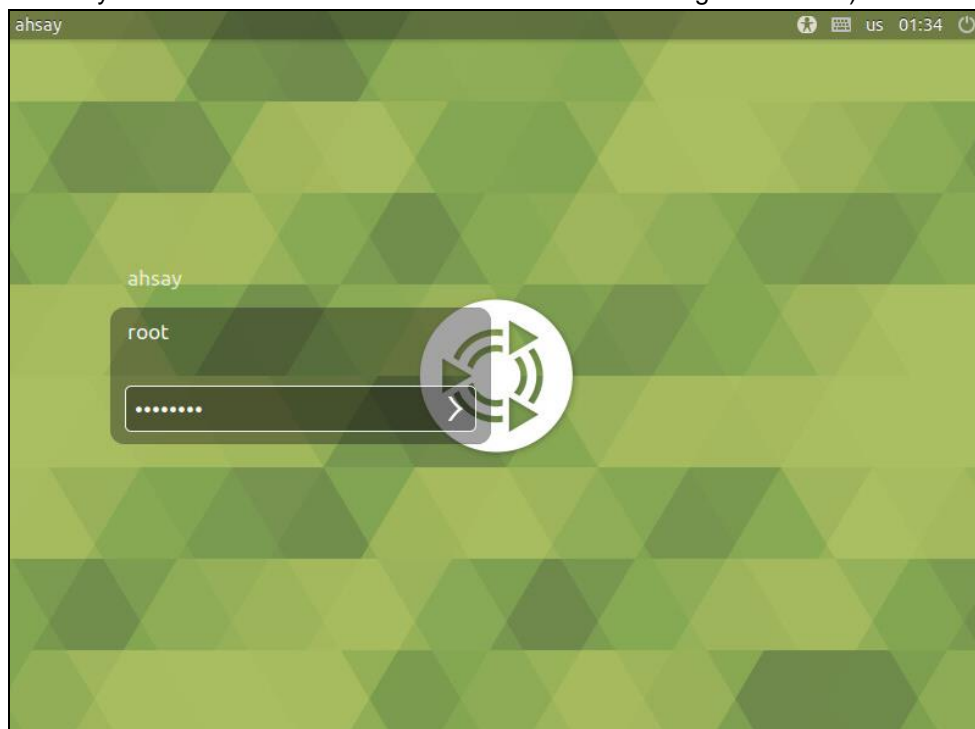


Another way is to click the **Applications** menu bar, then select **Other** to access **AhsayOBM**.



5.1.3 DEB online installer

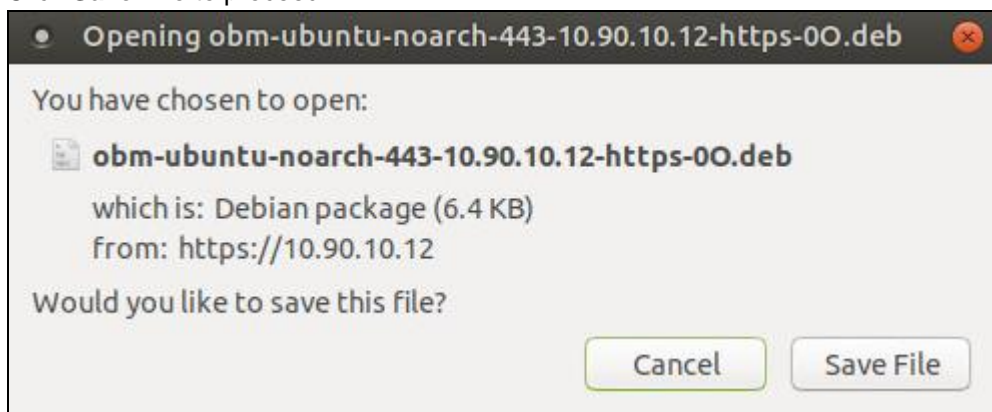
1. Log in to a Debian or Ubuntu machine using the root account. (Alternatively, you can remotely invoke the GUI of another Debian or Ubuntu using SSH client.)



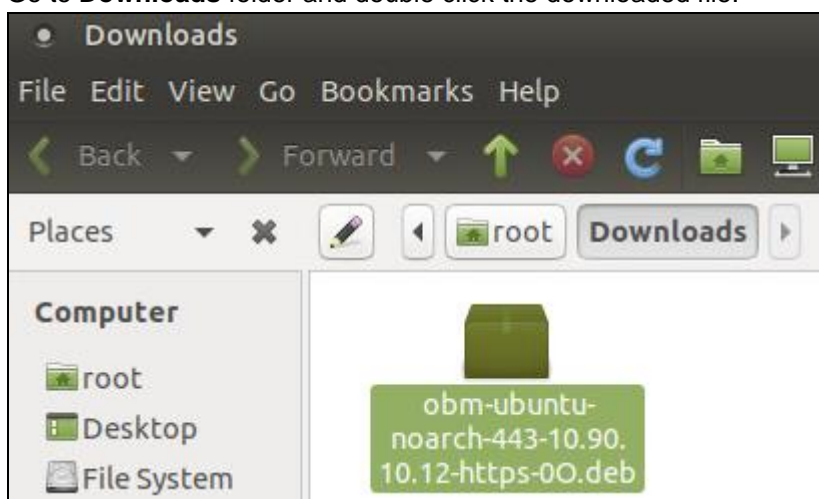
2. Go to the download page of your backup service provider's website and download the AhsayOBM **DEB online installer**.



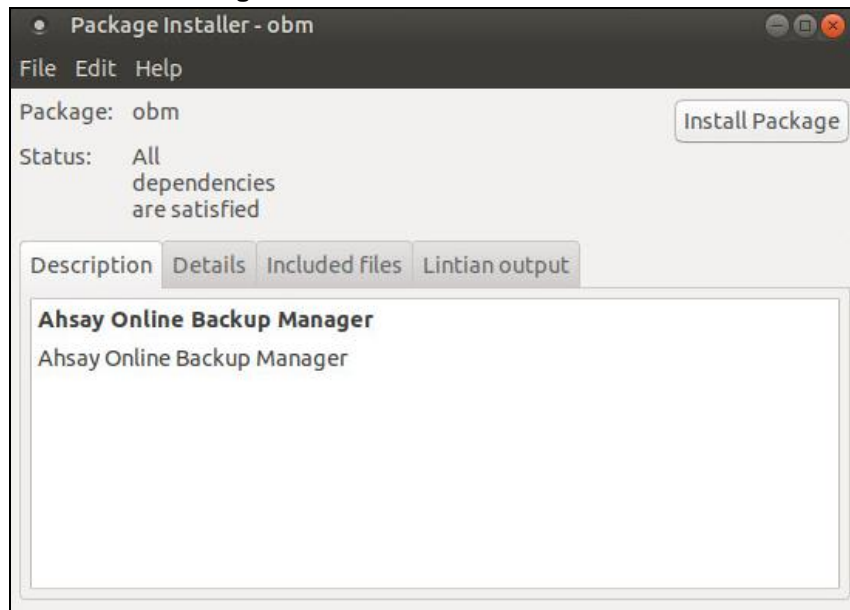
3. Click **Save File** to proceed.



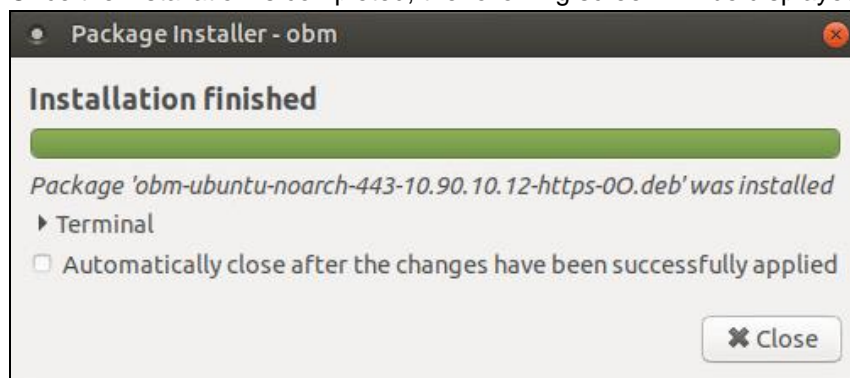
4. Go to **Downloads** folder and double click the downloaded file.



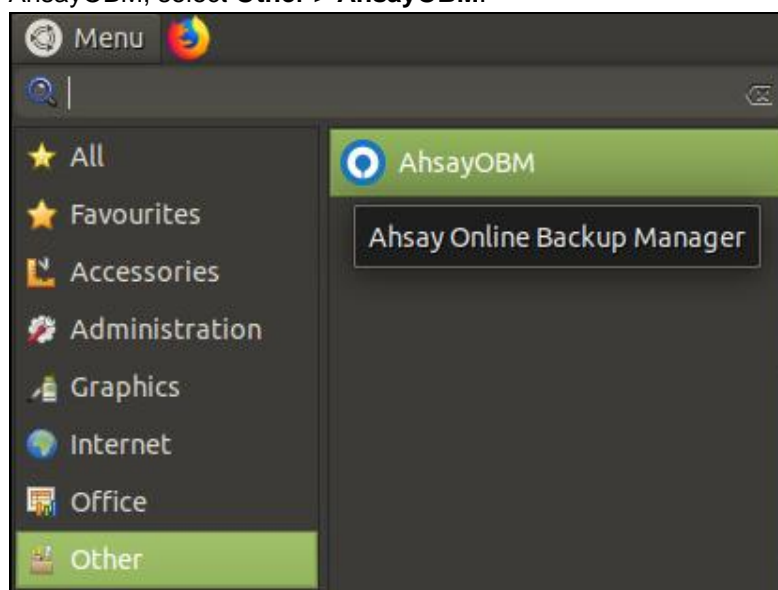
5. Click **Install Package** to start the installation.



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

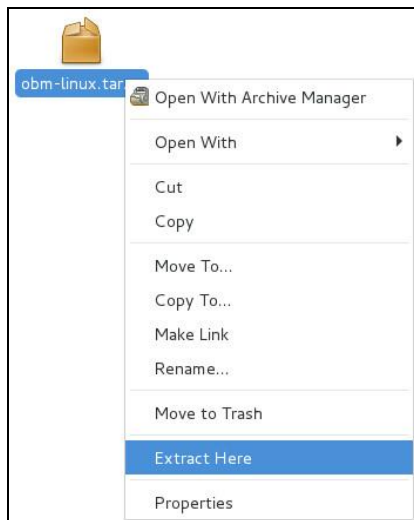
1. Log in to a Linux machine using the root account. (Alternatively, you can remotely invoke the GUI of another Linux machine using SSH client.)



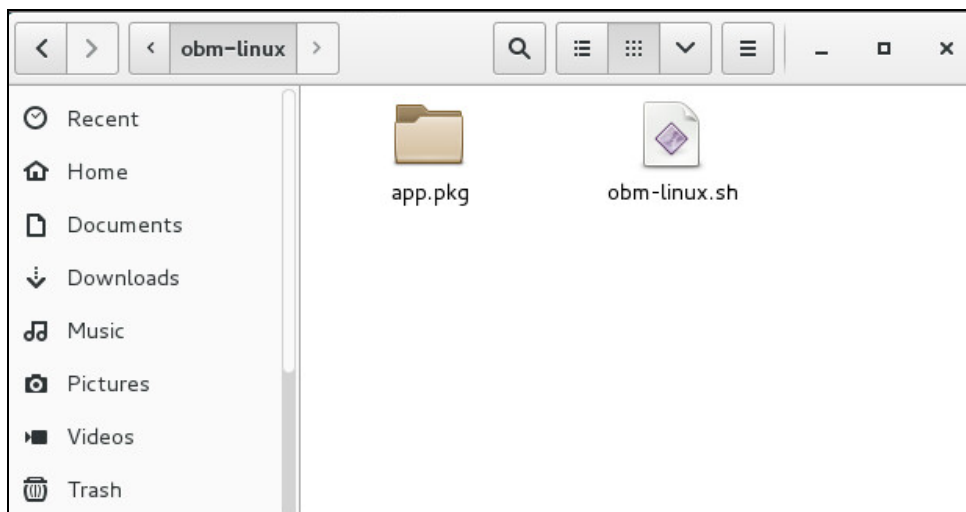
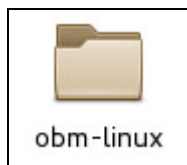
2. Go to the download page of your backup service provider's website and download the AhsayOBM **TAR GZ offline installer**.



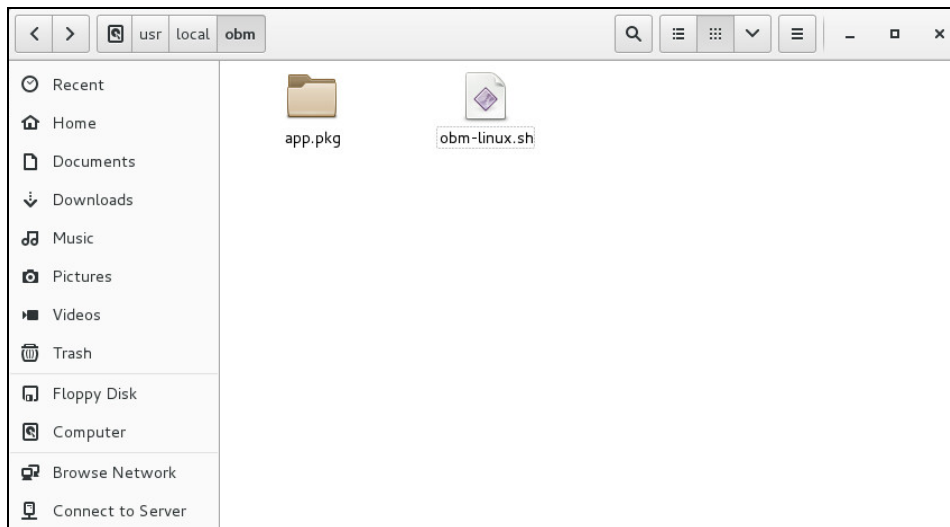
3. Right click on the AhsayOBM installation package **.gz** file to extract.



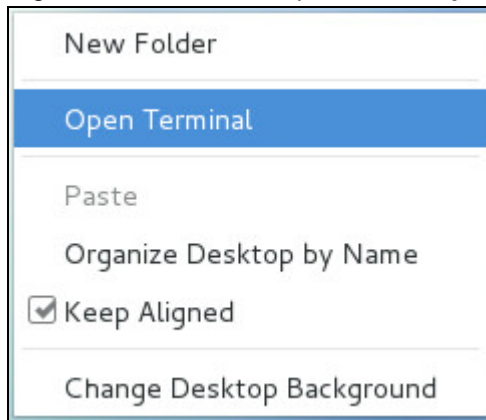
4. Open the folder to check the extracted installation package.



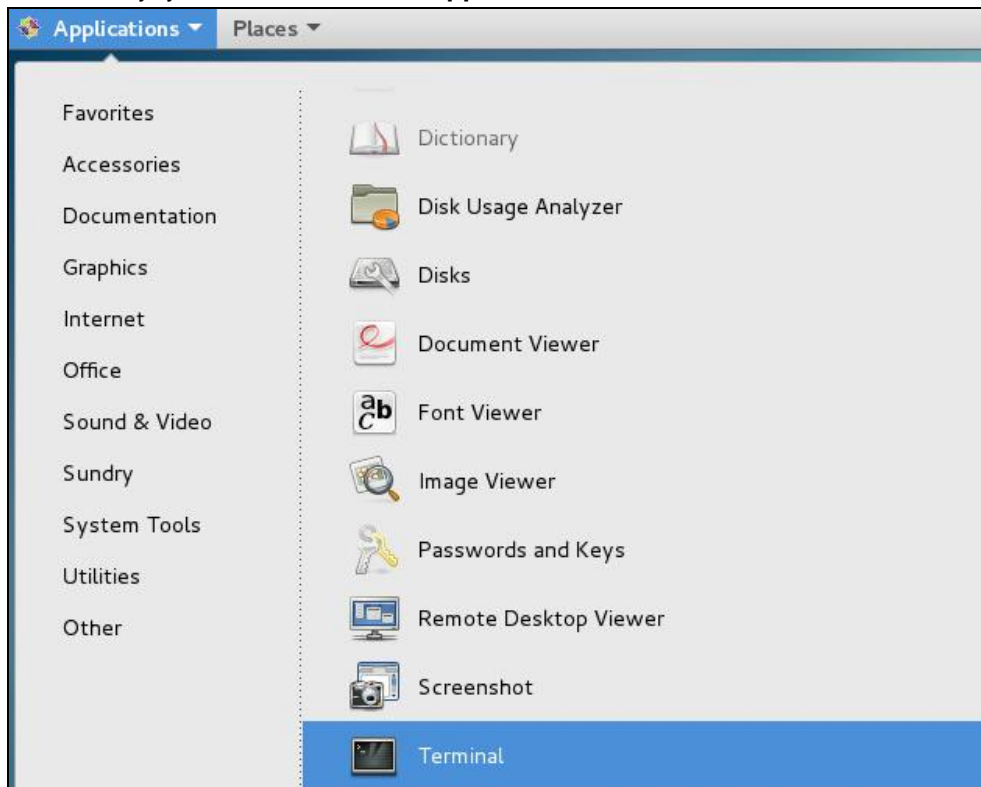
5. Create a folder for AhsayOBM under the **/usr/local** directory, then move the extracted **obm-linux.sh** file to the obm folder.



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
```

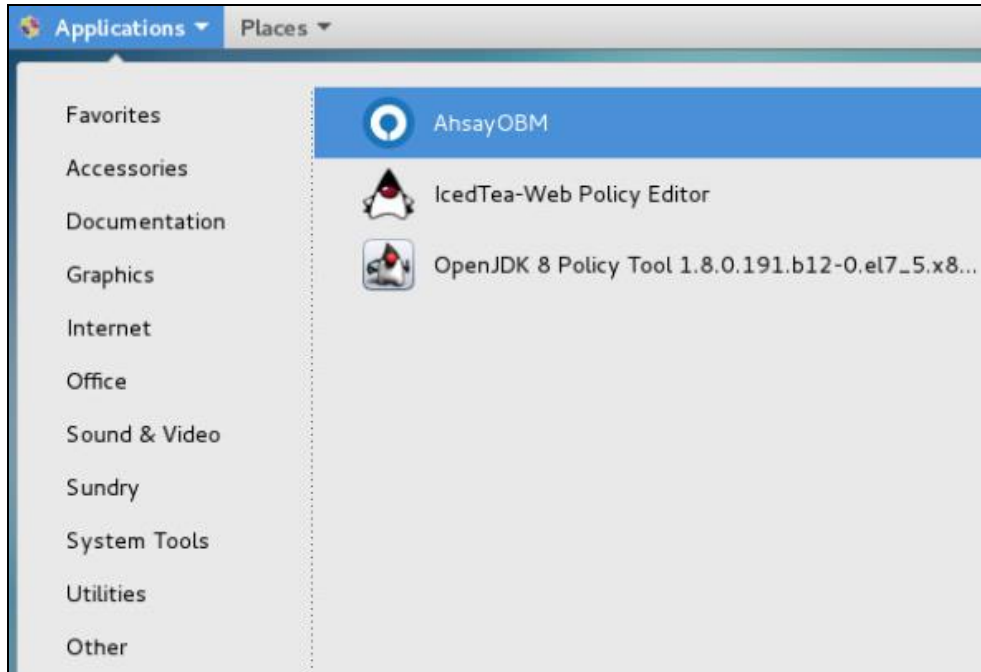
8. Use the **sh** command to install AhsayOBM.

```
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.

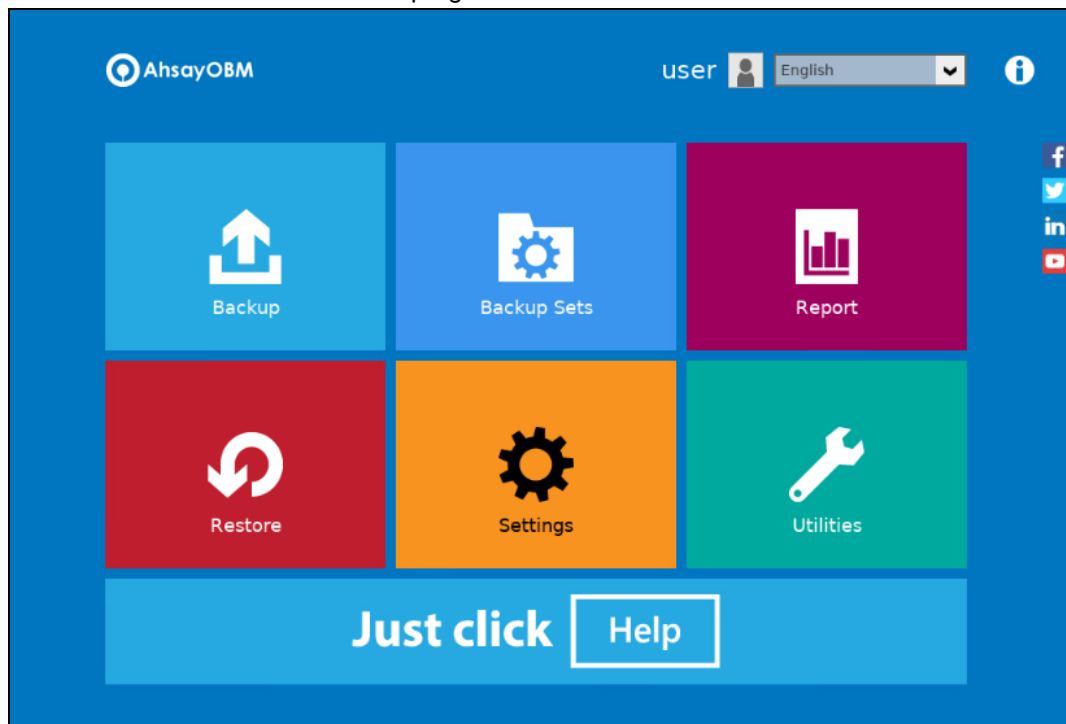


Another way is to click the **Applications** menu bar, then select **Other** to access **AhsayOBM**.

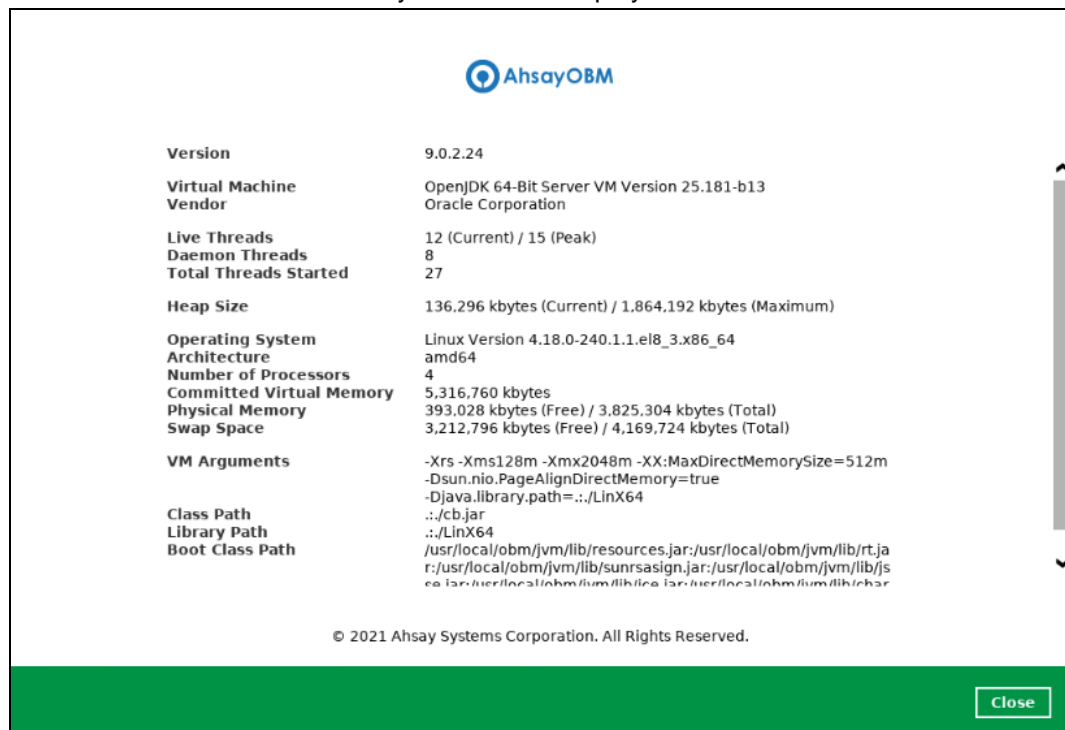


Check Version of AhsayOBM

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

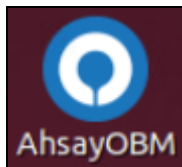
To register a device for 2FA in AhsayOBM using Ahsay Mobile, here are the two scenarios:

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

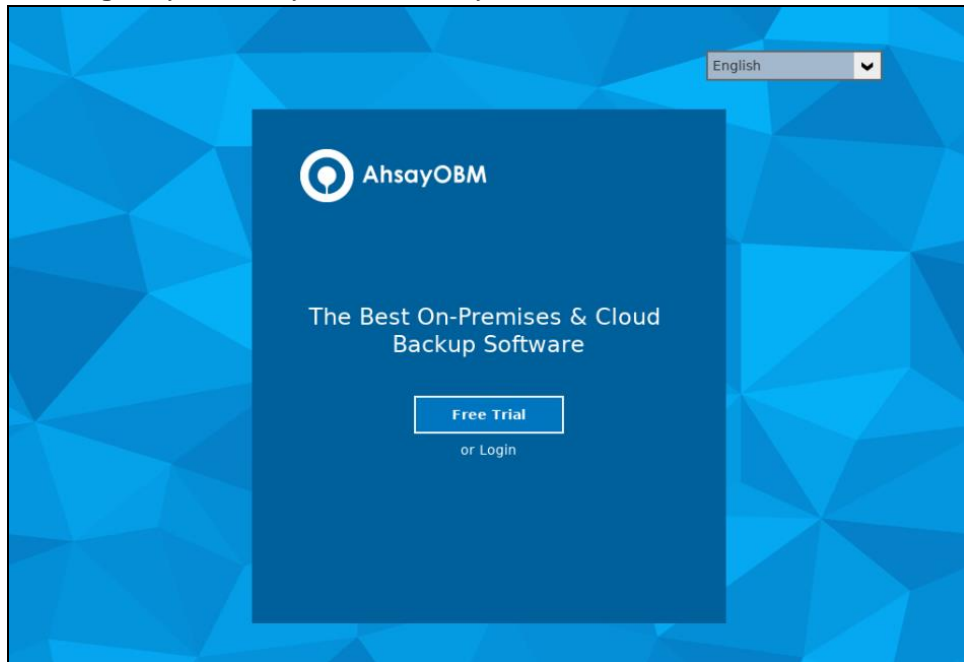
6.1.1 Without Mobile Add-on Module

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.



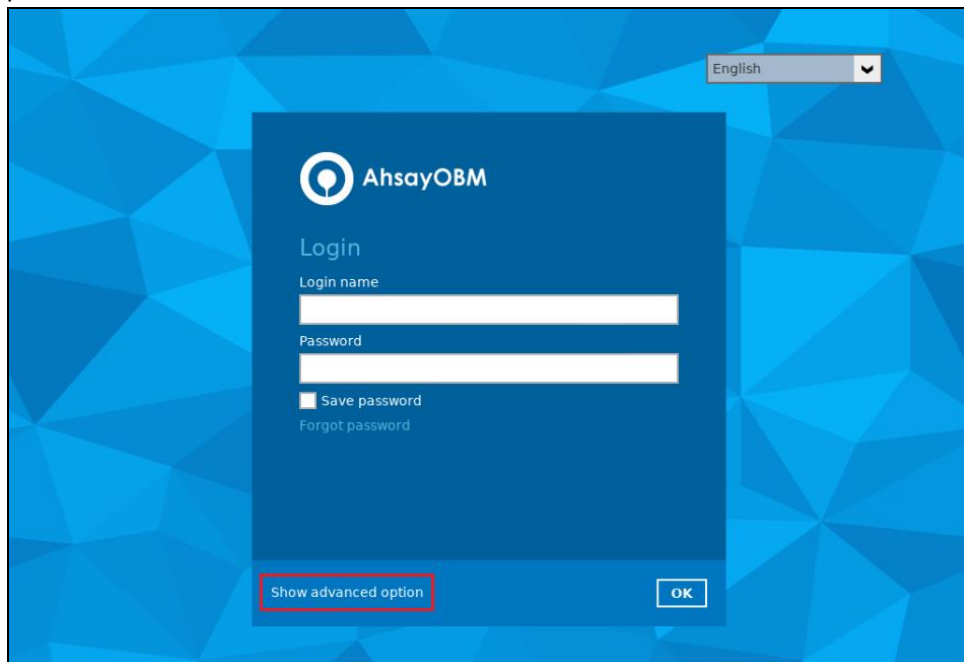
2. The Free Trial Registration option may be displayed when you login for the first time. If you want to create a free trial account please proceed to [Appendix G](#). Otherwise, click **Login** if you already have an AhsayOBM account.



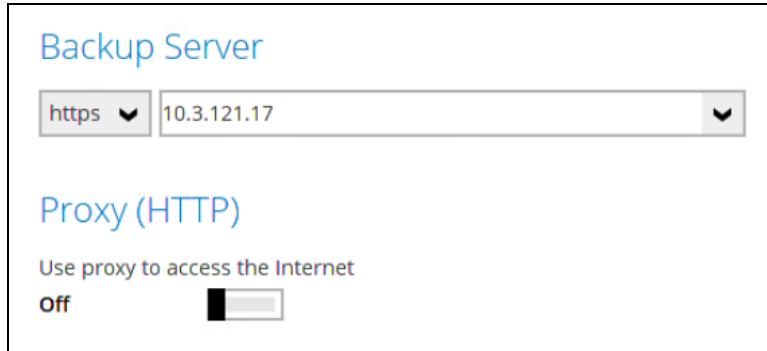
NOTE

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.

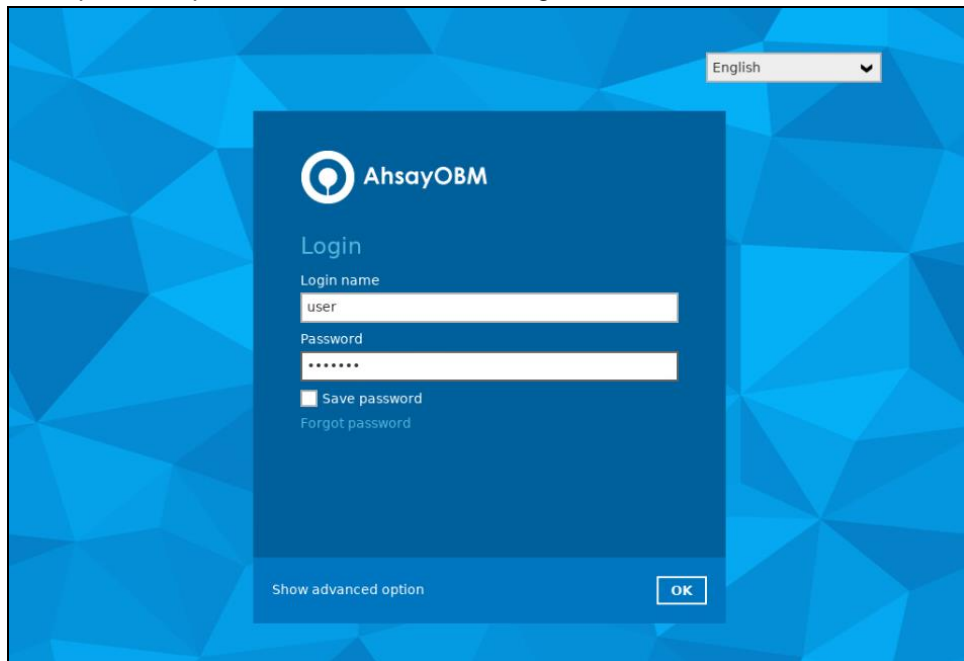


If **Show advanced option** is clicked, this will be displayed.



The screenshot shows a configuration window titled "Backup Server". It contains a dropdown menu set to "https" and a text field with the IP address "10.3.121.17". Below this is a section titled "Proxy (HTTP)" with the text "Use proxy to access the Internet" and a toggle switch currently set to "off".

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

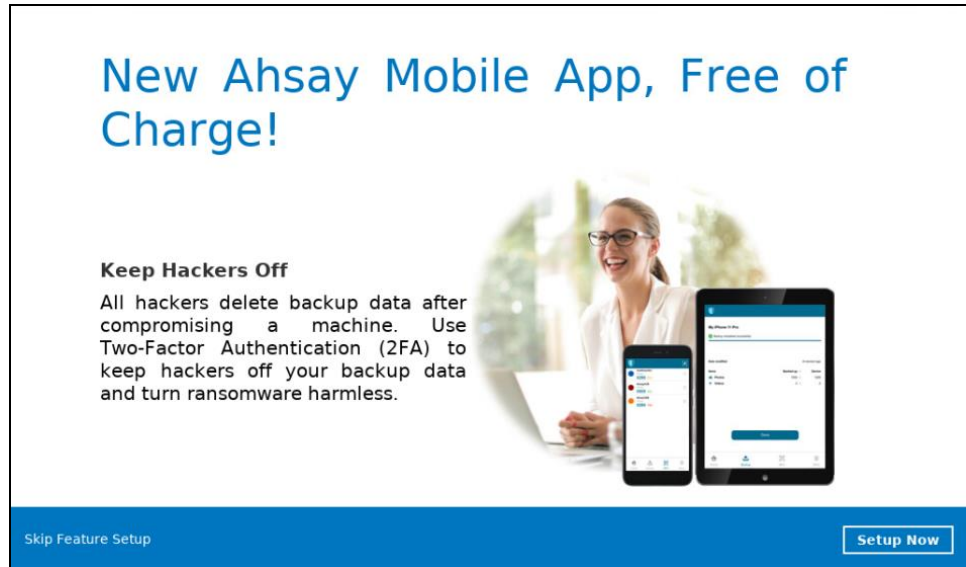


The screenshot shows the AhsayOBM login interface. It features a blue background with a geometric pattern. In the center is a dark blue login box with the AhsayOBM logo and the text "Login". Below the logo are input fields for "Login name" (containing "user") and "Password" (containing "*****"). There is a checkbox for "Save password" and a link for "Forgot password". At the bottom of the login box are the links "Show advanced option" and an "OK" button. In the top right corner of the main window, there is a language dropdown menu set to "English".

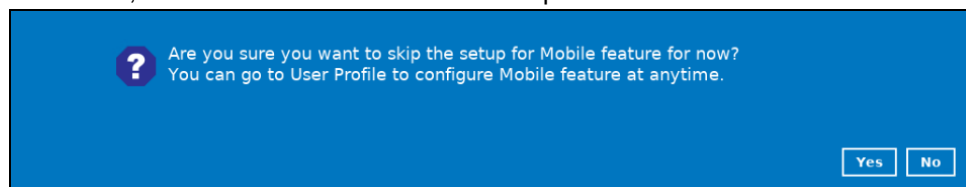
NOTE

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

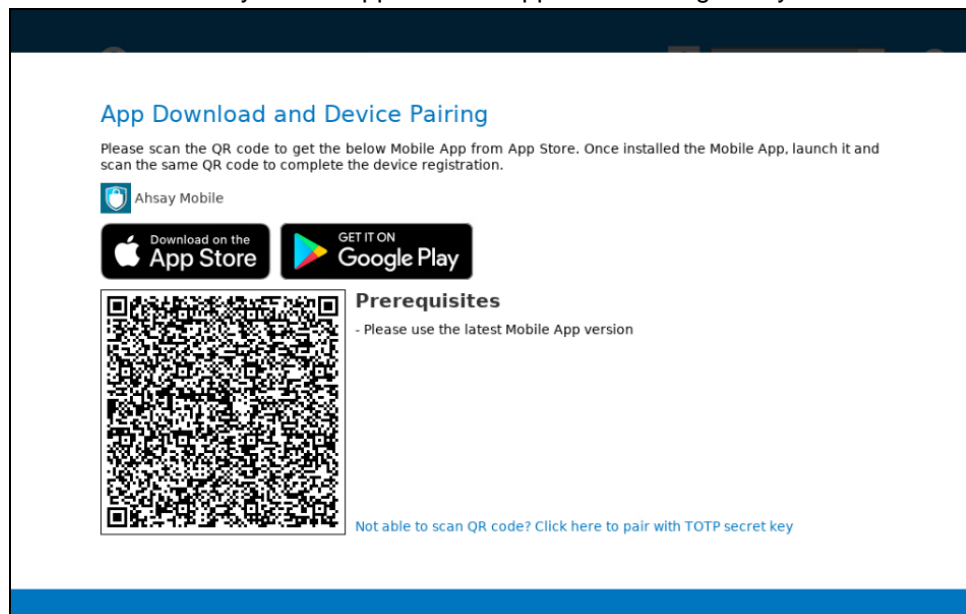
5. You will have the option to set up your 2FA. Click **Setup Now**.



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:

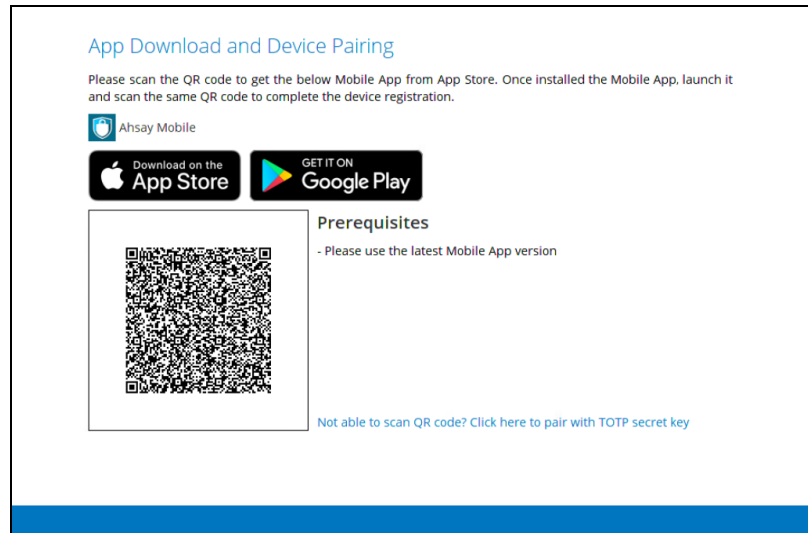
➤ [Push Notification and TOTP \(default mode\)](#)

or

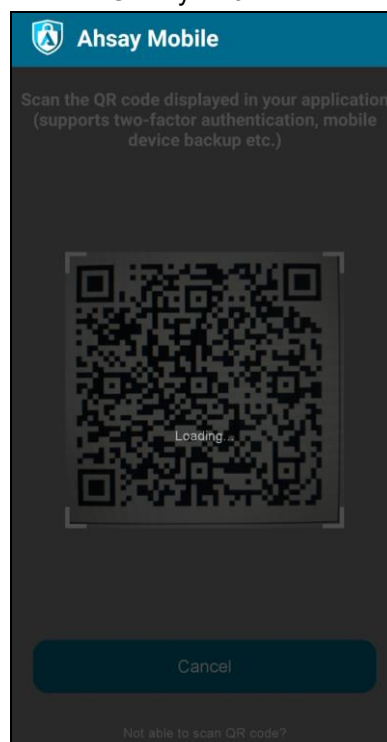
➤ [TOTP only](#)

Push Notification and TOTP (default mode)

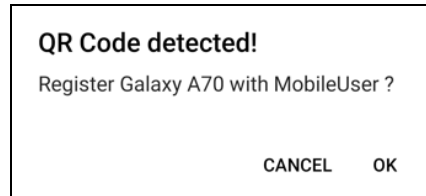
- i. To configure Push Notification and TOTP 2FA with Ahsay Mobile, simply scan the displayed QR code using the Ahsay Mobile app.



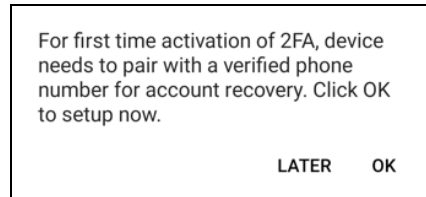
In this example, the Ahsay Mobile app is installed on a mobile device named "Galaxy A70".



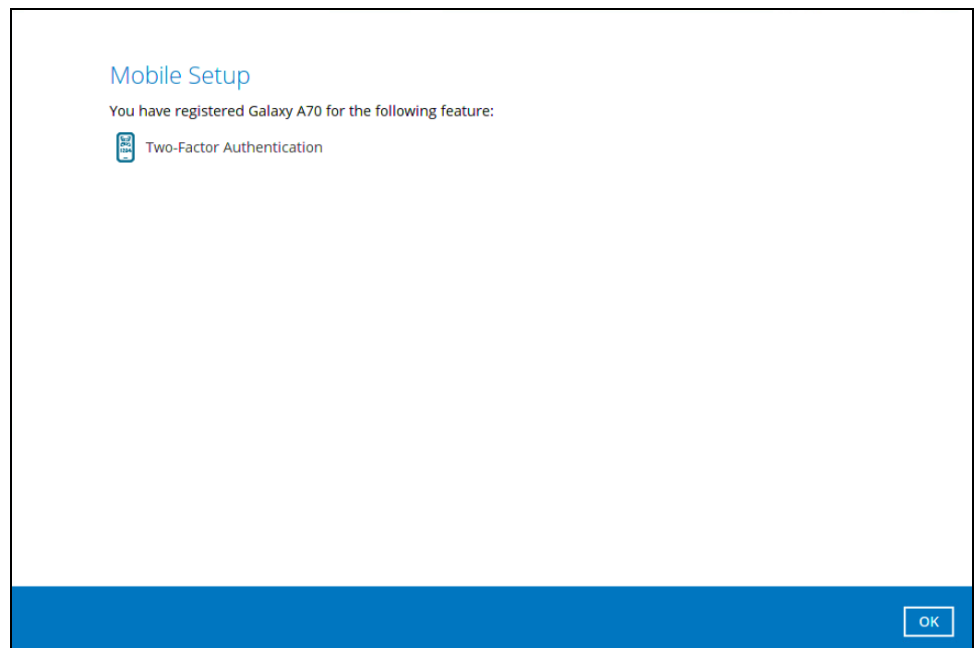
- ii. Tap **OK** to continue.



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.

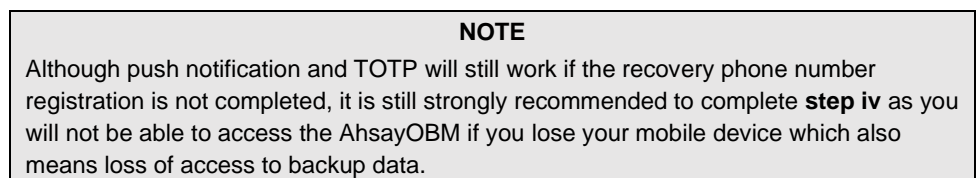


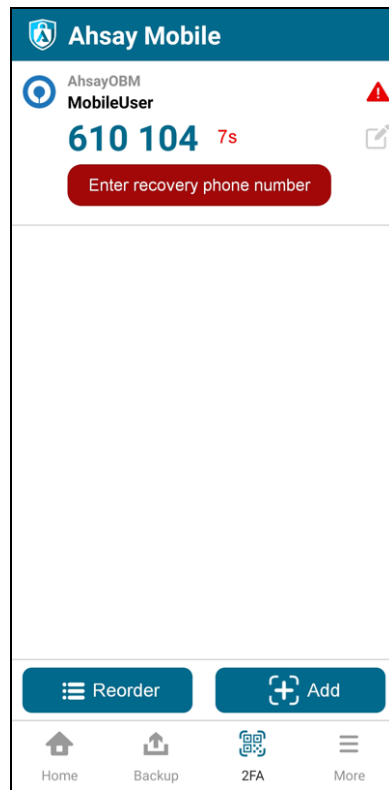
- iii. After successful scan of the QR code, you have now registered Ahsay Mobile for Push Notification and TOTP 2FA. Click **OK** to continue.



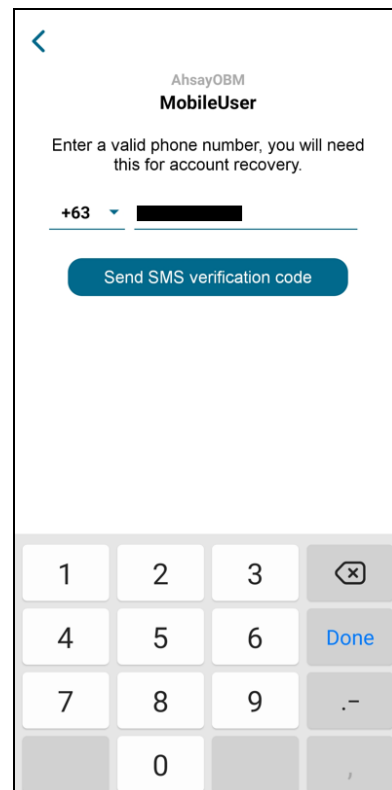
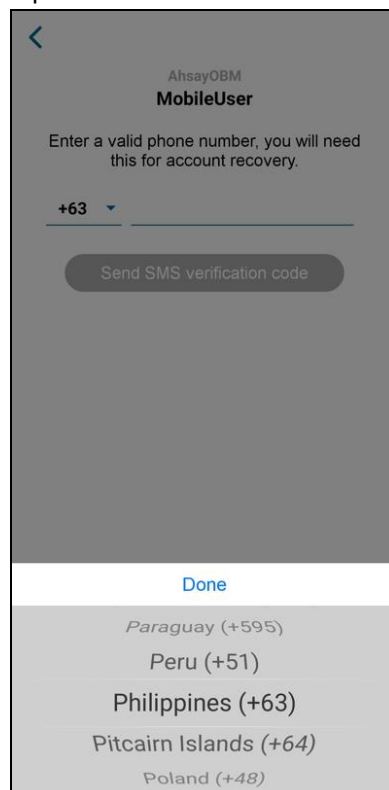
Phone number verification for account recovery

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

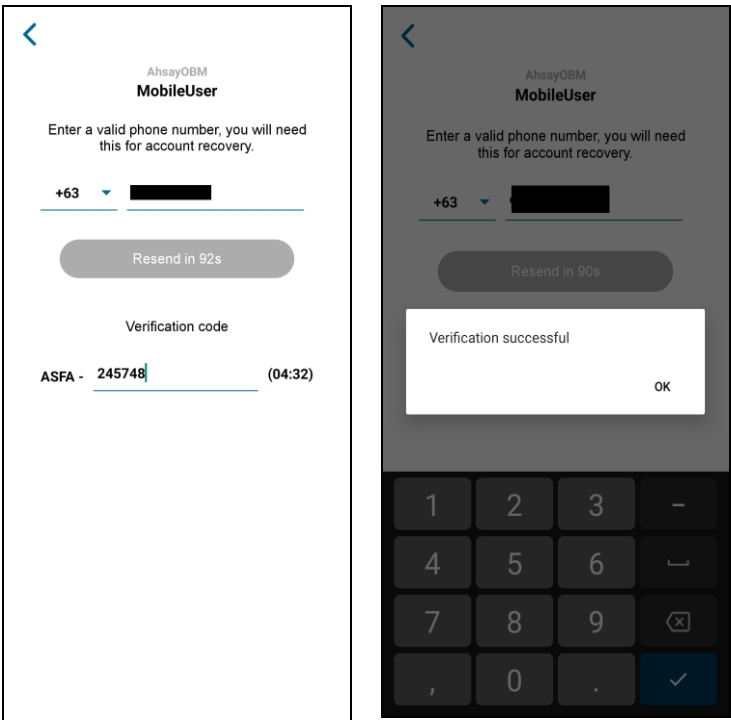




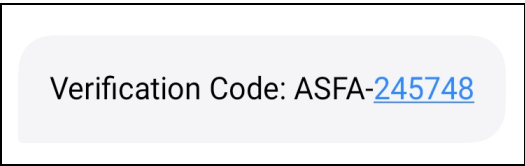
Select your country code and tap **Done**. Enter your phone number then tap **Send SMS verification code**.



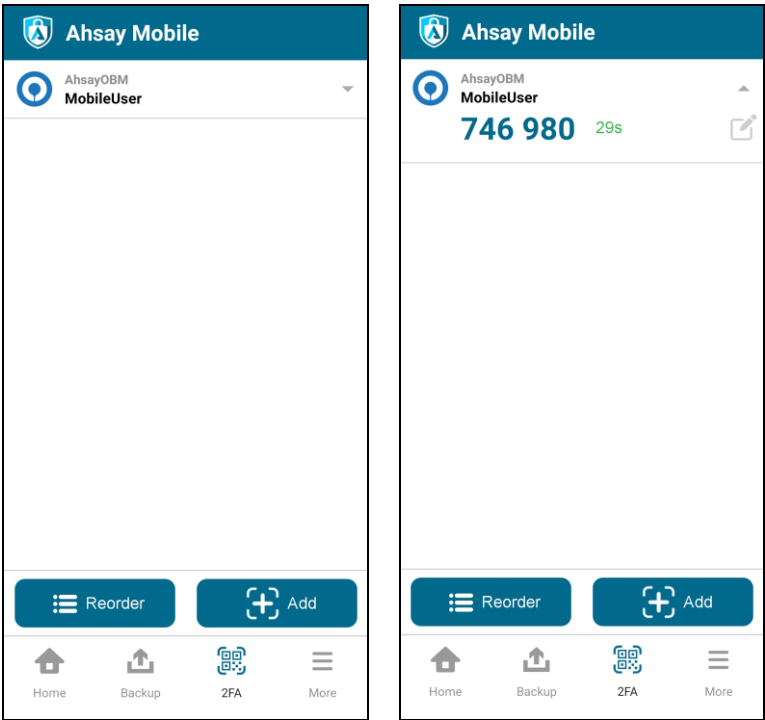
Enter the verification code sent to your mobile device.



Example of verification code.

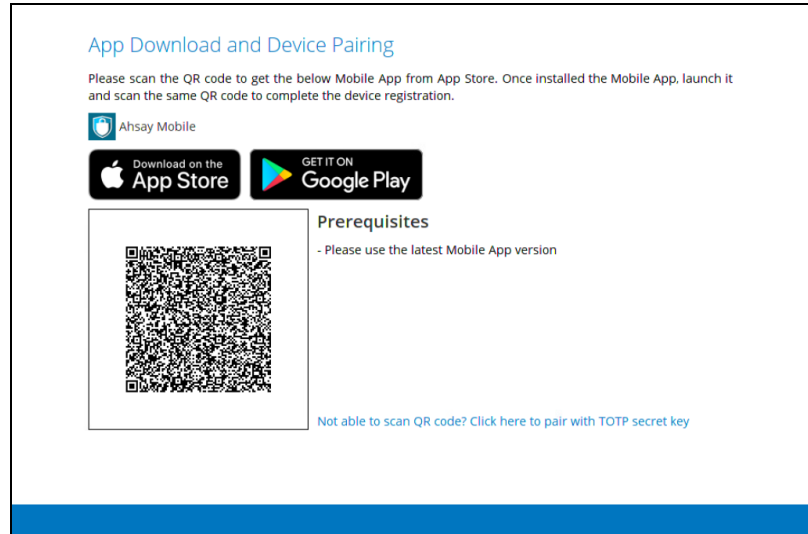


Your phone number for account recovery is successfully verified.

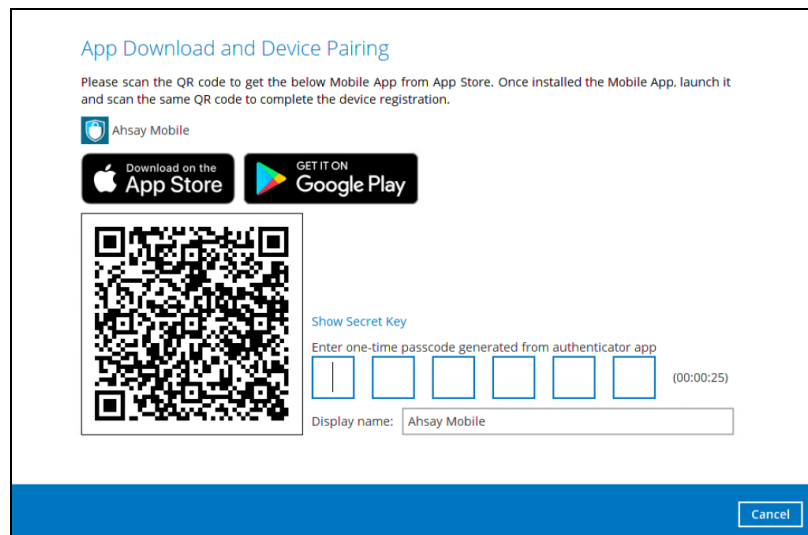


TOTP only

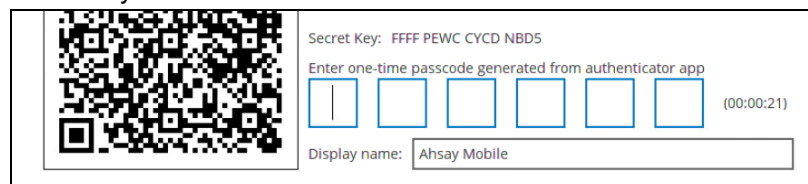
- i. To configure a TOTP only 2FA with Ahsay Mobile, click the **“Not able to scan QR code? Click here to pair with TOTP secret key”** link.



- 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.

The left screenshot shows the Ahsay Mobile app interface for QR code scanning. It has a blue header with the Ahsay Mobile logo. Below the header, it says "Scan the QR code displayed in your application (supports two-factor authentication, mobile device backup etc.)". There is a large black square representing the QR code. At the bottom, there is a blue "Cancel" button and a red-bordered link that says "Not able to scan QR code?".

The right screenshot shows the "Connect using Secret Key" screen. It has a blue header with a close button (X) and the title "Connect using Secret Key". Below the header, it says "Key in the Secret Key provided by the app". There are two input fields: "Username" and "Secret Key". At the bottom, there is a grey "Connect" button and a blue link that says "Scan QR Code".

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

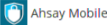
The left screenshot shows the "Connect using Secret Key" screen. It has a blue header with a close button (X) and the title "Connect using Secret Key". Below the header, it says "Key in the Secret Key provided by the app". There are two input fields: "Ahsay Mobile" and a field with asterisks. At the bottom, there is a blue "Connect" button and a blue link that says "Scan QR Code".



The right screenshot shows the "Connect using Secret Key" screen. It has a blue header with a close button (X) and the title "Connect using Secret Key". Below the header, it says "Key in the Secret Key provided by the app". There are two input fields: "Ahsay Mobile" and a field with asterisks. A white dialog box is displayed in the center with the text "Device paired successfully" and an "OK" button. At the bottom, there is a blue "Connect" button and a blue link that says "Scan QR Code".


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

App Download and Device Pairing

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

 Ahsay Mobile



Secret Key: FFFL OKJC 6URB SQHR

Enter one-time passcode generated from authenticator app


(00:00:03)


Display name:

[Cancel](#)





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

Ahsay Mobile

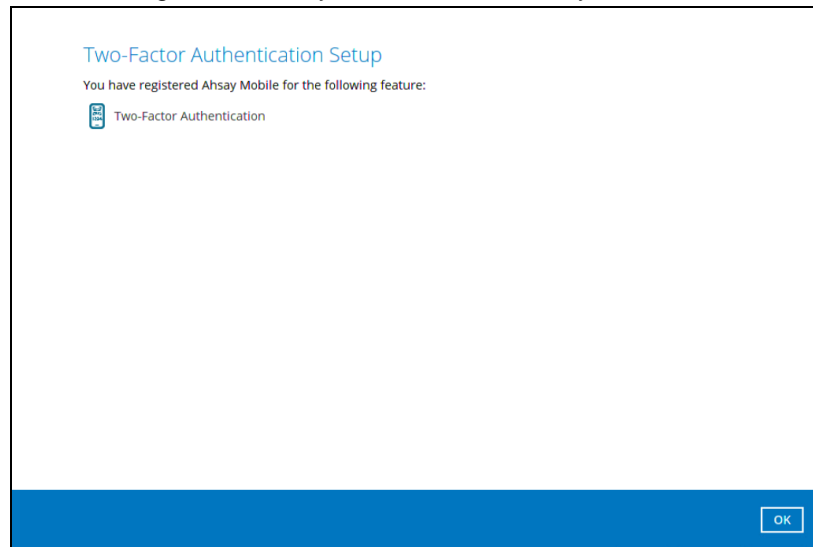
 AhsayOBM
MobileUser

 TOTP (Manual input)
Ahsay Mobile
450 694 3s

[Reorder](#) [Add](#)

 Home  Backup  2FA  More

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



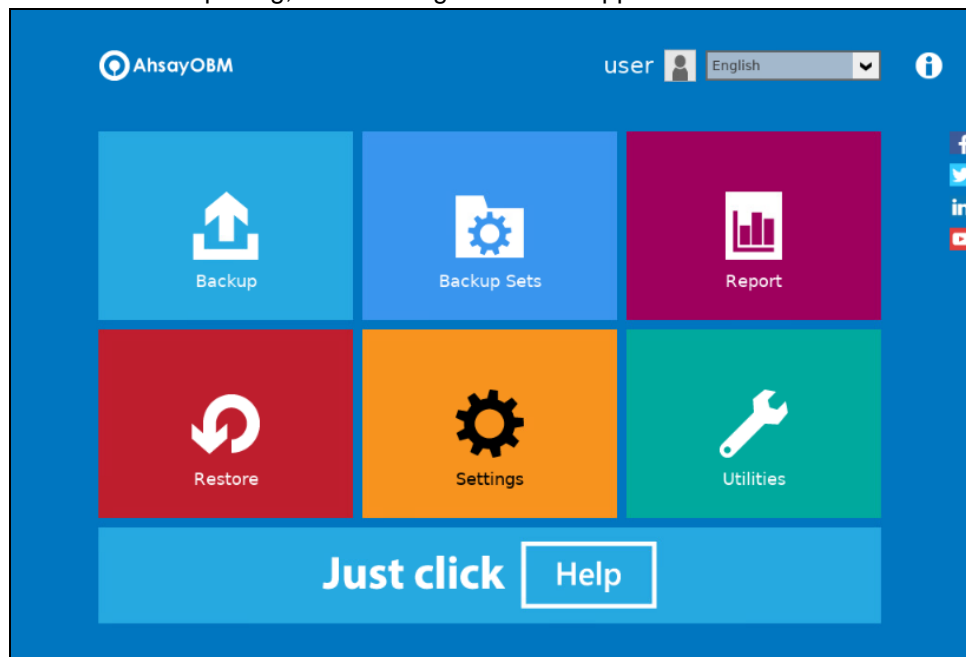
NOTE

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

Two-Factor Authentication Setup

Due to session timeout, Two-Factor Authentication feature failed to be configured.
Click [OK] to configure the feature again.

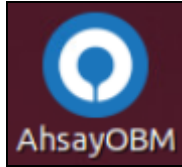
8. After successful pairing, the following screen will appear.



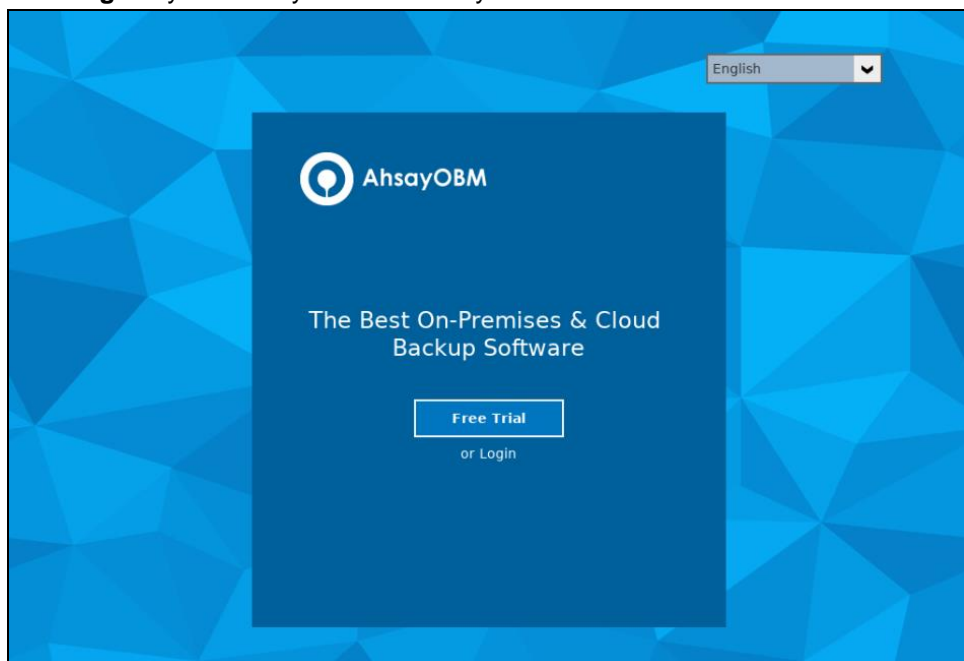
6.1.2 With Mobile Add-on Module

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.



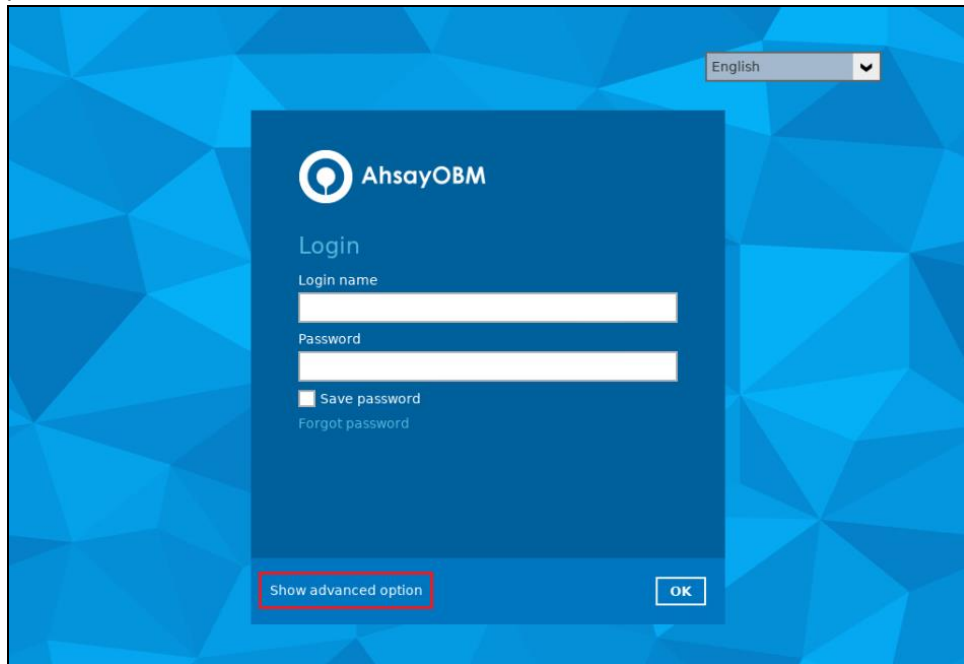
2. The Free Trial Registration option may be displayed when you login for the first time. If you want to create a free trial account please proceed to [Appendix G](#). Otherwise, click **Login** if you already have an AhsayOBM account.



NOTE

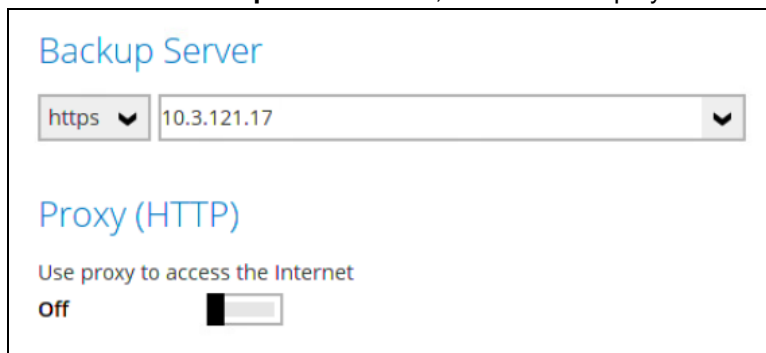
The Free Trial Registration option may not be available. This depends on the settings of your backup service provider. Please contact your backup service provider for more information.

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.



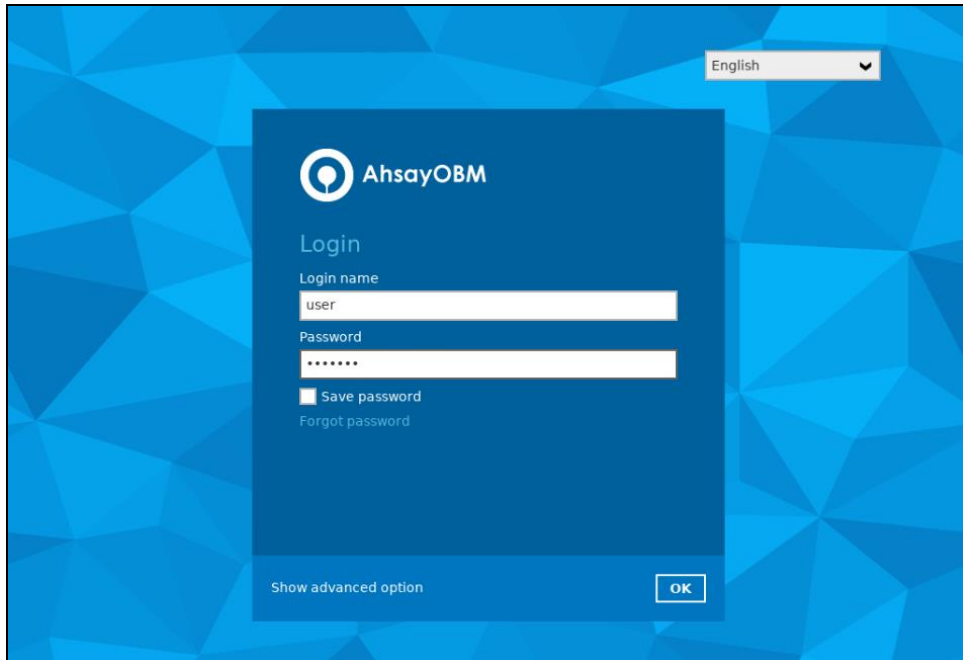
The image shows the AhsayOBM login interface. At the top right, there is a language dropdown menu set to 'English'. The main login panel is dark blue with the AhsayOBM logo and the word 'Login'. It contains two input fields for 'Login name' and 'Password'. Below these fields are a checkbox for 'Save password' and a link for 'Forgot password'. At the bottom of the login panel, there is a button labeled 'Show advanced option' which is highlighted with a red rectangle, and an 'OK' button to its right.

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



The image shows the 'Backup Server' settings dialog. It has a title 'Backup Server' in blue. Below the title is a dropdown menu for the protocol, currently set to 'https', and a text input field for the IP address, currently containing '10.3.121.17'. Below this is a section titled 'Proxy (HTTP)' in blue. Under this section, there is a label 'Use proxy to access the Internet' and a toggle switch. The toggle switch is currently in the 'off' position, indicated by a black slider.

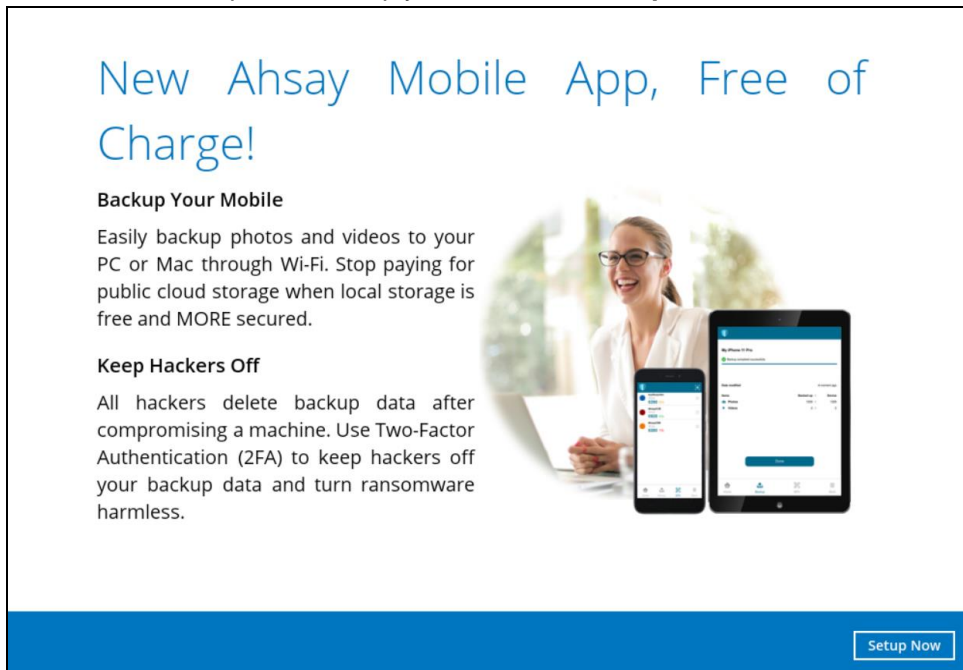
4. Enter the login name and password of your AhsayOBM account provided by your backup service provider. Then, click **OK** to log in.

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

NOTE

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

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

The image is a promotional banner for the 'New Ahsay Mobile App, Free of Charge!'. The text is in a light blue font. Below the headline, there are two sections: 'Backup Your Mobile' and 'Keep Hackers Off', each with a brief description. To the right of the text is a circular image of a smiling woman with glasses, wearing a white blazer, sitting at a desk with a laptop. In front of her are a smartphone and a tablet, both displaying the Ahsay mobile app interface. At the bottom right of the banner, there is a blue bar with a white 'Setup Now' button.

New Ahsay Mobile App, Free of Charge!

Backup Your Mobile
Easily backup photos and videos to your PC or Mac through Wi-Fi. Stop paying for public cloud storage when local storage is free and MORE secured.


Keep Hackers Off
All hackers delete backup data after compromising a machine. Use Two-Factor Authentication (2FA) to keep hackers off your backup data and turn ransomware harmless.



Setup Now

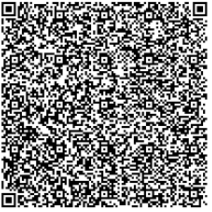
6. Download the Ahsay Mobile app from the App Store / Google Play Store. Ensure that the displayed Prerequisites are met.

App Download and Device Pairing

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

 Ahsay Mobile




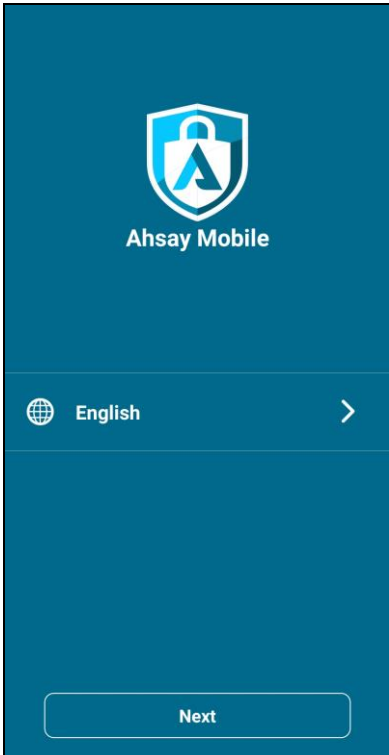


Prerequisites

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

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

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



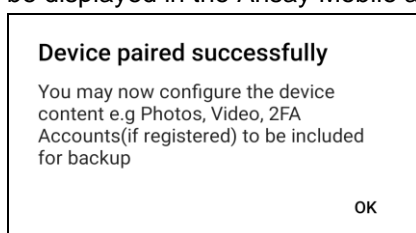
Tap **OK** to continue.

QR Code detected!

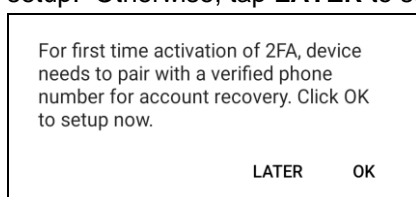
Register Galaxy A70 with MobileUser ?

CANCEL OK

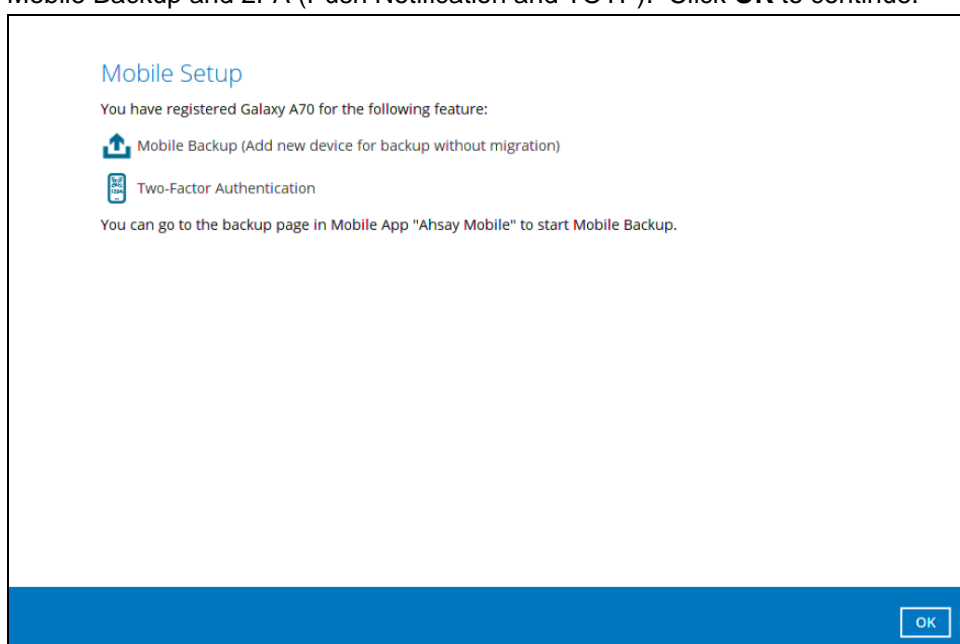
Once the device is successfully paired for mobile backup, the following message will be displayed in the Ahsay Mobile app. Tap **OK** to continue.



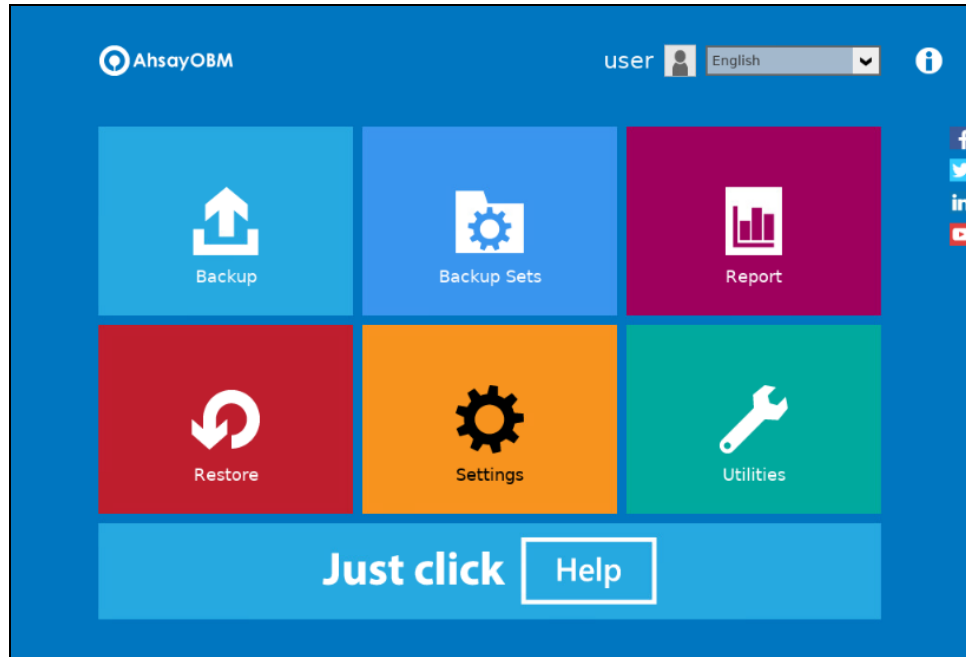
Once the device is successfully paired for 2FA, the following message will be displayed in the Ahsay Mobile app. You can set up a recovery number here that will be used in the “Authentication Recovery” procedure by tapping **OK**. You may refer to [Phone number verification for account recovery](#) in 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.



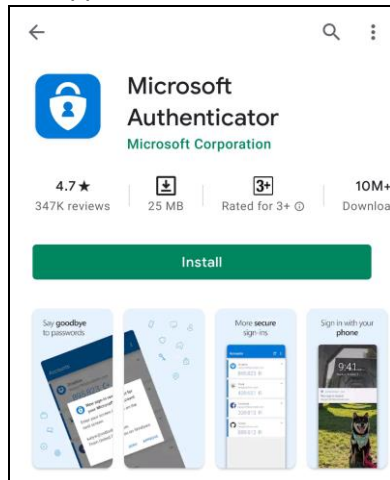
9. After successful pairing, the following screen will appear.



6.2 Using Microsoft Authenticator

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

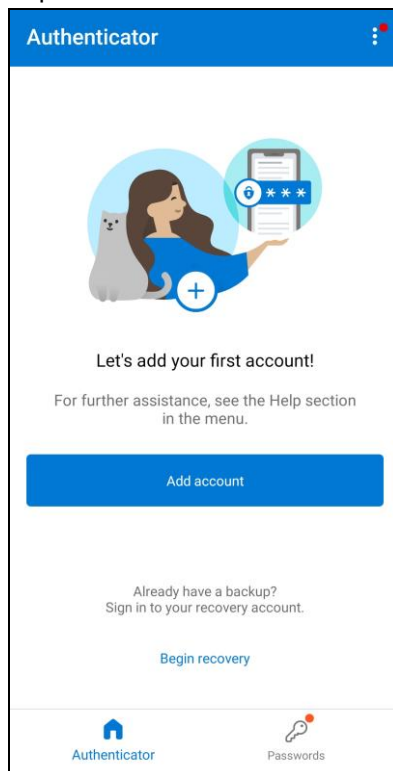
1. Download and install the Microsoft Authenticator from the Play Store for Android devices or the App Store for iOS devices.



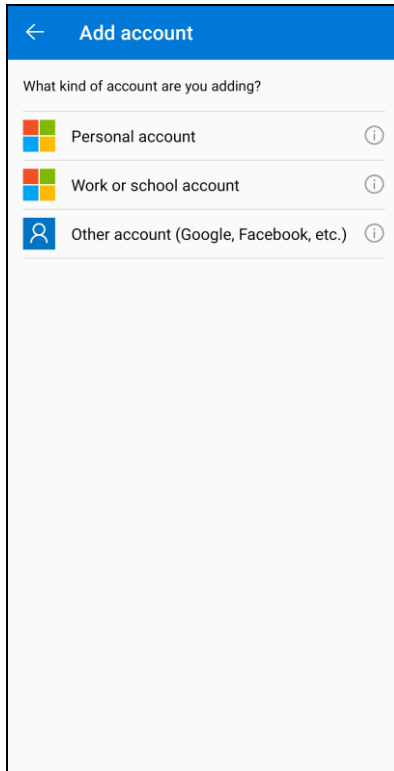
2. Launch the Microsoft Authenticator app.



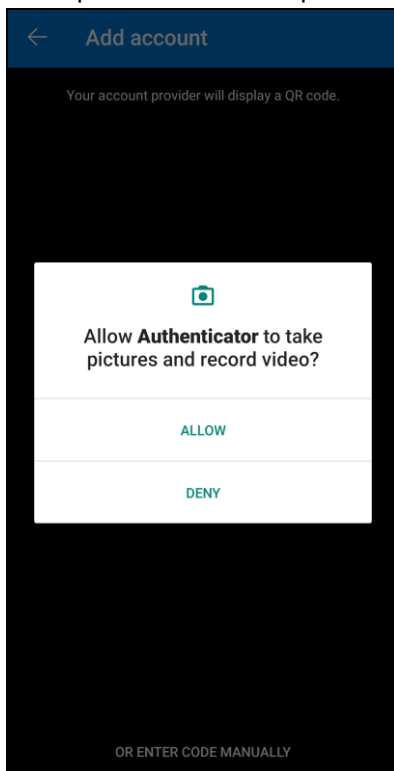
3. Tap **Add account**.



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



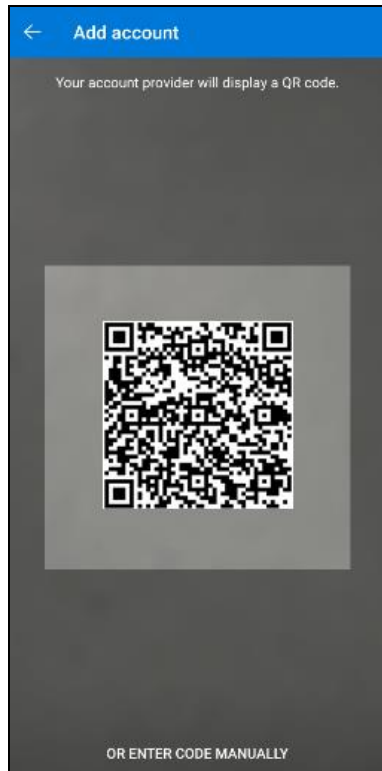
5. Allow permission to take pictures and record video.



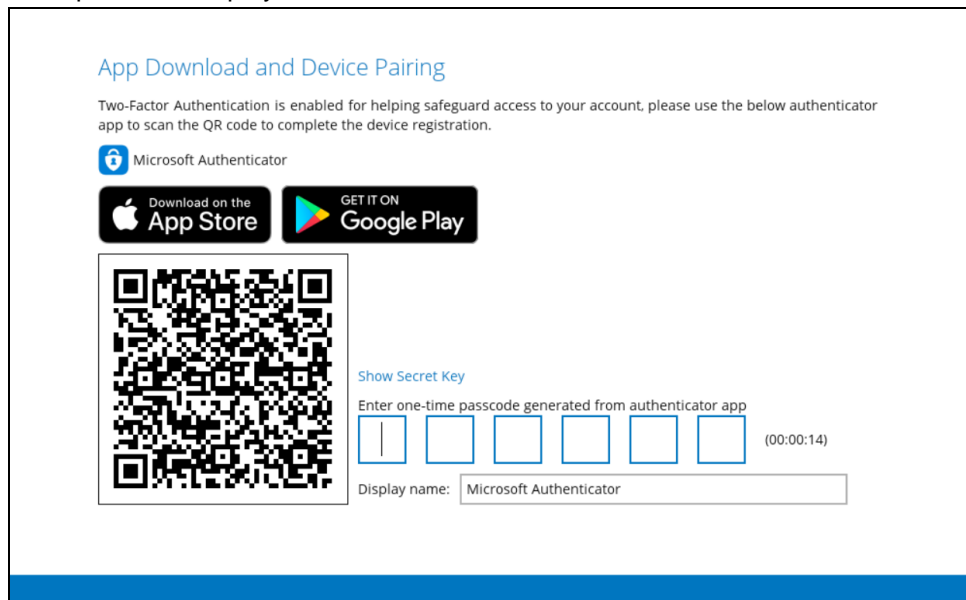
6. Set up the account by selecting from the following methods: [Scan the QR code](#) or [Enter code manually](#).

Method 1: Scan the QR code

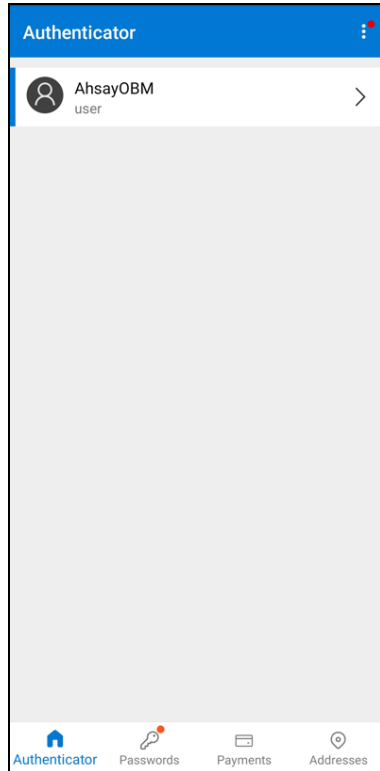
- i. Scan the QR code on AhsayOBM.



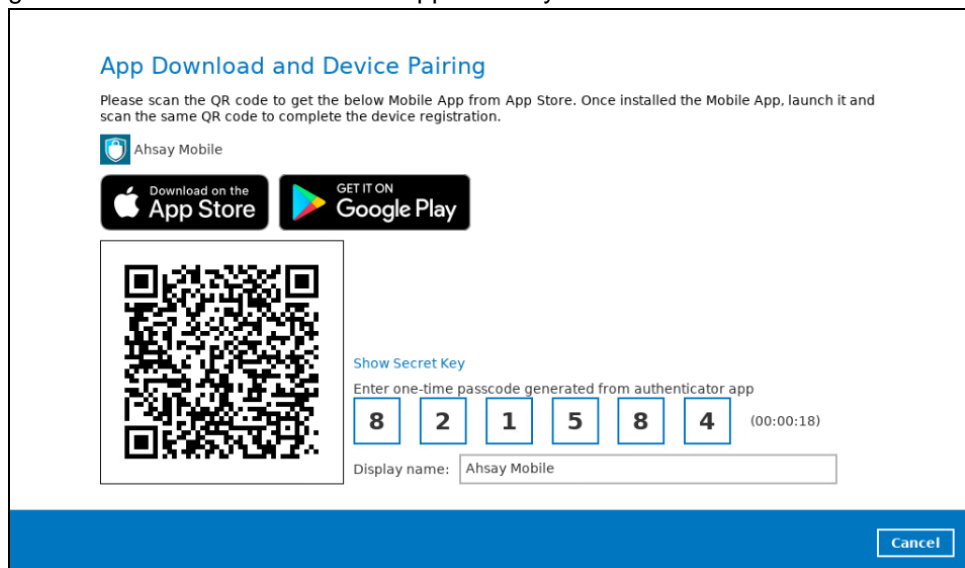
Example of the displayed QR code:



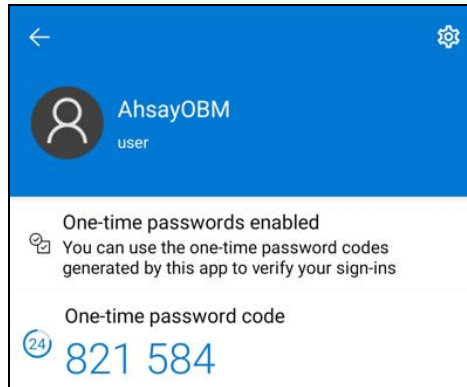
- ii. The AhsayOBM account is successfully added to Microsoft Authenticator.



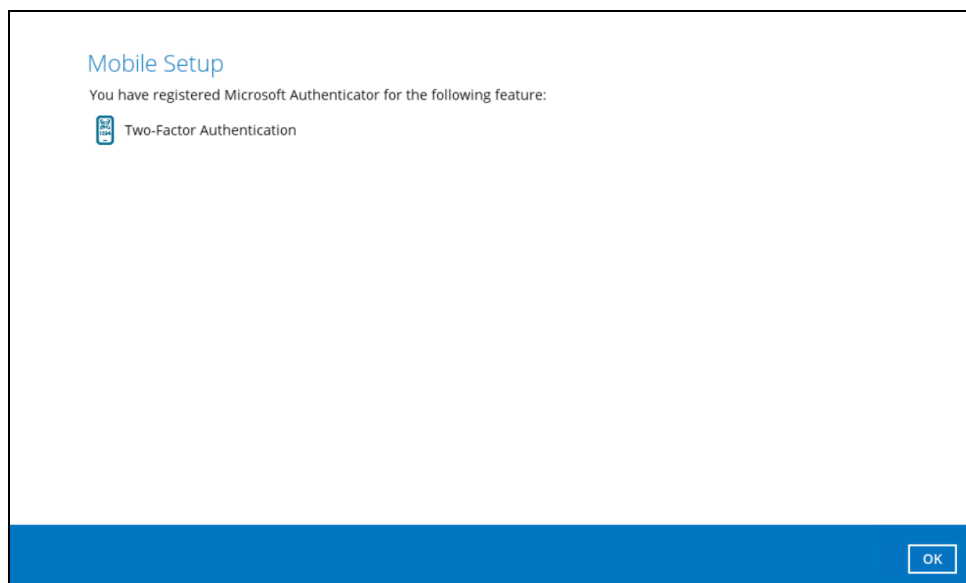
- iii. Once the account is added to Microsoft Authenticator, enter the one-time passcode generated from the authenticator app in AhsayOBM.



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.

The first screenshot shows the 'Add account' screen with the following fields:

- Account name
- Secret key
- FINISH (disabled)

The second screenshot shows the same screen with the following values entered:

- user
- CDNVBP3JAHHBFAAH
- FINISH (active)

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

App Download and Device Pairing

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

Ahsay Mobile

Download on the App Store | GET IT ON Google Play

QR Code

Secret Key: CDNV BP3J AHHB FAAH

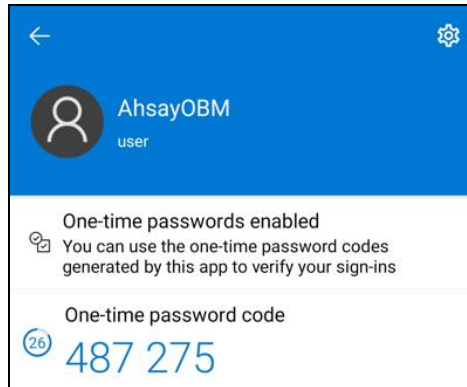
Enter one-time passcode generated from authenticator app

4 8 7 2 7 5 (00:00:22)

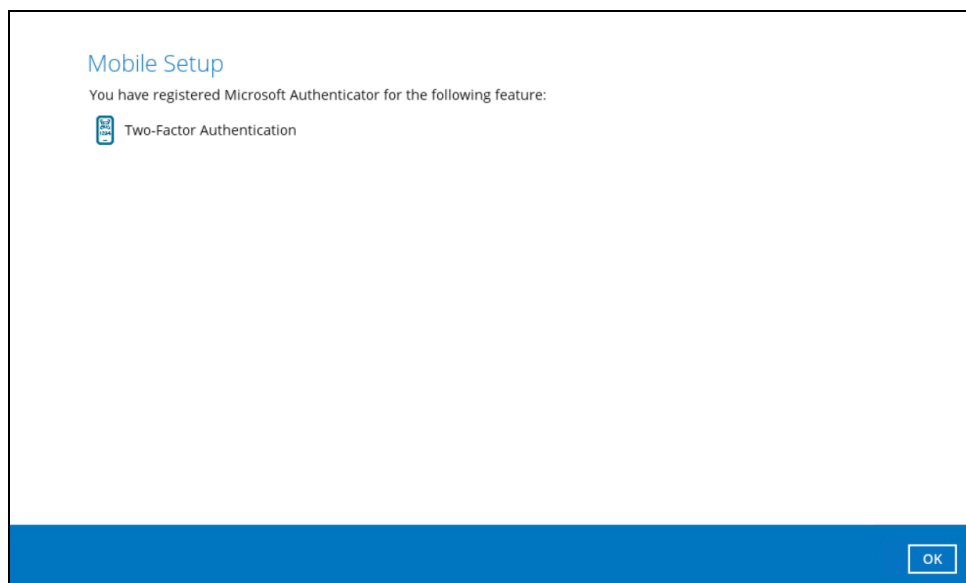
Display name: Microsoft Authenticator

Cancel

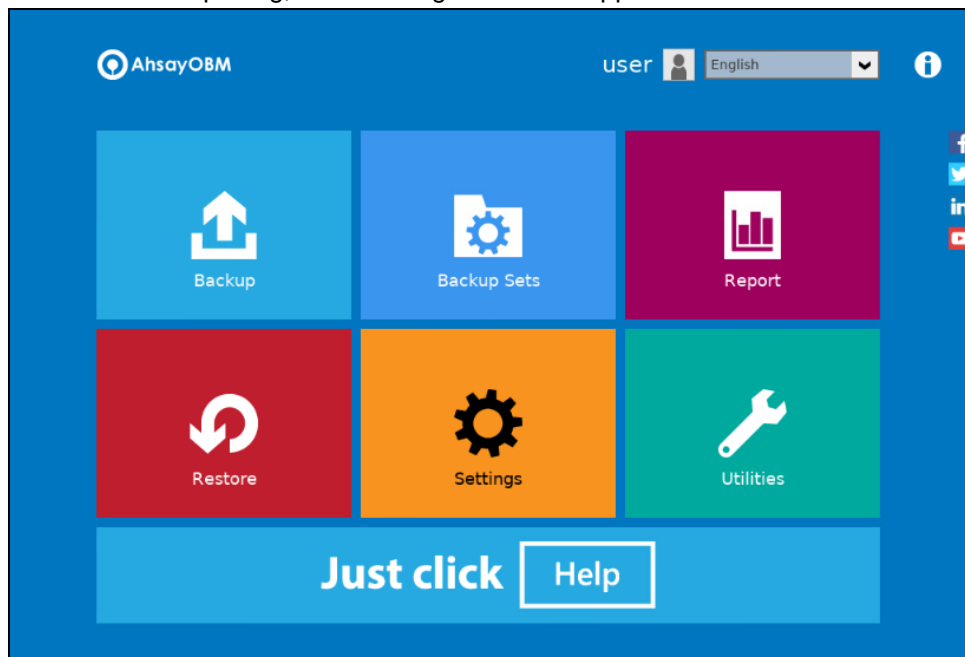
Example of the one-time passcode generated:



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



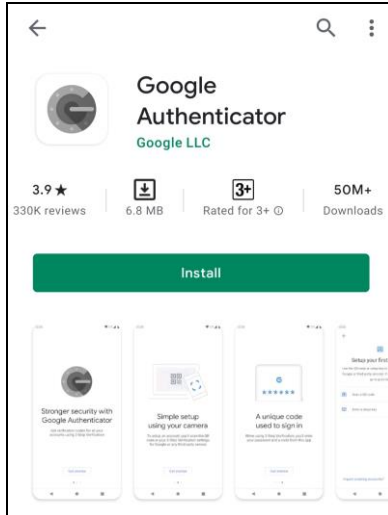
7. After successful pairing, the following screen will appear.



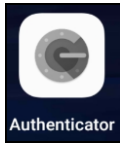
6.3 Using Google Authenticator

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.



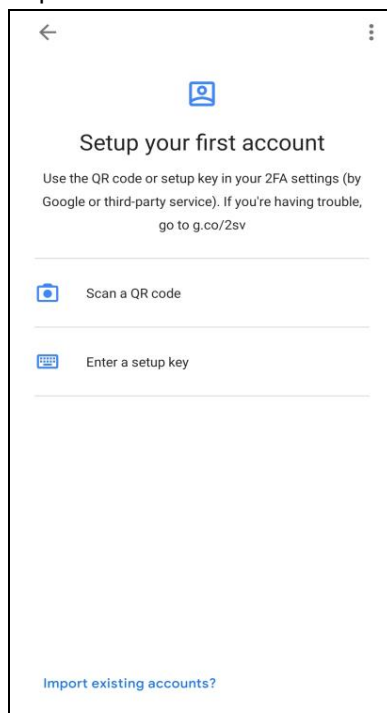
2. Launch the Google Authenticator app.



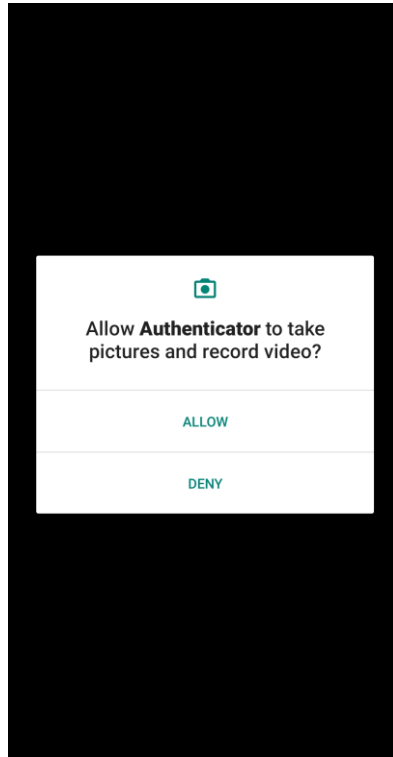
3. Set up the account by selecting from the following methods: [Scan the QR code](#) or [Enter a setup key manually](#).

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:

App Download and Device Pairing

Two-Factor Authentication is enabled for helping safeguard access to your account, please use the below authenticator app to scan the QR code to complete the device registration.

 Google Authenticator



[Show Secret Key](#)

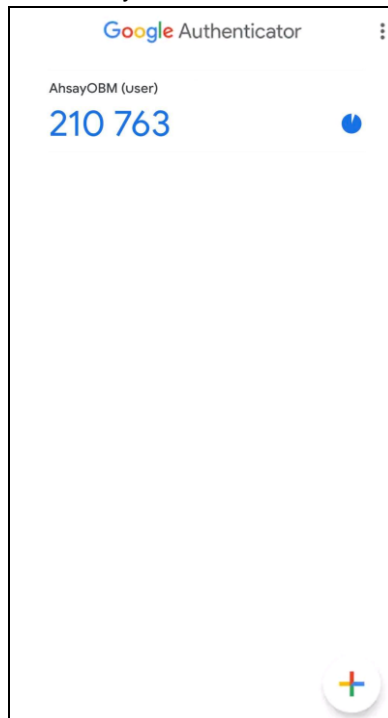
Enter one-time passcode generated from authenticator app

(00:00:02)

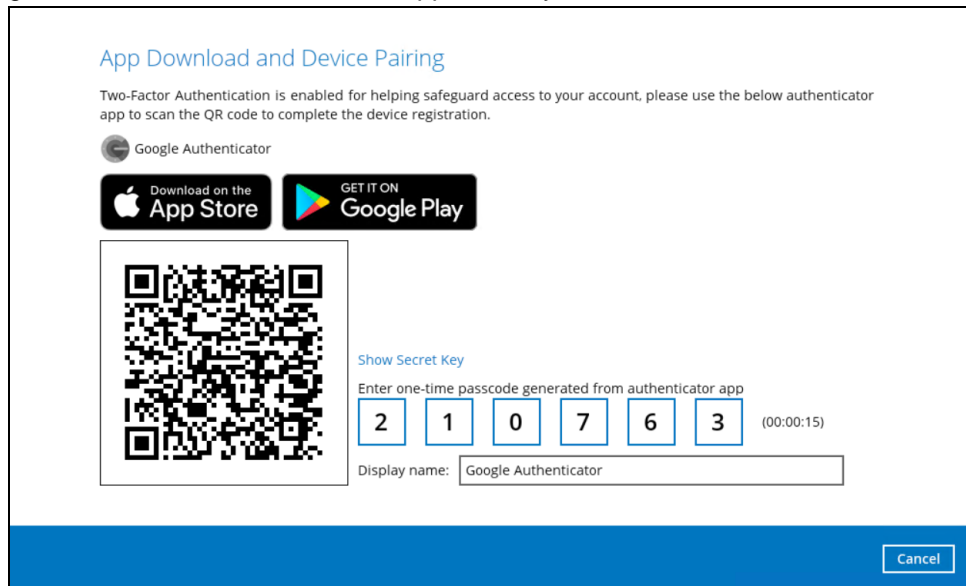
Display name:

[Cancel](#)

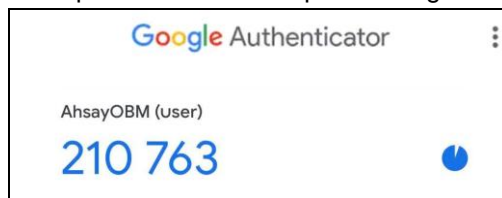
iv. The AhsayOBM account is successfully added to Google Authenticator.



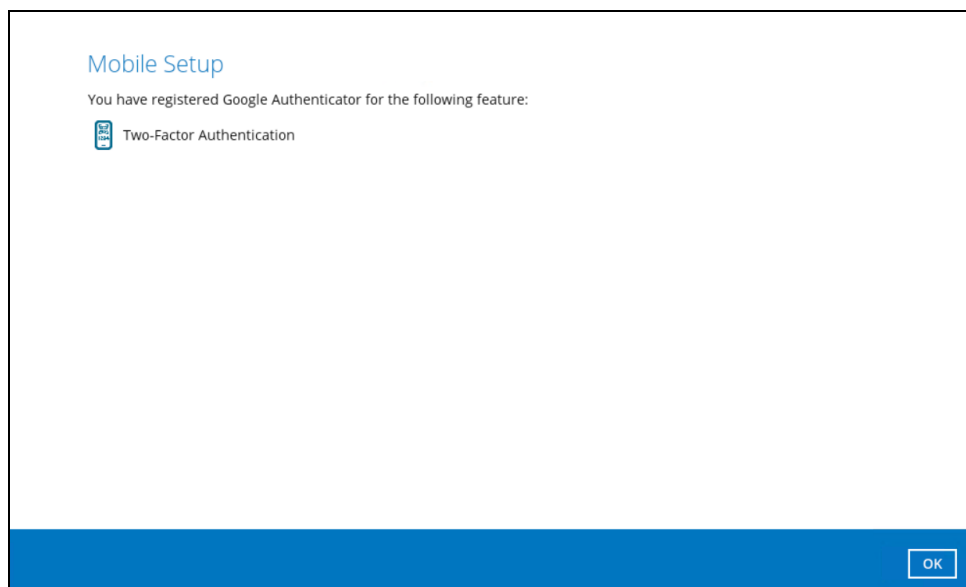
- v. Once the account is added to Google Authenticator, enter the one-time passcode generated from the authenticator app in AhsayOBM.



Example of the one-time passcode generated:

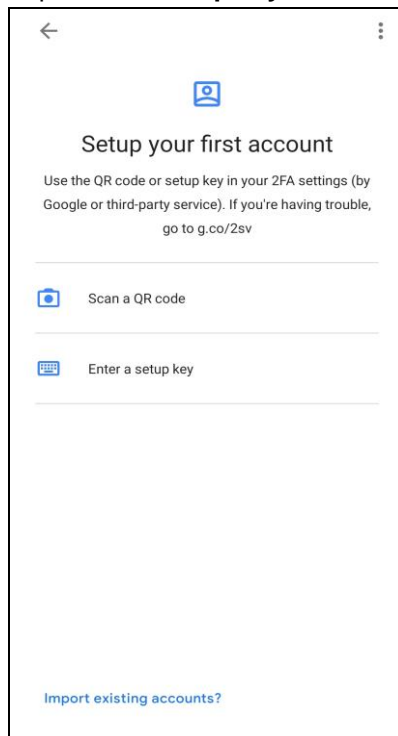


- vi. The device is successfully registered for TOTP 2FA in AhsayOBM using Google Authenticator. Click **OK** to continue.



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.

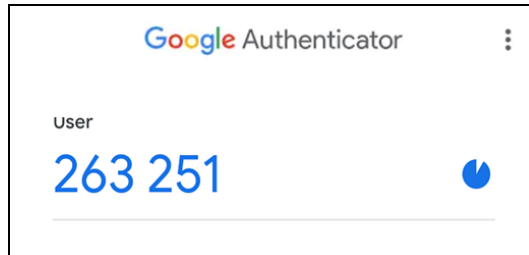
The first screenshot shows the 'Enter account details' screen with empty 'Account' and 'Key' input fields. A 'Time based' dropdown and an 'Add' button are at the bottom.

The second screenshot shows the same screen with 'User' entered in the 'Account' field and 'ZUGJKYFGCKI2WGJY' entered in the 'Key' field. The 'Add' button is still present.

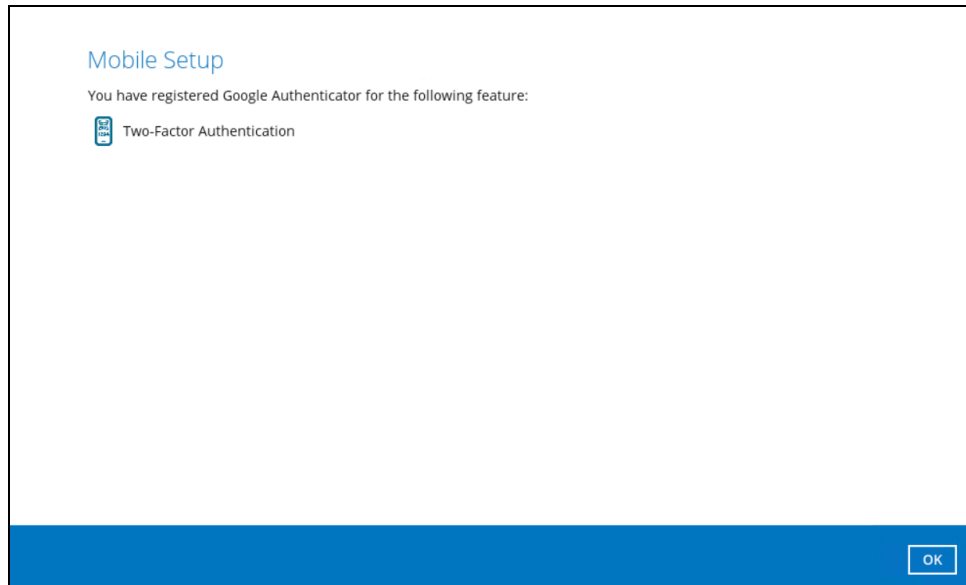
- iv. Once the account is added to Google Authenticator, enter the one-time passcode generated from the authenticator app in AhsayOBM.

The screenshot shows the 'App Download and Device Pairing' screen. It includes instructions to download Google Authenticator from the App Store or Google Play. A QR code is displayed for scanning. Below the QR code, the secret key 'ZUGJ KYFG CKI2 WGJY' is shown. A one-time passcode '263251' is entered in a row of boxes, with a timer '(00:00:15)' to the right. The 'Display name' is set to 'Google Authenticator'. A 'Cancel' button is at the bottom right.

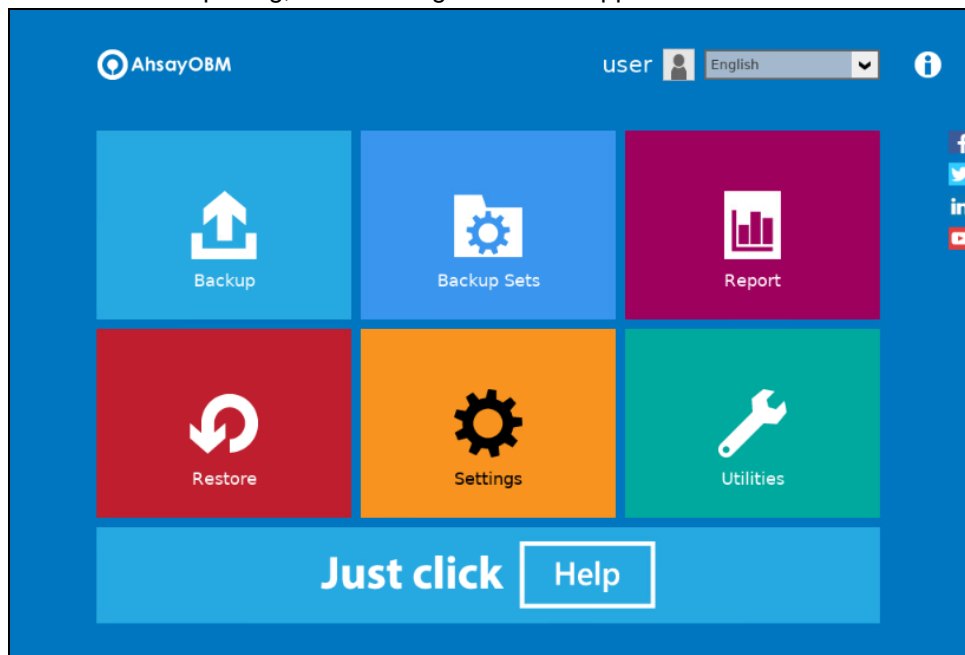
Example of the one-time passcode generated:



- 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

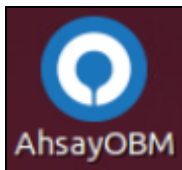
Login steps without 2FA and with 2FA using the different types of authenticator will be discussed in this chapter.

- ▶ [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](#)

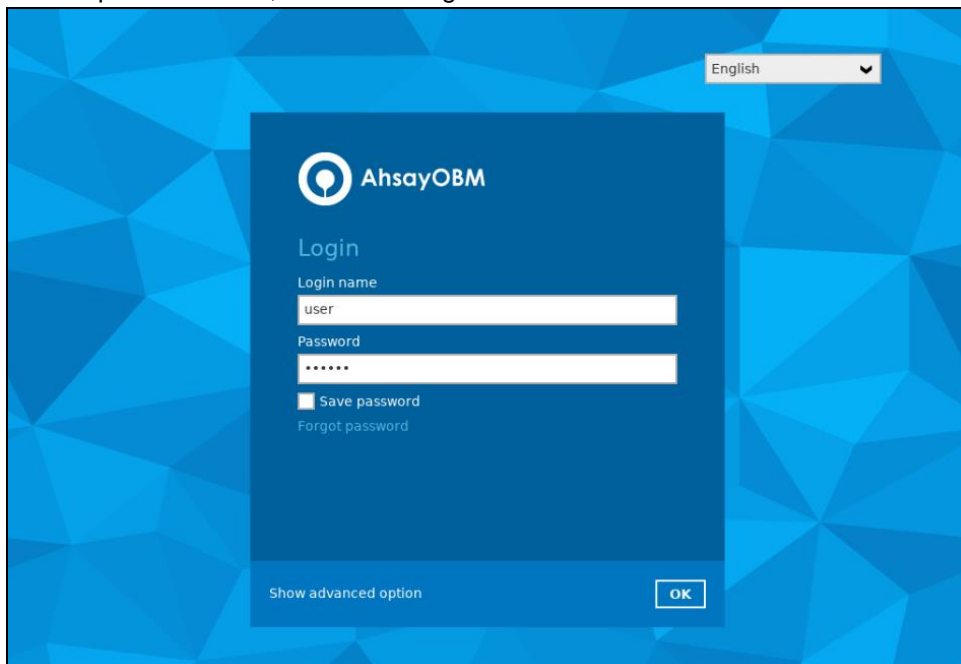
7.1 Login to AhsayOBM without 2FA

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

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



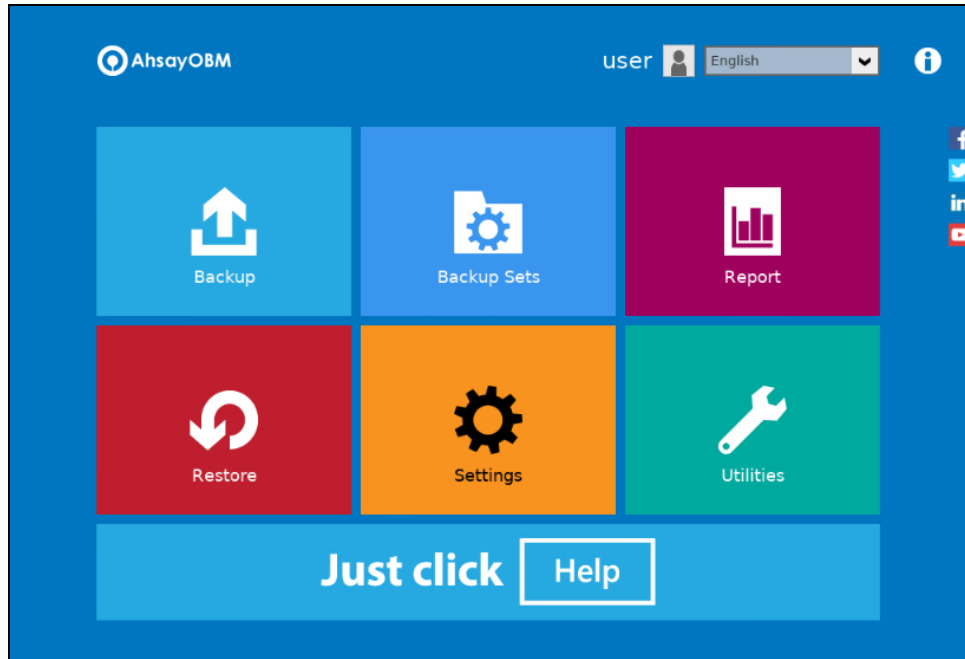
2. Enter the login name and password of your AhsayOBM account provided by your backup service provider. Then, click **OK** to login.

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

NOTE

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

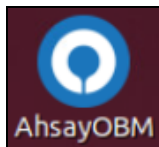
3. After successful login, the following screen will appear.



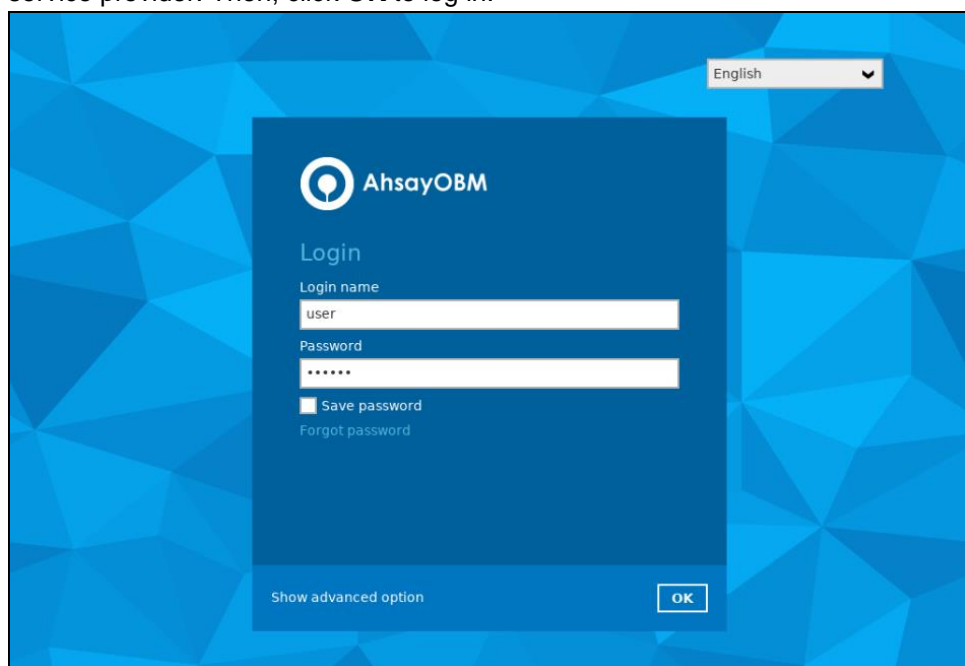
7.2 Login to AhsayOBM with 2FA using Ahsay Mobile Authenticator

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.

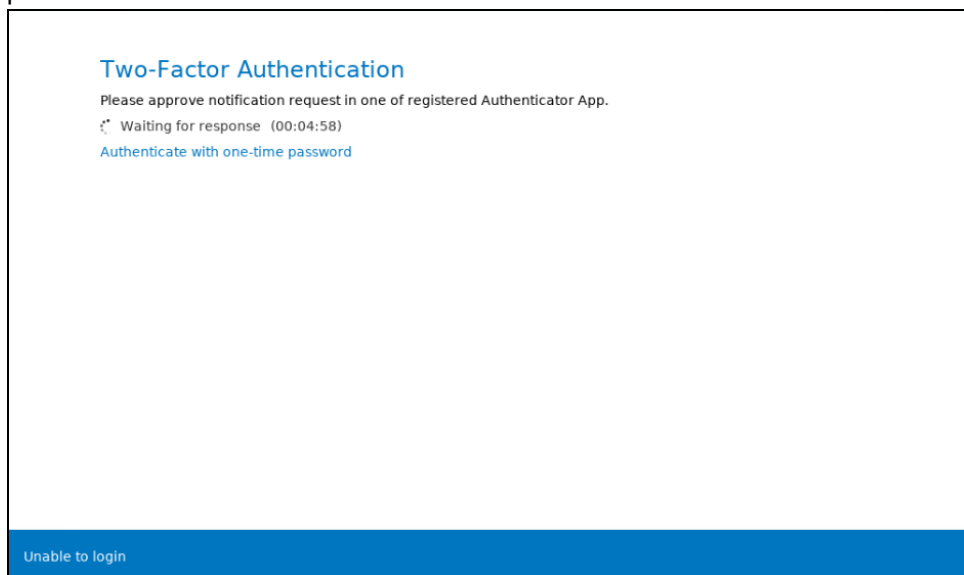
Please refer to the [Ahsay Mobile User Guide for Android and iOS – Appendix A: Troubleshooting Login](#) if you are experiencing problems logging into AhsayOBM with Two-Factor Authentication using Ahsay Mobile app.

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

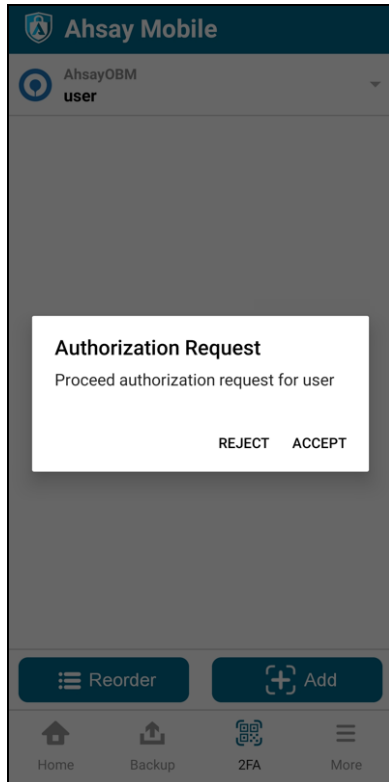
- **Push Notification and TOTP (default mode)**

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.

Two-Factor Authentication

Please approve notification request in one of registered Authenticator App.

⌚: Waiting for response (00:04:40)

Alternatively, input the one-time passcode generated in your Authenticator App.

7

0

0

4

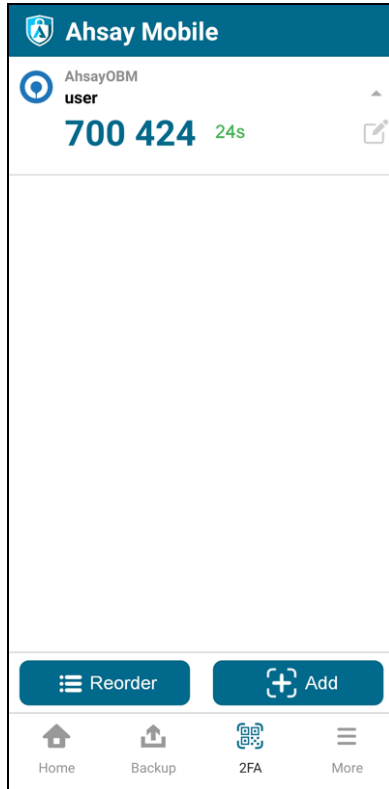
2

4

(00:00:25)

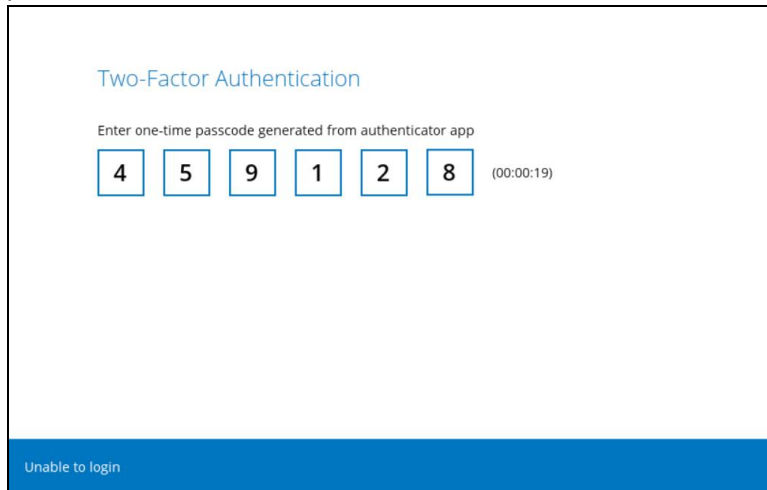
Unable to login

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



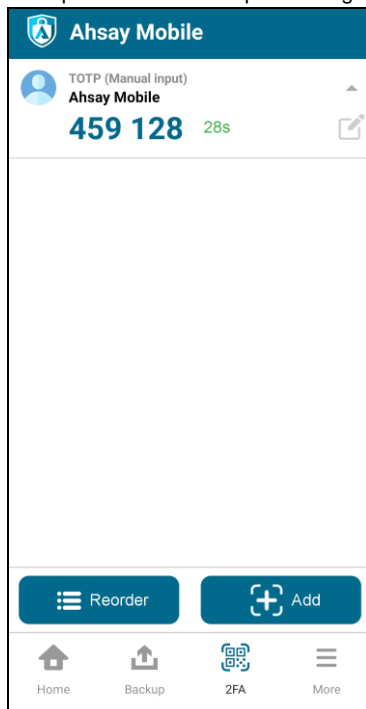
- **TOTP only**

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.



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

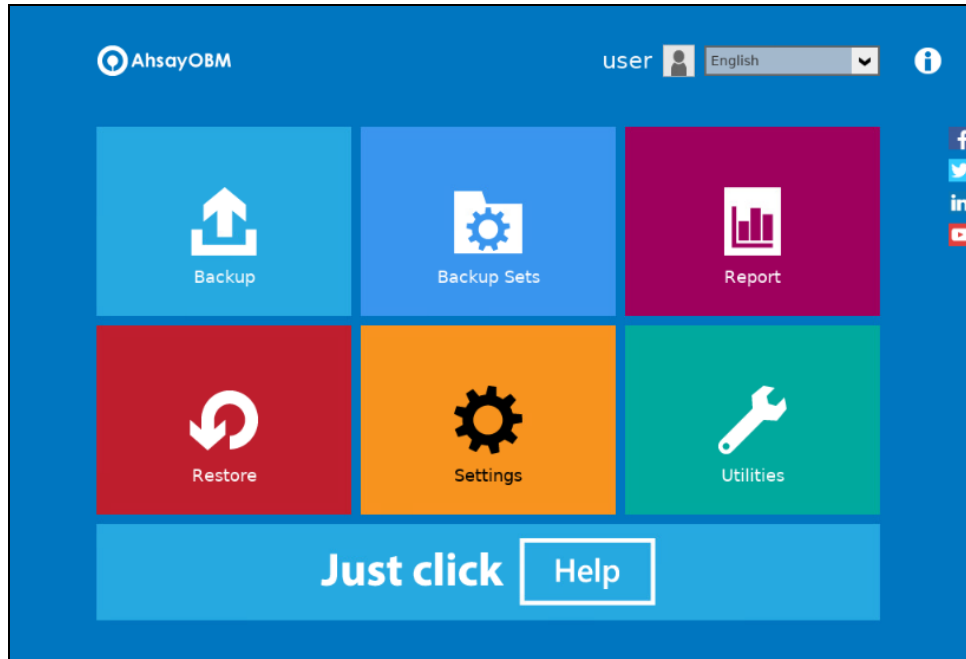
Example of the one-time password generated by Ahsay Mobile:



NOTE

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

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



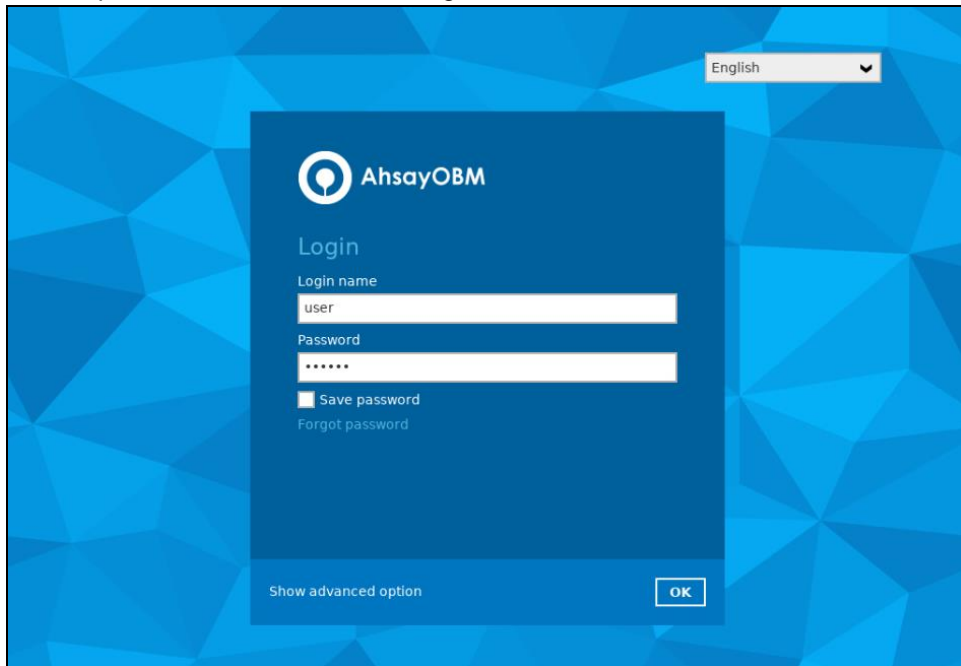
7.3 Login to AhsayOBM with 2FA using Microsoft Authenticator

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

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



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

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

NOTE

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

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

Two-Factor Authentication

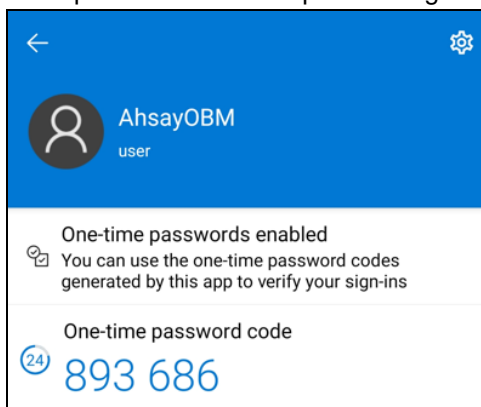
Enter one-time passcode generated from authenticator app

8	9	3	6	8	6
---	---	---	---	---	---

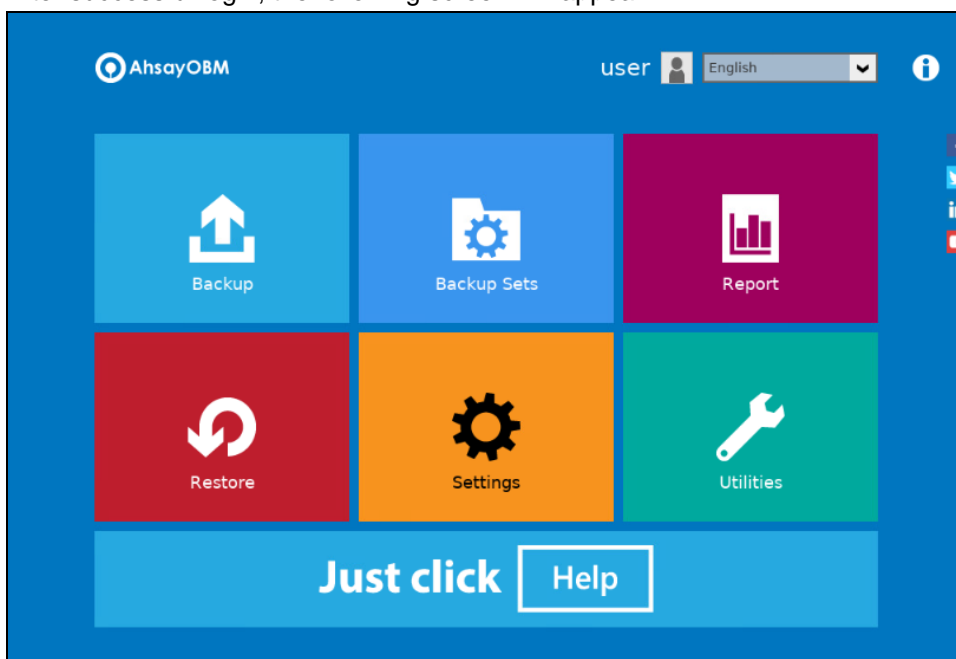
(00:00:19)

Unable to login

Example of the one-time passcode generated:



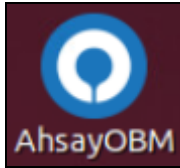
4. After successful login, the following screen will appear.



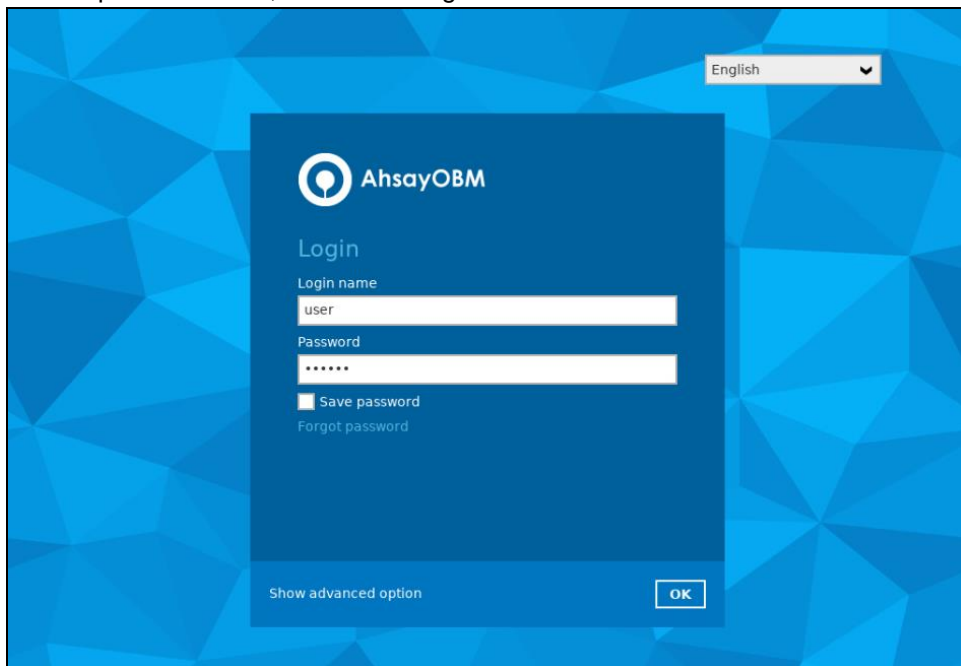
7.4 Login to AhsayOBM with 2FA using Google Authenticator

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.

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

NOTE

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

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

Two-Factor Authentication

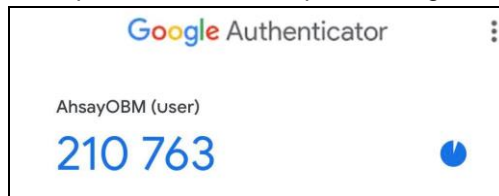
Enter one-time passcode generated from authenticator app

2	1	0	7	6	3
---	---	---	---	---	---

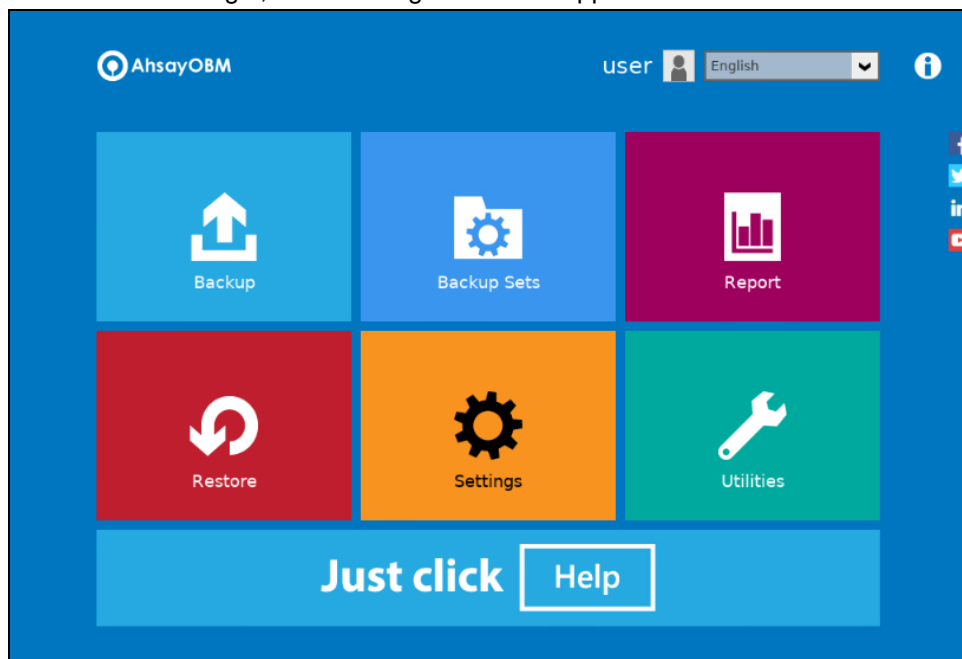
(00:00:15)

Unable to login

Example of the one-time passcode generated:



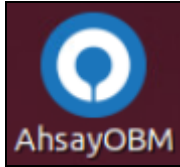
4. After successful login, the following screen will appear.



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.

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

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.

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

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

Two-Factor Authentication

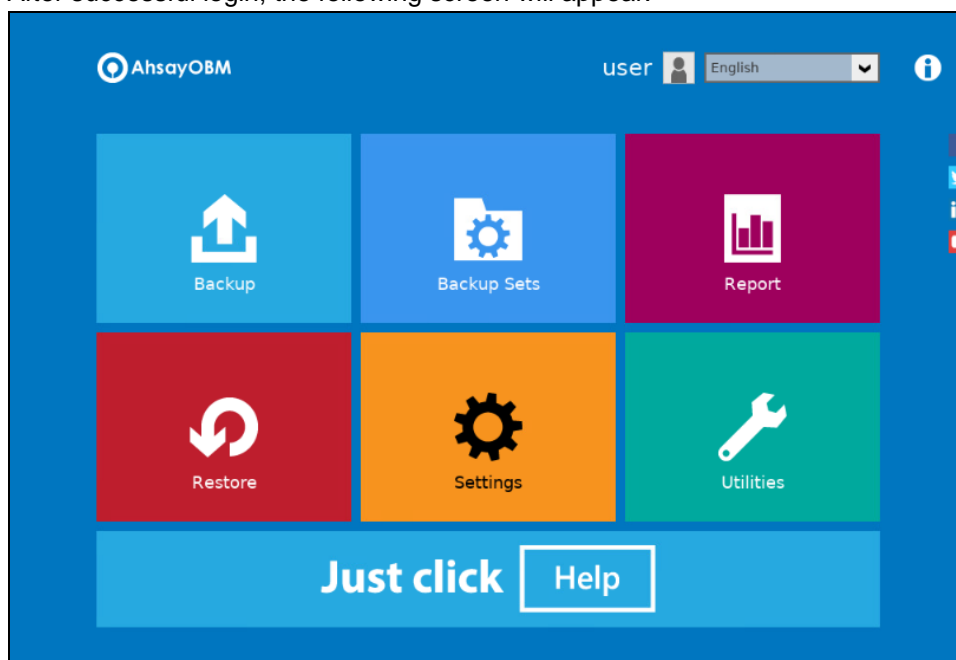
SMS message with a passcode was already sent to the phone number Philippines (+63) - *****8106
Please enter the passcode to continue login.

AMIE - (00:04:48)

[Resend passcode](#)

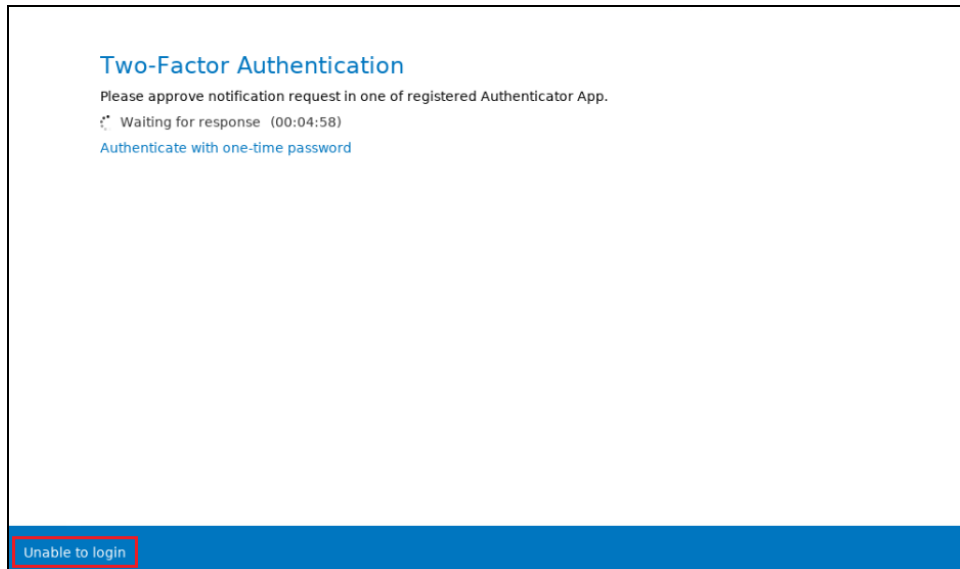
[Verify](#) [Cancel](#) [Help](#)

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



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.

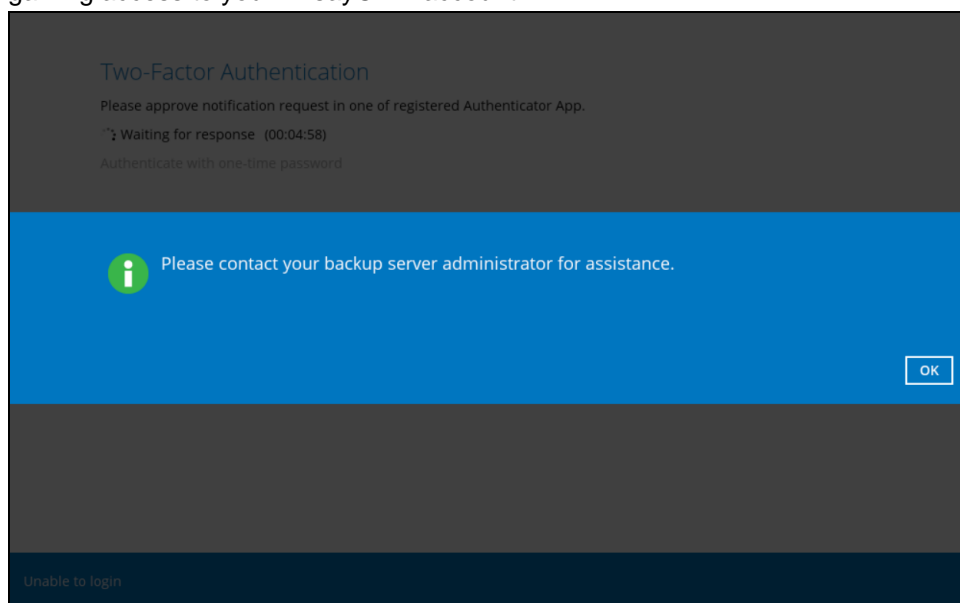


Here are the three scenarios after clicking the **Unable to login** link:

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

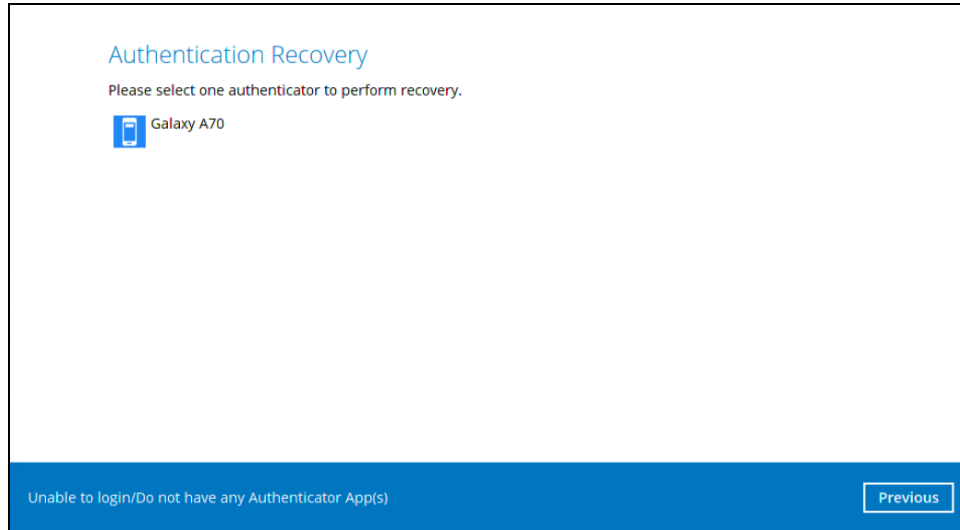
No recovery number was registered on Ahsay Mobile for the 2FA account

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.

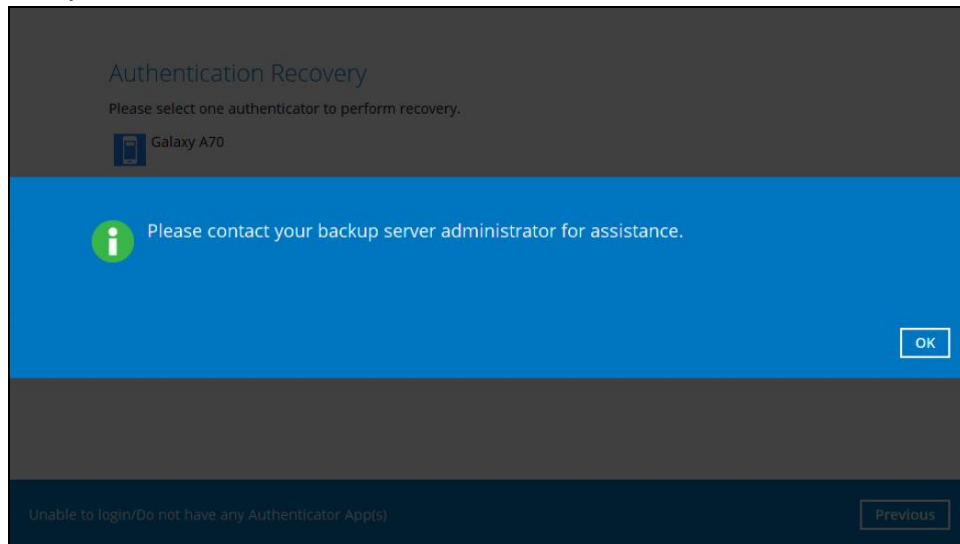


NOTE

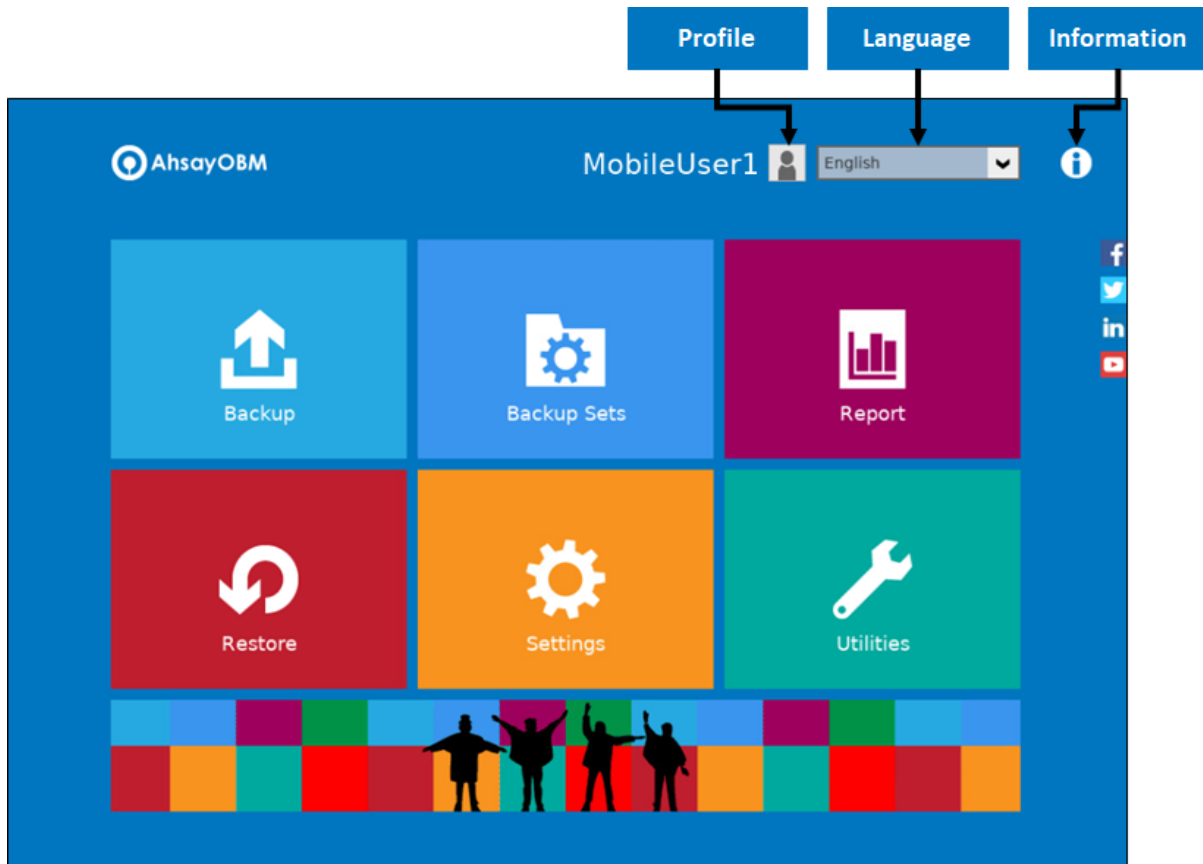
For the detailed steps in performing Authentication Recovery, please refer to the [Ahsay Mobile User Guide for Android and iOS – Appendix A: Troubleshooting Login](#).

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.

The screenshot shows the 'Profile' page with the 'General' tab selected. On the left is a sidebar with links: General, Contacts, Time Zone, Encryption Recovery, and Authentication. The main area is titled 'User Information' and contains two fields: 'Login name' with the value 'MobileUser1' and 'Display name' with an empty text box. At the bottom right are three buttons: 'Save', 'Cancel', and 'Help'.

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

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

Profile

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

User Information

Login name MobileUser1

Display name

Last Successful Login

Time: 10/09/2020 17:53 (CST)

IP address: 180. [REDACTED] 31

Phone number (MFA): 63- [REDACTED]

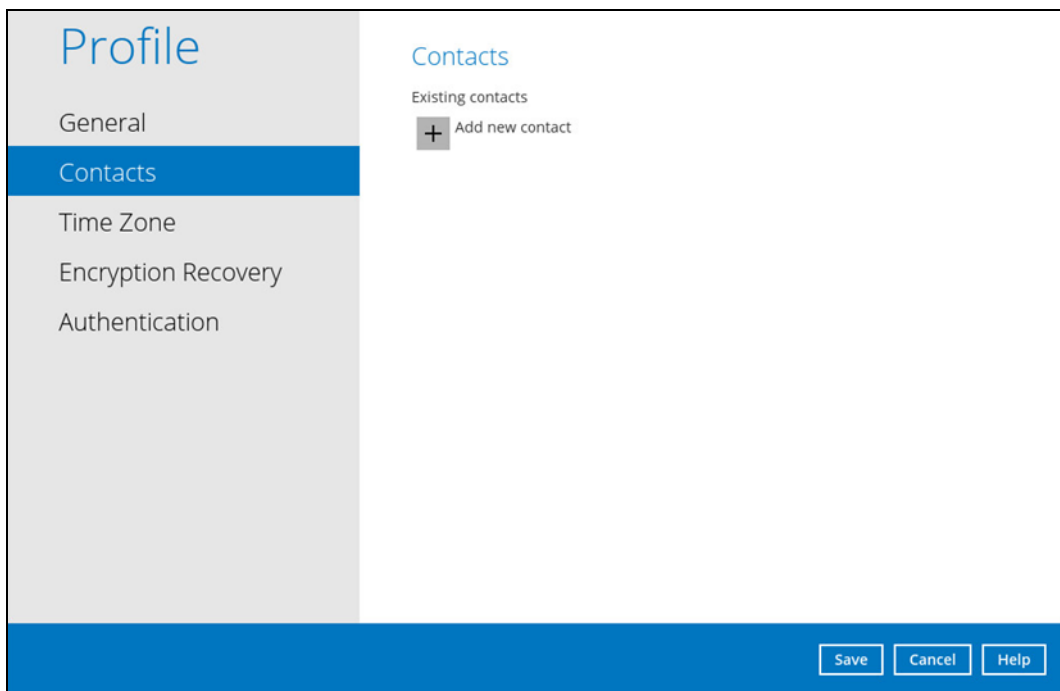
Browser / App: Windows / Chrome

SaveCancelHelp

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

New Contact

Name

Email

☐ Send me encrypted email (S/MIME)

Address

Company

Website

Phone 1

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

Profile

General

Contacts


Time Zone

Encryption Recovery

Authentication

Contacts

Existing contacts

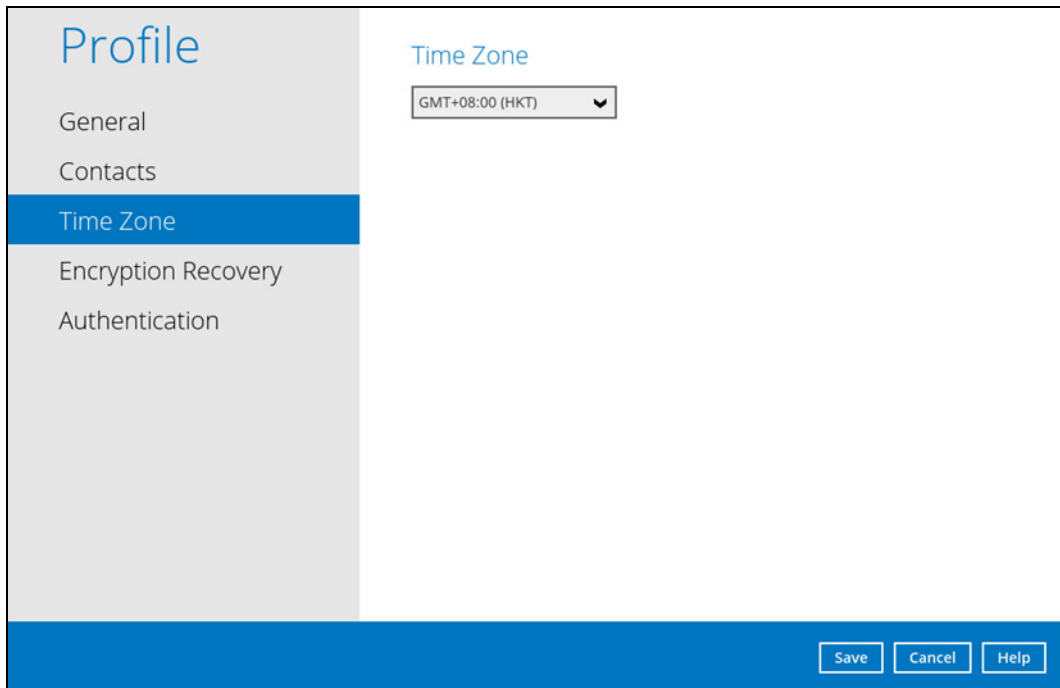
 **samplemail**
samplemail@email.com

Add

Save **Cancel** **Help**

9.1.3 Time Zone

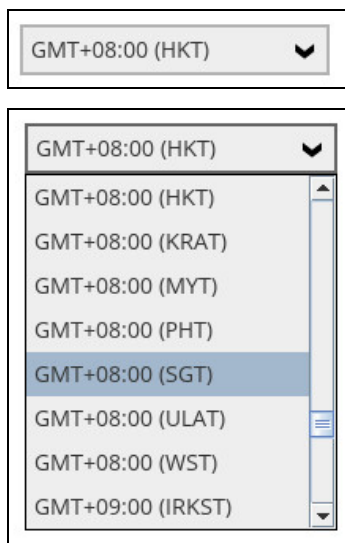
The time zone indicated



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

To modify the time zone, follow the instructions below:

1. Select from the dropdown list.



This image shows a close-up of the time zone dropdown menu. The top part shows the current selection 'GMT+08:00 (HKT)' with a downward arrow. Below it, the dropdown list is open, showing a scrollable list of time zones: 'GMT+08:00 (HKT)', 'GMT+08:00 (KRAT)', 'GMT+08:00 (MYT)', 'GMT+08:00 (PHT)', 'GMT+08:00 (SGT)' (which is highlighted), 'GMT+08:00 (ULAT)', 'GMT+08:00 (WST)', and 'GMT+09:00 (IRKST)'. There are upward and downward arrows on the right side of the list for scrolling.

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

The screenshot shows a web interface for a user profile. On the left is a sidebar with the title "Profile" and a list of settings: "General", "Contacts", "Time Zone", "Encryption Recovery" (which is highlighted with a blue background), and "Authentication". The main content area is titled "Encryption Recovery" in blue text. Below the title, it says "With this option enabled, you can recover your backup set encryption keys by sending a request to us." and "On" followed by a toggle switch that is currently turned on (blue). At the bottom right of the interface, there is a blue bar containing three buttons: "Save", "Cancel", and "Help".

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.).

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

Password

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

The screenshot shows the 'Profile' settings page with a sidebar on the left containing links for General, Contacts, Time Zone, Encryption Recovery, and Authentication (which is highlighted in blue). The main content area is titled 'Password' and includes a 'Change Password' button, a 'Save password' checkbox, and a 'Two-Factor Authentication' section with a toggle switch set to 'off'. Below this is a 'Last Successful Login' section showing 'No login record'. At the bottom right of the page are 'Save', 'Cancel', and 'Help' buttons.

NOTE

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

To change the password, follow the instructions below:

1. Click the **Change Password**.

This screenshot is identical to the one above, showing the 'Profile' settings page with the 'Password' section. The 'Change Password' button is highlighted with a grey background, indicating it is the next step in the process.

2. Enter the current password.

The screenshot shows a 'Change Password' screen. At the top, the title 'Change Password' is in blue. Below it, the text 'Please confirm current password' is followed by a text input field containing six asterisks. At the bottom right, there are two buttons: 'Next' and 'Cancel'.

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

The screenshot shows the 'Change Password' screen with two input fields. The first is labeled 'New Password' and contains six asterisks. The second is labeled 'Re-enter password' and contains seven asterisks. At the bottom right, there are two buttons: 'OK' and 'Cancel'.

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

The screenshot shows a 'Profile' settings screen. On the left is a sidebar with a blue header 'Profile' and a list of settings: 'General', 'Contacts', 'Time Zone', 'Encryption Recovery', and 'Authentication' (which is highlighted in blue). The main area on the right is titled 'Password' and contains a 'Change Password' button, a 'Save password' checkbox, and a 'Two-Factor Authentication' section with a toggle switch set to 'off'. Below that is a 'Last Successful Login' section showing 'No login record'. At the bottom right, there are three buttons: 'Save', 'Cancel', and 'Help'.

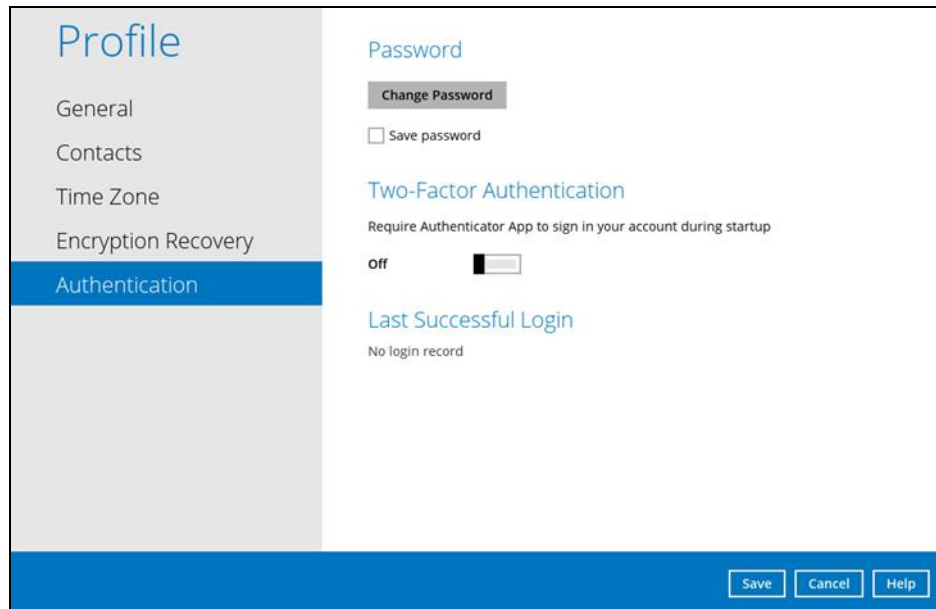
Two-Factor Authentication

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

NOTE

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

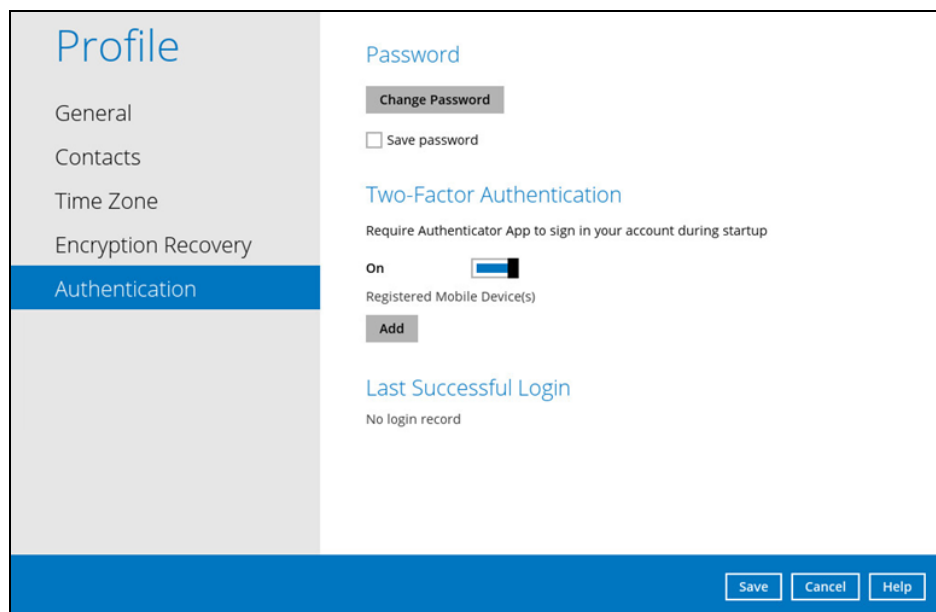
1. Go to **Settings > Authentication > Two-Factor Authentication**.



The screenshot shows the 'Authentication' settings page. On the left, a sidebar lists 'Profile', 'General', 'Contacts', 'Time Zone', 'Encryption Recovery', and 'Authentication' (which is highlighted in blue). The main content area is titled 'Two-Factor Authentication' and includes a 'Change Password' button, a 'Save password' checkbox, and a toggle switch for 'Require Authenticator App to sign in your account during startup'. The toggle is currently set to 'Off'. Below this, there is a section for 'Last Successful Login' showing 'No login record'. At the bottom right, there are 'Save', 'Cancel', and 'Help' buttons.


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

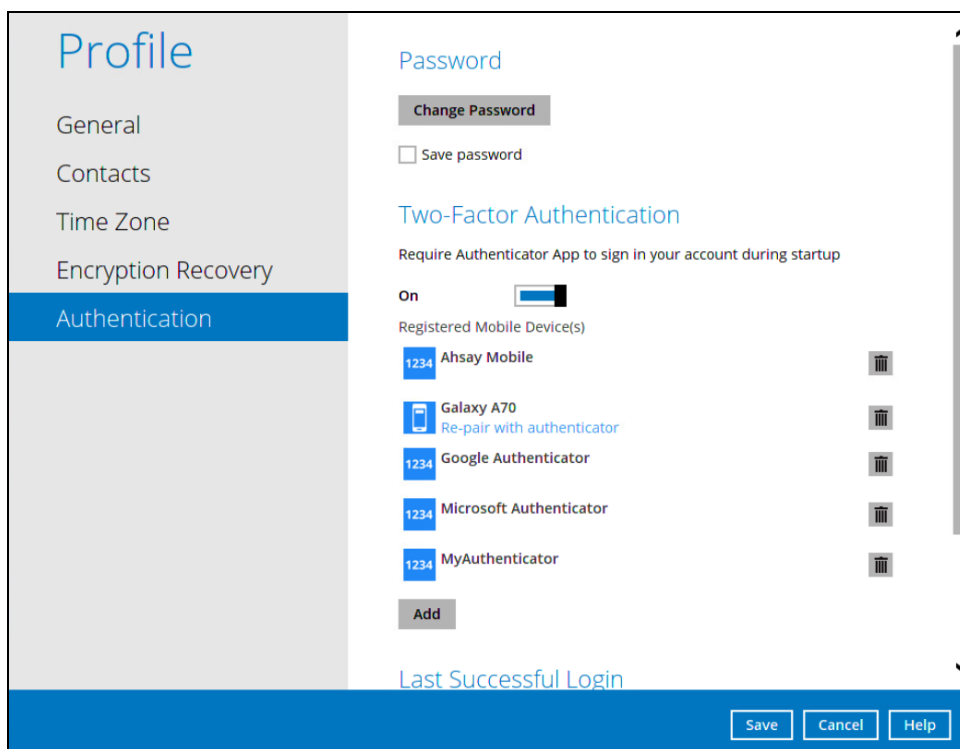
For the detailed step-by-step procedure on how to add a mobile device, please refer to [Ahsay Mobile User Guide for Android and iOS – Chapter 6.3.1](#)



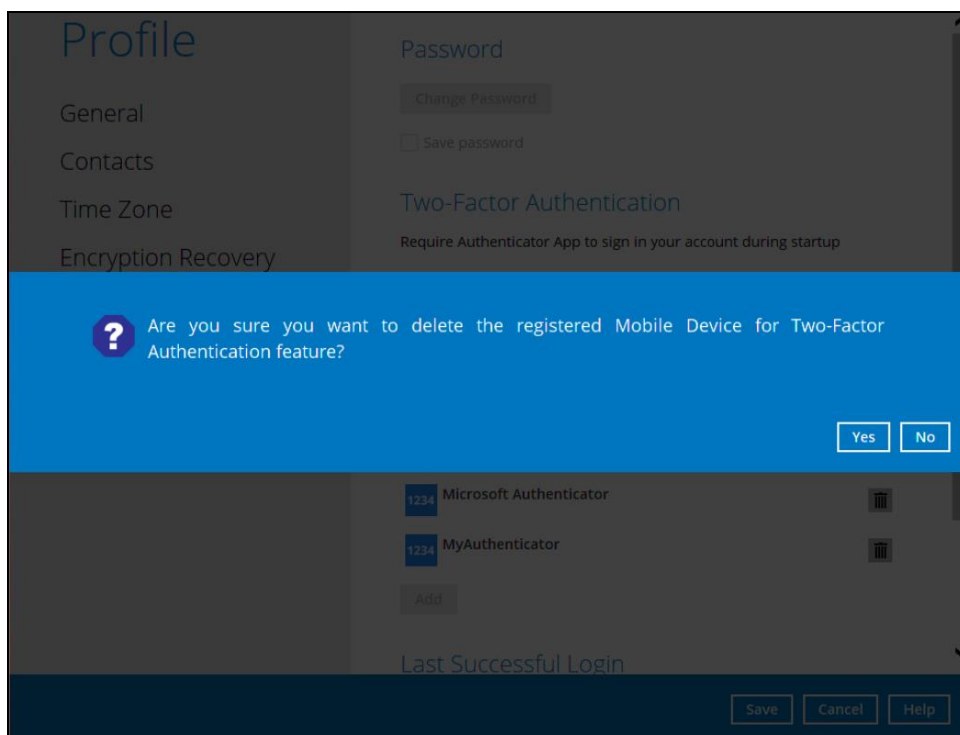
This screenshot shows the same 'Authentication' settings page, but the toggle switch for 'Require Authenticator App to sign in your account during startup' is now set to 'On'. Below the toggle, there is a section for 'Registered Mobile Device(s)' with an 'Add' button. The 'Last Successful Login' section still shows 'No login record'. The 'Save', 'Cancel', and 'Help' buttons remain at the bottom right.

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.

The screenshot displays the 'Profile' settings page in the Ahsay application. The left sidebar contains navigation links: 'General', 'Contacts', 'Time Zone', 'Encryption Recovery', and 'Authentication' (which is highlighted in blue). The main content area is titled 'Authentication' and includes a 'Password' section with a 'Change Password' button and a 'Save password' checkbox. Below this is the 'Two-Factor Authentication' section, which is currently 'On' as indicated by a blue toggle switch. It lists four registered mobile devices: 'Ahsay Mobile', 'Google Authenticator', 'Microsoft Authenticator', and 'MyAuthenticator', each with a trash icon for removal. An 'Add' button is located at the bottom of the list. The 'Last Successful Login' section shows the time '10/09/2021 11:25 (CST)'. At the bottom right, there are 'Save', 'Cancel', and 'Help' buttons.

Profile

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

Password

[Change Password](#)

☐ Save password

Two-Factor Authentication

Require Authenticator App to sign in your account during startup

On ☒

Registered Mobile Device(s)

- 1234 Ahsay Mobile
- 1234 Google Authenticator
- 1234 Microsoft Authenticator
- 1234 MyAuthenticator

[Add](#)

Last Successful Login

Time: 10/09/2021 11:25 (CST)

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

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

NOTE

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

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

The screenshot shows the 'Profile' page with a sidebar menu containing 'General', 'Contacts', 'Time Zone', 'Encryption Recovery', and 'Authentication'. The 'Authentication' section is active. Under 'Two-Factor Authentication', the toggle switch is in the 'On' position. Below the toggle, two mobile devices are listed: 'Galaxy A70' and 'Ahsay Mobile'. The 'Last Successful Login' section shows the time as 10/09/2021 11:25 (CST), IP address, browser/app as OBM, and mobile device as Galaxy A70. At the bottom right, there are 'Save', 'Cancel', and 'Help' buttons.

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

This screenshot is identical to the previous one, but the 'Two-Factor Authentication' toggle switch is now in the 'Off' position. The rest of the interface, including the sidebar, device list, login details, and bottom buttons, remains the same.

Re-pair with authenticator

AhsayOBM supports “Re-pair with authenticator” feature that enables user to re-pair their AhsayOBM account with Ahsay Mobile Authenticator as long as the mobile device used for 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.

The screenshot shows the 'Profile' page with the 'Authentication' tab selected. The left sidebar lists 'General', 'Contacts', 'Time Zone', 'Encryption Recovery', and 'Authentication'. The main content area is titled 'Password' and includes a 'Change Password' button and a 'Save password' checkbox. Below this is the 'Two-Factor Authentication' section, which is currently 'On'. It lists 'Registered Mobile Device(s)' with two entries: 'Galaxy A70' and 'Ahsay Mobile'. The 'Galaxy A70' entry has a red box around the 'Re-pair with authenticator' link. There is an 'Add' button below the list. At the bottom, the 'Last Successful Login' section shows the time, IP address, browser/app, and mobile device used.

Profile

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

Password

Change Password

☐ Save password

Two-Factor Authentication

Require Authenticator App to sign in your account during startup

On ☒

Registered Mobile Device(s)

- Galaxy A70
Re-pair with authenticator
- 1234 Ahsay Mobile

Add

Last Successful Login

Time: 10/09/2021 11:25 (CST)

IP address: [REDACTED]

Browser / App: OBM

Mobile Device: Galaxy A70

Save Cancel Help

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.

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

- Time: 10/09/2021 11:25 (CST)
- IP address: [Redacted]
- Browser / App: OBM
- Mobile Device: Galaxy A70

The 'Two-Factor Authentication' section shows it is 'On' with a toggle switch. Under 'Registered Mobile Device(s)', there are two entries: 'Galaxy A70' and 'Ahsay Mobile', each with a 'Re-pair with authenticator' link and a trash icon. An 'Add' button is at the bottom of this list.

At the bottom of the page are 'Save', 'Cancel', and 'Help' buttons.

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

This screenshot is similar to the one above but shows 'No login record' under the 'Last Successful Login' section. The 'Two-Factor Authentication' section shows it is 'On'. Under 'Registered Mobile Device(s)', there are two entries: 'Redmi Note 8' and 'MobileUser1', each with a trash icon. An 'Add' button is at the bottom of this list.

At the bottom of the page are 'Save', 'Cancel', and 'Help' buttons.

9.1.6 Password

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

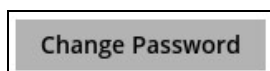
The screenshot shows the 'Profile' settings page with the 'Password' tab selected. On the left sidebar, the options are General, Contacts, Time Zone, Encryption Recovery, Password (highlighted), and Security Settings. The main content area is titled 'Password' and contains a 'Change Password' button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

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:

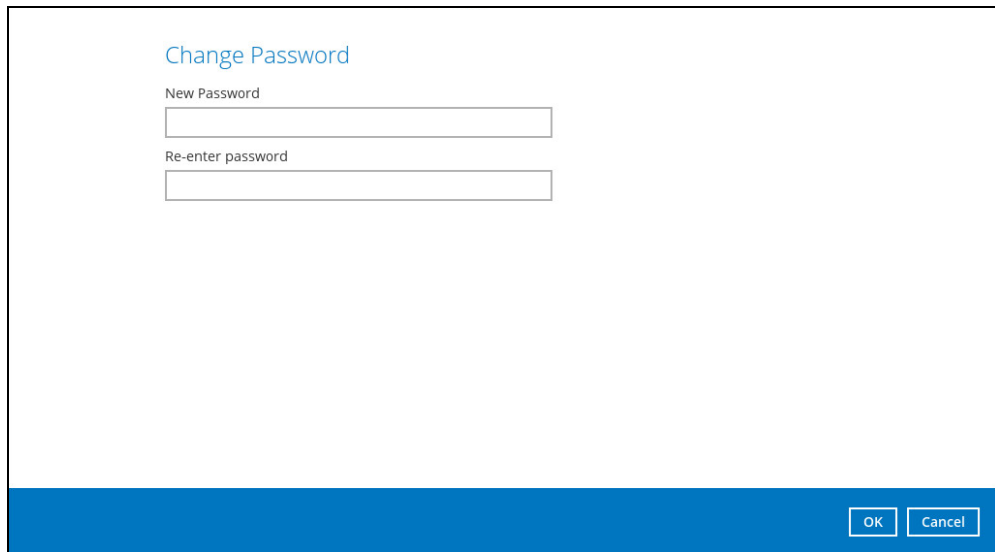
1. Click **Change Password** button.



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

The screenshot shows the 'Change Password' dialog box. It has a title bar 'Change Password' and a label 'Please confirm current password' above a text input field. At the bottom right, there are 'Next' and 'Cancel' buttons.

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



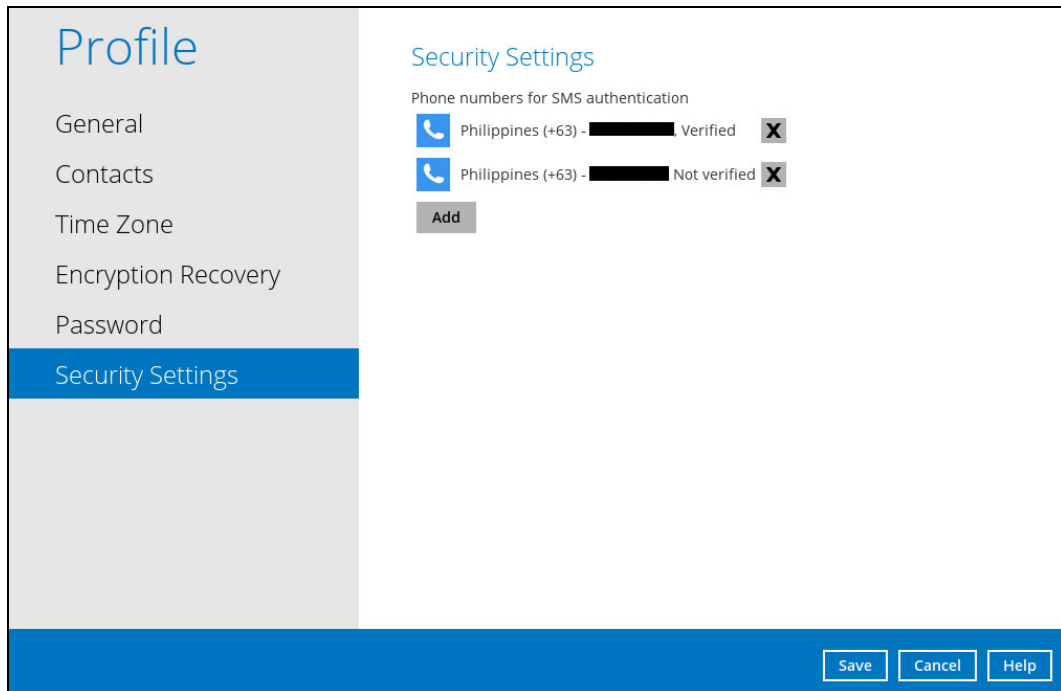
A screenshot of a 'Change Password' dialog box. The title 'Change Password' is in blue text at the top left. Below it are two text input fields: the first is labeled 'New Password' and the second is labeled 'Re-enter password'. At the bottom right, there are two buttons: 'OK' and 'Cancel'.

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.



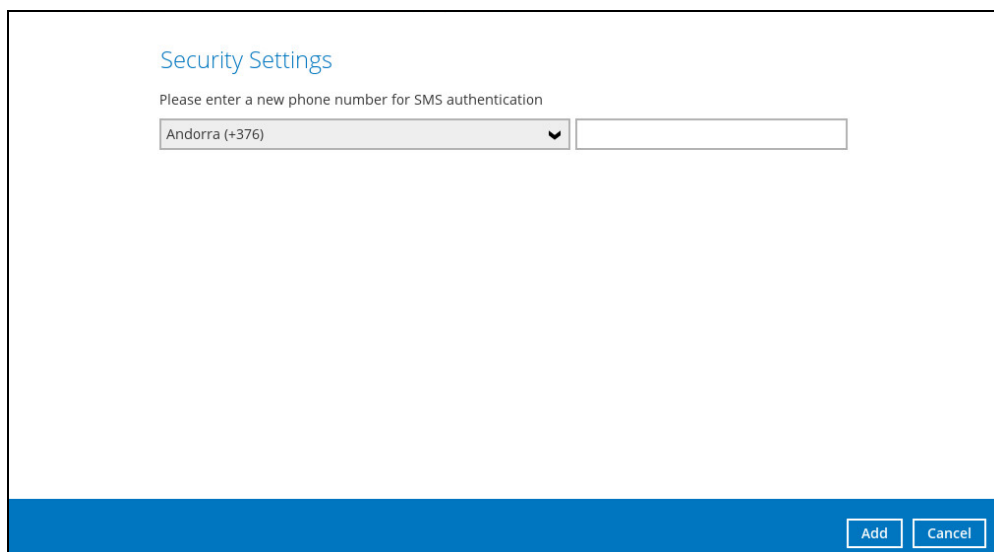
The screenshot shows the 'Security Settings' page. On the left is a sidebar with 'Profile' and several menu items: 'General', 'Contacts', 'Time Zone', 'Encryption Recovery', 'Password', and 'Security Settings' (which is highlighted in blue). The main content area is titled 'Security Settings' and contains the heading 'Phone numbers for SMS authentication'. Below this, there are two entries, each with a phone icon, a country code 'Philippines (+63)', a masked phone number, and a status: 'Verified' and 'Not verified' respectively. Each entry has a small 'X' icon to its right. Below the list is an 'Add' button. At the bottom right of the page are 'Save', 'Cancel', and 'Help' buttons.

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**.

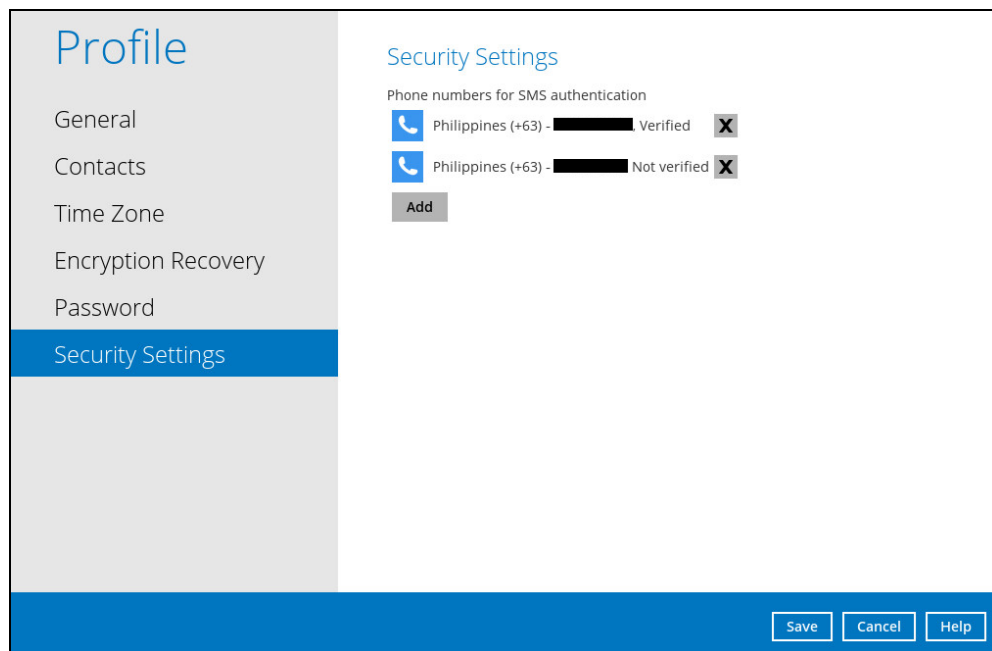


The screenshot shows the 'Security Settings' page with the heading 'Please enter a new phone number for SMS authentication'. Below this is a form with a dropdown menu for country codes (currently showing 'Andorra (+376)') and a text input field for the phone number. At the bottom right of the page are 'Add' and 'Cancel' buttons.

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.



The screenshot shows a web interface for a user's profile. On the left is a sidebar with the title "Profile" and a list of settings: General, Contacts, Time Zone, Encryption Recovery, Password, and Security Settings (which is highlighted in blue). The main content area is titled "Security Settings" and contains a section for "Phone numbers for SMS authentication". This section lists two phone numbers: "Philippines (+63) - [REDACTED] Verified" and "Philippines (+63) - [REDACTED] Not verified". Each entry has a blue phone icon on the left and a grey "X" button on the right. Below the list is a grey "Add" button. At the bottom right of the main content area are three buttons: "Save", "Cancel", and "Help".

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.





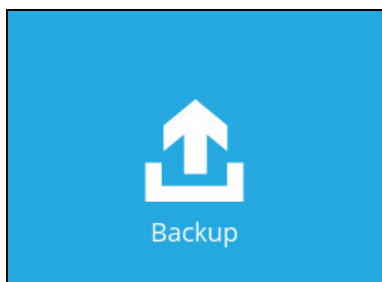
Version	9.0.2.24
Virtual Machine Vendor	OpenJDK 64-Bit Server VM Version 25.181-b13 Oracle Corporation
Live Threads	12 (Current) / 26 (Peak)
Daemon Threads	8
Total Threads Started	140
Heap Size	197,322 kbytes (Current) / 1,864,192 kbytes (Maximum)
Operating System	Linux Version 4.18.0-240.1.1.el8_3.x86_64
Architecture	amd64
Number of Processors	4
Committed Virtual Memory	5,728,456 kbytes
Physical Memory	176,080 kbytes (Free) / 3,825,304 kbytes (Total)
Swap Space	2,600,512 kbytes (Free) / 4,169,724 kbytes (Total)
VM Arguments	-Xrs -Xms128m -Xmx2048m -XX:MaxDirectMemorySize=512m -Dsun.nio.PageAlignDirectMemory=true -Djava.library.path=./LinX64 ./cb.jar
Class Path	./LinX64
Library Path	./usr/local/obm/jvm/lib/resources.jar:/usr/local/obm/jvm/lib/rt.jar:/usr/local/obm/jvm/lib/sunrsasign.jar:/usr/local/obm/jvm/lib/jsse.jar:/usr/local/obm/jvm/lib/jce.jar:/usr/local/obm/jvm/lib/charsets.jar:/usr/local/obm/jvm/lib/jfr.jar:/usr/local/obm/jvm/classes
Boot Class Path	

© 2021 Ahsay Systems Corporation. All Rights Reserved.

Close

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](#).

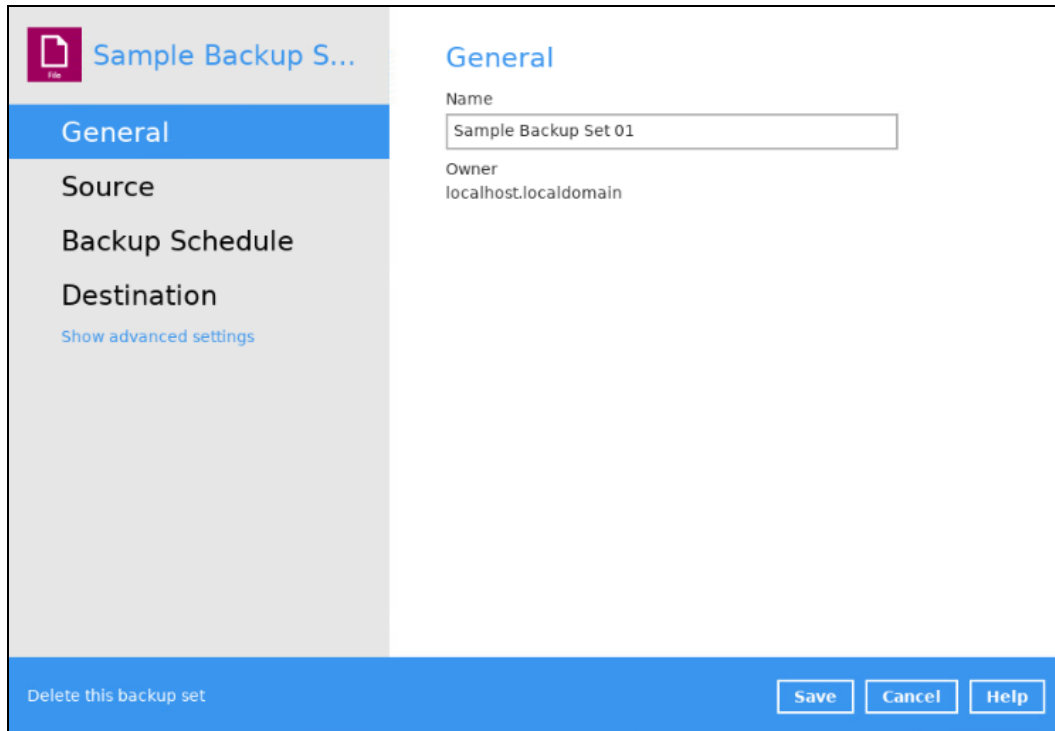
Backup Set Settings

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.



The screenshot shows a software window titled "Sample Backup S...". On the left is a sidebar with a blue header "General" and three grey options: "Source", "Backup Schedule", and "Destination". Below "Destination" is a link "Show advanced settings". The main area is titled "General" and contains two fields: "Name" with a text box containing "Sample Backup Set 01", and "Owner" with the text "localhost.localdomain". At the bottom is a blue bar with the text "Delete this backup set" on the left and three buttons "Save", "Cancel", and "Help" on the right.

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.

Sample Backup S...

General

Source

Backup Schedule

Destination

[Show advanced settings](#)

Backup Source
Select the files and folders that you want to backup
☐ root

Filter
Apply filters to the backup source
off ☐

I would like to choose the files to backup

Quick Selection

Filter

Advanced Backup Source

Delete this backup set

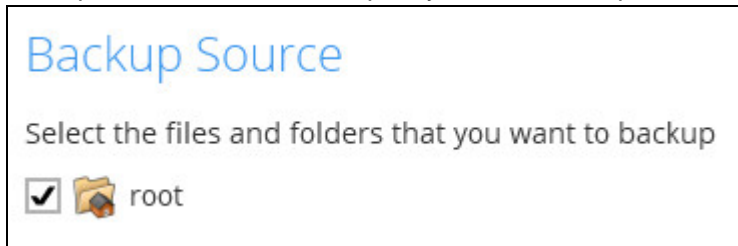
Save Cancel Help

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

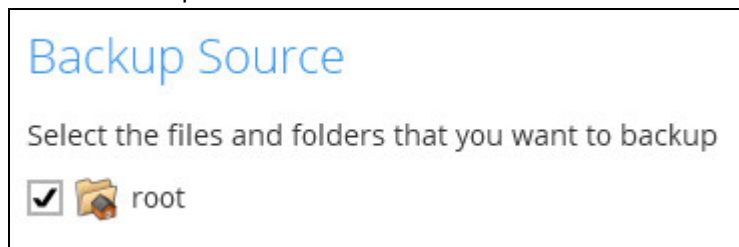
This option allows the user to quickly select a backup source to be backed up.



The screenshot shows a screen titled "Backup Source" in blue text. Below the title is the instruction "Select the files and folders that you want to backup". At the bottom, there is a checked checkbox next to a folder icon and the text "root".

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

1. Select a backup source.

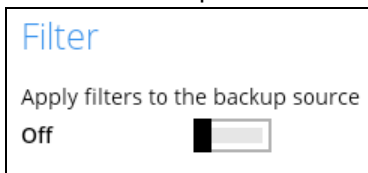


This is a duplicate of the screenshot above, showing the "Backup Source" screen with "root" selected.

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

Option no. 2: Filter

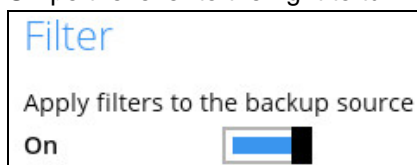
The Filter Backup Source is an alternative way to select a backup source.



The screenshot shows a screen titled "Filter" in blue text. Below the title is the instruction "Apply filters to the backup source". At the bottom, the word "Off" is displayed next to a toggle switch that is currently in the "off" position (black bar on the left).

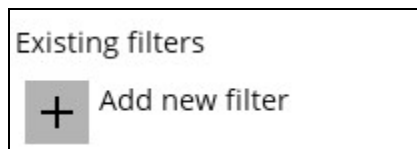
To select files and/or folders to back up using the Filter Backup Source, follow the steps below:

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



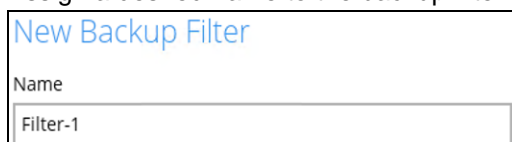
The screenshot shows the "Filter" screen with the toggle switch now in the "on" position (blue bar on the left, black bar on the right). The word "On" is displayed below the switch.

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



The screenshot shows a screen titled "Existing filters". Below the title is a grey button with a plus sign and the text "Add new filter".

3. Assign a desired name to the backup filter.



The screenshot shows a screen titled "New Backup Filter". Below the title is a label "Name" followed by a text input field containing the text "Filter-1".

4. Select from the options below.

For each of the matched files/folders under top directory

☒ Include them

☐ Exclude them

☐ Exclude all unmatched files/folders



Match file/folder names by

☒ Simple comparison ▼

☐ Regular expression (UNIX-style)

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

Existing patterns to match

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

Apply this filter in

☐ All hard disk drives

☒ This folder only


Apply to


☒ File ☒ Folder

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

8. Multiple backup filters can be created.

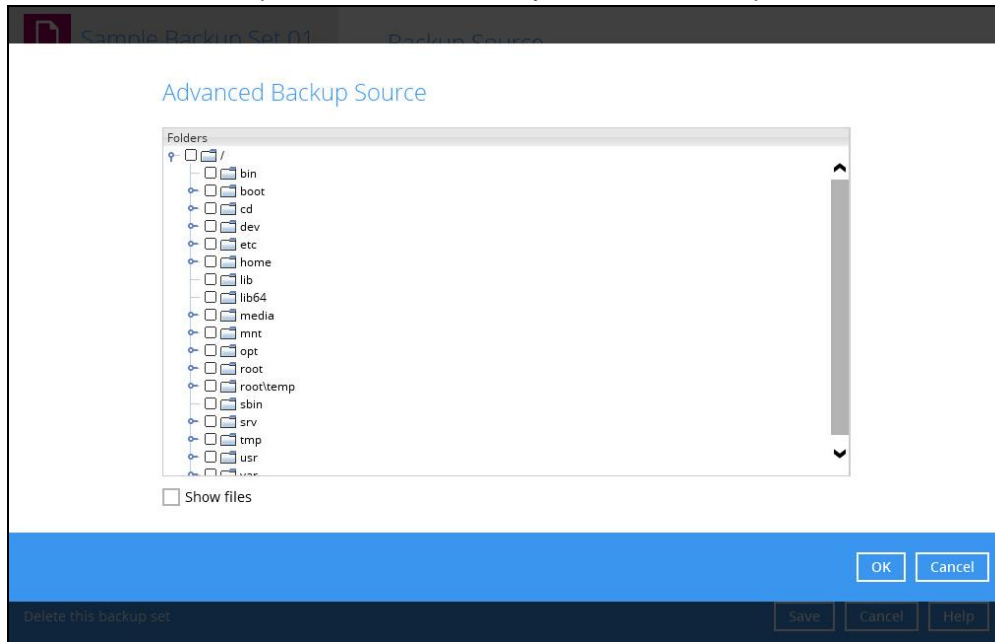
Existing filters

 Filter-1
/root/Documents

 Filter-2
All hard disk drives

Option no. 3: Advanced Backup Source

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

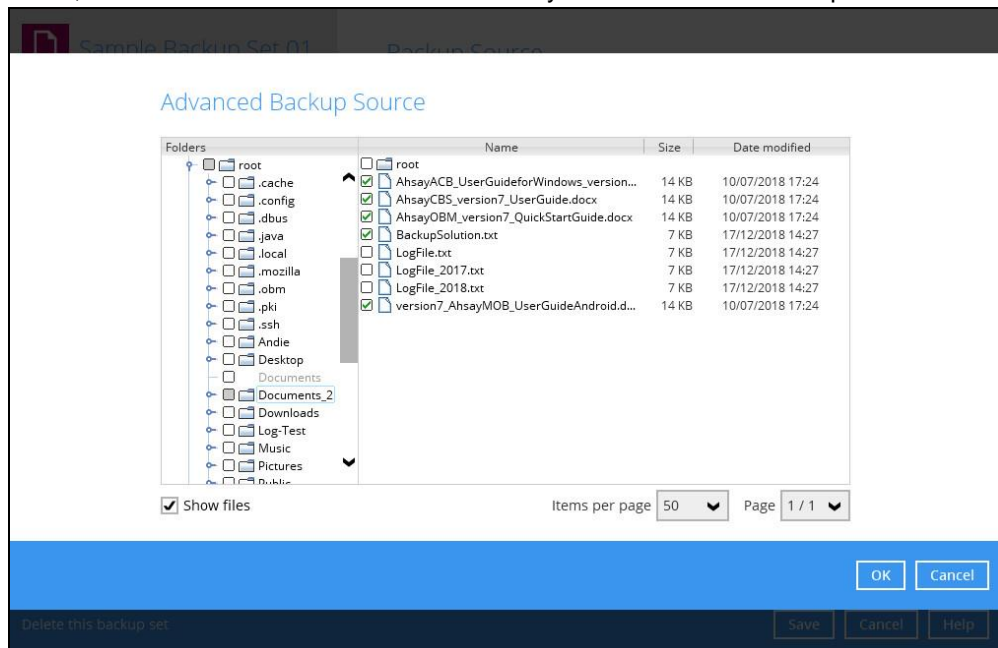


To select files and/or folders using the Advanced Backup Source, follow the steps below:

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

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.



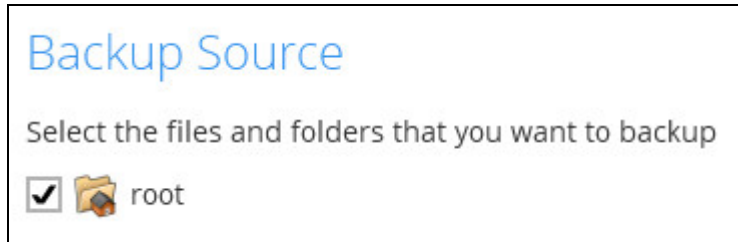
3. Click the **OK** button to save the selection, then click the **Save** button to save settings.

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:

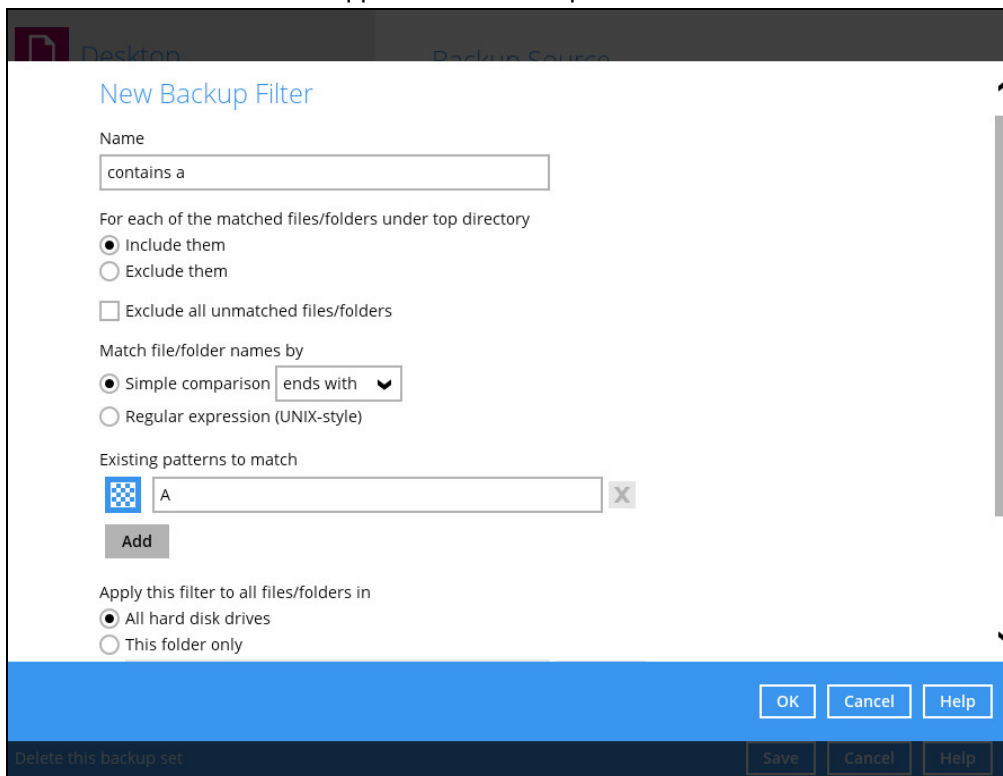
Scenario 1 (Quick Selection + Filter)

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.

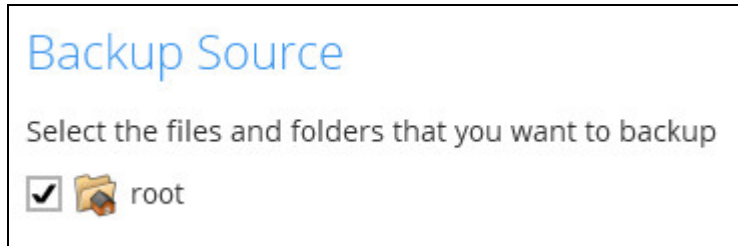


3. Click the **OK** button to save the created filter, then click the **Save** button to save settings.

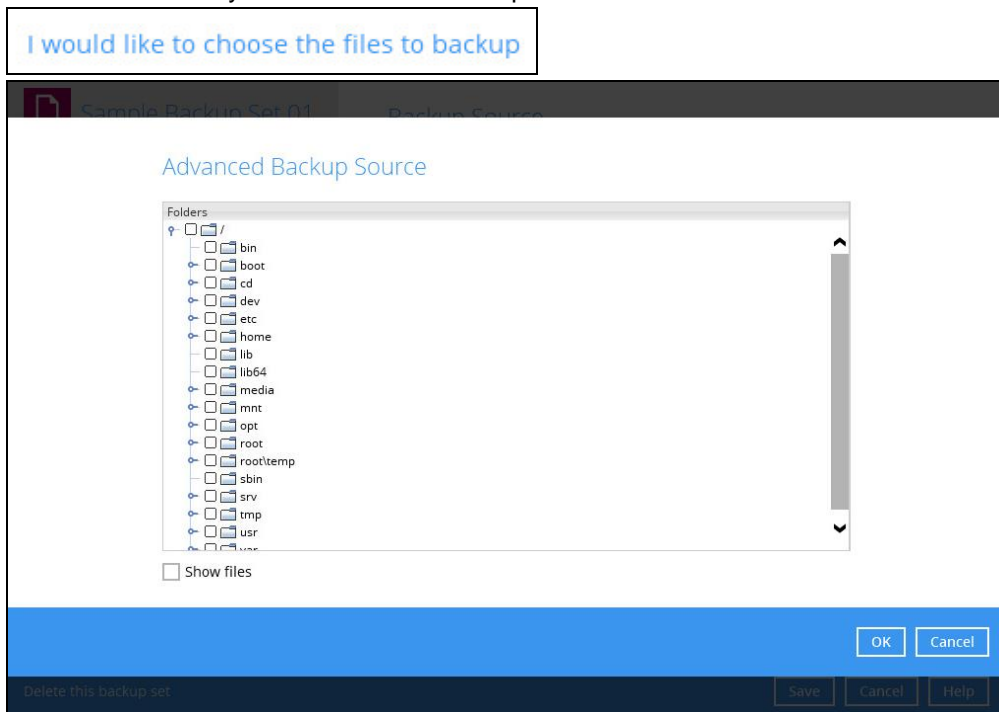
Scenario 2 (Quick Selection + Advanced Backup Source)

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

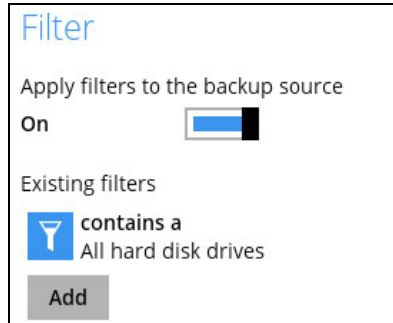


3. Click the **OK** button to save the selection, then click the **Save** button to save settings.

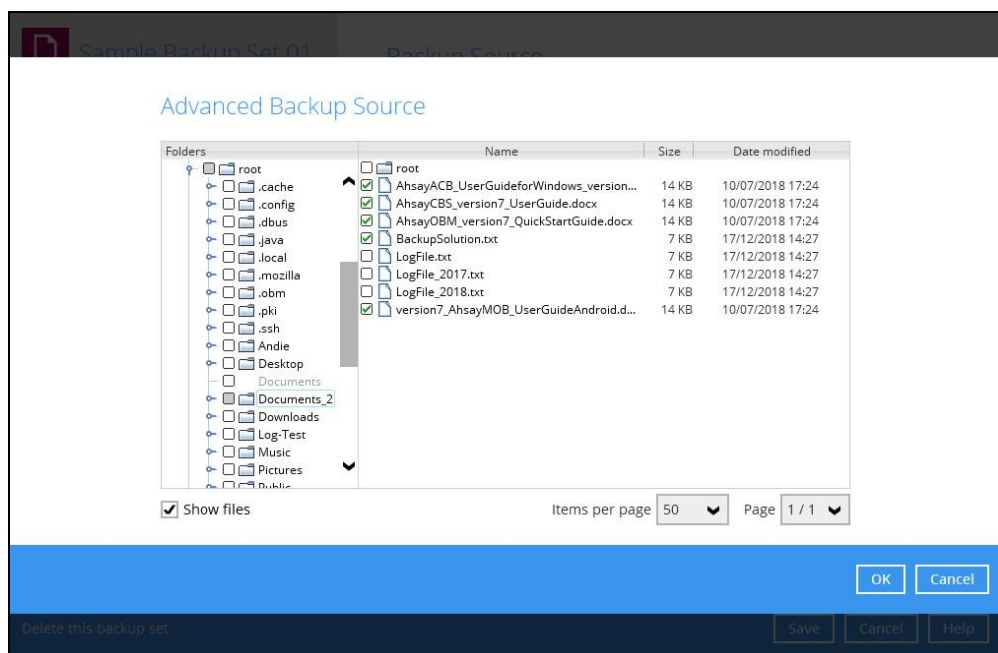
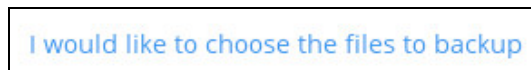
Scenario 3 (Filter + Advanced Backup Source)

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

1. Create a filter.



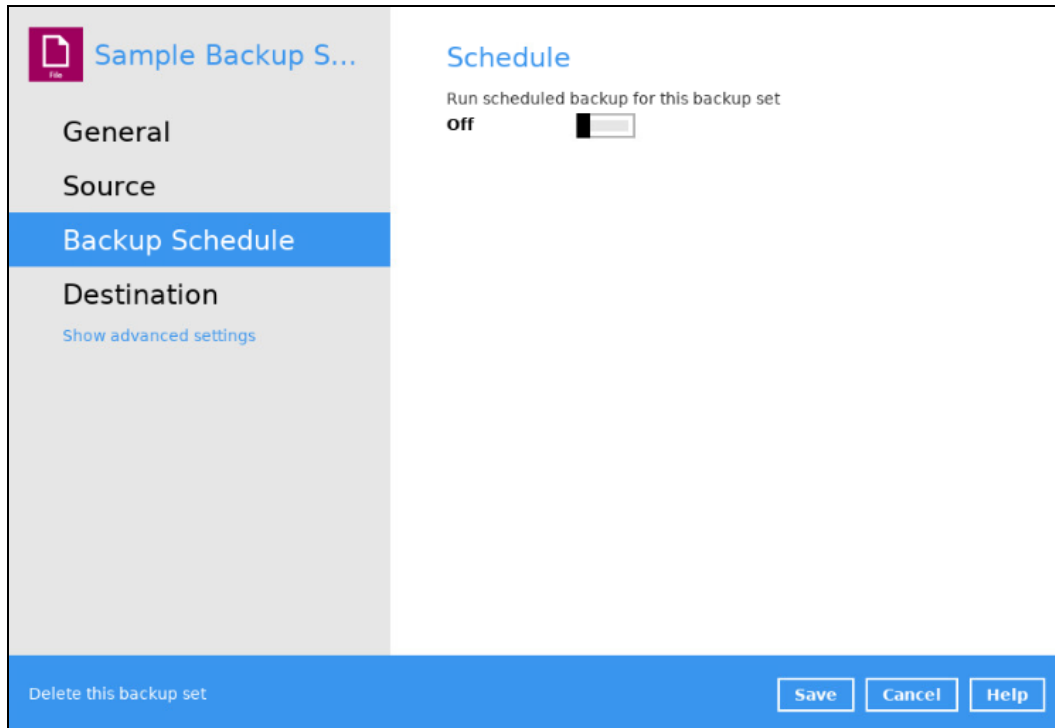
2. In the source window, select 'I would like to choose the files to backup' to choose files and/or folders that you would like to back up.



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

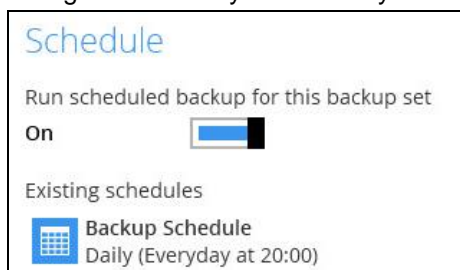
Backup Schedule

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

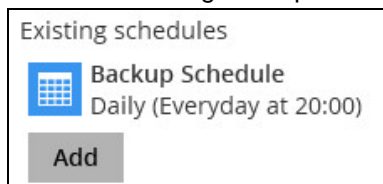


To configure a backup schedule, follow the steps below:

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.

New Backup Schedule

Name
Daily-1

Type
Daily

Start backup
at 00 : 00

Stop
until full backup completed

☒ Run Retention Policy after backup

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

New Backup Schedule

Name
Weekly-1

Type
Weekly

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

Start backup
at 00 : 00

Stop
until full backup completed

☒ Run Retention Policy after backup

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

New Backup Schedule

Name
Monthly-1

Type
Monthly

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

Start backup at
00 : 00 on the selected days

Stop
until full backup completed

☒ Run Retention Policy after backup

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

New Backup Schedule

Name
Custom-1

Type
Custom

Backup on the following day once
2020 December 31

Start backup at
00 : 00

Stop
until full backup completed

☒ Run Retention Policy after backup

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

- **at** – this option will start a backup job at a specific time.
- **every** – this option will start a backup job in intervals of minutes or hours.
 - 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

Start backup
every

Stop
until full backup completed

☒ Run Retention Policy after backup

1 minute
1 minute
2 minutes
3 minutes
4 minutes
5 minutes
6 minutes
10 minutes
12 minutes

Start backup
every

Stop
until full backup completed

☒ Run Retention Policy after backup

1 minute
30 minutes
1 hour
2 hours
3 hours
4 hours
6 hours
8 hours
12 hours

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

The image shows two side-by-side screenshots of the 'New Backup Schedule' configuration form. The left form is for a backup named 'Daily-1' with a 'Daily' type. It is configured to start 'every 4 hours' and stop 'until full backup completed'. The checkbox 'Run Retention Policy after backup' is checked. The right form is for a backup named 'Weekly-1' with a 'Weekly' type. It is configured to start 'every 4 hours' on 'Tue' and 'Thu' (indicated by checked checkboxes in the 'Backup on these days of the week' section). It also stops 'until full backup completed' and has the 'Run Retention Policy after backup' checkbox checked.

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.

Schedule

Run scheduled backup for this backup set

On ☒

Existing schedules

-  **Daily-1**
Daily (Everyday at 18:00)
-  **Weekly-1**
Weekly - Saturday (Every week at 19:00)
-  **Monthly-1**
Monthly - The Last Weekday (Every month at 20:00)
-  **Custom-1**
Custom (12/31/2020 at 21:00)

Add

NOTE

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

1. Backup type: Full > Differential

While for Schedules that have selectable Backup Type:

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

2. Stop: after X hours > after Y hours > until full backup completed (where X < Y)

3. Run Retention Policy after backup: enabled > disabled

4. Schedule type: Daily > Weekly > Monthly > Custom

5. Creation order

Examples:

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

Destination

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

The screenshot shows the 'Destination' configuration window for a backup set named 'Sample Backup S...'. On the left is a sidebar with navigation tabs: 'General', 'Source', 'Backup Schedule', and 'Destination' (which is selected and highlighted in blue). Below the 'Destination' tab is a link that says 'Show advanced settings'. The main area of the window is titled 'Destination' and contains the following elements: a 'Backup mode' dropdown menu currently set to 'Sequential'; a section titled 'Existing storage destinations' which lists one destination: 'AhsayCBS' with 'Host: 10.3.121.17:80'; an 'Add' button; and up/down arrow icons. At the bottom of the window is a blue bar containing the text 'Delete this backup set' on the left and three buttons: 'Save', 'Cancel', and 'Help' on the right.

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.

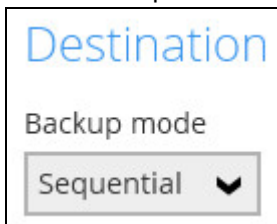
Comparison between Sequential and Concurrent Backup mode

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

Concurrent	<ul style="list-style-type: none"> ➤ Backup job is faster than in Sequential mode. ➤ Maximum number of concurrent backup destinations can be configured. 	<ul style="list-style-type: none"> ➤ Requires more resources in the local machine (e.g. memory, CPU, bandwidth, etc.) to complete a backup job.
-------------------	--	--

To modify the Backup mode, follow the steps below:

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




Destination

Backup mode

Sequential ▼

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



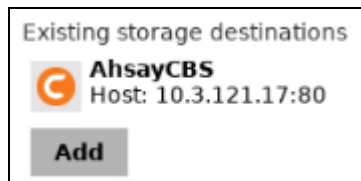
Maximum concurrent backup destinations

2 ▼


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

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

1. Click the **Add** button.

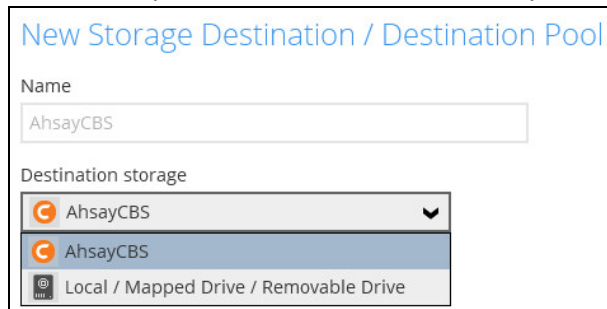


Existing storage destinations

 **AhsayCBS**
Host: 10.3.121.17:80

Add

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





New Storage Destination / Destination Pool


Name

AhsayCBS

Destination storage


 AhsayCBS ▼

 AhsayCBS

 Local / Mapped Drive / Removable Drive

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.

Destination storage

 Local / Mapped Drive / Removable Drive

▼

Local path

Change

Test

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.

The screenshot shows the 'Deduplication' settings for 'Sample Backup Set 01'. On the left is a sidebar with navigation links: General, Source, Backup Schedule, Destination, Deduplication (selected), Retention Policy, Command Line Tool, Bandwidth Control, Others, and a 'Hide advanced settings' link. The main panel is titled 'Deduplication' and contains the following settings: 'Enable Deduplication' is set to 'On' with a toggle switch; 'Deduplication scope' has two radio buttons, 'Same file path within the same backup set' and 'All files within the same backup set' (which is selected); 'Block size' is a dropdown menu showing '64 k - 256 k (optimal settings)' with a 'Bytes' unit indicator; and 'Migrate existing data to latest version' is an unchecked checkbox. At the bottom of the window are three buttons: 'Delete this backup set', 'Save', 'Cancel', and 'Help'.

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.

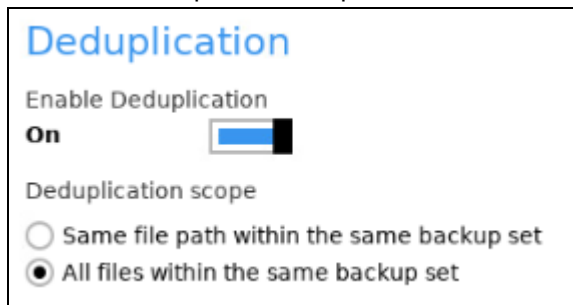
Migrate Data

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.

The screenshot shows a single checkbox labeled 'Migrate Data' with the text 'Migrate existing data to latest version' next to it. The checkbox is currently unchecked.

To configure the deduplication settings, follow the instructions below:

1. Select the Deduplication scope.



Deduplication

Enable Deduplication
On

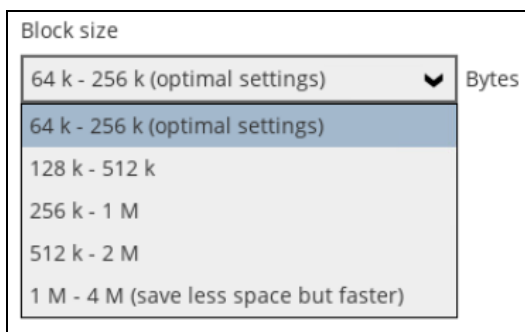
Deduplication scope

☐ Same file path within the same backup set

☒ All files within the same backup set

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

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



Block size

64 k - 256 k (optimal settings) ▼ Bytes

64 k - 256 k (optimal settings)

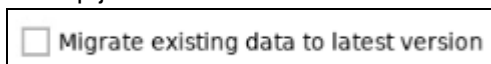
128 k - 512 k

256 k - 1 M

512 k - 2 M

1 M - 4 M (save less space but faster)

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



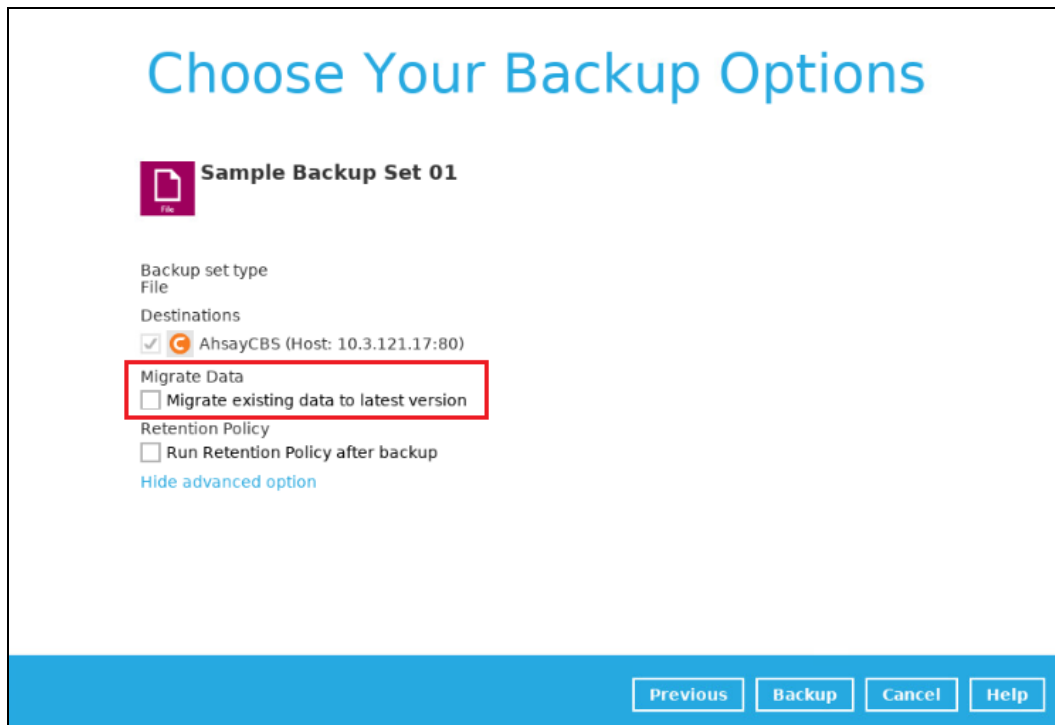
☐ Migrate existing data to latest version

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


Run Backup Job

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


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



Choose Your Backup Options

 **Sample Backup Set 01**

Backup set type
File

Destinations
☒  AhsayCBS (Host: 10.3.121.17:80)

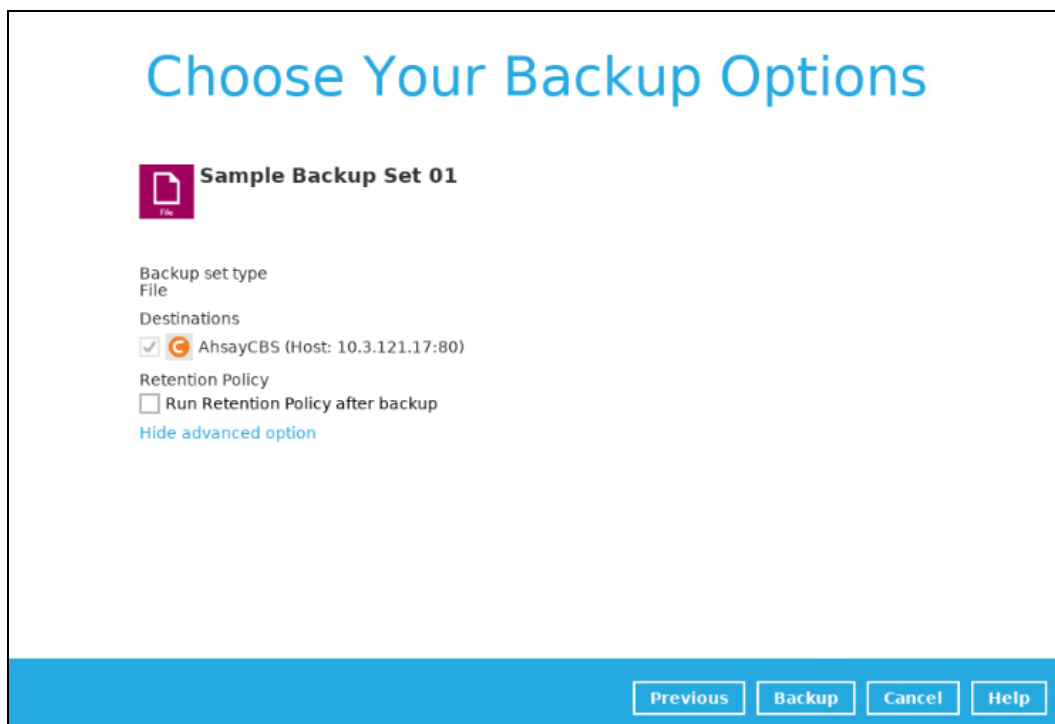
Migrate Data
☐ Migrate existing data to latest version

Retention Policy
☐ Run Retention Policy after backup


[Hide advanced option](#)

[Previous](#) [Backup](#) [Cancel](#) [Help](#)


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



Choose Your Backup Options

 **Sample Backup Set 01**

Backup set type
File

Destinations
☒  AhsayCBS (Host: 10.3.121.17:80)

Retention Policy
☐ Run Retention Policy after backup

[Hide advanced option](#)

[Previous](#) [Backup](#) [Cancel](#) [Help](#)

Retention Policy

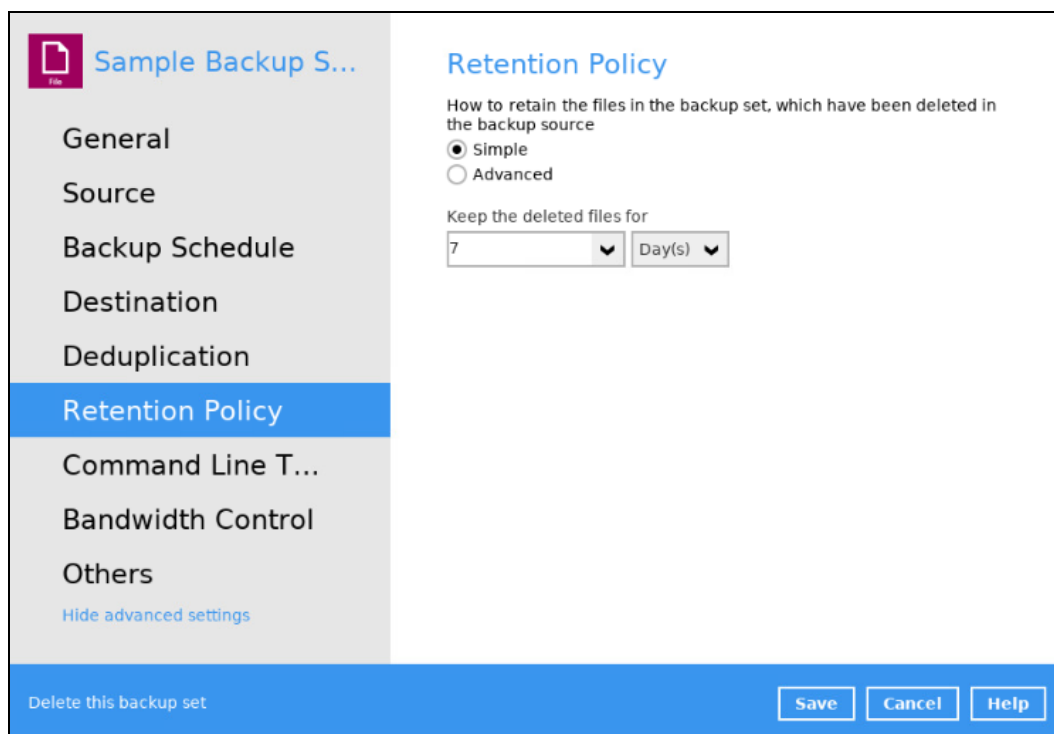
When the AhsayOBM identifies files and/or folders that are deleted, updated, or with updated permission/attributes during a backup job, these files and/or folders will then be moved from the Data Area to the Retention Area.

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.



The screenshot shows the 'Retention Policy' configuration window for a 'Sample Backup S...' backup set. On the left is a sidebar with navigation links: General, Source, Backup Schedule, Destination, Deduplication, Retention Policy (highlighted), Command Line T..., Bandwidth Control, and Others. Below 'Others' is a link for 'Hide advanced settings'. The main panel is titled 'Retention Policy' and contains the text: 'How to retain the files in the backup set, which have been deleted in the backup source'. There are two radio buttons: 'Simple' (selected) and 'Advanced'. Below this is a section 'Keep the deleted files for' with a text input field containing '7' and a dropdown menu set to 'Day(s)'. At the bottom of the window is a blue bar with a 'Delete this backup set' link on the left and 'Save', 'Cancel', and 'Help' buttons on the right.

NOTE

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

There are two (2) 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	<ul style="list-style-type: none"> ➤ Daily ➤ Weekly ➤ Monthly ➤ Quarterly ➤ Yearly ➤ Custom
User-defined name	Not applicable	Applicable

WARNING

When files and/or folders in the retention area exceed the Retention Policy setting, they 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.

Retention Policy

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

☒ Simple
☐ Advanced

Keep the deleted files for

▼

Day(s) ▼

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.


Retention Policy

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

☐ Simple

☒ Advanced

Existing advanced retention policies

 Add new advanced retention policy

2. Enter a name for the retention policy.

New Retention Policy

Name

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

Type

Daily

▼

Daily

Weekly

Monthly

Quarterly

Yearly

Custom

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

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

1

1

2

3

4

5

6

7

8

- 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:

Name

Daily-1

Type

Daily

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

7

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

Name

Weekly-1

Type

Weekly

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

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

The number of weeks to repeat the above selection

4

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

Name
Monthly-1

Type
Monthly

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

☒ Day 1

☐ First ☐ Sunday

The number of months to repeat the above selection
3

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

Name
Quarterly-1

Type
Quarterly

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

☒ Day 1

☐ First ☐ Sunday

Months of quarter
January, April, July, October

The number of quarters to repeat the above selection
4

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

Name
Yearly-1

Type
Yearly

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

☒ January

☒ Day 1

☐ First ☐ Sunday

☐ Sunday of Week 1

The number of years to repeat the above selection
7

NOTE

Multiple advanced retention policy can be created.

There are three (3) different ways to 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.

The screenshot shows the 'Sample Backup Set 01' settings window. The left sidebar has tabs for 'General', 'Source', 'Backup Schedule' (which is selected and highlighted in blue), and 'Destination'. Below the 'Destination' tab is a link 'Show advanced settings'. The main content area is titled 'Schedule' and contains the text 'Run scheduled backup for this backup set' followed by a toggle switch labeled 'On' which is currently turned on. Below this, it says 'Existing schedules' and lists one schedule: 'Backup Schedule' with a calendar icon and the text 'Daily (Everyday at 20:00)'. There is an 'Add' button below the list. At the bottom of the window, there is a blue bar with the text 'Delete this backup set' on the left and three buttons: 'Save', 'Cancel', and 'Help' on the right.

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

This screenshot is identical to the one above, showing the 'Backup Schedule' tab for 'Sample Backup Set 01'. It displays the 'Schedule' section with the 'On' toggle switch and the existing 'Backup Schedule' (Daily at 20:00). The interface includes the same sidebar, main content area, and bottom bar with 'Delete this backup set' text and 'Save', 'Cancel', and 'Help' buttons.

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

The screenshot shows a 'Backup Schedule' window with the following fields and options:

- Name:** A text box containing 'Backup Schedule'.
- Type:** A dropdown menu set to 'Daily'.
- Start backup at:** Time selection fields showing '20' and ': 00'.
- Stop:** A dropdown menu set to 'until full backup completed'.
- Run Retention Policy after backup:** A checked checkbox.

At the bottom, there are two blue bars with buttons:

- The top bar contains the text 'Delete this backup schedule' and buttons 'OK', 'Cancel', and 'Help'.
- The bottom bar contains the text 'Delete this backup set' and buttons 'Save', 'Cancel', and 'Help'.

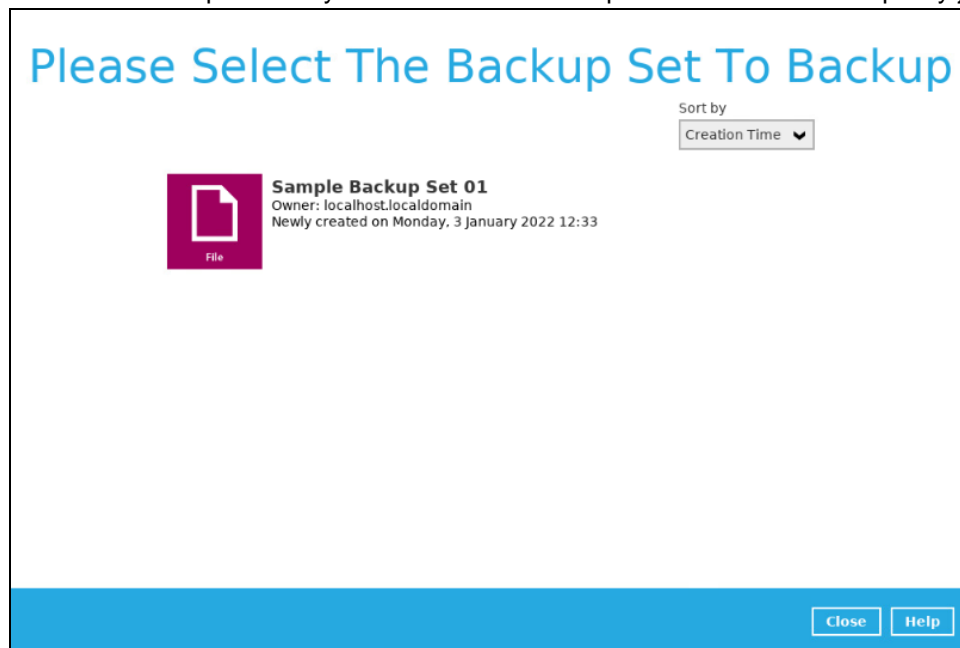
Manual Backup

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

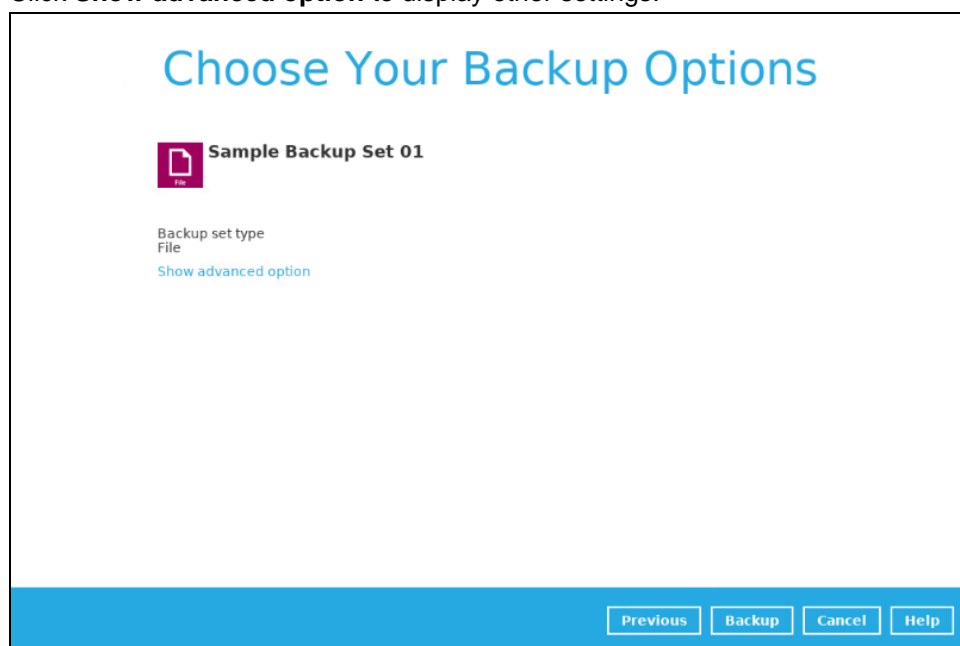
1. Click the **Backup** icon in the AhsayOBM main interface.



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.

Choose Your Backup Options

 **Sample Backup Set 01**

Backup set type
File

Destinations

☒  AhsayCBS (Host: 10.3.121.17:80)

Migrate Data

☐ Migrate existing data to latest version

Retention Policy

☒ Run Retention Policy after backup

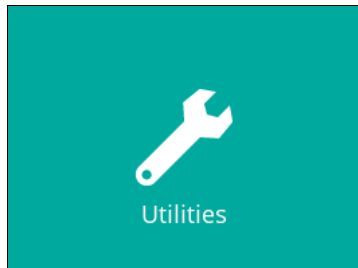
[Hide advanced option](#)

PreviousBackupCancelHelp

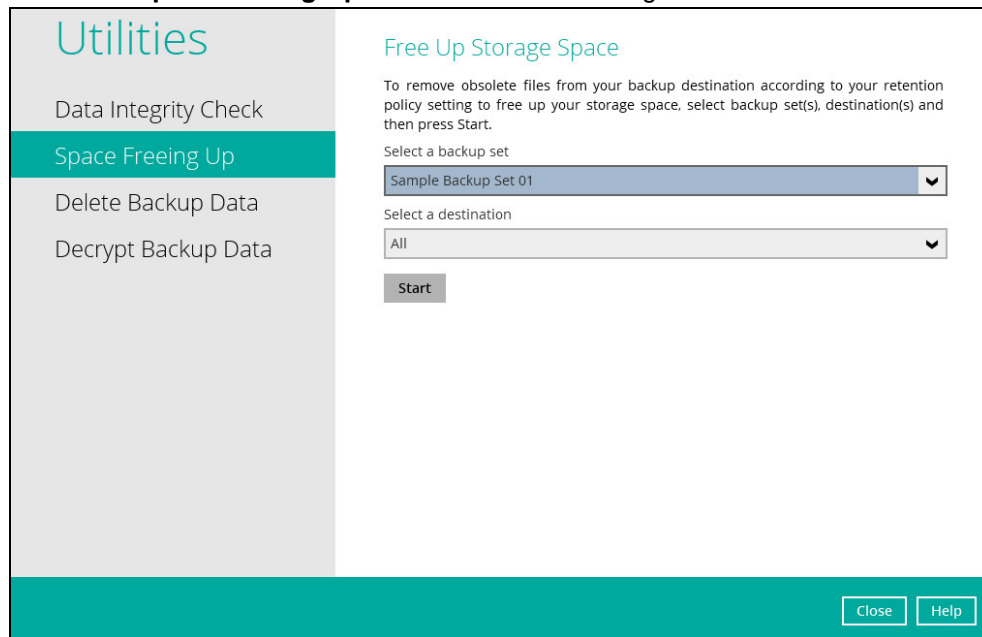
Space Freeing Up

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.



The screenshot shows the 'Utilities' settings window. On the left is a sidebar with the title 'Utilities' and four options: 'Data Integrity Check', 'Space Freeing Up' (which is highlighted with a teal background), 'Delete Backup Data', and 'Decrypt Backup Data'. The main area on the right is titled 'Free Up Storage Space' and contains the following text: 'To remove obsolete files from your backup destination according to your retention policy setting to free up your storage space, select backup set(s), destination(s) and then press Start.' Below this text are two dropdown menus: 'Select a backup set' with 'Sample Backup Set 01' selected, and 'Select a destination' with 'All' selected. A 'Start' button is located below the destination dropdown. At the bottom right of the window are 'Close' and 'Help' buttons.

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.

Utilities

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

Free Up Storage Space

To remove obsolete files from your backup destination according to your retention policy setting to free up your storage space, select backup set(s), destination(s) and then press Start.

Select a backup set

Sample Backup Set 01

Select a destination

All

All

AhsayCBS

Local-1 (/root/tmp)

GoogleDrive-1 (Ahsay)

Close Help

4. Click the **Start** button to run the retention policy job.

Utilities

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

Free Up Storage Space

To remove obsolete files from your backup destination according to your retention policy setting to free up your storage space, select backup set(s), destination(s) and then press Start.

Select a backup set

Sample Backup Set 01

Select a destination

AhsayCBS

Start

Close Help

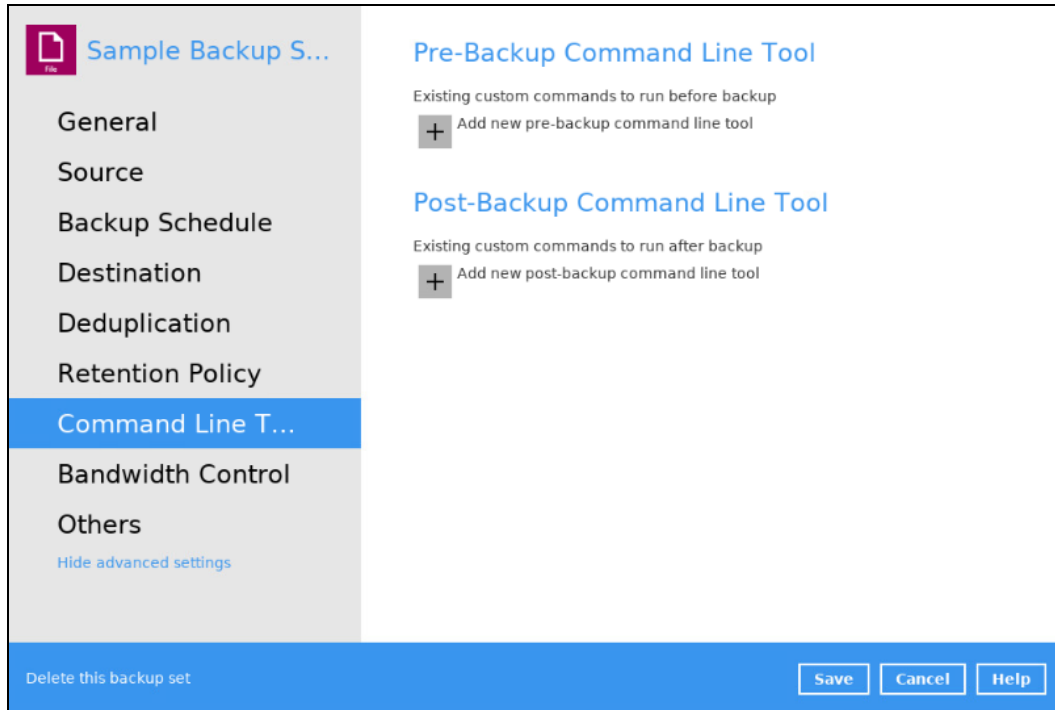
NOTE

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.

User Profile
Backup Set
Settings
Report
Statistics
Effective Policy

BackupRestore

Backup Report for This User

ViewToday

Backup Set	Destination	Start Time	End Time	Status
Sample Backup Set 01(1569312781514)	AhsayCBS	25-Sep-2019 11:12	--	Backup not yet finished
Sample Backup Set 01(1569312781514)	AhsayCBS	25-Sep-2019 11:21	25-Sep-2019 11:21	Warn

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.

New Post-Backup Command Line Tool

Name

Working Directory

Command

[Change](#)

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:

Show All		
Type	Log	Time
	Total New Links = 0	25/09/2019 11:22:05
	Total Updated Files = 0	25/09/2019 11:22:05
	Total Attributes Changed Files = 0	25/09/2019 11:22:05
	Total Deleted Files = 0	25/09/2019 11:22:05
	Total Deleted Directories = 0	25/09/2019 11:22:05
	Total Deleted Links = 0	25/09/2019 11:22:05
	Total Moved Files = 0	25/09/2019 11:22:05
	Start running retention policy on backup set "Sample Backup Set 01(1569312781514)", "AhsayCBS(1569312804851)"	25/09/2019 11:22:05
	Start processing space freeing up on backup set= "Sample Backup Set 01 (1569312781514)" destination= "AhsayCBS (1569..."	25/09/2019 11:22:05
	Space freeing up on backup set= "Sample Backup Set 01 (1569312781514)" destination= "AhsayCBS (1569312804851)" is c...	25/09/2019 11:22:05
	Finished running retention policy on backup set "Sample Backup Set 01(1569312781514)", "AhsayCBS(1569312804851)"	25/09/2019 11:22:05
	Saving encrypted backup file index to 1569312781514/blocks at destination AhsayCBS...	25/09/2019 11:22:06
	Saving encrypted backup file index to 1569312781514/blocks/2019-09-25-11-21-41 at destination AhsayCBS...	25/09/2019 11:22:06
	Start running post-commands	25/09/2019 11:22:06
	[Post-Backup-1] shutdown +5	25/09/2019 11:22:06
	[Post-Backup-1] Shutdown scheduled for Wed 2019-09-25 11:27:06 HKT, use 'shutdown -c' to cancel.	25/09/2019 11:22:07
	Finished running post-commands	25/09/2019 11:22:07
	Deleting temporary file /root/temp/1569312781514/OBS@1569312804851	25/09/2019 11:22:10
	Backup completed with warning(s)	25/09/2019 11:22:10

Logs per page 50
Page 1 / 1

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.

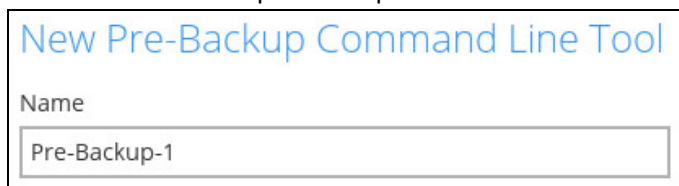


Pre-Backup Command Line Tool

Existing custom commands to run before backup

 Add new pre-backup command line tool

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

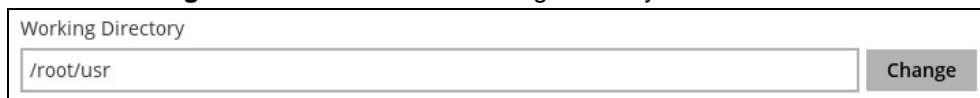


New Pre-Backup Command Line Tool


Name

Pre-Backup-1

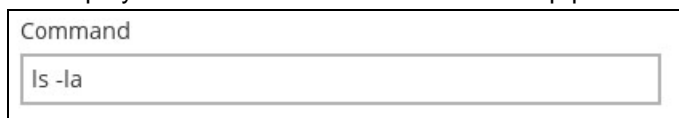
3. Click the **Change** button to locate the working directory of the command.



Working Directory

/root/usr 


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.

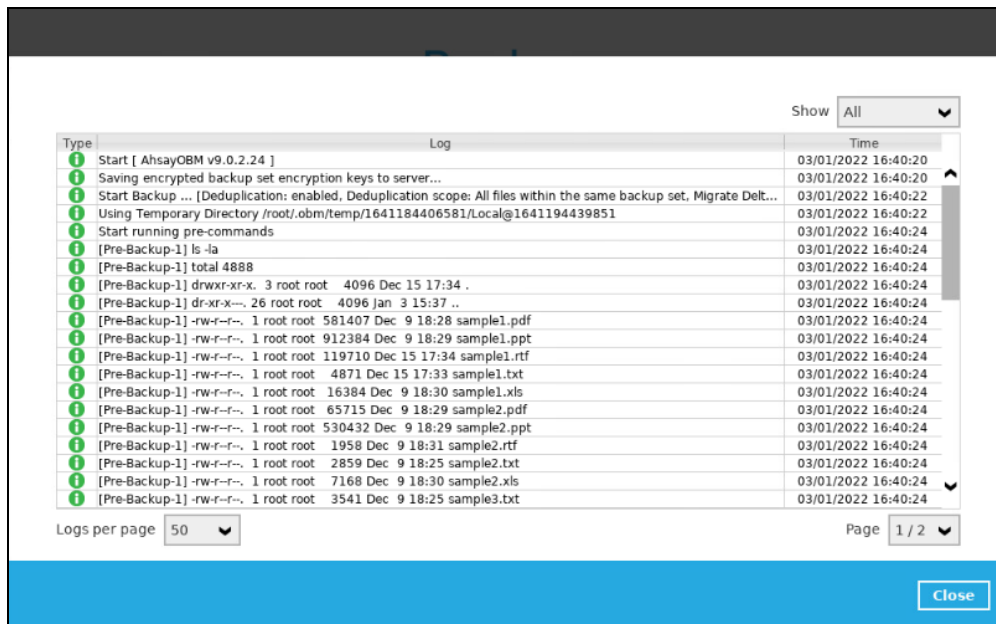


Command

ls -la

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.



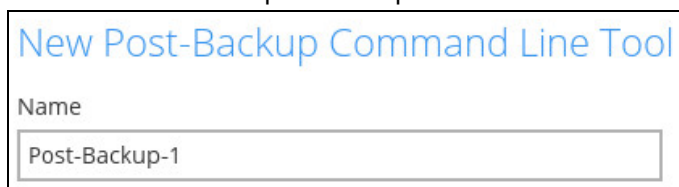
Post-backup Command

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:

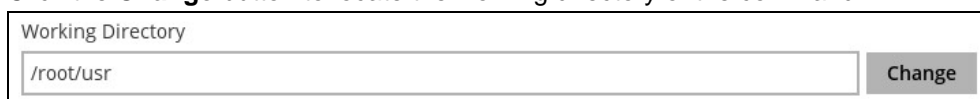
1. Click the **Add** button.



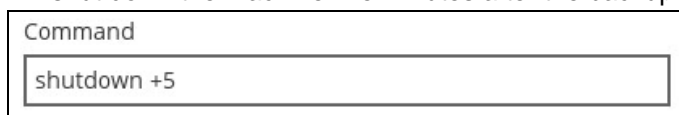
2. Enter a name for the post-backup command.




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.

Type	Log	Time
	Start running retention policy on backup set "Sample Backup Set 01(1641184406581)", "Local-1(1641194439851)"	03/01/2022 16:40:27
	Start processing space freeing up on backup set= "Sample Backup Set 01 (1641184406581)" destination= "Local-1 (1641194439851)"	03/01/2022 16:40:27
	Space freeing up on backup set= "Sample Backup Set 01 (1641184406581)" destination= "Local-1 (1641194439851)"	03/01/2022 16:40:27
	Finished running retention policy on backup set "Sample Backup Set 01(1641184406581)", "Local-1(1641194439851)"	03/01/2022 16:40:27
	Saving server information to destination.	03/01/2022 16:40:27
	Saving encrypted backup file index to 1641184406581/blocks/2022-01-03-16-40-04 at destination Local-1...	03/01/2022 16:40:28
	Start running post-commands	03/01/2022 16:40:28
	[Post-Backup-1] ls -la	03/01/2022 16:40:28
	[Post-Backup-1] total 4	03/01/2022 16:40:28
	[Post-Backup-1] drwxr-xr-x. 4 root root 43 Jan 3 16:40 .	03/01/2022 16:40:28
	[Post-Backup-1] dr-xr-x--. 26 root root 4096 Jan 3 15:37 ..	03/01/2022 16:40:28
	[Post-Backup-1] drwxr-xr-x. 4 root root 61 Jan 3 15:34 1641184406581	03/01/2022 16:40:28
	[Post-Backup-1] drwxr-xr-x. 2 root root 6 Jan 3 15:20 settings	03/01/2022 16:40:28
	Finished running post-commands	03/01/2022 16:40:28
	Deleting temporary file /root/.obm/temp/1641184406581/Local@1641194439851	03/01/2022 16:40:31
	Backup Completed Successfully	03/01/2022 16:40:32

Logs per page 50 Page 2 / 2

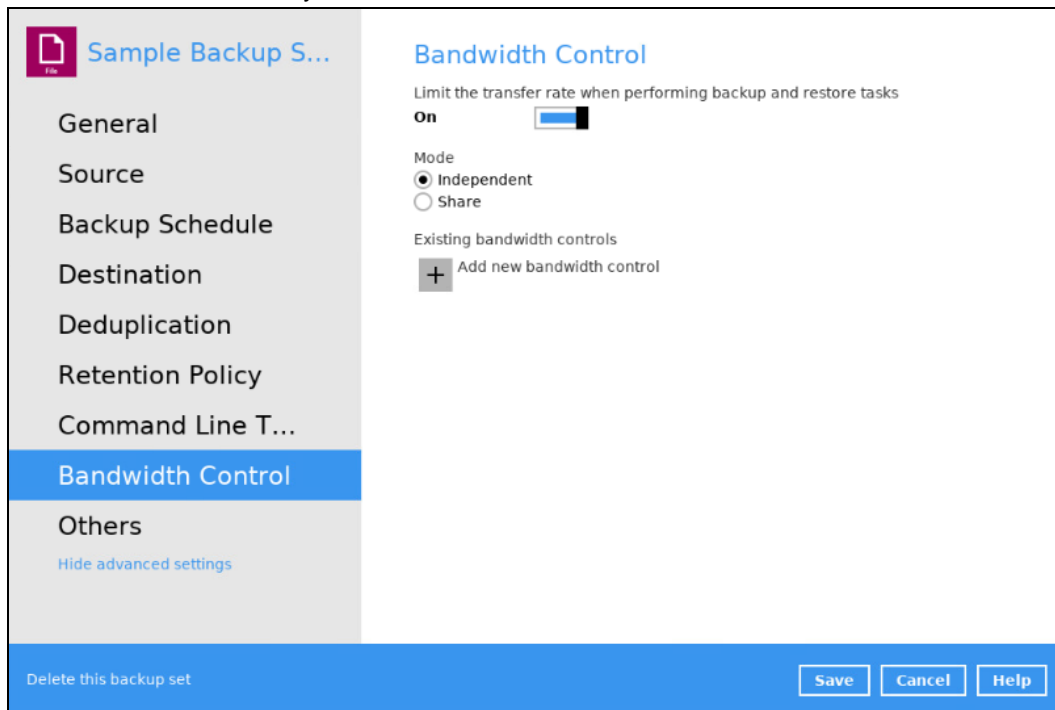
Close

NOTE

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

Bandwidth Control

This 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:

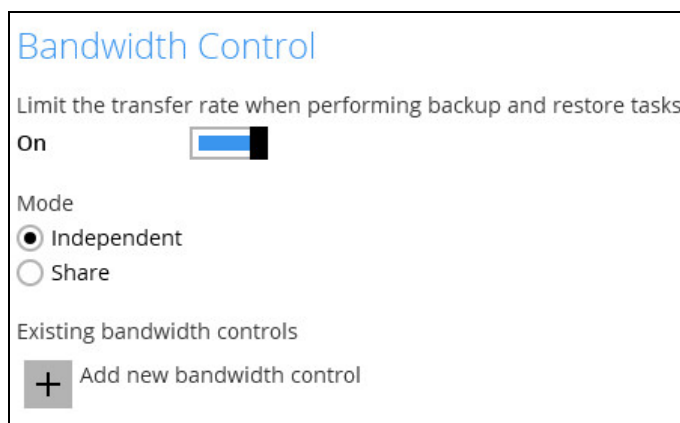
Bandwidth Control Type	Description
Independent	Each backup and restore has its assigned bandwidth.
Share	All backup and restore operations are sharing the same assigned bandwidth.

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.


Mode

☒ Independent

☐ Share

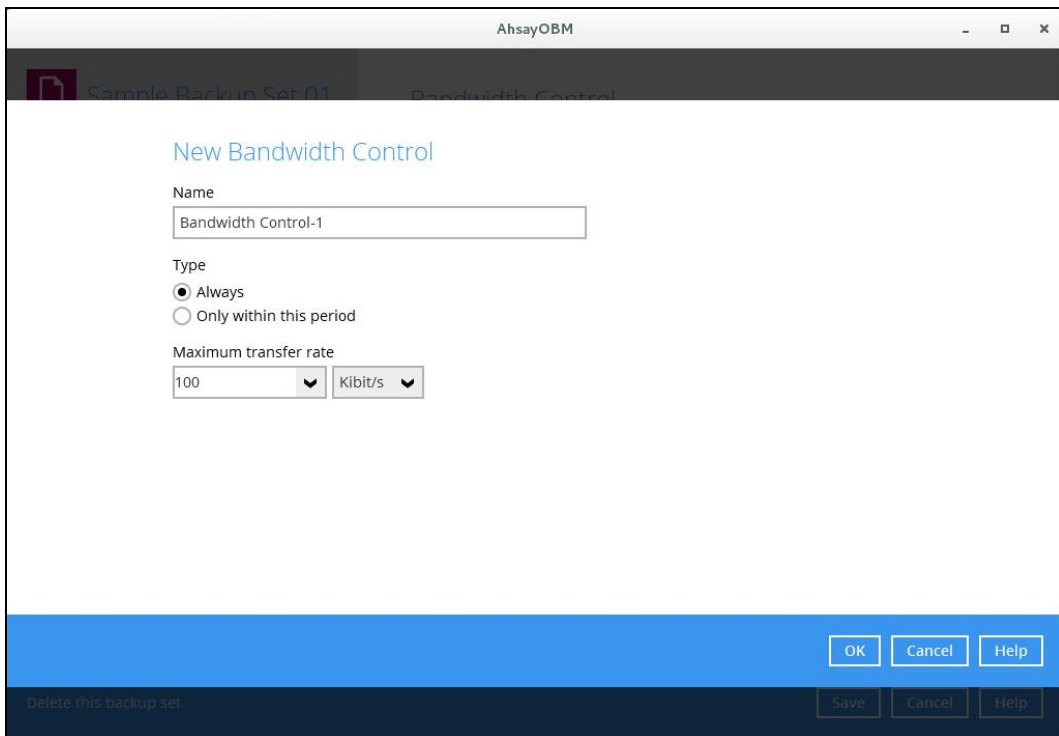
3. If you want to add a modified bandwidth control, click the **Add** button.

Existing bandwidth controls

 Add new bandwidth control

4. Complete the following fields:

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



AhsayOBM

Sample Backup Set 01 Bandwidth Control

New Bandwidth Control

Name

Bandwidth Control-1

Type

☒ Always

☐ Only within this period

Maximum transfer rate

100 Kibit/s

OK Cancel Help

Delete this backup set Save Cancel Help

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](#)
- [Recycle Bin](#)

The screenshot shows a settings window titled "Sample Backup S...". On the left is a sidebar with a list of settings categories: General, Source, Backup Schedule, Destination, Deduplication, Retention Policy, Command Line T..., Bandwidth Control, and Others. The "Others" category is selected and highlighted in blue. Below the sidebar, there is a link that says "Hide advanced settings". The main area of the window displays the settings for the "Others" category. It includes sections for "Temporary Directory", "Follow Link", "File Permissions", "OpenDirect", and "Compressions". The "Temporary Directory" section shows a text input field with "/root/temp" and a "Change" button. Below it, a status message reads "35.71GB free out of total 49.98GB space in /root/temp", and a checkbox labeled "Remove temporary files after backup" is checked. The "Follow Link" section has a label "Follow link of the backup files" and a toggle switch set to "On". The "File Permissions" section has a label "Backup files' permissions" and a toggle switch set to "On". The "OpenDirect" section has a label "Support of opening backup data directly without restoration" and a toggle switch set to "Off". The "Compressions" section has a label "Select compression type". At the bottom of the window, there is a blue bar with the text "Delete this backup set" on the left and three buttons: "Save", "Cancel", and "Help" on the right.

Sample Backup S...

General

Source

Backup Schedule

Destination

Deduplication

Retention Policy

Command Line T...

Bandwidth Control

Others

[Hide advanced settings](#)

Temporary Directory

Temporary directory for storing backup files

/root/temp [Change](#)

35.71GB free out of total 49.98GB space in /root/temp

☒ Remove temporary files after backup

Follow Link

Follow link of the backup files

On ☒

File Permissions

Backup files' permissions

On ☒

OpenDirect

Support of opening backup data directly without restoration

Off ☐

Compressions

Select compression type

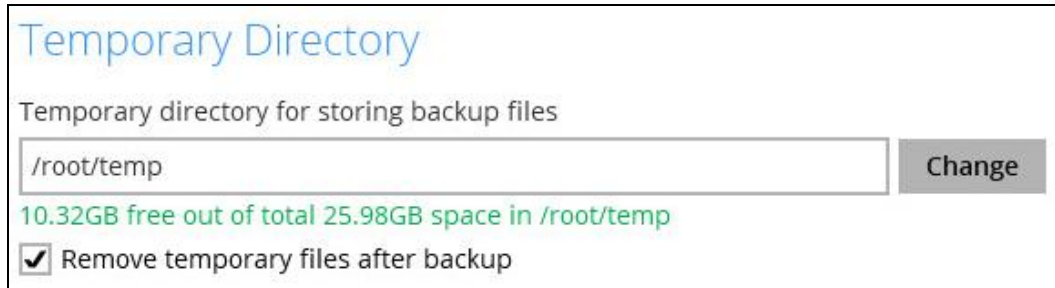
Delete this backup set

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

Temporary Directory

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

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



The screenshot shows a web interface titled "Temporary Directory". Below the title is the text "Temporary directory for storing backup files". There is a text input field containing the path "/root/temp" and a "Change" button to its right. Below the input field, a green status message reads "10.32GB free out of total 25.98GB space in /root/temp". At the bottom, there is a checkbox labeled "Remove temporary files after backup" which is currently checked.

- 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:

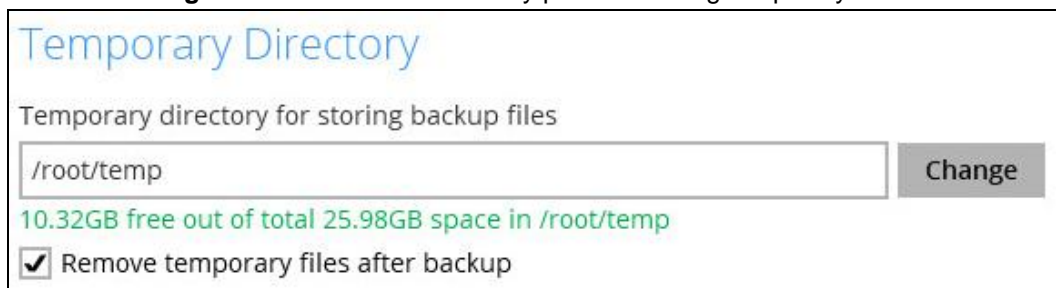
- Full and Incremental/Differential delta files retrieved from the backup destination.
- Merging of the Full and Incremental/Differential delta files as part of the restore process.

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.



This screenshot is identical to the one above, showing the "Temporary Directory" settings. The "Change" button next to the "/root/temp" input field is highlighted with a grey background, indicating it is the button to be clicked to change the directory.

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.



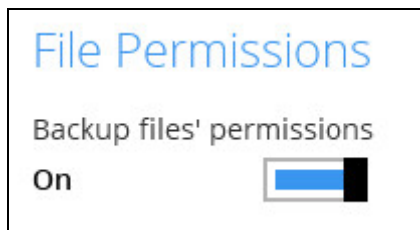
1. Slide the lever to the right to turn on the Follow Link option. Otherwise, slide to the left to turn it off.
2. Click the **Save** button to save the settings.

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.



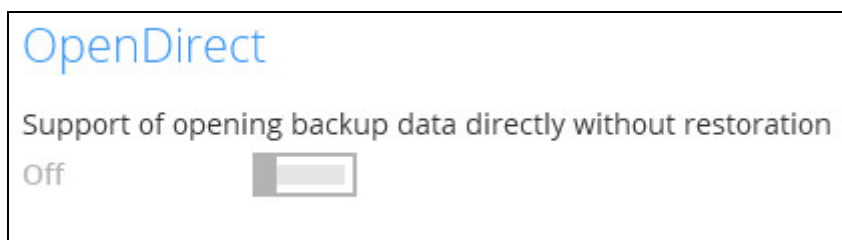
1. Slide the lever to the right to turn on the File Permissions option. Otherwise, slide to the left to turn it off.
2. Click the **Save** button to save the settings.

NOTE

Applicable for File Backup Sets only

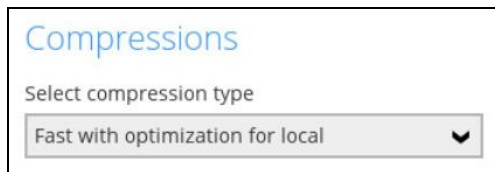
OpenDirect

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 compress all files before it is backed up to the backup destination(s). Newly created backup sets are configured to use Fast with optimization for local by default.



There are four (4) different data compression types:

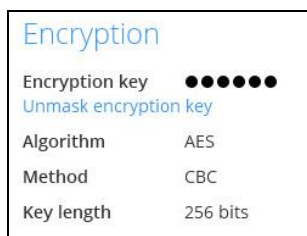
- **No Compression** – file will not be compressed before backup.
- **Normal** – compression is comparable to gzip Normal compression ratio.
- **Fast (Compressed size larger than normal)** – compression will be faster but with less compression and lower CPU usage compared to Normal.
- **Fast with optimization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

NOTE

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

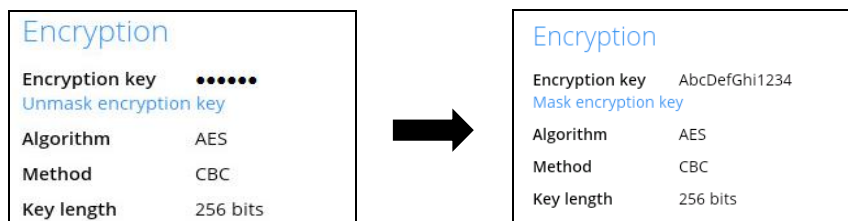
Encryption

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](#).

Recycle Bin

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

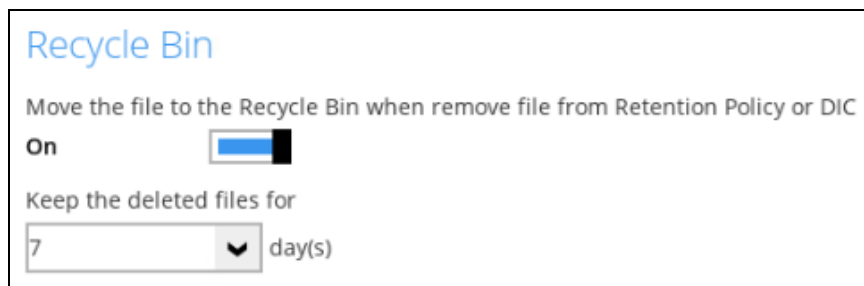
This is how the Recycle Bin will treat deleted data:

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

WARNING

When reverting index, new data will be lost.

This is enabled by default set with 7 days.

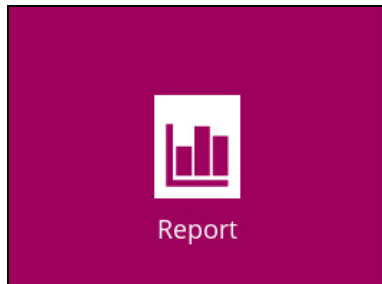


To set the number of days, follow the steps below:

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

9.6 Report

This feature allows 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

Report

- Backup**
- Restore
- Usage

Backup Report

From To

Backup set	Destination	Completion	Status
BackupSet-1	AhsayCBS	Today 15:40	Warning
Sample Back...	AhsayCBS	Today 15:37	Interrupted
Sample Back...	Local-1	Today 15:34	Completed

No. of records per page Page

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

Report

- Backup
- Restore
- Usage

Backup Report

From

27 ▼

Dec ▼

2021 ▼







To

03 ▼

Jan ▼

2022 ▼

Go

Backup set ▼	Destination ▼	Completion	Status ▼
 BackupSet-1	 AhsayCBS	Today 15:40	Warning
 Sample Back...	 AhsayCBS	Today 15:37	Interrupted
 Sample Back...	 Local-1	Today 15:34	Completed

No. of records per page 50 ▼

Page 1 / 1 ▼

Close

Help

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

Report

- Backup
- Restore
- Usage

Backup Report

From

27 ▼

Dec ▼

2021 ▼







To

03 ▼

Jan ▼

2022 ▼

Go

Backup set ▼	Destination ▼	Completion	Status ▼
 Backup set	 AhsayCBS	Today 15:40	Warning
 BackupSet-1	 AhsayCBS	Today 15:37	Interrupted
 Sample Backup S	 Local-1	Today 15:34	Completed

No. of records per page 50 ▼

Page 1 / 1 ▼

Close

Help

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

Report

- Backup
- Restore
- Usage

Backup Report

From 27 Dec 2021 To 03 Jan 2022 [Go](#)

Backup set	Destination	Completion	Status
BackupSet-1	Destination	Today 15:40	Warning
Sample Back...	AhsayCBS	Today 15:37	Interrupted
Sample Back...	AhsayCBS	Today 15:34	Completed
	Local-1		

No. of records per page 50 Page 1 / 1

[Close](#) [Help](#)

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

Report

- Backup
- Restore
- Usage

Backup Report

From 27 Dec 2021 To 03 Jan 2022 [Go](#)

Backup set	Destination	Completion	Status
BackupSet-1	AhsayCBS	Today 15:40	Status
Sample Back...	AhsayCBS	Today 15:37	Completed
Sample Back...	Local-1	Today 15:34	Warning
			Interrupted

No. of records per page 50 Page 1 / 1

[Close](#) [Help](#)

To view the backup log, follow the instructions below:

1. Select and click the backup report.

Report

Backup Report

From: 27 Dec 2021 To: 03 Jan 2022 Go

Backup set	Destination	Completion	Status
Sample Back...	AhsayCBS	Today 15:37	Interrupted

Backup set Sample Backup Set 01

Destination Local-1

Job 03/01/2022 15:34

Time Today 15:34 - 15:34 (HKT)

Status Completed successfully

New files * 15 [4.3MB/4.7MB (7%)]

Updated files * 0

Attributes Changed Files * 0

Moved files * 0

Deleted files * 0

Dedupe Saving 0/4.7M [0.0%]

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

View log

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

Close **Help**

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.

Report

Backup Report

Backup set: Sample Backup Set 01 Destination: Local-1

Log: 03/01/2022 15:34 Show: All

Type	Log	Time
i	Start [AhsayOBM v9.0.2.24]	03/01/2022 15:34:31
i	Saving encrypted backup set encryption keys to server...	03/01/2022 15:34:31
i	Start Backup ... [Deduplication: enabled, Deduplication scope: All files within the same backup set. Migrate Delt...	03/01/2022 15:34:33
i	Using Temporary Directory /root/.obm/temp/1641184406581/Local@1641194439851	03/01/2022 15:34:33
i	Start running pre-commands	03/01/2022 15:34:34
i	[Pre-Backup-1] ls -la	03/01/2022 15:34:34
i	[Pre-Backup-1] total 4888	03/01/2022 15:34:34
i	[Pre-Backup-1] drwxr-xr-x. 3 root root 4096 Dec 15 17:34 .	03/01/2022 15:34:34
i	[Pre-Backup-1] dr-xr-x--. 25 root root 4096 Jan 3 15:19 ..	03/01/2022 15:34:34
i	[Pre-Backup-1] -rw-r--r--. 1 root root 581407 Dec 9 18:28 sample1.pdf	03/01/2022 15:34:34
i	[Pre-Backup-1] -rw-r--r--. 1 root root 912384 Dec 9 18:29 sample1.ppt	03/01/2022 15:34:34
i	[Pre-Backup-1] -rw-r--r--. 1 root root 119710 Dec 15 17:34 sample1.rtf	03/01/2022 15:34:34
i	[Pre-Backup-1] -rw-r--r--. 1 root root 4871 Dec 15 17:33 sample1.txt	03/01/2022 15:34:34
i	[Pre-Backup-1] -rw-r--r--. 1 root root 16384 Dec 9 18:30 sample1.xls	03/01/2022 15:34:34
i	[Pre-Backup-1] -rw-r--r--. 1 root root 65715 Dec 9 18:29 sample2.pdf	03/01/2022 15:34:34
i	[Pre-Backup-1] -rw-r--r--. 1 root root 530432 Dec 9 18:29 sample2.ppt	03/01/2022 15:34:34
i	[Pre-Backup-1] -rw-r--r--. 1 root root 1958 Dec 9 18:31 sample2.rtf	03/01/2022 15:34:34
i	[Pre-Backup-1] -rw-r--r--. 1 root root 2859 Dec 9 18:25 sample2.txt	03/01/2022 15:34:34

Logs per page: 50 Page: 1 / 3

Close **Close** **Help**

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

Report

- Backup
- Restore**
- Usage

Restore Report

From

27 ▼

Dec ▼

2021 ▼









To

03 ▼

Jan ▼

2022 ▼

Go

Backup set ▼	Destination ▼	Job	Status ▼
 Sample Back...	 Local-1	Today 16:26	Interrupted
 Sample Back...	 Local-1	Today 16:06	Completed
 Sample Back...	 Local-1	Today 16:05	Completed
 BackupSet-1	 AhsayCBS	Today 15:41	Completed

No. of records per page

50 ▼

Page

1 / 1 ▼

Close

Help

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

Report

- Backup
- Restore**
- Usage

Restore Report

From

27 ▼

Dec ▼

2021 ▼









To

03 ▼

Jan ▼

2022 ▼

Go

Backup set ▼	Destination ▼	Job	Status ▼
 Sample Back...	 Local-1	Today 16:26	Interrupted
 Sample Back...	 Local-1	Today 16:06	Completed
 Sample Back...	 Local-1	Today 16:05	Completed
 BackupSet-1	 AhsayCBS	Today 15:41	Completed

No. of records per page 50 ▼

Page 1 / 1 ▼

Close

Help

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

Report

- Backup
- Restore**
- Usage

Restore Report

From

27 ▼

Dec ▼

2021 ▼









To

03 ▼

Jan ▼

2022 ▼

Go

Backup set ▼	Destination ▼	Job	Status ▼
 Backup set	 Local-1	Today 16:26	Interrupted
 Sample Backup S	 Local-1	Today 16:06	Completed
 BackupSet-1	 Local-1	Today 16:05	Completed
 BackupSet-1	 AhsayCBS	Today 15:41	Completed

No. of records per page 50 ▼

Page 1 / 1 ▼

Close

Help

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

Report

- Backup
- Restore**
- Usage

Restore Report

From 27 Dec 2021 To 03 Jan 2022 Go

Backup set	Destination	Job	Status
Sample Back...	Destination	Today 16:26	Interrupted
Sample Back...	Local-1	Today 16:06	Completed
Sample Back...	AhsayCBS	Today 16:05	Completed
BackupSet-1	AhsayCBS	Today 15:41	Completed

No. of records per page 50 Page 1 / 1

CloseHelp

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

Report

- Backup
- Restore**
- Usage

Restore Report

From 27 Dec 2021 To 03 Jan 2022 Go

Backup set	Destination	Job	Status
Sample Back...	Local-1	Today 16:26	Status
Sample Back...	Local-1	Today 16:06	Completed
Sample Back...	Local-1	Today 16:05	Interrupted
BackupSet-1	AhsayCBS	Today 15:41	Completed

No. of records per page 50 Page 1 / 1

CloseHelp

To view the restore log, follow the instructions below:

1. Select and click the restore report.

Report

Backup

Restore

Usage

Restore Report

From: 27 Dec 2021 To: 03 Jan 2022 Go

Backup set	Destination	Job	Status
Sample Back...	Local-1	Today 16:26	Interrupted
Sample Back...	Local-1	Today 16:06	Completed

Backup set Sample Backup Set 01

Destination Local-1

Job 03/01/2022 16:05

Time Today 16:05 - 16:05 (HKT)

Status ✓ Completed successfully

Downloaded files* 15 (4.3MB)

* Unit = No of files (Download size)

[View log](#)

BackupSet-1 AhsayCBS Today 15:41 Completed

No. of records per page 50 Page 1 / 1

[Close](#) [Help](#)

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.

Report

Restore Report

Backup set Sample Backup Set 01

Log 03/01/2022 16:05 Show All

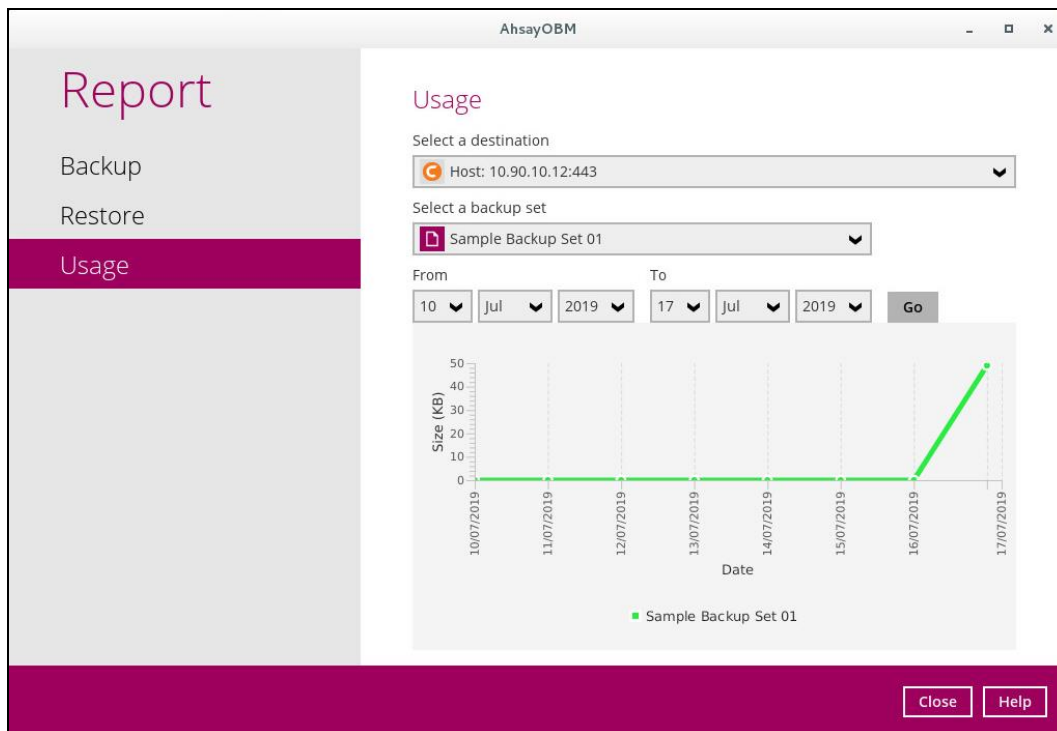
Type	Log	Time
Start	AhsayOBM v9.0.2.24	03/01/2022 16:05:56
Creating new directory...	"/root/restored/root"	03/01/2022 16:05:57
Creating new directory...	"/root/restored/root/Documents"	03/01/2022 16:05:57
Creating new directory...	"/root/restored/root/Documents/testfiles"	03/01/2022 16:05:57
Downloading...	"/root/restored/root/Documents/testfiles/sample1.pdf" (Total 567K bytes)	03/01/2022 16:05:57
Downloading...	"/root/restored/root/Documents/testfiles/sample1.rtf" (Total 102K bytes)	03/01/2022 16:05:57
Downloading...	"/root/restored/root/Documents/testfiles/sample2.xls" (Total 7K bytes)	03/01/2022 16:05:57
Downloading...	"/root/restored/root/Documents/testfiles/sample2.txt" (Total 2K bytes)	03/01/2022 16:05:57
Downloading...	"/root/restored/root/Documents/testfiles/sample3.xls" (Total 13K bytes)	03/01/2022 16:05:58
Downloading...	"/root/restored/root/Documents/testfiles/sample1.txt" (Total 607 bytes)	03/01/2022 16:05:58
Downloading...	"/root/restored/root/Documents/testfiles/sample1.xls" (Total 16K bytes)	03/01/2022 16:05:58
Downloading...	"/root/restored/root/Documents/testfiles/sample2.pdf" (Total 64K bytes)	03/01/2022 16:05:58
Downloading...	"/root/restored/root/Documents/testfiles/sample2.rtf" (Total 1K bytes)	03/01/2022 16:05:58
Downloading...	"/root/restored/root/Documents/testfiles/sample1.ppt" (Total 891K bytes)	03/01/2022 16:05:58
Downloading...	"/root/restored/root/Documents/testfiles/sample_960x540.mkv" (Total 1.26M bytes)	03/01/2022 16:05:58
Downloading...	"/root/restored/root/Documents/testfiles/sample3.txt" (Total 3K bytes)	03/01/2022 16:05:58
Downloading...	"/root/restored/root/Documents/testfiles/sample2.ppt" (Total 518K bytes)	03/01/2022 16:05:58
Downloading...	"/root/restored/root/Documents/testfiles/sample_640x360.avi" (Total 569K bytes)	03/01/2022 16:05:58

Logs per page 50 Page 1 / 1

[Close](#) [Close](#) [Help](#)

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

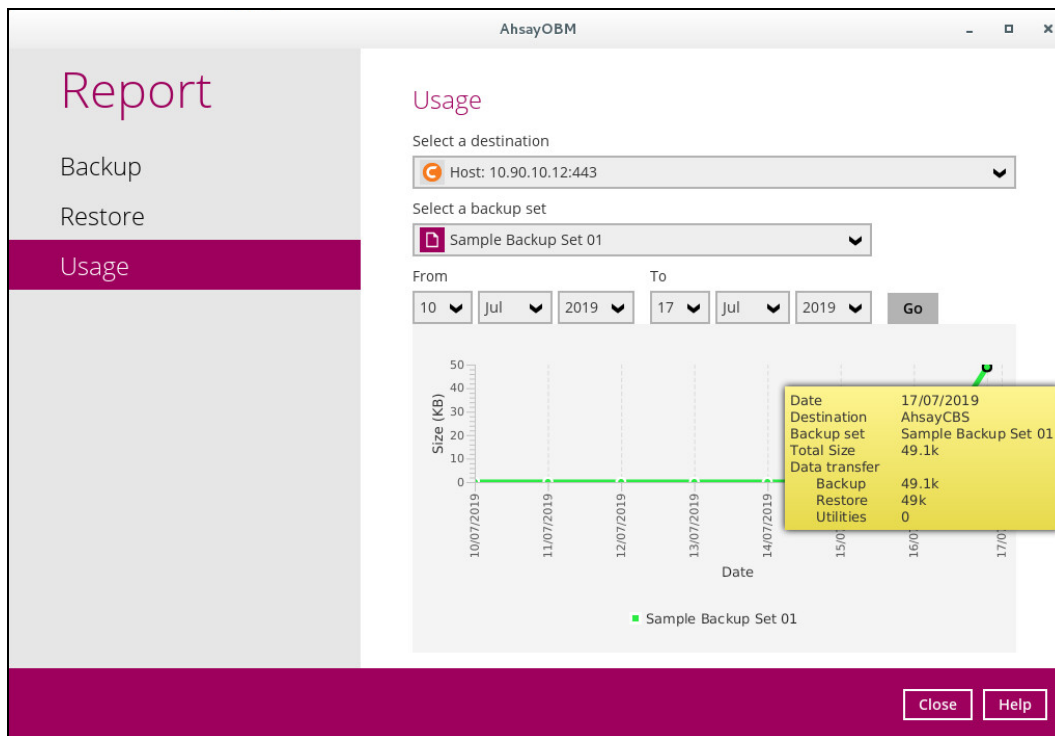
Total Size: displays the total amount of backed up data on the backup destination

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:

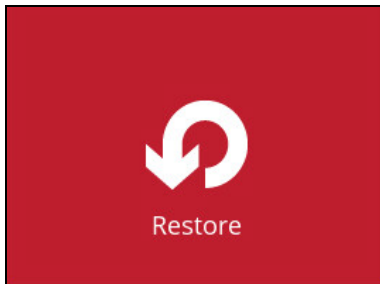
The data transfer statistics will pop up when mouse pointer moves over a specific date.



- 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

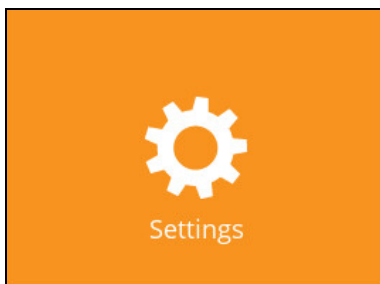
This feature is used to restore backed-up files to its original or alternate location.



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:

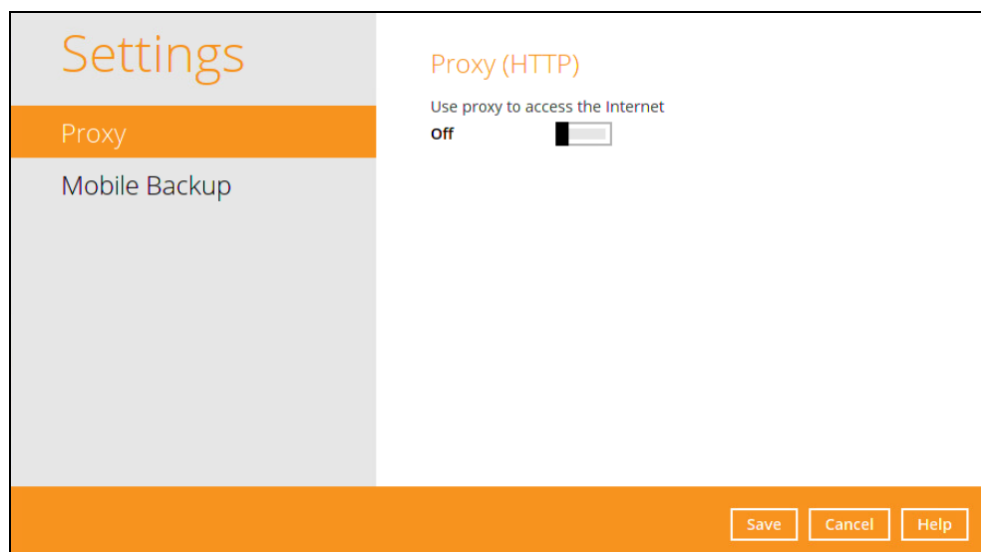
- Proxy
- Mobile Backup

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

Settings

Proxy

Mobile Backup

Proxy (HTTP)

Use proxy to access the Internet

On

IP address

Port

Login ID

Password

Test connection

Save Cancel Help

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

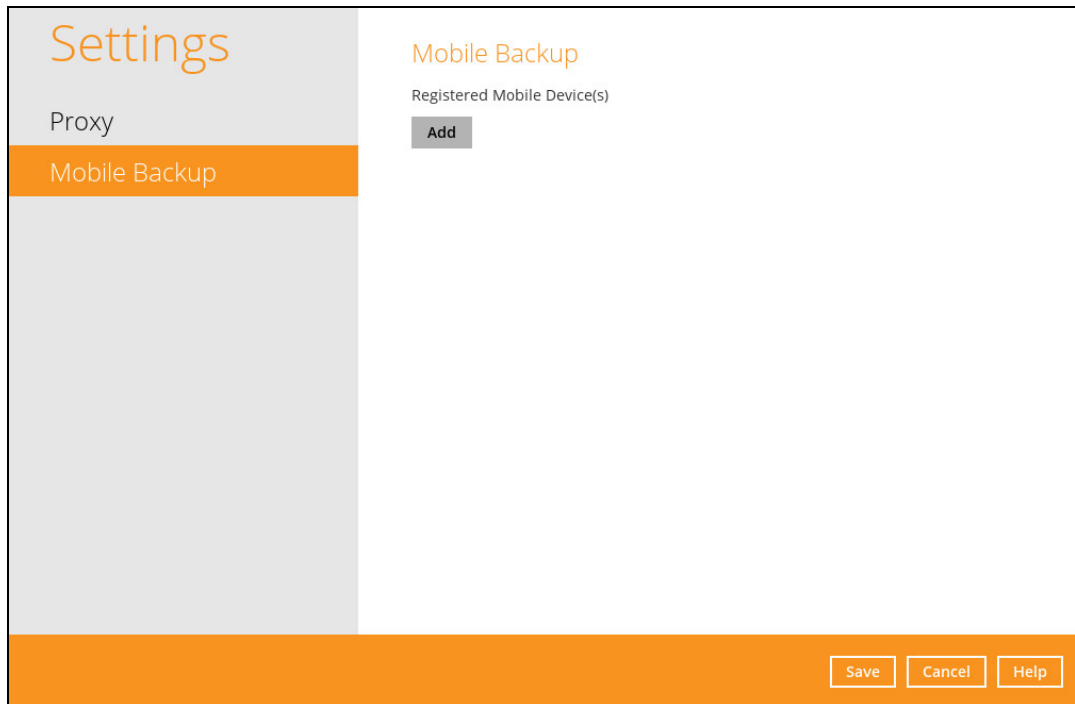
Please refer to the [Ahsay Mobile User Guide for Android and iOS – Chapter 7](#) for the detailed step-by-step procedure.

- [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.

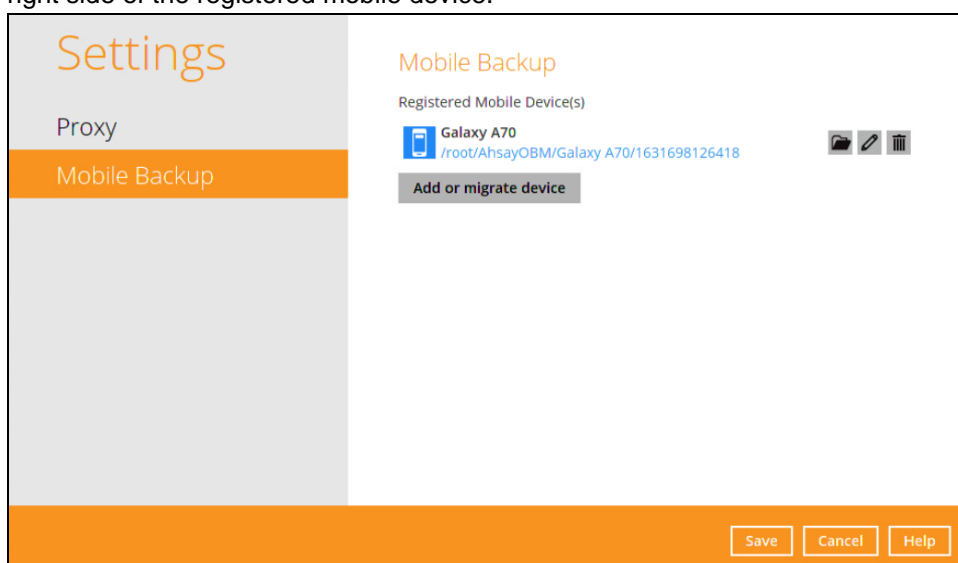
- Restore to a different mobile device on the same operating system.
- Restore to a different mobile device on another operating system, i.e., Android to iOS or iOS to Android.



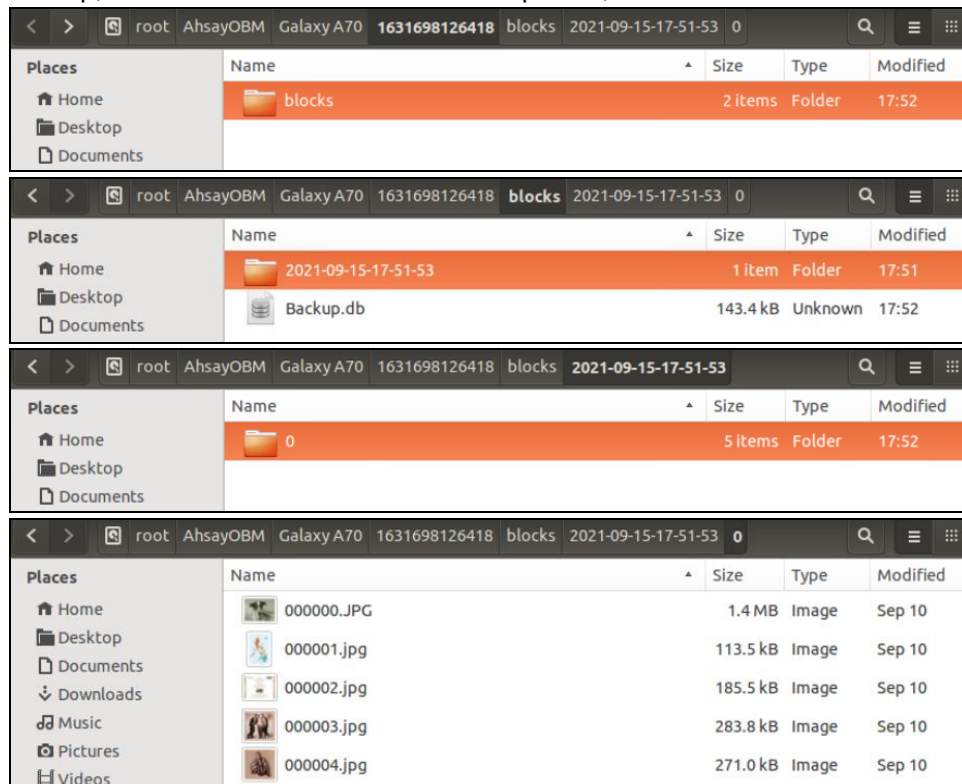
View backed up photos, videos and documents saved in the mobile backup destination

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.

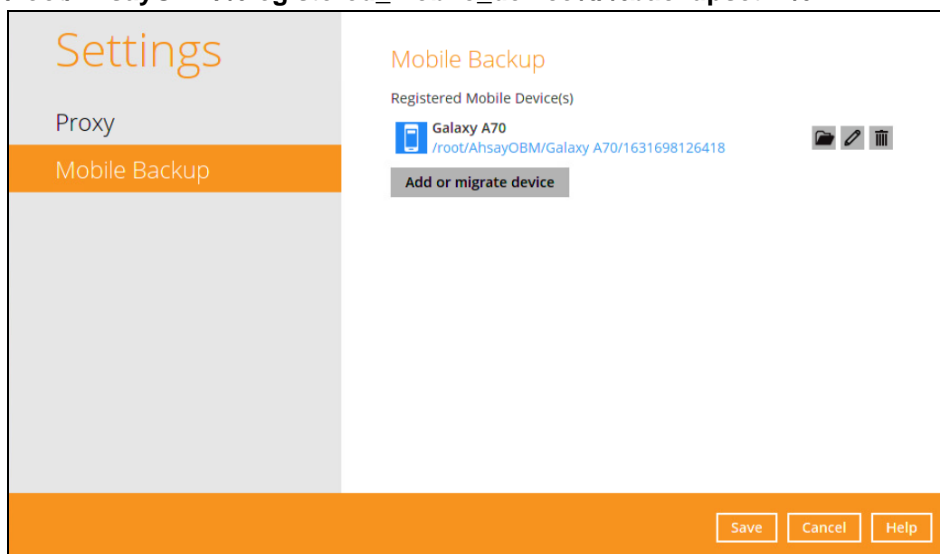
In case the previously backed-up photos, videos, documents and 2FA accounts were not copied to the new location, the backup will re-upload all the photos, videos, documents and 2FA accounts again from the mobile device.

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**

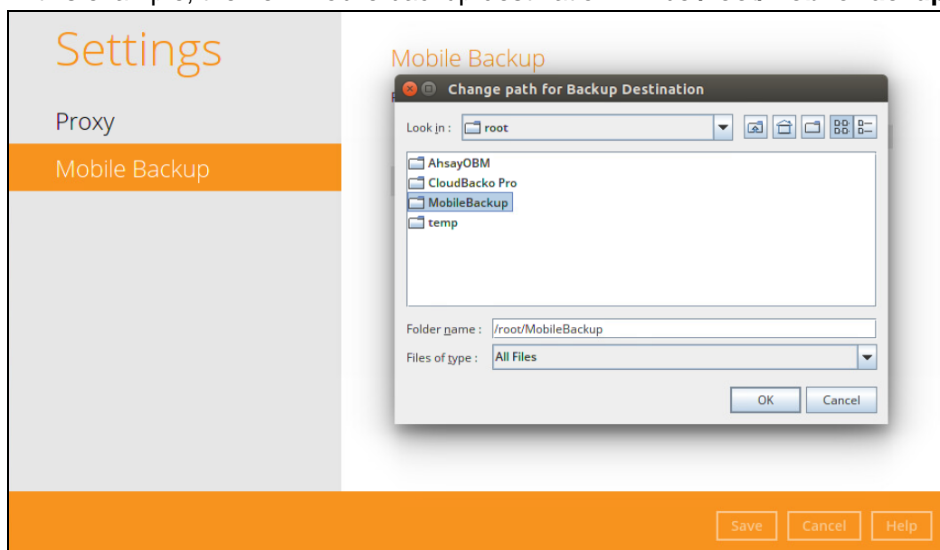
1. From the old location, secure a copy of the previously backed-up photos, videos and 2FA accounts.
2. Copy the previously backed-up photos, videos, documents and 2FA accounts from the original location to the new mobile backup destination (if applicable).
3. Go to **Settings > Mobile Backup**. Click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



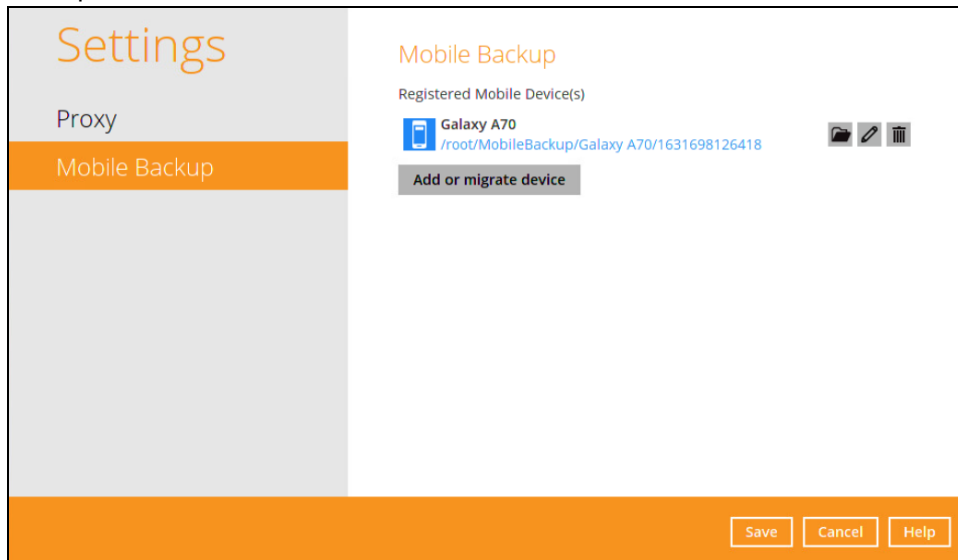
4. **Change path for Backup Destination** screen will be displayed. Select a new mobile backup destination then click **OK**.

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



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

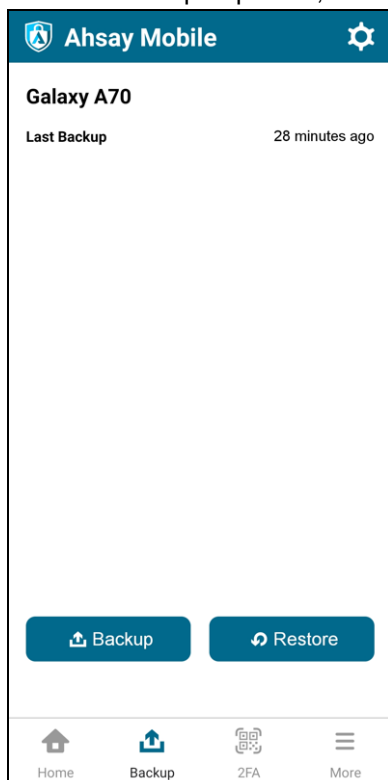
Mobile backup destination is successfully changed to **/root/MobileBackup**. All mobile backups will now be saved in this destination.



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.

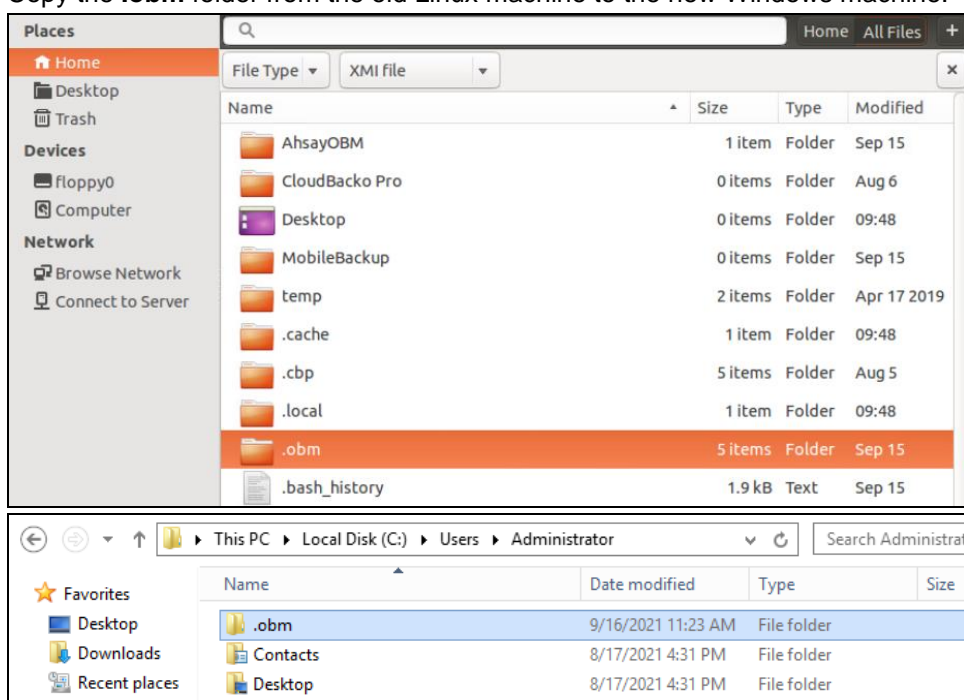
To change the mobile backup destination to a new machine, follow the instructions below:

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.

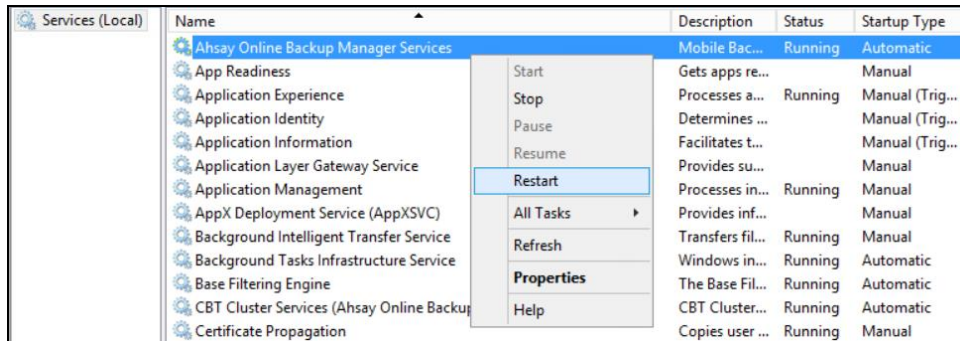


- Copy the previously backed-up photos, videos, documents and 2FA accounts from the original location to the new mobile backup destination.

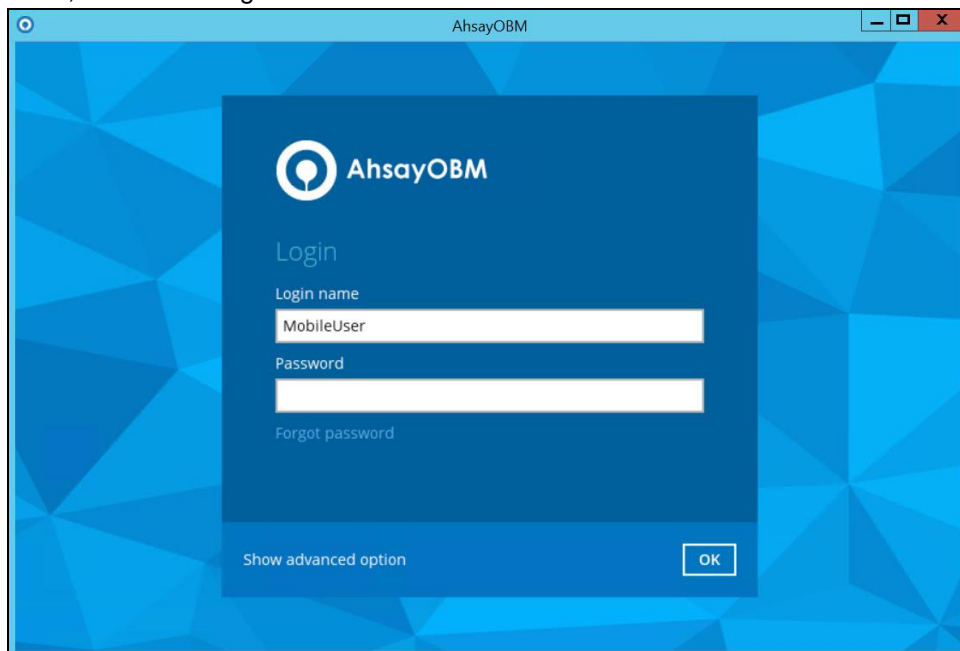
NOTE

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

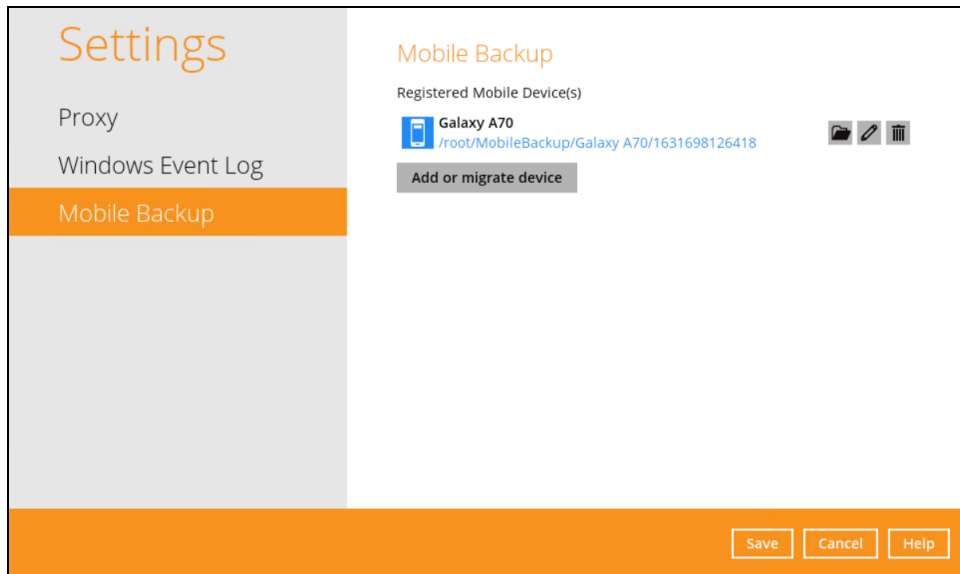
- Restart the **AhsayOBM Services** because copying the **.obm** folder on a newly installed AhsayOBM will not trigger the MBS.



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

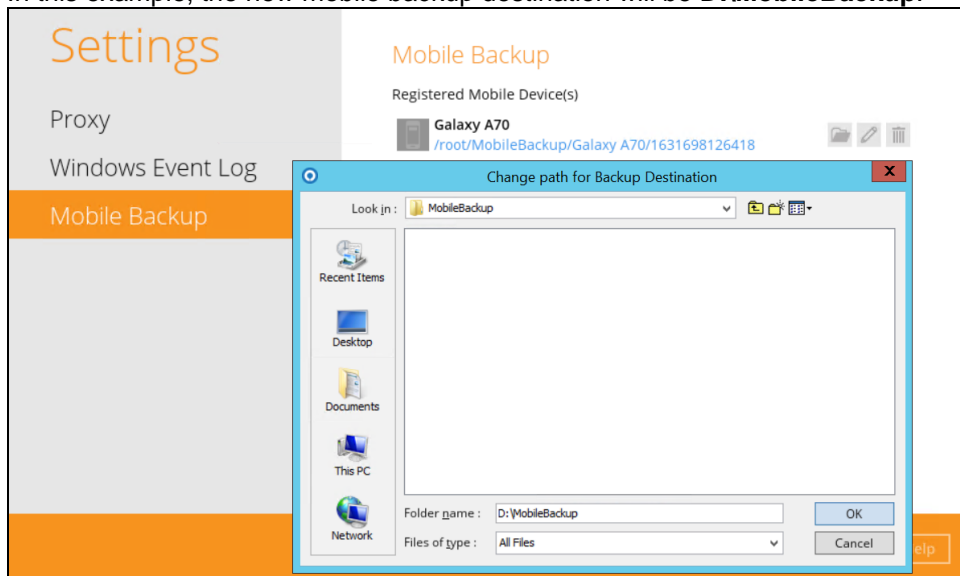


6. Go to **Settings > Mobile Backup**. Click the **Edit** icon on the right side of the registered mobile device.



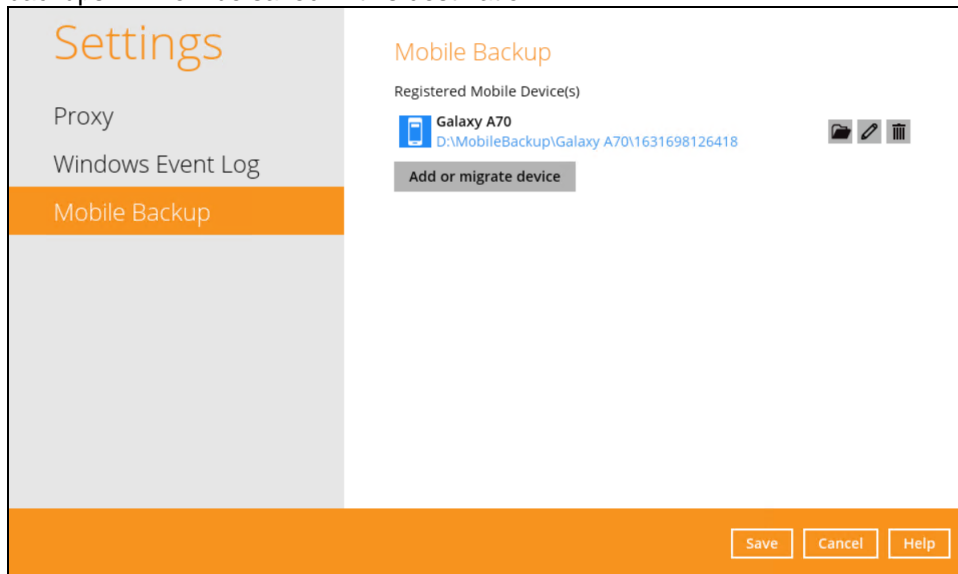
7. **Change path for Backup Destination** screen will be displayed, select the new mobile backup destination then click **OK**.

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



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

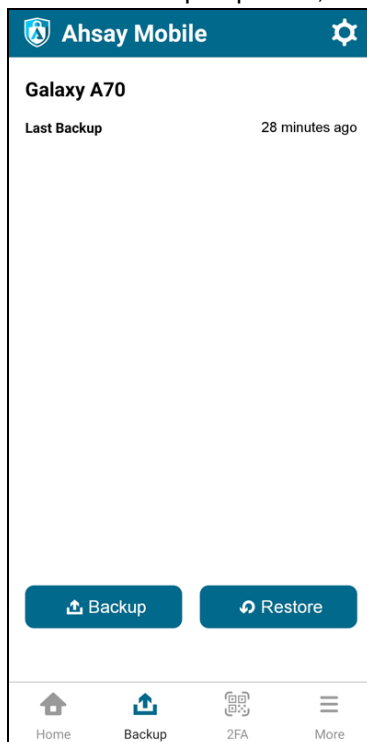
Mobile backup destination is successfully changed to **D:\MobileBackup**. All mobile backups will now be saved in this destination.



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

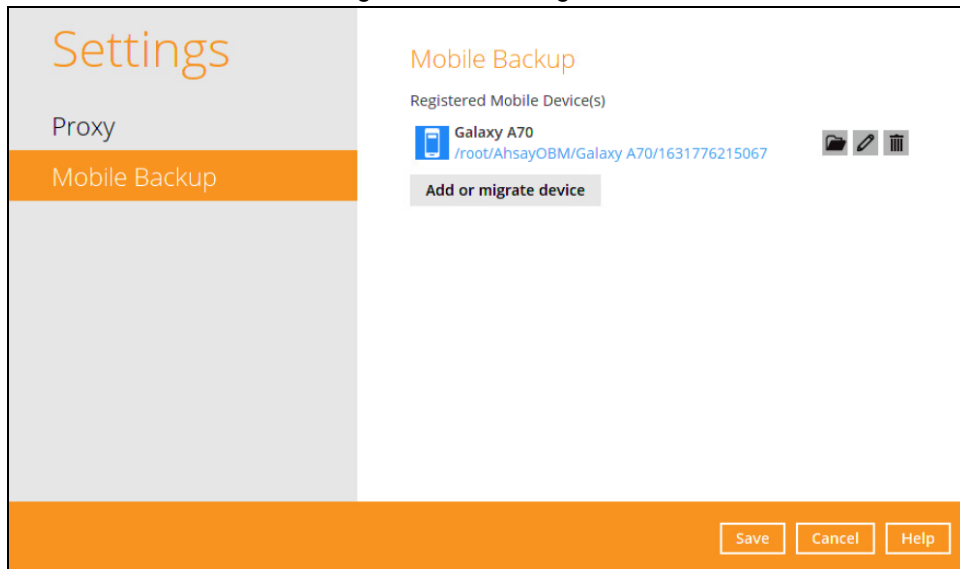
For instructions on changing the mobile backup destination of:

- 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](#).

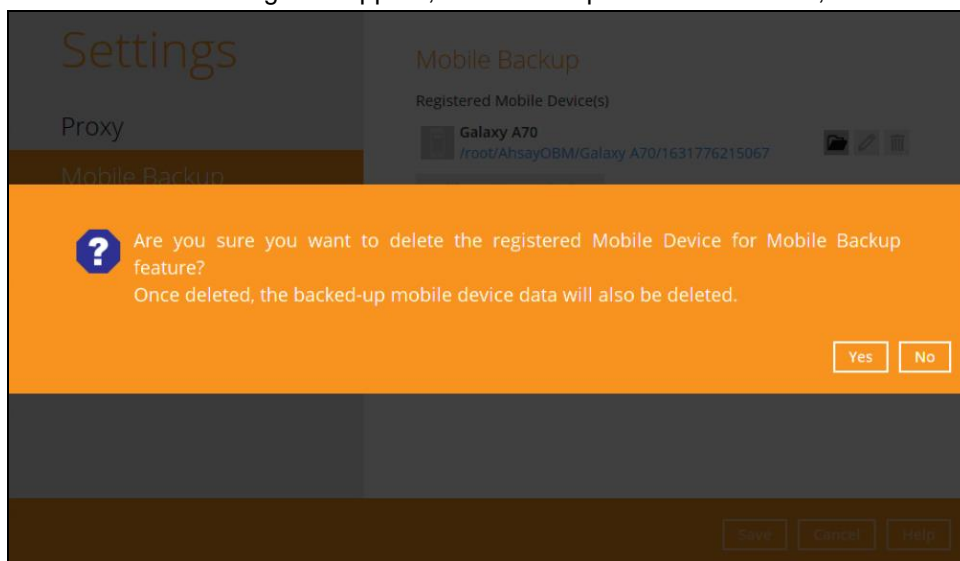
Remove one or more device(s) registered for Mobile Backup

To remove a mobile device, follow the instructions below:

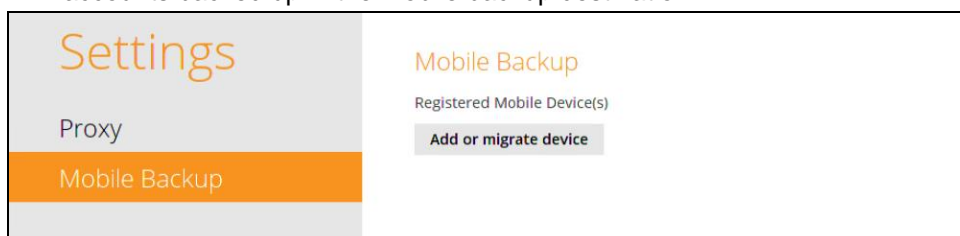
1. Click the **Delete** icon on the right side of the registered mobile device.



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

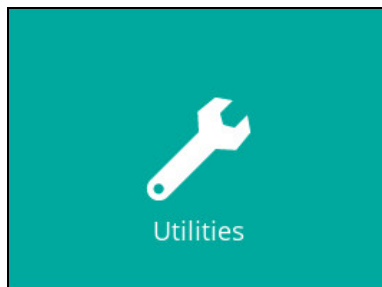


3. Mobile device is successfully removed along with any photos, videos, documents and 2FA accounts backed up in the mobile backup destination.



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.



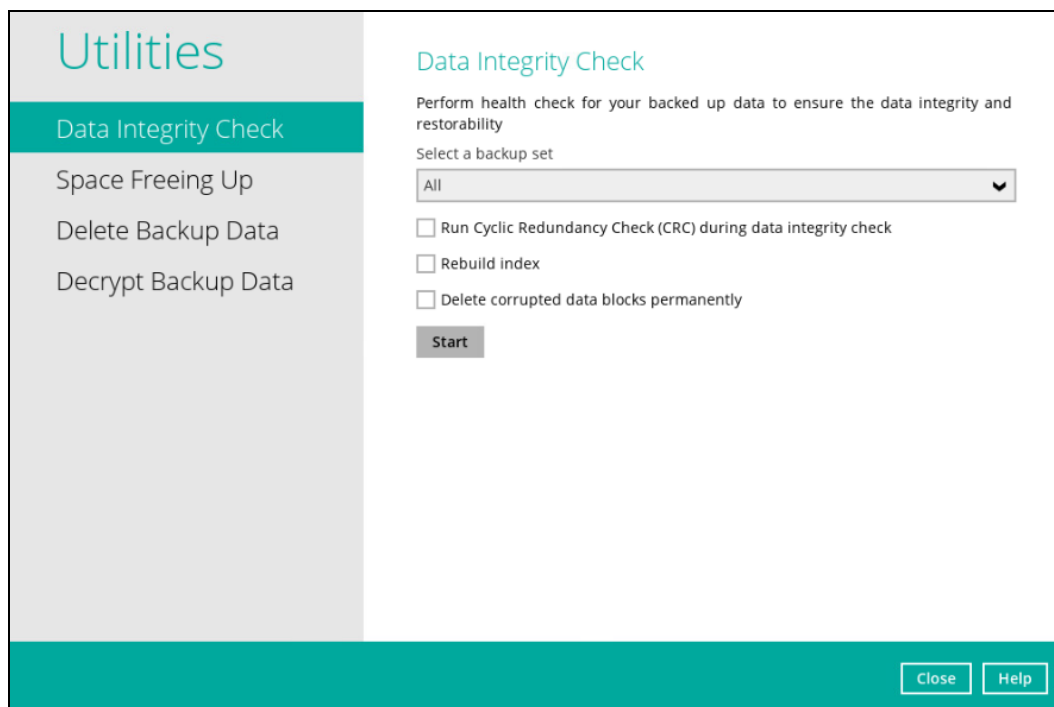
These are the four (4) options available for this feature:

- [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).

A screenshot of the "Data Integrity Check" utility window. The window has a teal header bar with the word "Utilities" in white. Below the header, there is a sidebar with four options: "Data Integrity Check" (highlighted in teal), "Space Freeing Up", "Delete Backup Data", and "Decrypt Backup Data". The main area of the window is titled "Data Integrity Check" and contains the following text: "Perform health check for your backed up data to ensure the data integrity and restorability". Below this, there is a dropdown menu labeled "Select a backup set" with "All" selected. There are three checkboxes: "Run Cyclic Redundancy Check (CRC) during data integrity check", "Rebuild index", and "Delete corrupted data blocks permanently". A "Start" button is located below the checkboxes. At the bottom right of the window, there are "Close" and "Help" buttons.

NOTES

1. Data Integrity Check CANNOT fix or repair files that are already corrupted.
2. Data Integrity Check can only be started if there is NO active backup or restore job(s) running on the backup set selected for the DIC job. As the **backup**, **restore** and **data integrity check** are using the same index for read and write operations. Otherwise, an error message will be displayed in the post-DIC to indicate that the data integrity check is completed with error(s) and had skipped a backup set with an active backup job.

Run Cyclic Redundancy Check (CRC)

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

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

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

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

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

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.

Delete corrupted data blocks permanently

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

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

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

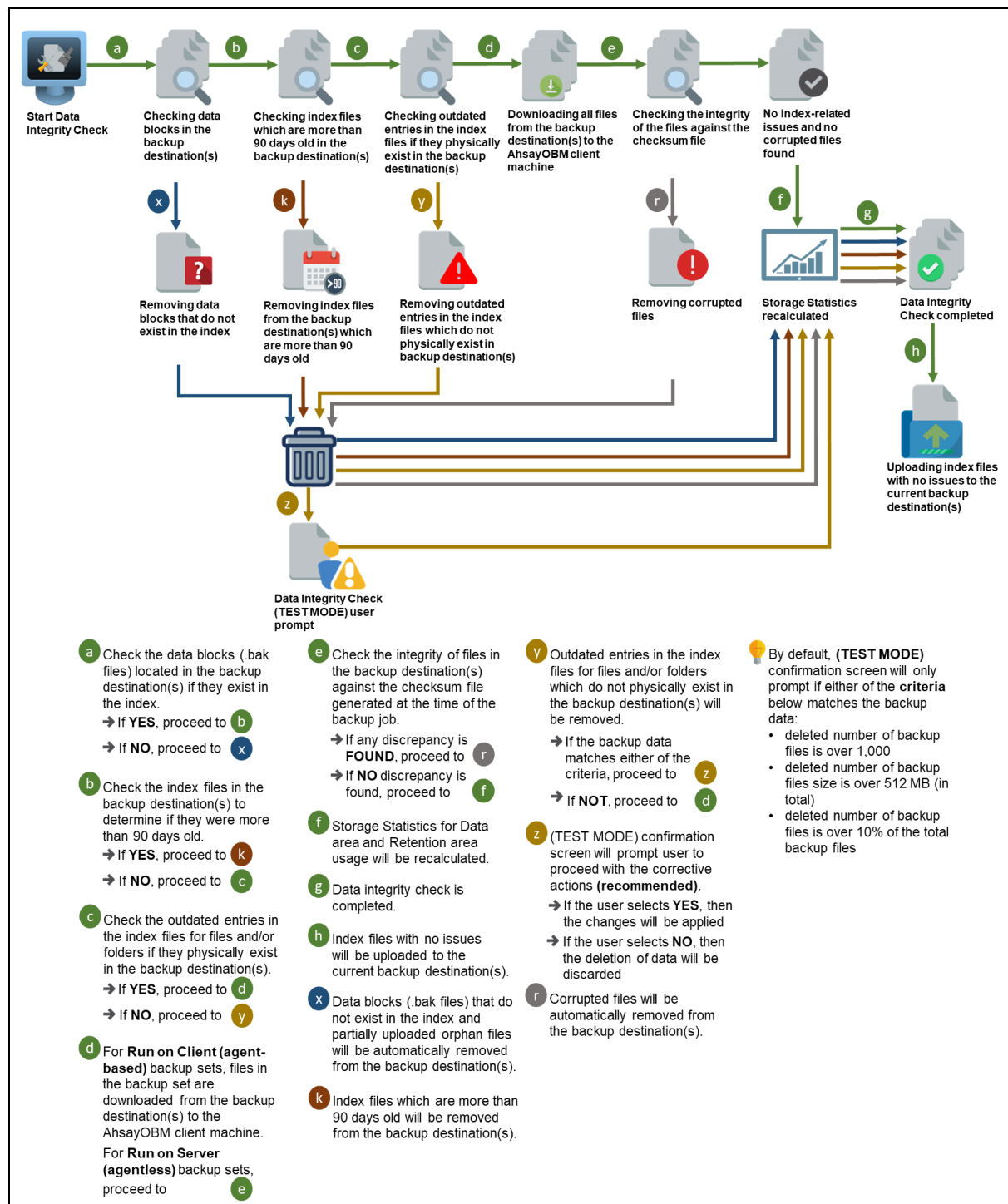
Data Integrity Check (TEST MODE) process flow:

- Start Data Integrity Check**
- Checking data blocks in the backup destination(s)**
 - If YES, proceed to **c**
 - If NO, proceed to **x**
- Checking index files which are more than 90 days old in the backup destination(s)**
 - If YES, proceed to **k**
 - If NO, proceed to **c**
- Checking outdated entries in the index files if they physically exist in the backup destination(s)**
 - If YES, proceed to **y**
 - If NO, proceed to **d**
- Removing data blocks that do not exist in the index** (marked with **x**)
- Removing index files from the backup destination(s) which are more than 90 days old** (marked with **k**)
- Removing outdated entries in the index files which do not physically exist in backup destination(s)** (marked with **y**)
- Data Integrity Check (TEST MODE) user prompt** (marked with **z**)
 - If YES, proceed to **d**
 - If NO, proceed to **f**
- Storage Statistics recalculated** (marked with **d**)
- Data Integrity Check completed** (marked with **f**)
- Uploading index files with no issues to the current backup destination(s)** (marked with **e**)

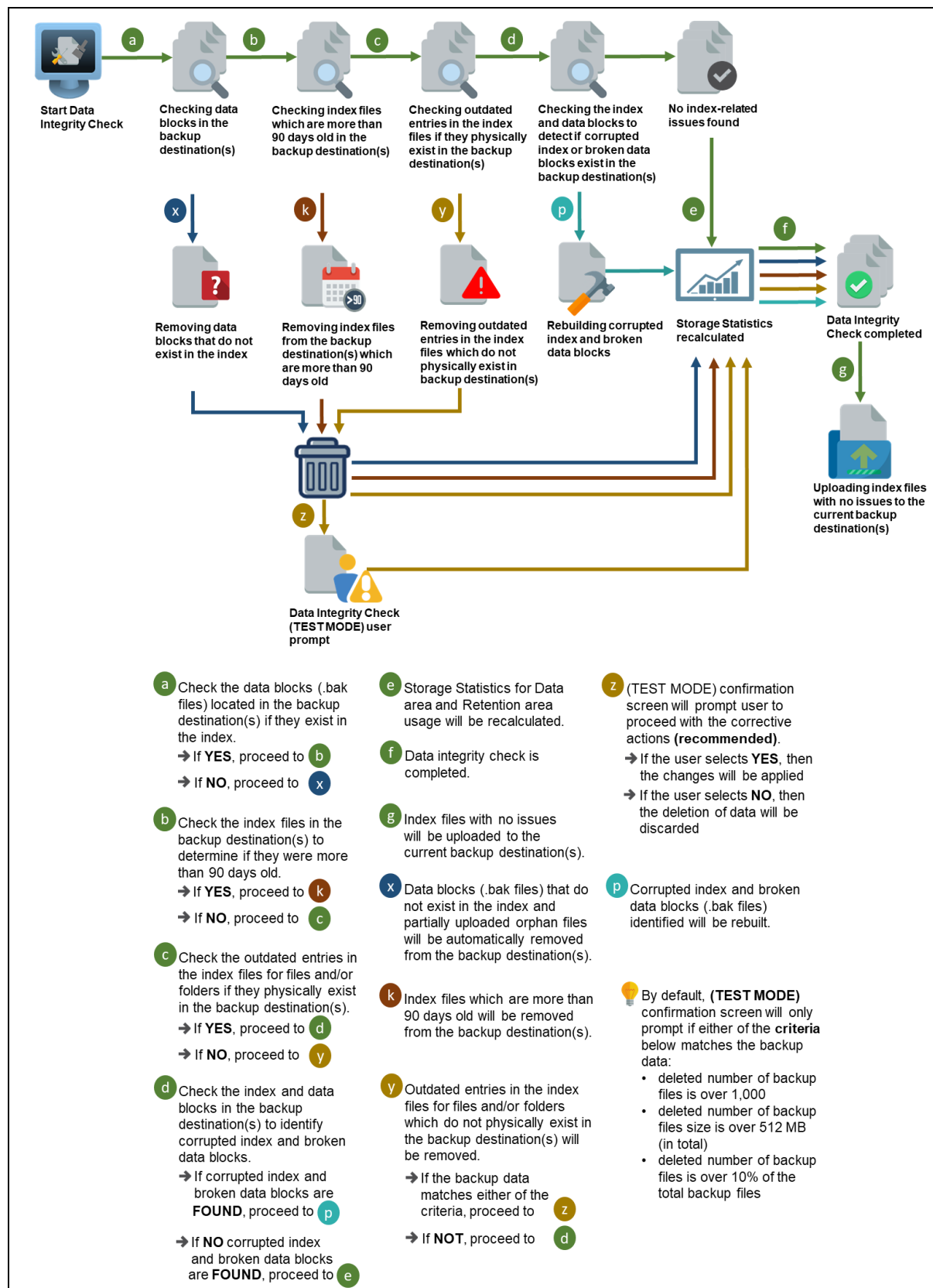
Criteria for (TEST MODE) confirmation screen:

- 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

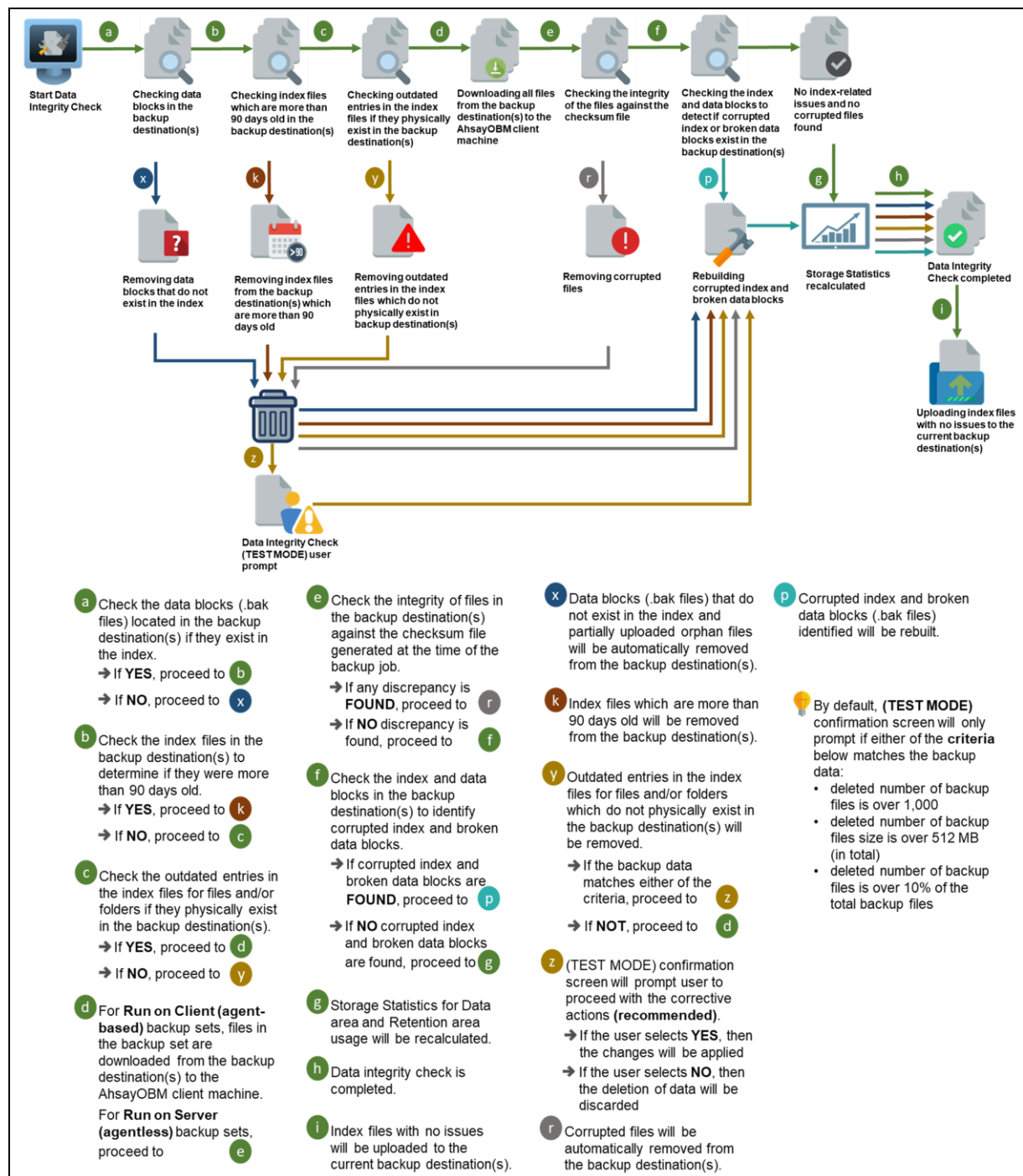
Option 2 - Data Integrity Check (DIC) Process with Run Cyclic Redundancy Check (CRC) **ENABLED** and Rebuild index **DISABLED**



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



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



Perform a Data Integrity Check

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

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

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

- A description: 'Perform health check for your backed up data to ensure the data integrity and restorability'.
- A label 'Select a backup set' above a dropdown menu currently showing 'All'.
- Three checkboxes:
 - ☐ Run Cyclic Redundancy Check (CRC) during data integrity check
 - ☐ Rebuild index
 - ☐ Delete corrupted data blocks permanently
- A 'Start' button.
- At the bottom right, 'Close' and 'Help' buttons.

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

This screenshot shows the same interface as the previous one, but the dropdown menu for 'Select a backup set' is open, displaying a list of options:

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

The 'Start' button and the 'Close'/'Help' buttons at the bottom remain visible.

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

Utilities

Data Integrity Check

Space Freeing Up

Delete Backup Data

Decrypt Backup Data

Data Integrity Check

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

Select a backup set

Backup Set 1

Select a destination

All

All

AhsayCBS

Rebuild index

☐ Delete corrupted data blocks permanently

Start

Close Help

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

Utilities

Data Integrity Check

Space Freeing Up

Delete Backup Data

Decrypt Backup Data

Data Integrity Check

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

Select a backup set

Backup Set 1

Select a destination

All

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

☐ Rebuild index

☐ Delete corrupted data blocks permanently

Start processing data integrity check on backup set= "Backup Set 1" destination...

Stop

Close Help

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

Utilities

Data Integrity Check

Space Freeing Up

Delete Backup Data

Decrypt Backup Data

Data Integrity Check

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

Select a backup set

Backup Set 1

Select a destination

All

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

☐ Rebuild index

☐ Delete corrupted data blocks permanently

✓ Data Integrity Check is completed successfully

[View log](#)

[Close](#) [Help](#)

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

Utilities

Data Integrity Check

Log 29/09/2022 11:20

Show All

Type	Log	Time
i	Start [AhsayOBM v9.4.2.0]	29/09/2022 11:20:03
i	Start data integrity check on backup set "Backup Set 1(1663644856198)" all destination, crc disabled, rebuild index disabled, ...	29/09/2022 11:20:03
i	Start processing data integrity check on backup set= "Backup Set 1" destination= "AhsayCBS"	29/09/2022 11:21:35
i	Download valid index files from backup job "2022-09-27-14-34-53" to "/usr/local/obm/bin/C:\Users\Administrator\obm\temp..."	29/09/2022 11:23:45
i	Vacuuming index	29/09/2022 11:24:29
i	Vacuuming index... Completed	29/09/2022 11:24:29
i	Existing statistics of backup set= "Backup Set 1" destination= "AhsayCBS": Data area compressed size: 15.64 MB, Data area ...	29/09/2022 11:24:30
i	Recalculated statistics of backup set= "Backup Set 1" destination= "AhsayCBS": Data area compressed size: 15.64 MB, Data ...	29/09/2022 11:24:30
i	The statistics of backup set= "Backup Set 1" destination= "AhsayCBS" is correct.	29/09/2022 11:24:30
i	Deleting out of retention period recycled files...	29/09/2022 11:25:08
i	Delete out of retention period recycled files result - Size: 0 B, File Count: 0	29/09/2022 11:25:08
i	Deleting out of retention period recycled files... Completed	29/09/2022 11:25:08
i	Saving encrypted backup file index to 1663644856198/blocks/2022-09-29-11-20-03 at destination AhsayCBS...	29/09/2022 11:25:13
i	[ObsStorageService.uploadFile] Retry after 1 seconds, count #1. Error: [ProcessingException] [b.a] Retry: 0; exception: javax...	29/09/2022 11:27:08
i	[RetryController.run] methodName=ObsStorageService.uploadFile, callback=135910967, retry #1 succeed.	29/09/2022 11:27:09
i	Data integrity check on backup set= "Backup Set 1" destination= "AhsayCBS" is completed	29/09/2022 11:27:10
i	Finished data integrity check on backup set "Backup Set 1(1663644856198)" all destination, crc disabled, rebuild index disabl...	29/09/2022 11:27:11
i	Completed data integrity check on backup set "Backup Set 1(1663644856198)" all destination, crc disabled, rebuild index dis...	29/09/2022 11:27:11

Logs per page 50

Page 1 / 1

[Close](#)

[Close](#) [Help](#)

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

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

Utilities

Data Integrity Check

Log 29/09/2022 11:20

Show All

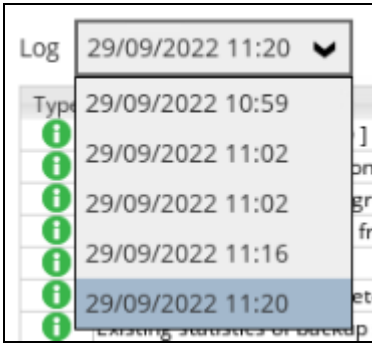
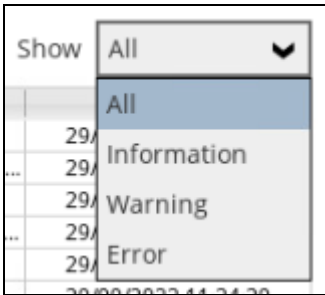
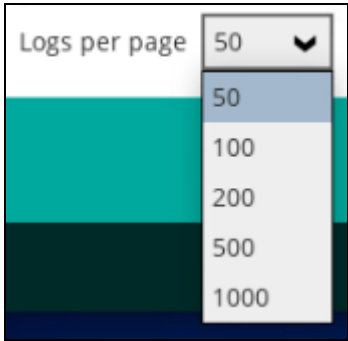
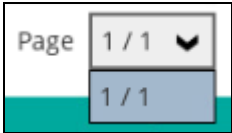
Type	Log	Time
i	Start [AhsayOBM v9.4.2.0]	29/09/2022 11:20:03
i	Start data integrity check on backup set "Backup Set 1(1663644856198)" all destination, crc disabled, rebuild index disabled, ...	29/09/2022 11:20:03
i	Start processing data integrity check on backup set= "Backup Set 1" destination= "AhsayCBS"	29/09/2022 11:21:35
i	Download valid index files from backup job "2022-09-27-14-34-53" to "/usr/local/obm/bin/C:\Users\Administrator\obm\temp..."	29/09/2022 11:23:45
i	Vacuuming index	29/09/2022 11:24:29
i	Vacuuming index... Completed	29/09/2022 11:24:29
i	Existing statistics of backup set= "Backup Set 1" destination= "AhsayCBS": Data area compressed size: 15.64 MB, Data area ...	29/09/2022 11:24:30
i	Recalculated statistics of backup set= "Backup Set 1" destination= "AhsayCBS": Data area compressed size: 15.64 MB, Data ...	29/09/2022 11:24:30
i	The statistics of backup set= "Backup Set 1" destination= "AhsayCBS" is correct.	29/09/2022 11:24:30
i	Deleting out of retention period recycled files...	29/09/2022 11:25:08
i	Delete out of retention period recycled files result - Size: 0 B, File Count: 0	29/09/2022 11:25:08
i	Deleting out of retention period recycled files... Completed	29/09/2022 11:25:08
i	Saving encrypted backup file index to 1663644856198/blocks/2022-09-29-11-20-03 at destination AhsayCBS...	29/09/2022 11:25:13
i	[ObsStorageService.uploadFile] Retry after 1 seconds, count #1. Error: [ProcessingException] [b.a] Retry: 0; exception: javax....	29/09/2022 11:27:08
i	[RetryController.run] methodName=ObsStorageService.uploadFile, callback=135910967, retry #1 succeed.	29/09/2022 11:27:09
i	Data integrity check on backup set= "Backup Set 1" destination= "AhsayCBS" is completed	29/09/2022 11:27:10
i	Finished data integrity check on backup set "Backup Set 1(1663644856198)" all destination, crc disabled, rebuild index disabl...	29/09/2022 11:27:11
i	Completed data integrity check on backup set "Backup Set 1(1663644856198)" all destination, crc disabled, rebuild index dis...	29/09/2022 11:27:11

Logs per page 50

Page 1 / 1

Close

Close Help

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

Data Integrity Check Completed with Errors

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

The screenshot shows the 'Utilities' section with 'Data Integrity Check' selected. The interface includes a sidebar with options: 'Data Integrity Check', 'Space Freeing Up', 'Delete Backup Data', and 'Decrypt Backup Data'. The main area is titled 'Data Integrity Check' and contains the following elements:

- Instruction: 'Perform health check for your backed up data to ensure the data integrity and restorability'
- 'Select a backup set' dropdown menu showing 'Backup Set 3'
- 'Select a destination' dropdown menu showing 'All'
- Three checkboxes: 'Run Cyclic Redundancy Check (CRC) during data integrity check', 'Rebuild index', and 'Delete corrupted data blocks permanently' (all are unchecked).
- A red error message: 'Data Integrity Check is completed with error(s)'
- A 'View log' button
- 'Close' and 'Help' buttons at the bottom right.

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

The screenshot shows the log details for the Data Integrity Check. It includes a 'Log' dropdown set to '29/09/2022 11:02' and a 'Show' dropdown set to 'All'. The log entries are as follows:

Type	Log	Time
Start [AhsayOBM v9.4.2.0]		29/09/2022 11:02:31
Start data integrity check on backup set "Backup Set 3(1663663778743)" all destination, crc disabled, rebuild index disabled, ...		29/09/2022 11:02:31
Skipped Backup Set = "Backup Set 3". Reason = "Scheduled backup set "Backup Set 3" is still running."		29/09/2022 11:02:37
Finished data integrity check with error on backup set "Backup Set 3(1663663778743)" all destination, crc disabled, rebuild in...		29/09/2022 11:02:37
Completed data integrity check on backup set "Backup Set 3(1663663778743)" all destination, crc disabled, rebuild index dis...		29/09/2022 11:02:37

At the bottom, there is a 'Logs per page' dropdown set to '50' and a 'Page' indicator showing '1 / 1'. 'Close', 'Close', and 'Help' buttons are visible at the bottom right.

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.

The screenshot displays the 'Data Integrity Check' log window. At the top, there's a 'Log' dropdown set to '29/09/2022 11:20' and a 'Show' dropdown set to 'All'. Below these is a table with columns 'Type', 'Log', and 'Time'. The log entries show a successful check process, including starting the check, downloading index files, vacuuming the index, and recalculating statistics. The final entry states 'Completed data integrity check on backup set "Backup Set 1(1663644856198)" all destination, crc disabled, rebuild index disabled...'. At the bottom, there are controls for 'Logs per page' (set to 50) and 'Page' (1 / 1). A 'Close' button is located at the bottom right of the log area.

Type	Log	Time
Start [AhsayOBM v9.4.2.0]		29/09/2022 11:20:03
Start data integrity check on backup set "Backup Set 1(1663644856198)" all destination, crc disabled, rebuild index disabled, ...		29/09/2022 11:20:03
Start processing data integrity check on backup set= "Backup Set 1" destination= "AhsayCBS"		29/09/2022 11:21:35
Download valid index files from backup job "2022-09-27-14-34-53" to "/usr/local/obm/bin/C:\Users\Administrator\obm\temp..."		29/09/2022 11:23:45
Vacuuming index...		29/09/2022 11:24:29
Vacuuming index... Completed		29/09/2022 11:24:29
Existing statistics of backup set= "Backup Set 1" destination= "AhsayCBS": Data area compressed size: 15.64 MB, Data area ...		29/09/2022 11:24:30
Recalculated statistics of backup set= "Backup Set 1" destination= "AhsayCBS": Data area compressed size: 15.64 MB, Data ...		29/09/2022 11:24:30
The statistics of backup set= "Backup Set 1" destination= "AhsayCBS" is correct.		29/09/2022 11:24:30
Deleting out of retention period recycled files...		29/09/2022 11:25:08
Delete out of retention period recycled files result - Size: 0 B, File Count: 0		29/09/2022 11:25:08
Deleting out of retention period recycled files... Completed		29/09/2022 11:25:08
Saving encrypted backup file index to 1663644856198/blocks/2022-09-29-11-20-03 at destination AhsayCBS...		29/09/2022 11:25:13
[ObsStorageService.uploadFile] Retry after 1 seconds, count #1. Error: [ProcessingException] [b.a] Retry: 0; exception: javax...		29/09/2022 11:27:08
[RetryController.run] methodName=ObsStorageService.uploadFile, callback=135910967, retry #1 succeed.		29/09/2022 11:27:09
Data integrity check on backup set= "Backup Set 1" destination= "AhsayCBS" is completed		29/09/2022 11:27:10
Finished data integrity check on backup set "Backup Set 1(1663644856198)" all destination, crc disabled, rebuild index disabl...		29/09/2022 11:27:11
Completed data integrity check on backup set "Backup Set 1(1663644856198)" all destination, crc disabled, rebuild index dis...		29/09/2022 11:27:11

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

The screenshot shows the 'Data Integrity Check' window in 'TEST MODE'. A yellow warning icon is displayed with the message: 'The result of data integrity check (TEST MODE) is as follow. No actions are performed yet. Data corrupted items, checksum incorrect items and index broken data blocks will be deleted. Are you sure you want to continue?'. Below this, it specifies 'Backup set: Sample Backup Set 01'. A table shows the results for 'Local-1': 19 (4.7MB) items found in index, 1 (891KB) data corrupted items, and 0 (0B) index broken data blocks. The overall statistics are 'Incorrect'. A note at the bottom left says '* File count (File size)'. At the bottom right, there are buttons for 'Yes', 'No', and 'View log'. A 'Close' button is at the very bottom right.

Destination	Items found in index	Data corrupted items	Index broken data blocks	Statistics
Local-1	19 (4.7MB)	1 (891KB)	0 (0B)	Incorrect

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:

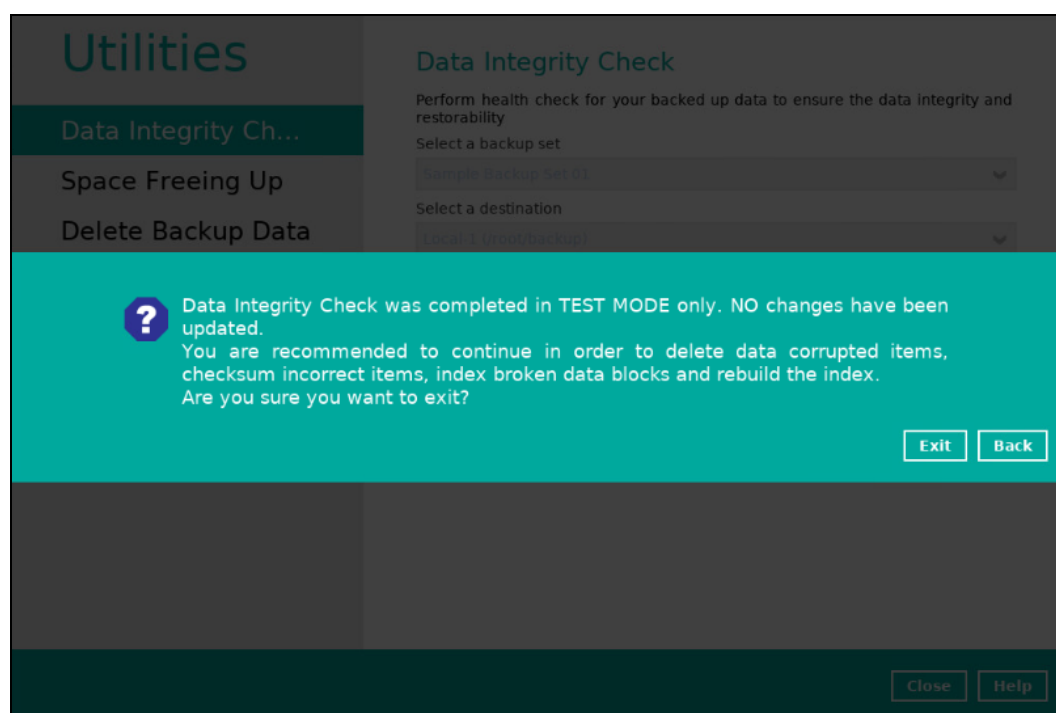
- deleted number of backup files is over 1,000
- deleted number of backup file size is over 512 MB (in total)
- deleted number of backup files is over 10% of total backup files

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

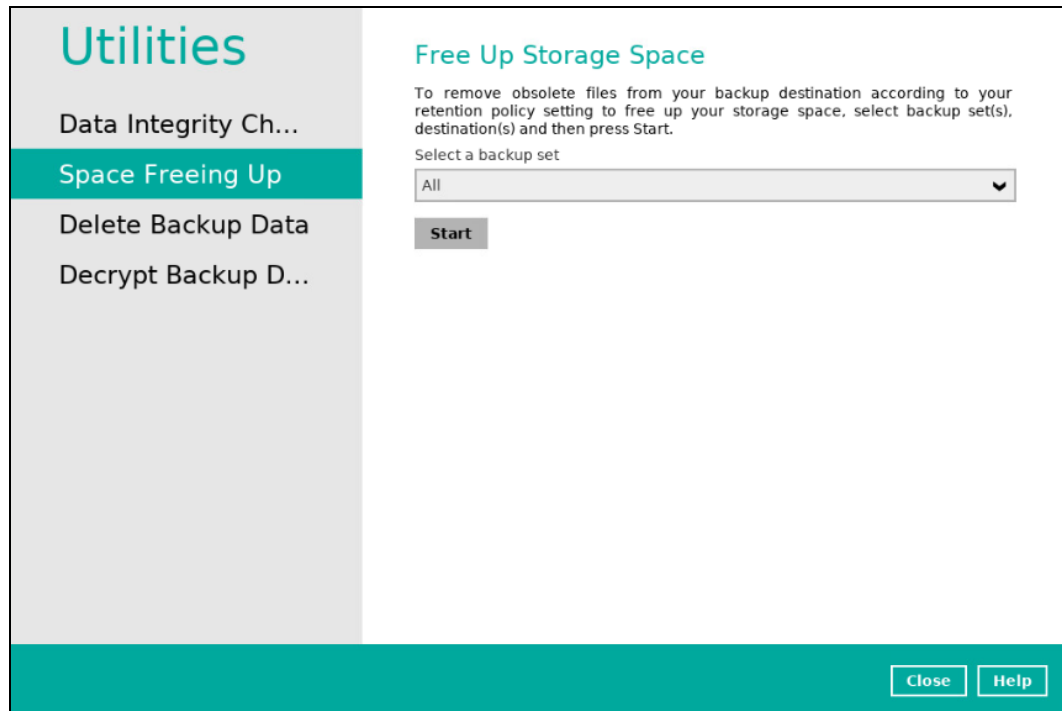
Home .obm system IntegrityCheck			
	Name	Size	Modified
Recent	2022-09-29-10-59-17.log	53.2 kB	10:59
Starred	2022-09-29-11-02-15.log	3.2 kB	11:02
Home	2022-09-29-11-02-31.log	1.3 kB	11:02
Documents	2022-09-29-11-16-49.log	1.3 kB	11:16
Downloads	2022-09-29-11-20-03.log	14.2 kB	11:27
Music			
Pictures			

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.

The screenshot shows the 'Free Up Storage Space' utility window. On the left, under the 'Utilities' header, there is a sidebar with four options: 'Data Integrity Ch...', 'Space Freeing Up' (which is highlighted in teal), 'Delete Backup Data', and 'Decrypt Backup D...'. The main area of the window has a title 'Free Up Storage Space' and a description: 'To remove obsolete files from your backup destination according to your retention policy setting to free up your storage space, select backup set(s), destination(s) and then press Start.' Below this, there are two dropdown menus. The first is labeled 'Select a backup set' and has 'Sample Backup Set 01' selected. The second is labeled 'Select a destination' and has 'All' selected. Below the second dropdown, a list of destinations is visible: 'All', 'AhsayCBS', and 'Local-1 (/root/backup)'. At the bottom right of the window, there are two buttons: 'Close' and 'Help'.

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

The screenshot shows the 'Free Up Storage Space' utility window with 'All' selected in the 'Select a backup set' dropdown. The 'Select a destination' dropdown is no longer visible. Instead, a 'Start' button is now visible below the 'Select a backup set' dropdown. The rest of the interface, including the sidebar and footer buttons ('Close' and 'Help'), remains the same as in the previous screenshot.

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

Utilities

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

Free Up Storage Space

To remove obsolete files from your backup destination according to your retention policy setting to free up your storage space, select backup set(s), destination(s) and then press Start.

Select a backup set

Sample Backup Set 01

Select a destination

AhsayCBS

Start

Close Help

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

Utilities

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

Free Up Storage Space

To remove obsolete files from your backup destination according to your retention policy setting to free up your storage space, select backup set(s), destination(s) and then press Start.

Select a backup set

Sample Backup Set 01

Select a destination

AhsayCBS

Start processing space freeing up on backup set= "Sample Backup Set 01 (1...

Stop

Close Help

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

Utilities

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

Free Up Storage Space

To remove obsolete files from your backup destination according to your retention policy setting to free up your storage space, select backup set(s), destination(s) and then press Start.

Select a backup set

Sample Backup Set 01

Select a destination

AhsayCBS

✓ Space freeing up is completed successfully

View log

Close **Help**

Utilities

Free Up Storage Space

Log 05/01/2022 09:39

Show All

Type	Log	Time
1	Start [AhsayOBM v9.0.2.24]	05/01/2022 09:39:21
1	Start space freeing up on backup set "Sample Backup Set 01(1641184406581)", "AhsayCBS(1641184474265)"	05/01/2022 09:39:21
1	Start processing space freeing up on backup set= "Sample Backup Set 01 (1641184406581)" destination= "Ahsa...	05/01/2022 09:39:28
1	Download valid index files from backup job "Current" to "/root/.obm/temp/1641184406581/OBS@1641184474265..."	05/01/2022 09:39:29
1	Saving encrypted backup file index to 1641184406581/blocks/2022-01-05-09-39-21 at destination AhsayCBS...	05/01/2022 09:39:30
1	Space freeing up on backup set= "Sample Backup Set 01 (1641184406581)" destination= "AhsayCBS (1641184..."	05/01/2022 09:39:30
1	Finished space freeing up on backup set "Sample Backup Set 01(1641184406581)", "AhsayCBS(1641184474265)"	05/01/2022 09:39:30

Logs per page 50

Page 1 / 1

Close

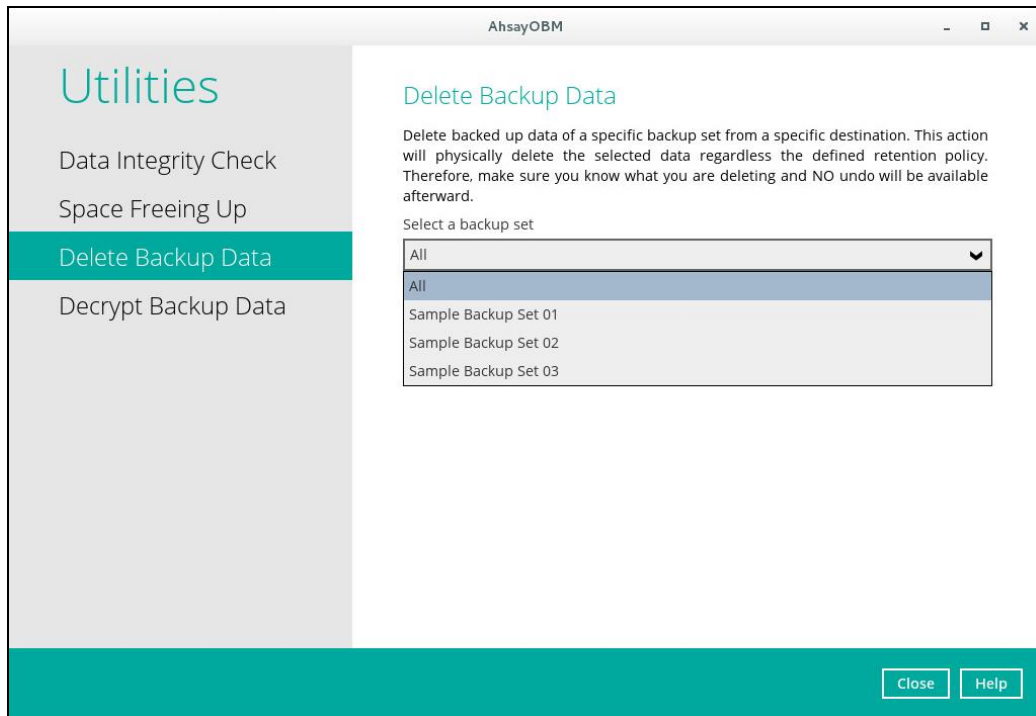
Close **Help**

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.

AhsayOBM

Utilities

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

Delete Backup Data

Delete backed up data of a specific backup set from a specific destination. This action will physically delete the selected data regardless the defined retention policy. Therefore, make sure you know what you are deleting and NO undo will be available afterward.

Select a backup set

Sample Backup Set 01

Select a destination

All

All

AhsayCBS

Close Help

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

AhsayOBM

Utilities

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

Delete Backup Data

Delete backed up data of a specific backup set from a specific destination. This action will physically delete the selected data regardless the defined retention policy. Therefore, make sure you know what you are deleting and NO undo will be available afterward.

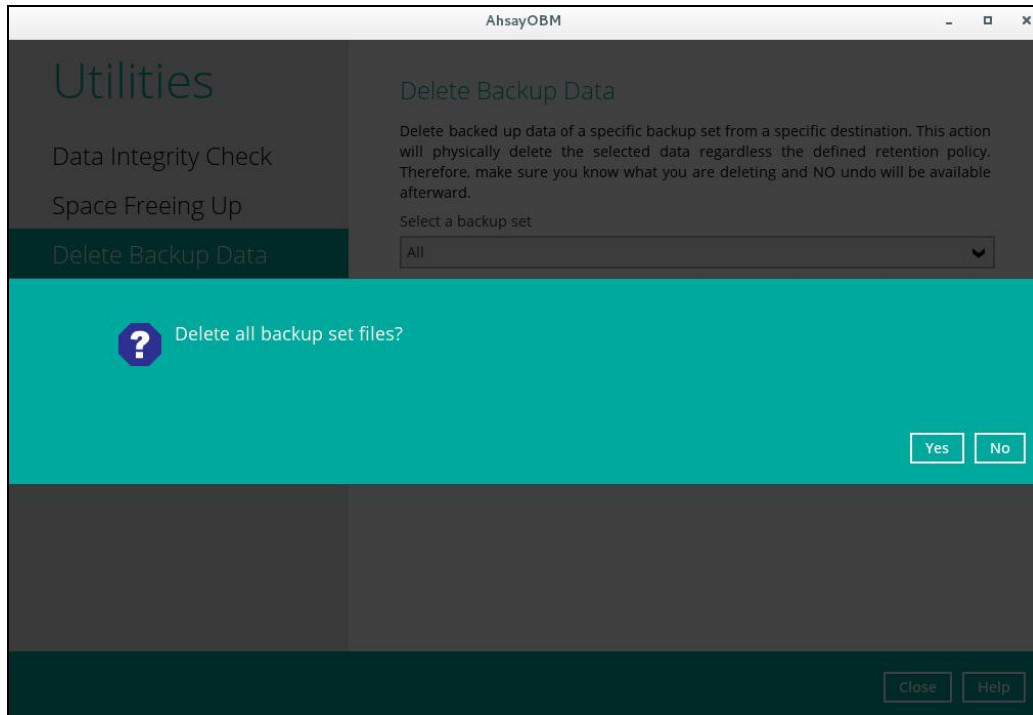
Select a backup set

All

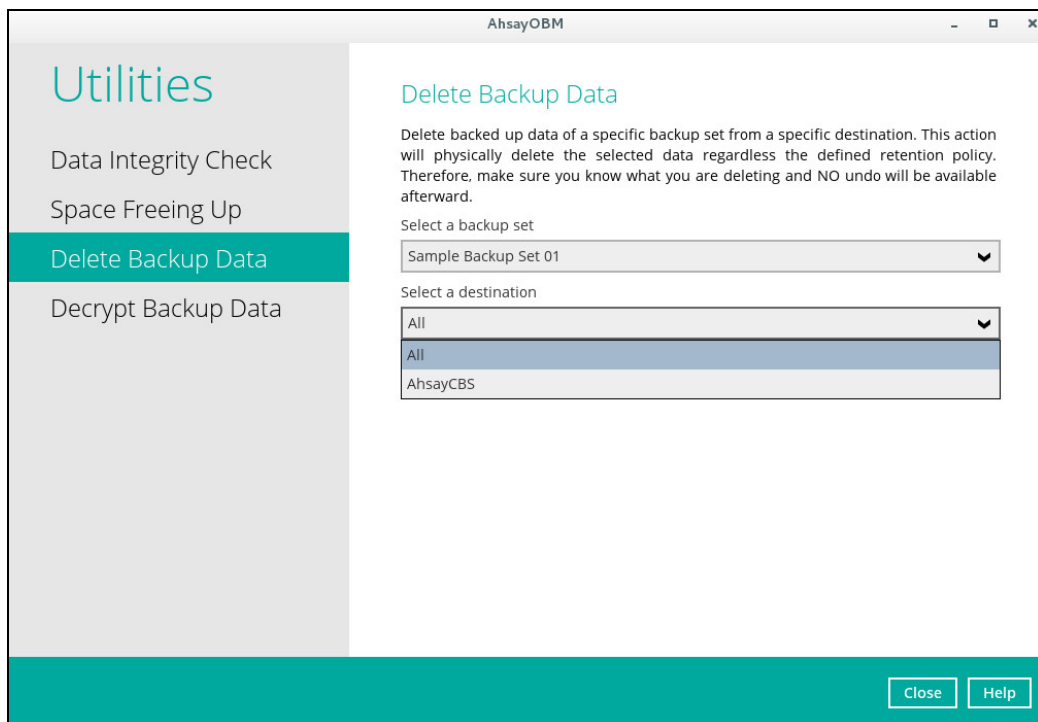
Delete

Close Help

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.

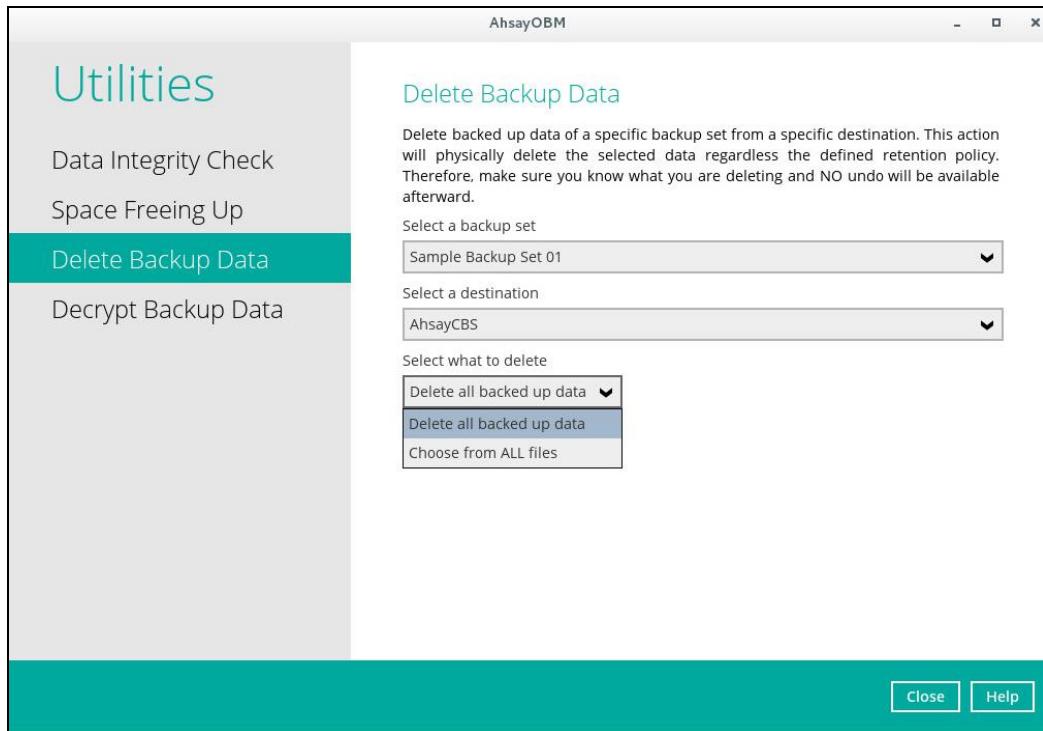


If you select a specific backup set, you will have an option to choose a destination.



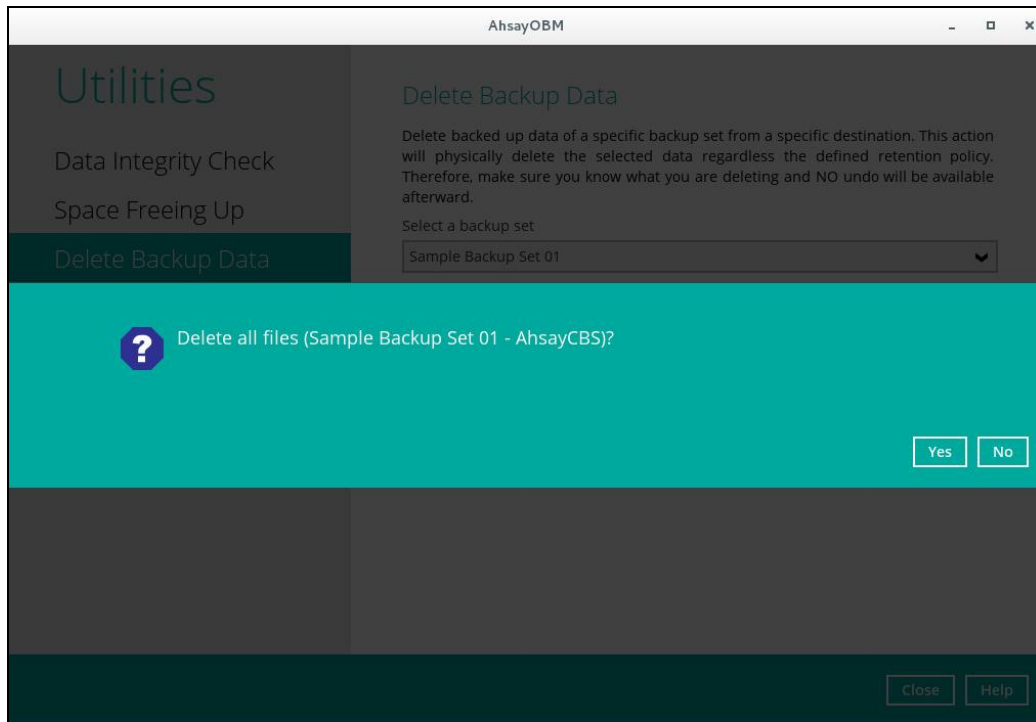
If you select a specific destination, there are two (2) available options for the type of files you wish to delete.

- Delete all backed up data
- Choose from ALL files



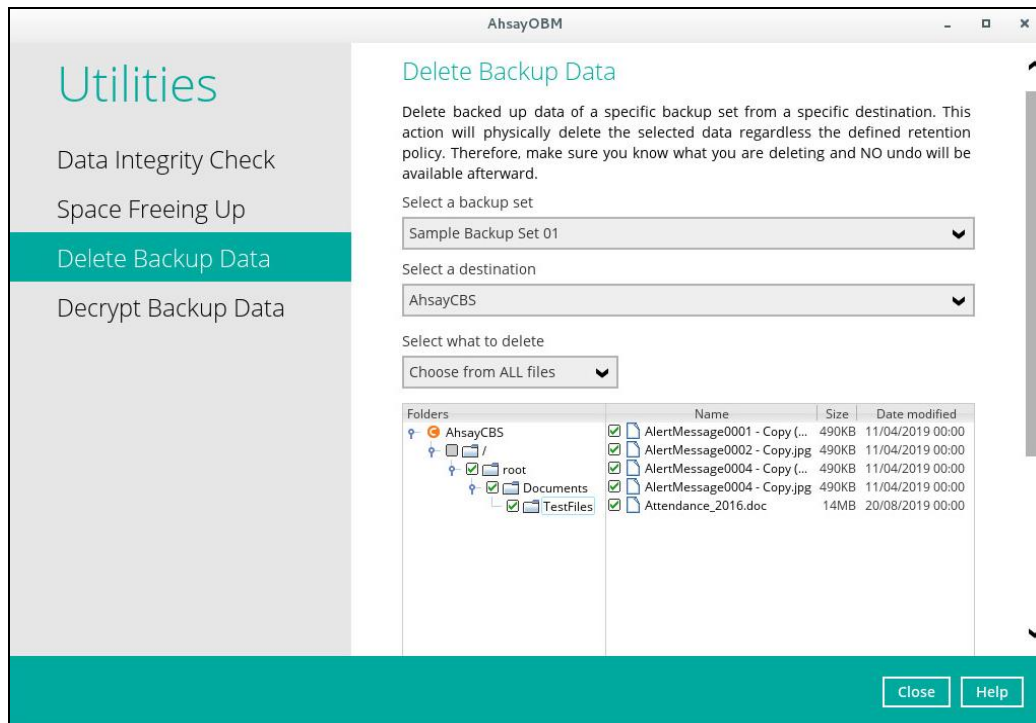
Delete all backed up data

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.

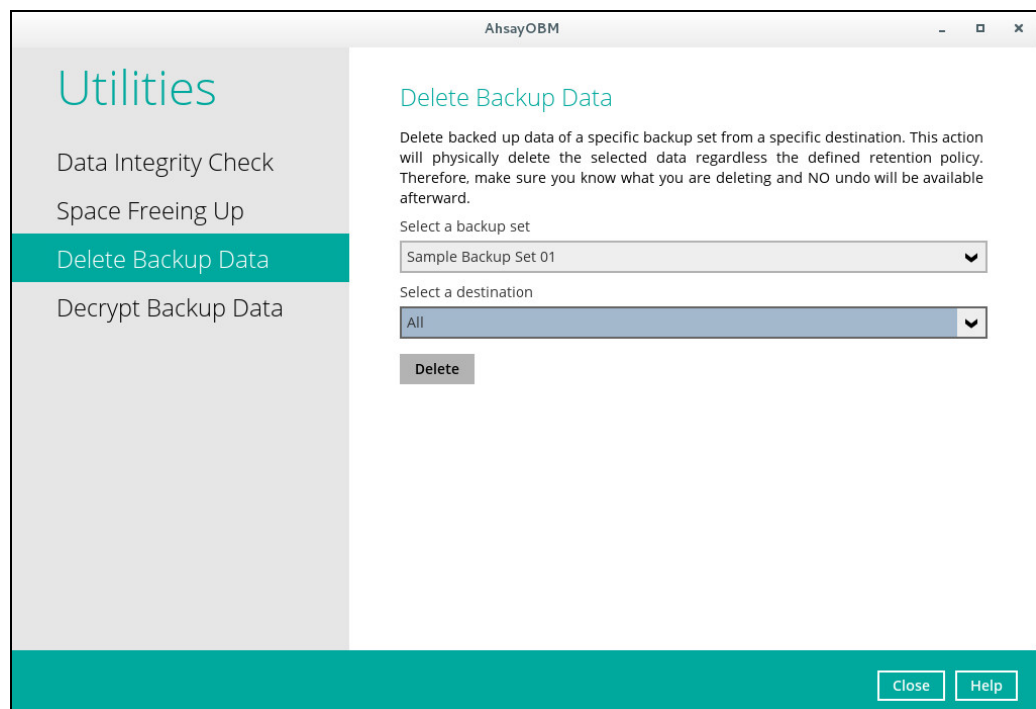


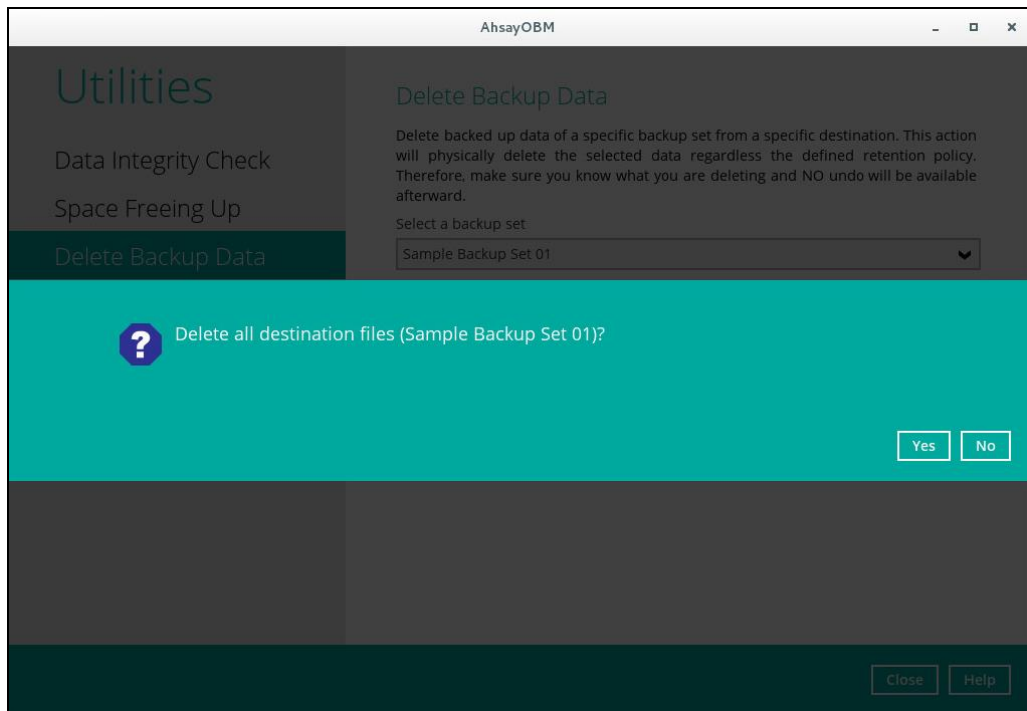
Choose from ALL files

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

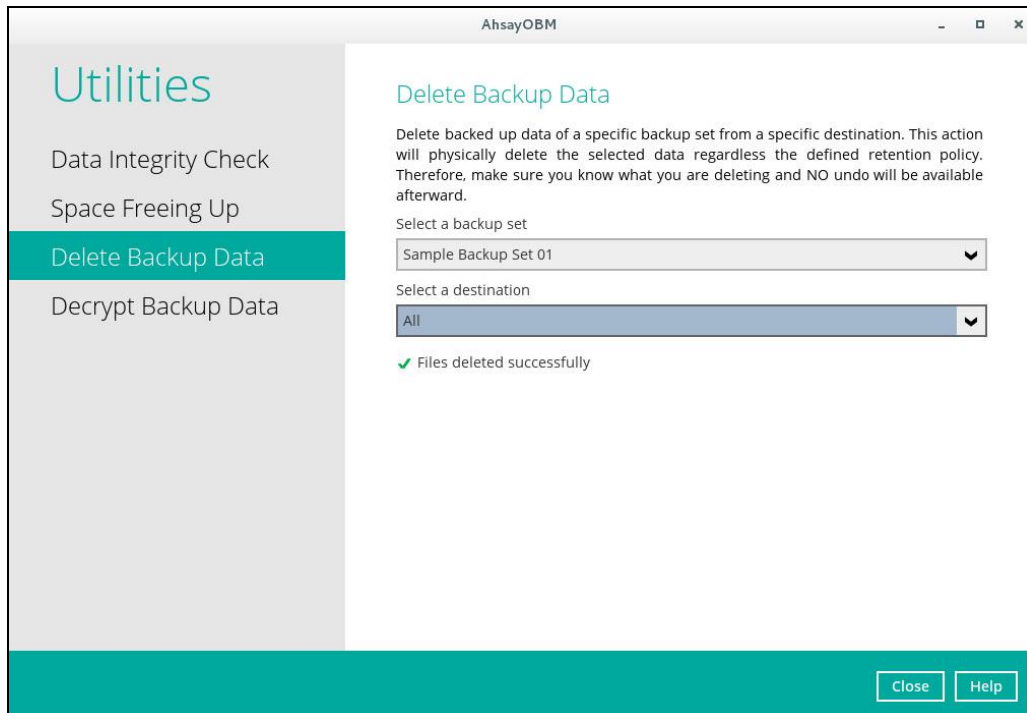


3. Click the **Delete** button, then click **Yes** to start the deletion of files.



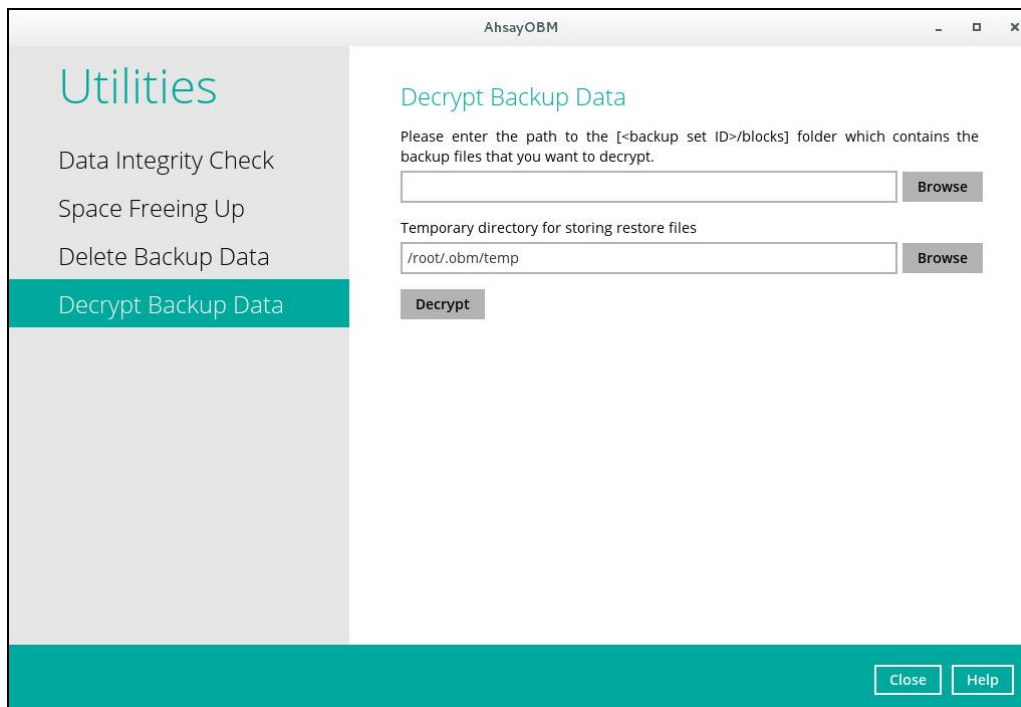


4. Files are successfully deleted.



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.



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

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.

Profile

- General
- Contacts
- Time Zone
- Encryption Recov...
- Authentication**

Password

Change Password

☐ Save password

Two-Factor Authentication

Require Authenticator App to sign in your account during startup

On ☒

Registered Mobile Device(s)

1234

Ahsay Mobile

Galaxy A70

Re-pair with authenticator

Add

Last Successful Login

No login record

Save **Cancel** **Help**

Profile

Password

Profile

You can change the password of the user, add or remove one or more mobile device(s) used for authentication and view the last successful login.

Password:

Field	Description
Save password	Automatically login everytime AhsayOBM is launched.

Two-Factor Authentication:

Field	Description
Registered Mobile Device(s)	List of mobile device(s) paired with the backup account.

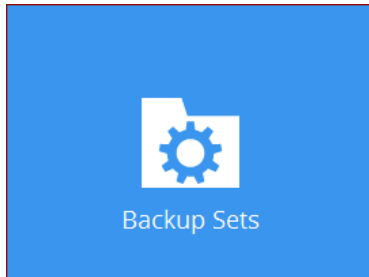
Last Successful Login:

Print **Close**

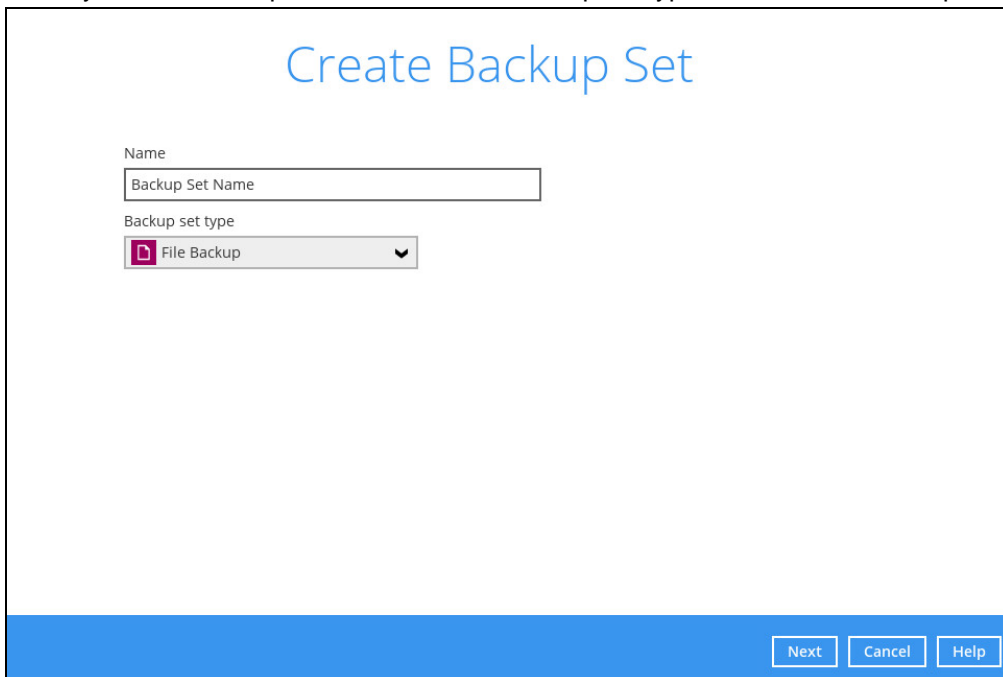
Save **Cancel** **Help**

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.

A dialog box titled "Create Backup Set" in blue text. It contains two input fields: "Name" with a text box containing "Backup Set Name", and "Backup set type" with a dropdown menu showing "File Backup" and a downward arrow. At the bottom right, there are three buttons: "Next", "Cancel", and "Help".

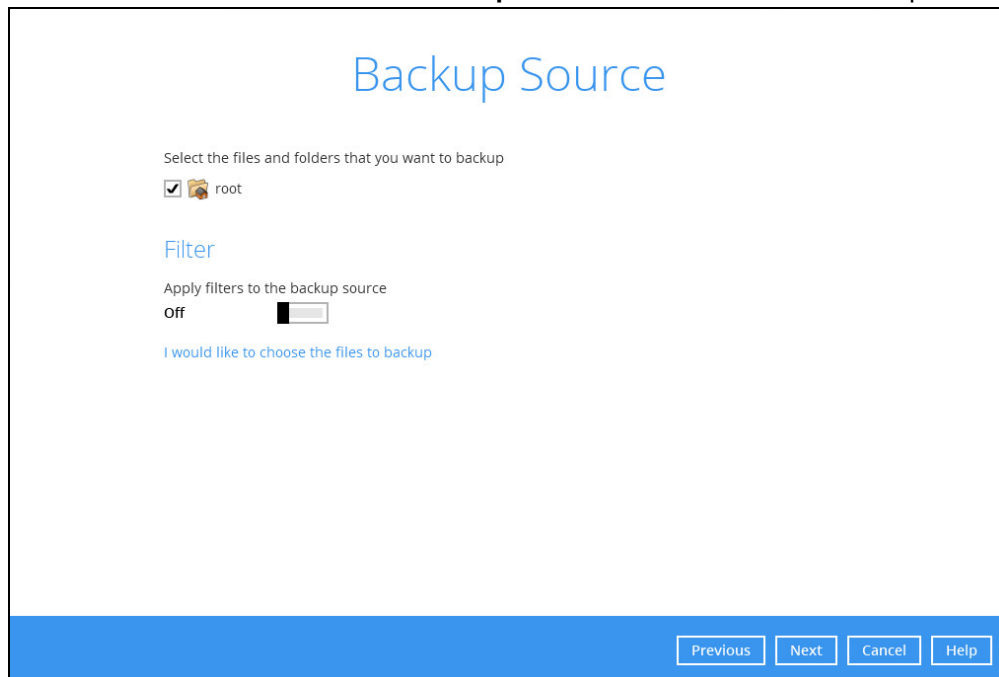
Create Backup Set

Name
Backup Set Name

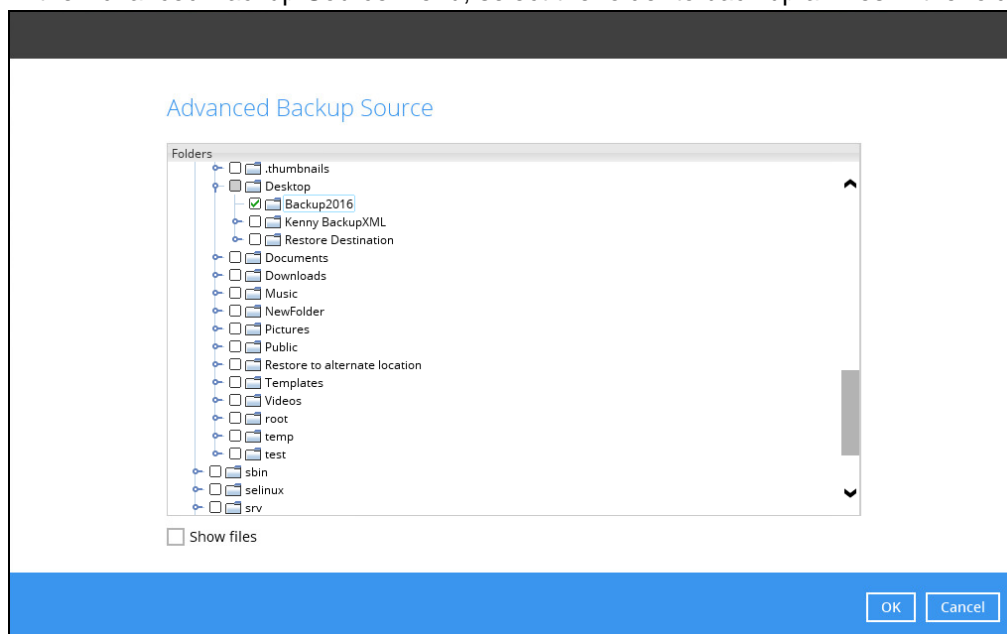
Backup set type
File Backup

Next Cancel Help

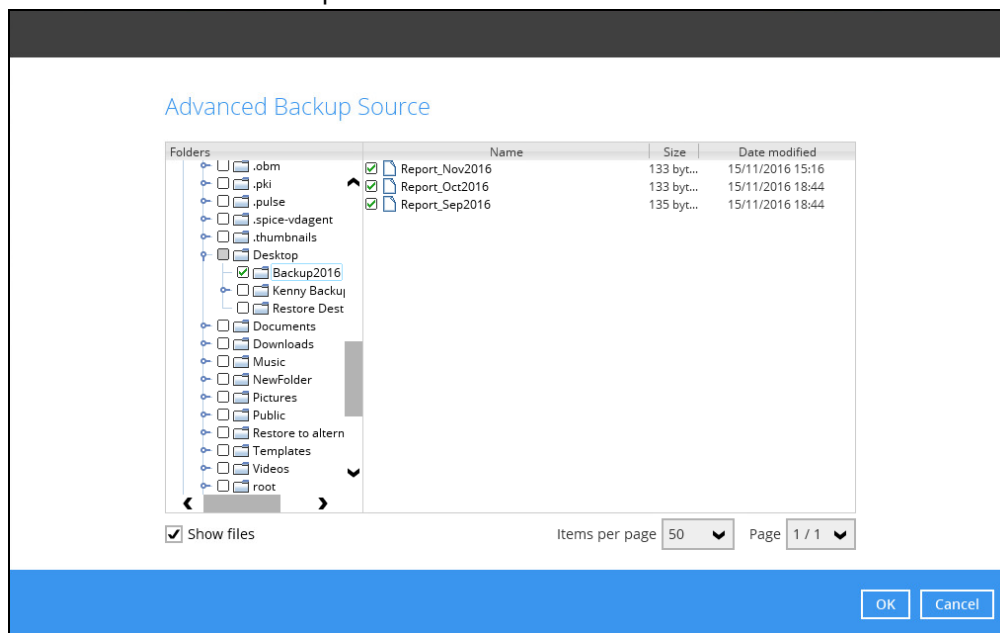
4. In the Backup Source menu, select the files and folder that you would like to backup. Click **I would like to choose the files to backup** to select individual files for backup.



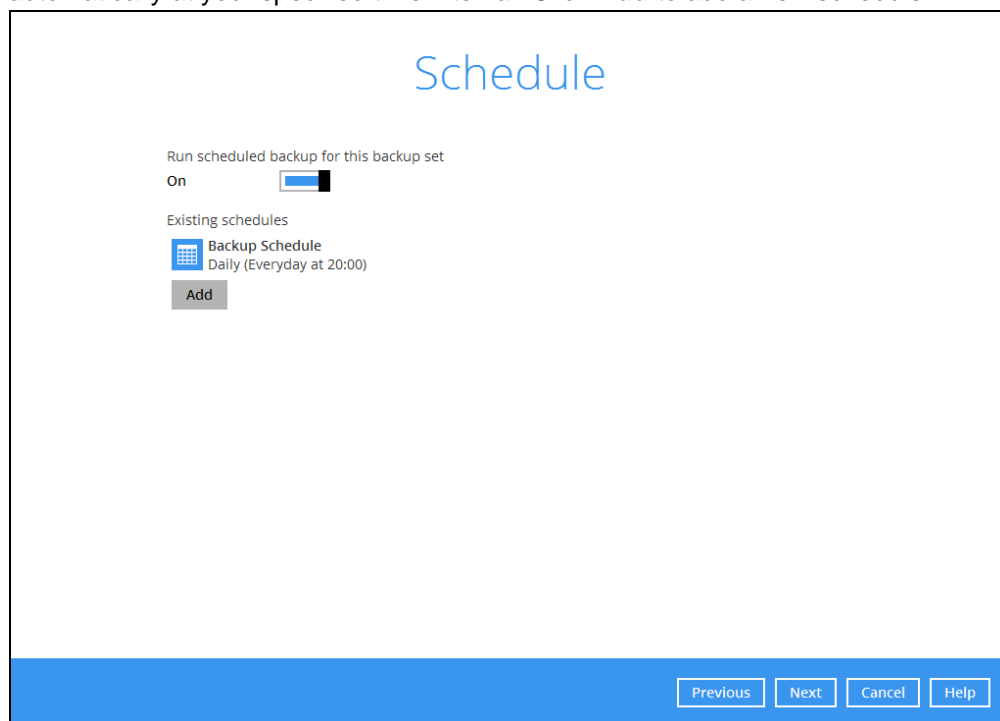
5. In the Advanced Backup Source menu, select the folder to back up all files in the folder.



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.

Destination

Backup mode

Concurrent

Maximum concurrent backup destinations

Unlimited

Unlimited
2
3
4
5
6
7
8

destinations
storage destination / destination pool

Previous

Next

Cancel

Help

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.**

Destination

Backup mode

Sequential

Existing storage destinations

+ Add new storage destination / destination pool

^ v

Previous

Next

Cancel

Help

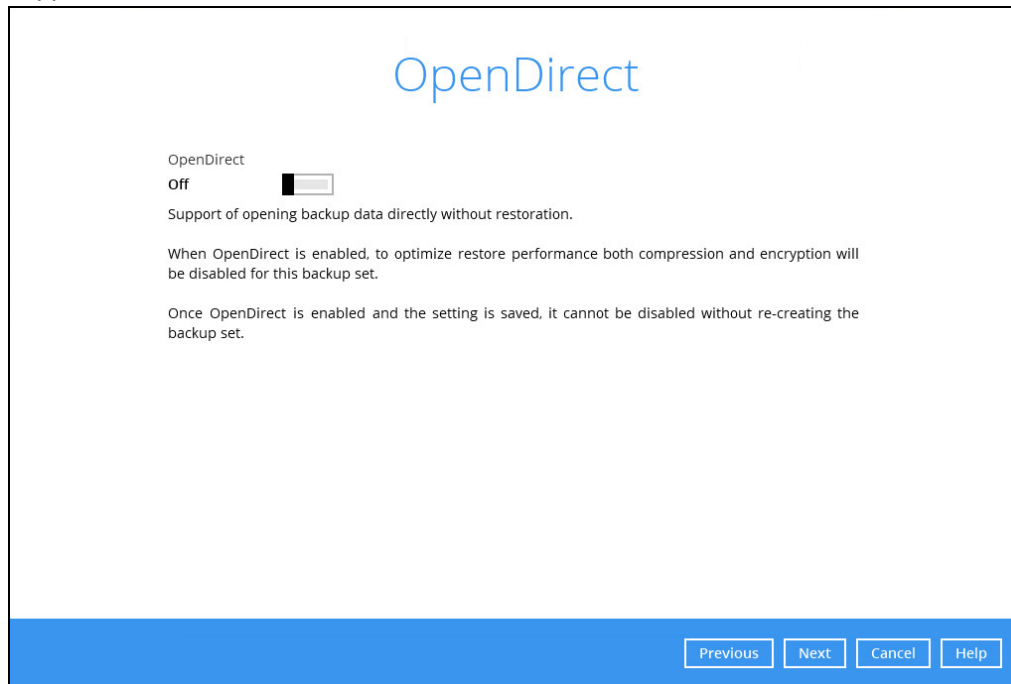
Select the destination storage. Then, click **OK** to proceed.

The screenshot shows a dialog box titled "New Storage Destination / Destination Pool". It has a "Name" field containing "AhsayCBS" and a "Destination storage" dropdown menu also showing "AhsayCBS". At the bottom right, there are three buttons: "OK", "Cancel", and "Help".

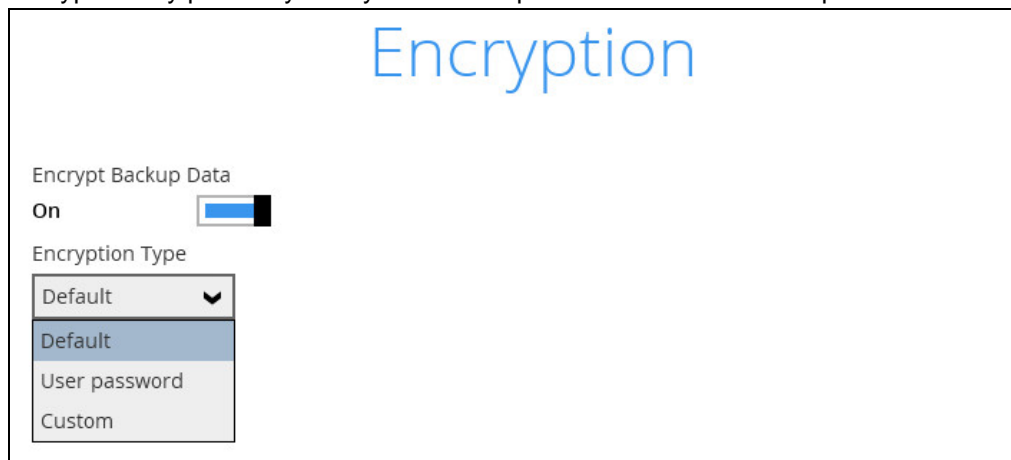
11. Click **Next** on the Destination menu page to proceed.

The screenshot shows a page titled "Destination". It features a "Backup mode" dropdown set to "Sequential". Below this, under "Existing storage destinations", there is a list item for "AhsayCBS" with the host "10.16.30.34:443" and an "Add" button. At the bottom right, there are four buttons: "Previous", "Next", "Cancel", and "Help".

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.

Encryption

Encrypt Backup Data
On ☒

Encryption Type
Custom ▼

Algorithm
AES ▼

Encryption key
.....

Re-enter encryption key
.....

Method
☐ ECB ☒ CBC

Key length
☐ 128-bit ☒ 256-bit

Previous Next Cancel Help

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.

Encryption

Encrypt Backup Data
On ☒

Encryption Type
Custom

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

.....

Unmask encryption key

Copy to clipboard Confirm

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

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

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

Smvg5y769Me9BUuevSx1qCL4aGHRXpAErK9Emo+IJ2s=

Mask encryption key

Copy to clipboard Confirm

- **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.

Congratulations!

"Backup Set Name" is successfully created.

Backup now Close

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.

The screenshot shows the 'Backup Set Name' configuration window with the 'Others' tab selected. The 'Temporary Directory' section is active, showing the current path as '/root/temp' with a 'Change' button. Below it, a status bar indicates '35.67GB free out of total 49.98GB space in /root/.obm/temp' and a checked checkbox for 'Remove temporary files after backup'. The 'Follow Link' section has a toggle set to 'On'. The 'File Permissions' section also has a toggle set to 'On'. The 'OpenDirect' section has a toggle set to 'Off'. The 'Compressions' section is partially visible at the bottom. At the bottom of the window, there is a 'Delete this backup set' link and 'Save', 'Cancel', and 'Help' buttons.

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:

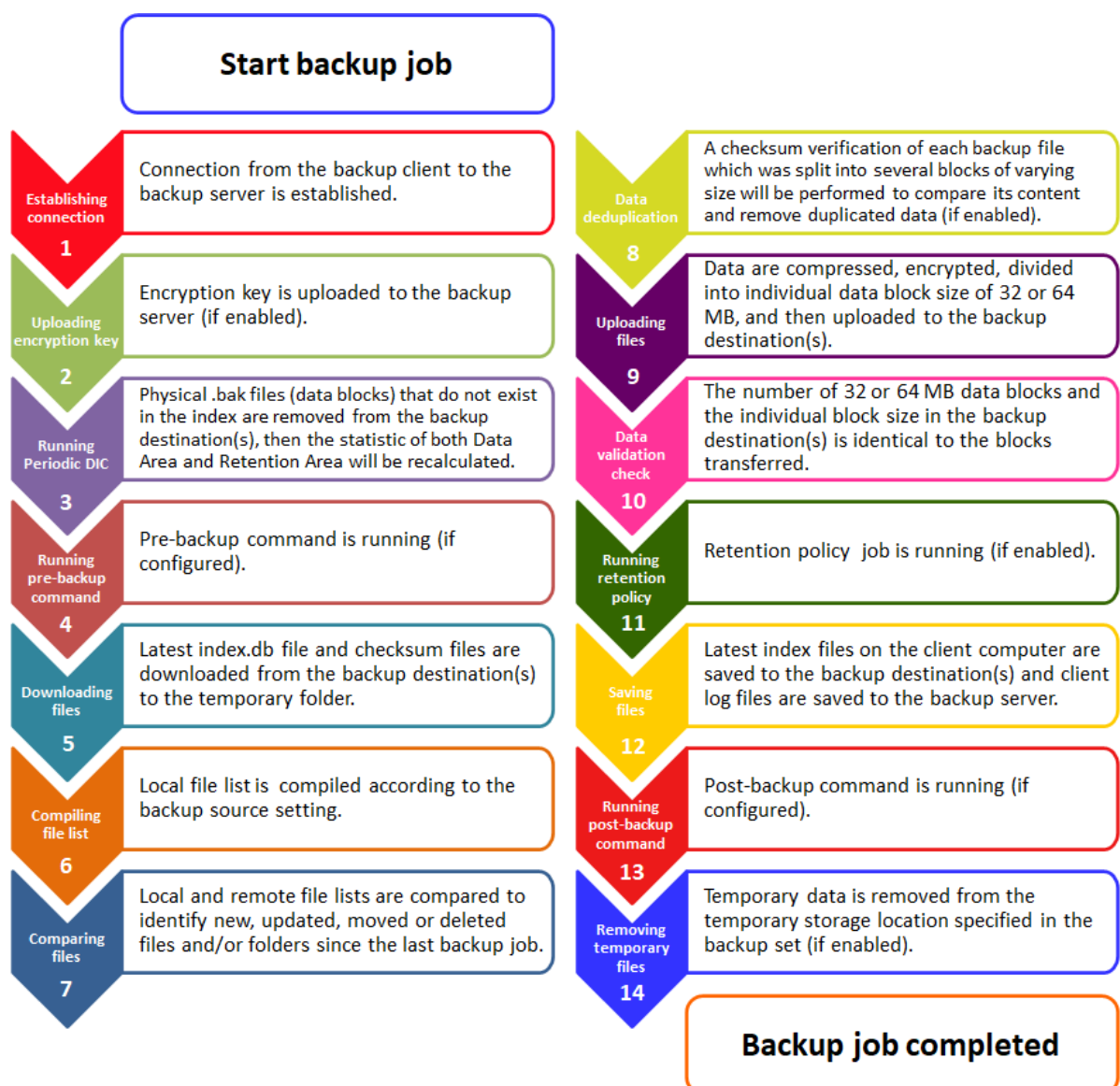
- No Compression
- Normal
- Fast (Compressed size larger than normal)
- Fast with optimization for local

The screenshot shows the 'Backup Set Name' configuration window with the 'Others' tab selected. The 'Compressions' section is active, showing a dropdown menu for 'Select compression type' with the following options: 'Fast with optimization for local' (selected), 'No Compression', 'Normal', 'Fast (Compressed size larger than normal)', and 'Fast with optimization for local'. Below the dropdown, the 'Algorithm' is set to 'AES', the 'Method' is set to 'CBC', and the 'Key length' is set to '256 bits'. At the bottom of the window, there is a 'Delete this backup set' link and 'Save', 'Cancel', and 'Help' buttons.

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: $1594627447932 \text{ mod } 5 = 2$

2	Wednesday
----------	------------------

In this example:

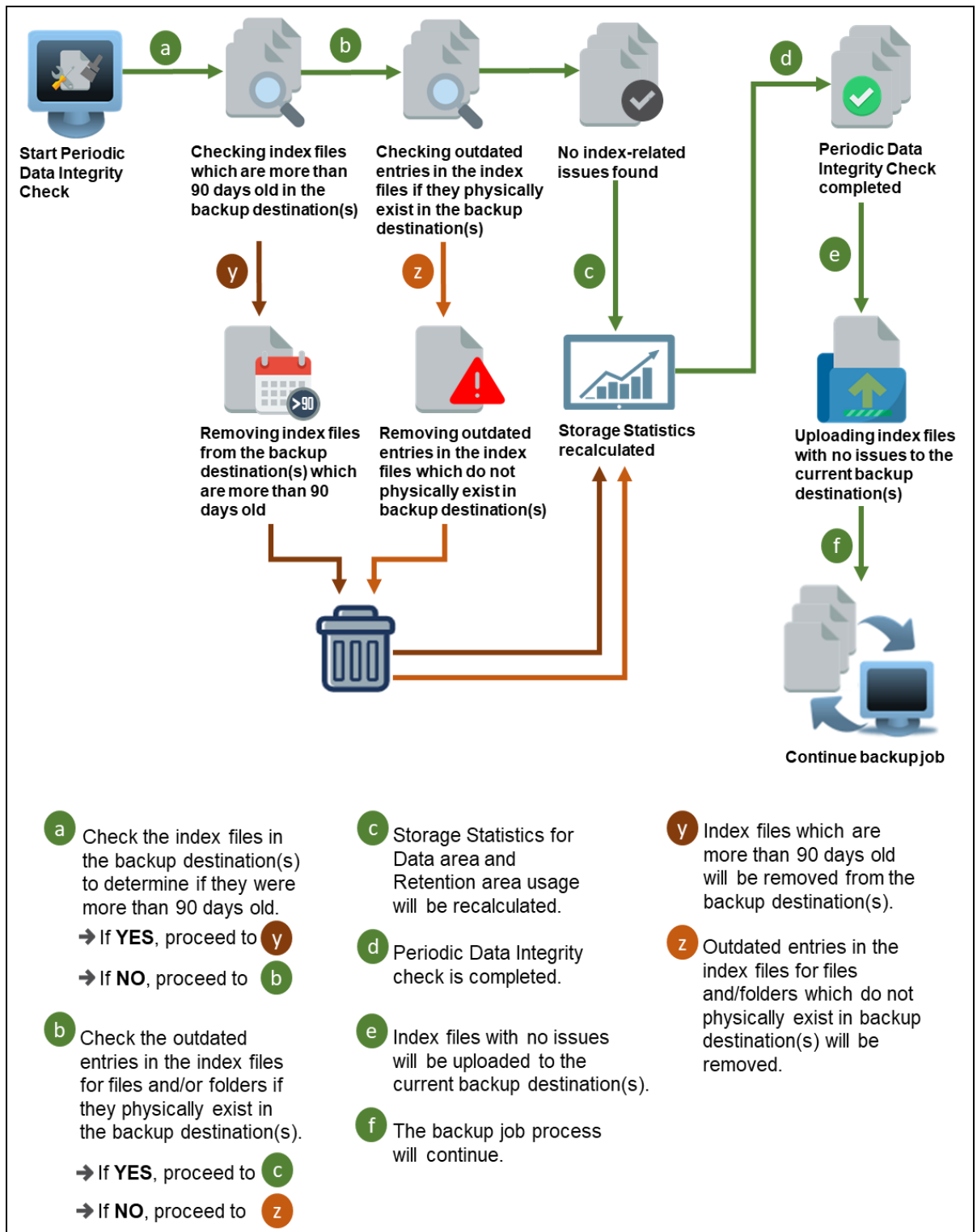
- the PDIC will run on the first backup job that falls on Wednesday; or
- if there is no active backup job(s) running from Monday to Friday, then the PDIC will run on the next available backup job.

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:

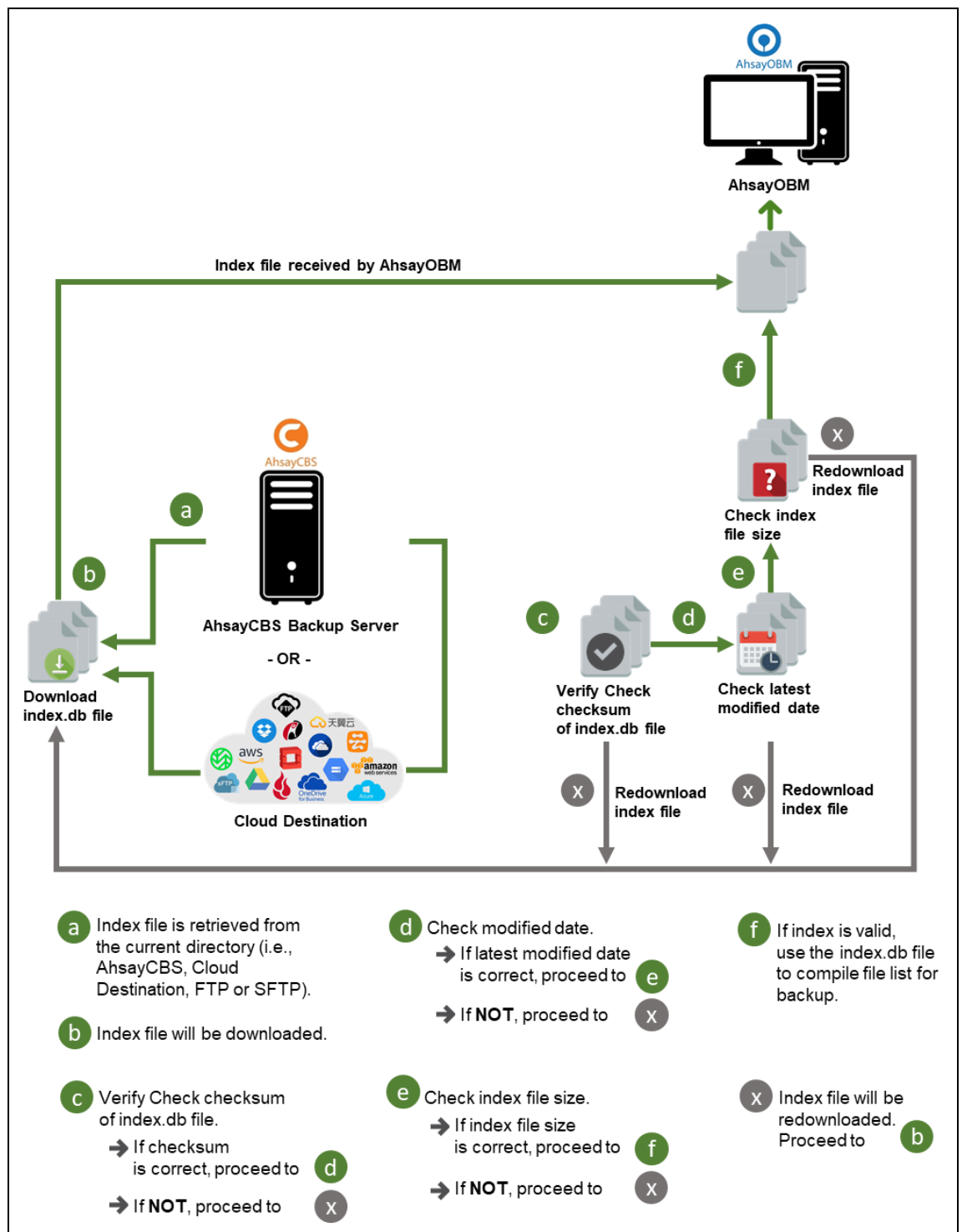
1. The PDIC job will run on the first backup job after upgrade to the latest client version from AhsayOBM v6, v7, or pre-8.3.6.0 version.
2. If backup jobs for a backup set are not run on a regular daily backup schedule (for example: on a weekly or monthly schedule), then the PDIC job will run if it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



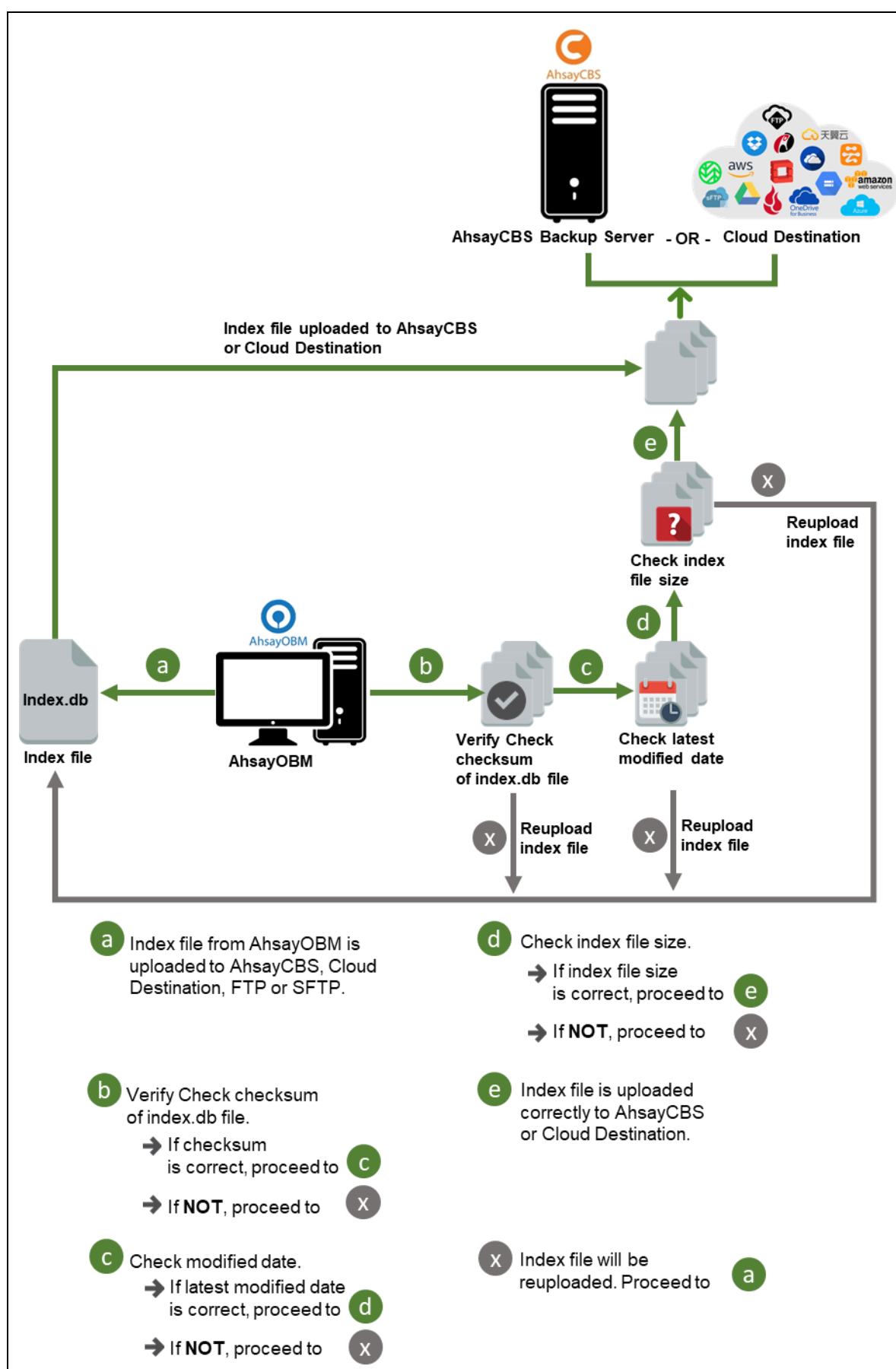
11.2 Backup Set Index Handling Process

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

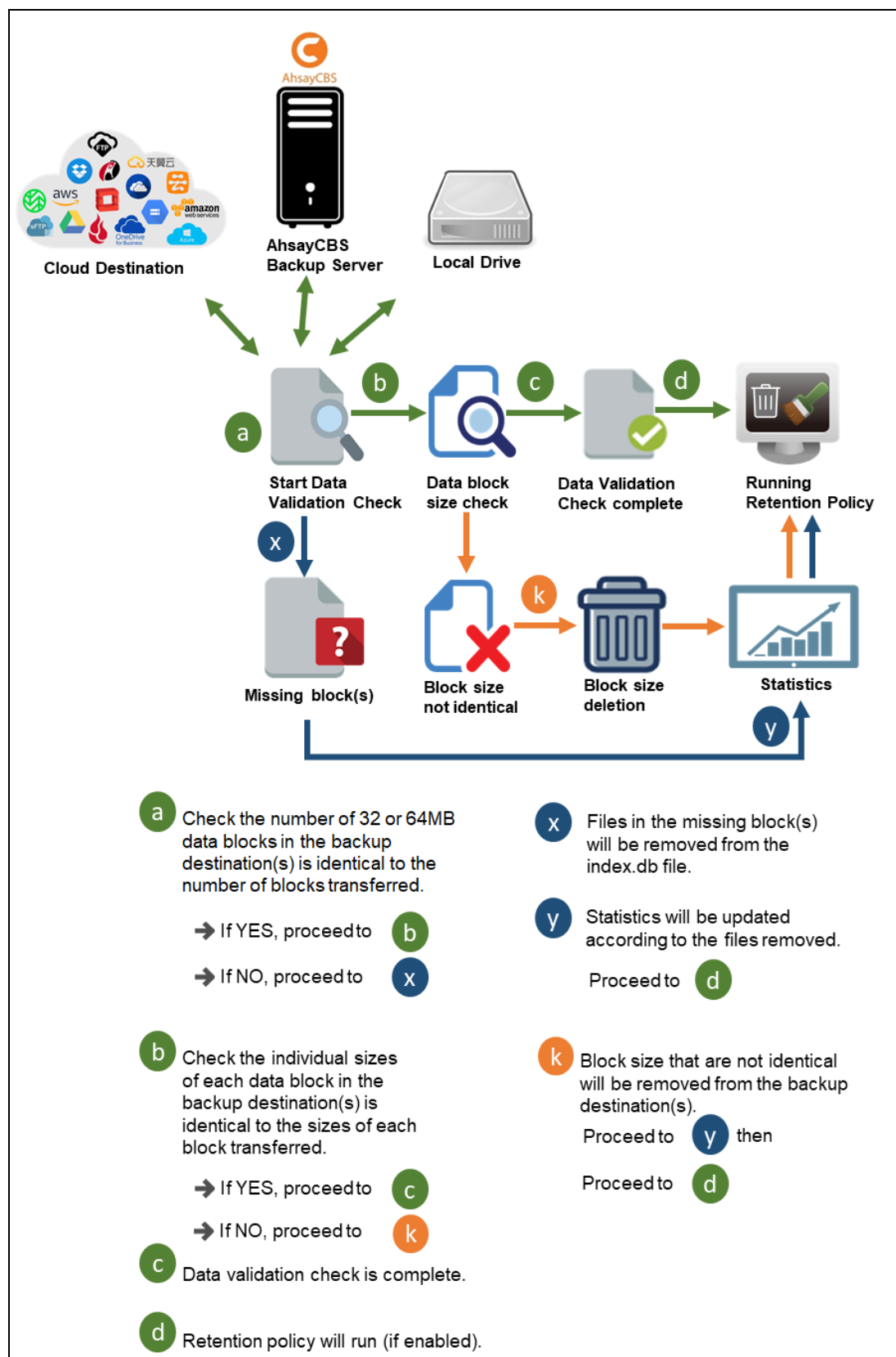


11.2.2 Completed Backup Job



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

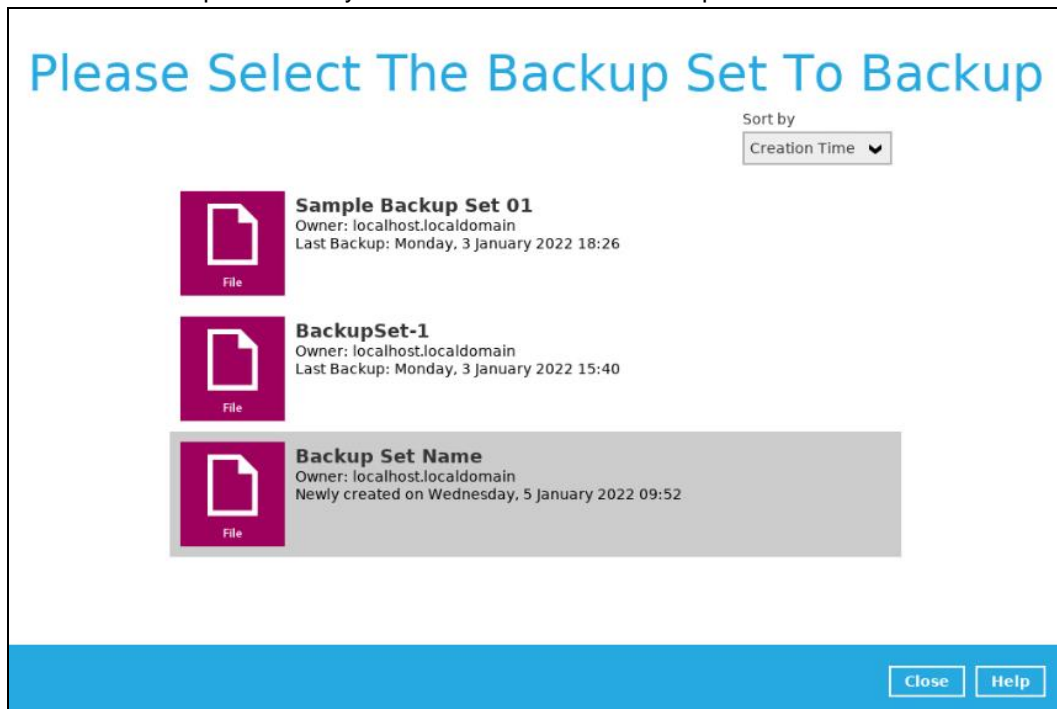
Login to the AhsayOBM application according to the instructions in [Chapter 7: Logging in to AhsayOBM](#).

12.2 Start a Manual Backup

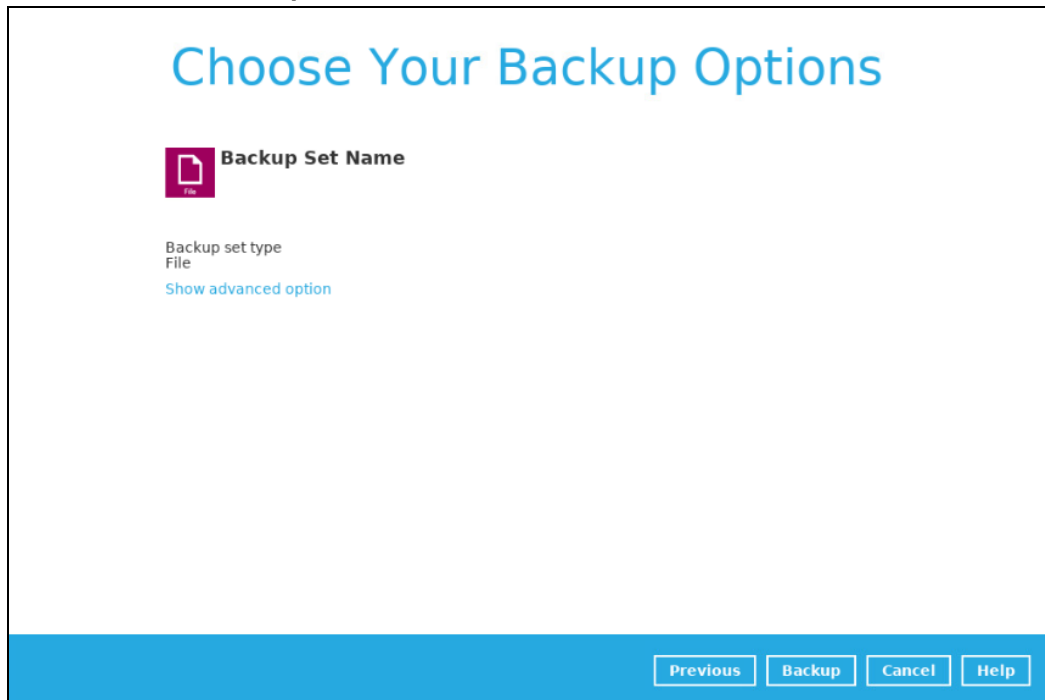
1. Click **Backup** on the main interface of AhsayOBM.




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**.



Choose Your Backup Options

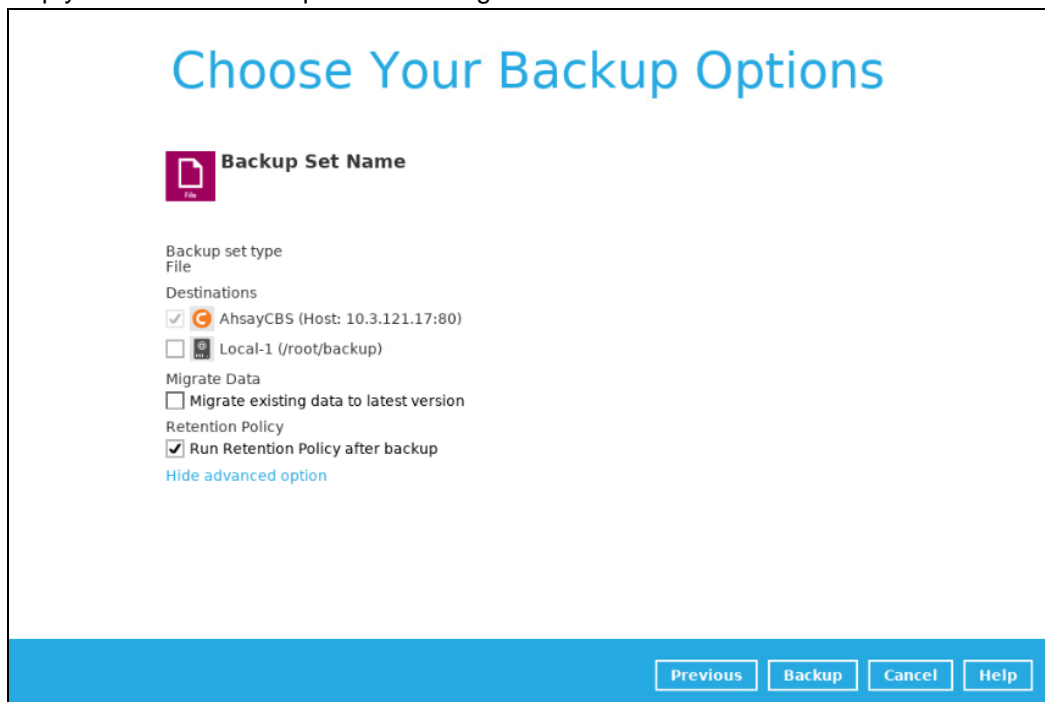
 Backup Set Name

Backup set type
File


[Show advanced option](#)

Previous Backup Cancel Help

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.





Choose Your Backup Options

 Backup Set Name

Backup set type
File

Destinations

☒  AhsayCBS (Host: 10.3.121.17:80)

☐  Local-1 (/root/backup)

Migrate Data

☐ Migrate existing data to latest version

Retention Policy

☒ Run Retention Policy after backup

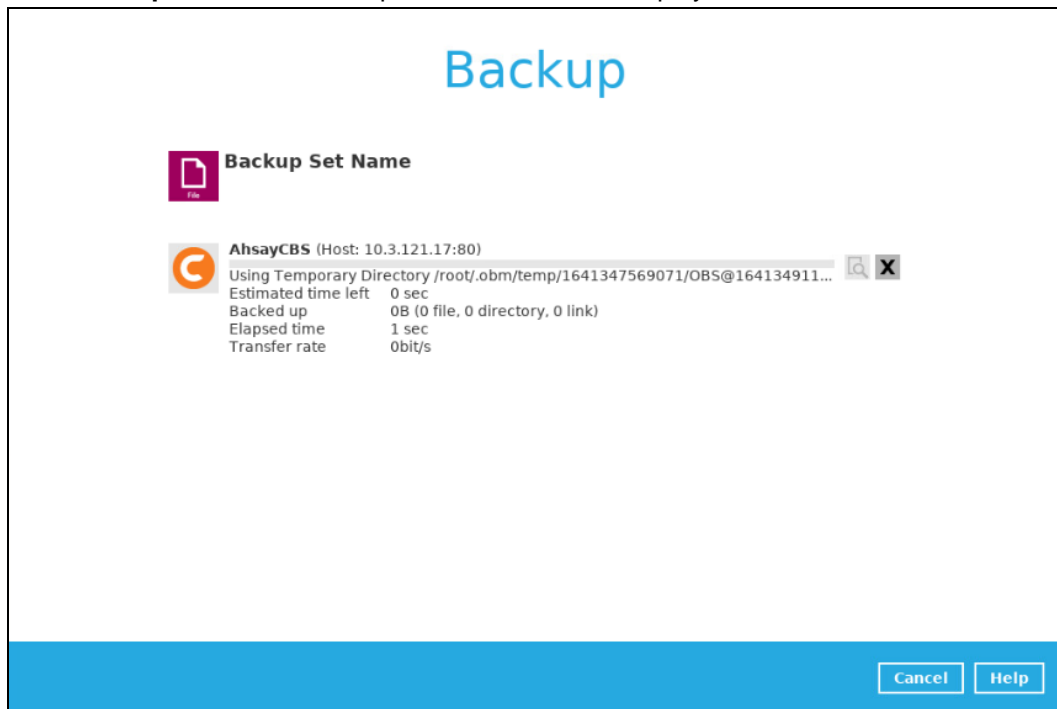
[Hide advanced option](#)

Previous Backup Cancel Help

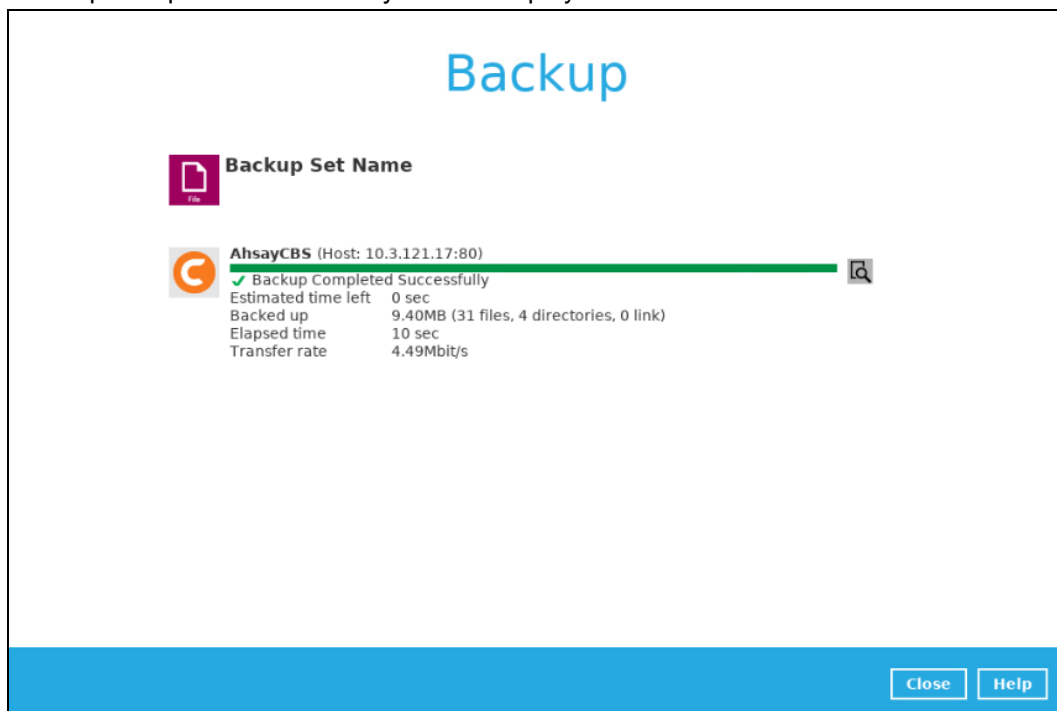
NOTE


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](#).

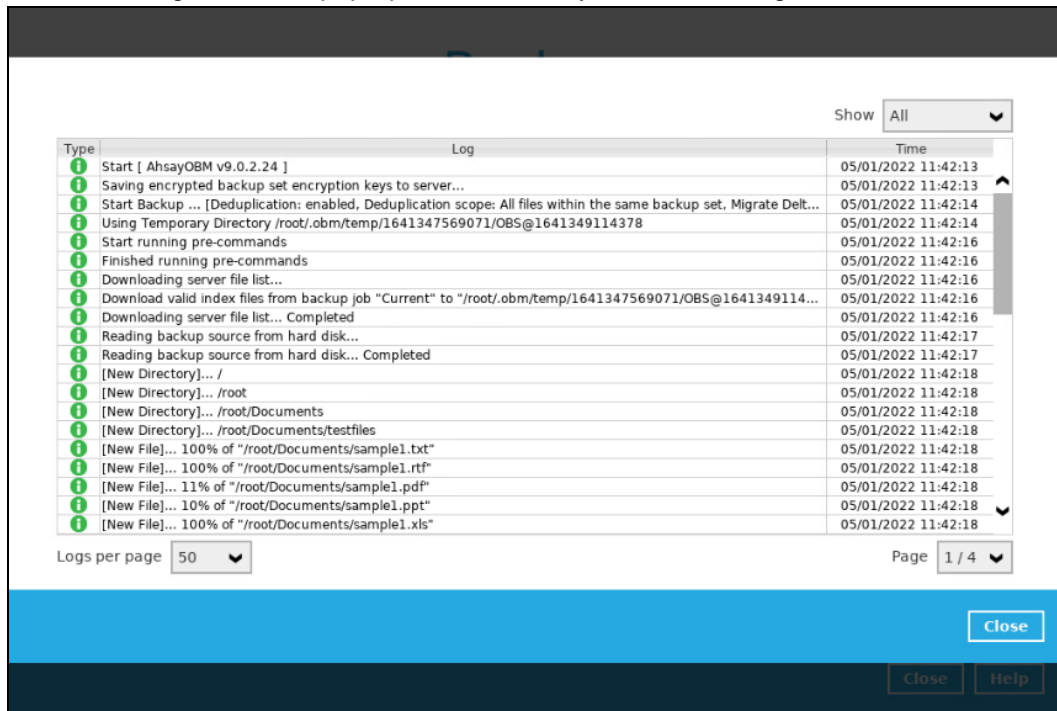
5. Click **Backup** to start the backup. The status will be displayed.



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.



The screenshot shows a log viewer window with a table of log entries. The table has three columns: Type, Log, and Time. The log entries show the progress of a backup job, including starting the backup, saving encryption keys, downloading server file lists, and reading backup sources. The window includes a 'Show' dropdown menu set to 'All', a 'Logs per page' dropdown set to '50', and a 'Page' indicator showing '1 / 4'. There are 'Close' and 'Help' buttons at the bottom right.

Type	Log	Time
i	Start [AhsayOBM v9.0.2.24]	05/01/2022 11:42:13
i	Saving encrypted backup set encryption keys to server...	05/01/2022 11:42:13
i	Start Backup ... [Deduplication: enabled, Deduplication scope: All files within the same backup set, Migrate Delt...	05/01/2022 11:42:14
i	Using Temporary Directory /root/.obm/temp/1641347569071/OBS@1641349114378	05/01/2022 11:42:14
i	Start running pre-commands	05/01/2022 11:42:16
i	Finished running pre-commands	05/01/2022 11:42:16
i	Downloading server file list...	05/01/2022 11:42:16
i	Download valid index files from backup job "Current" to "/root/.obm/temp/1641347569071/OBS@1641349114..."	05/01/2022 11:42:16
i	Downloading server file list... Completed	05/01/2022 11:42:16
i	Reading backup source from hard disk...	05/01/2022 11:42:17
i	Reading backup source from hard disk... Completed	05/01/2022 11:42:17
i	[New Directory]... /	05/01/2022 11:42:18
i	[New Directory]... /root	05/01/2022 11:42:18
i	[New Directory]... /root/Documents	05/01/2022 11:42:18
i	[New Directory]... /root/Documents/testfiles	05/01/2022 11:42:18
i	[New File]... 100% of "/root/Documents/sample1.txt"	05/01/2022 11:42:18
i	[New File]... 100% of "/root/Documents/sample1.rtf"	05/01/2022 11:42:18
i	[New File]... 11% of "/root/Documents/sample1.pdf"	05/01/2022 11:42:18
i	[New File]... 10% of "/root/Documents/sample1.ppt"	05/01/2022 11:42:18
i	[New File]... 100% of "/root/Documents/sample1.xls"	05/01/2022 11:42:18

Logs per page 50 Page 1 / 4

Close

Close Help

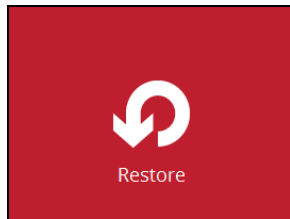
13 Restoring Data

13.1 Login to AhsayOBM

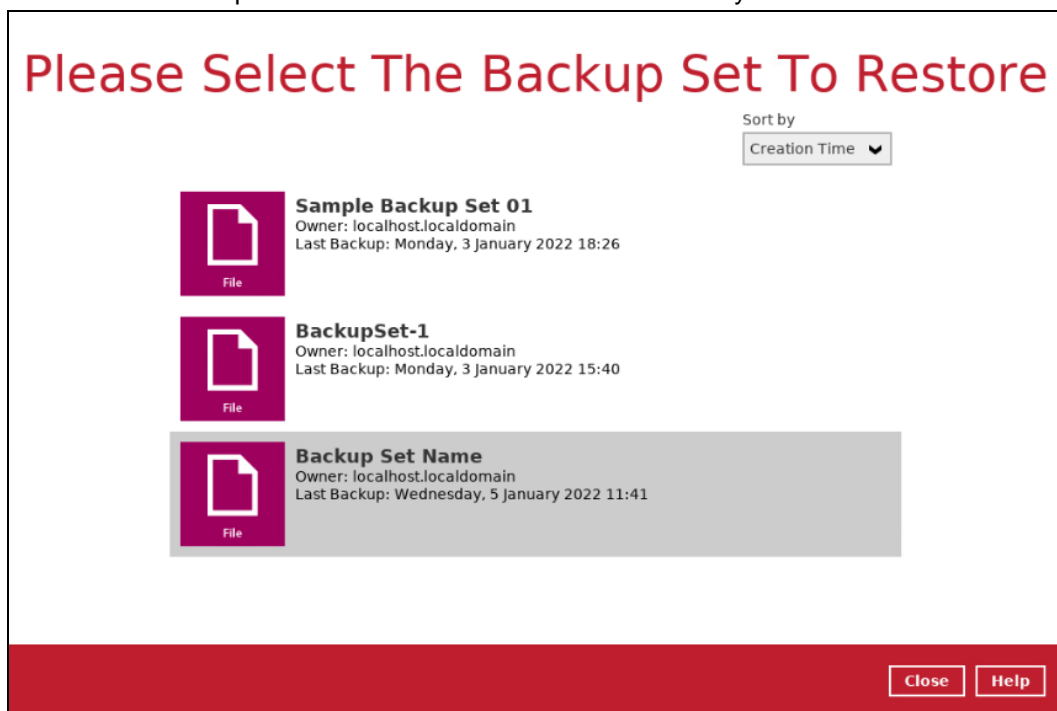
Login to the AhsayOBM application according to the instructions in [Chapter 7: Logging in to AhsayOBM](#).

13.2 Restore Data

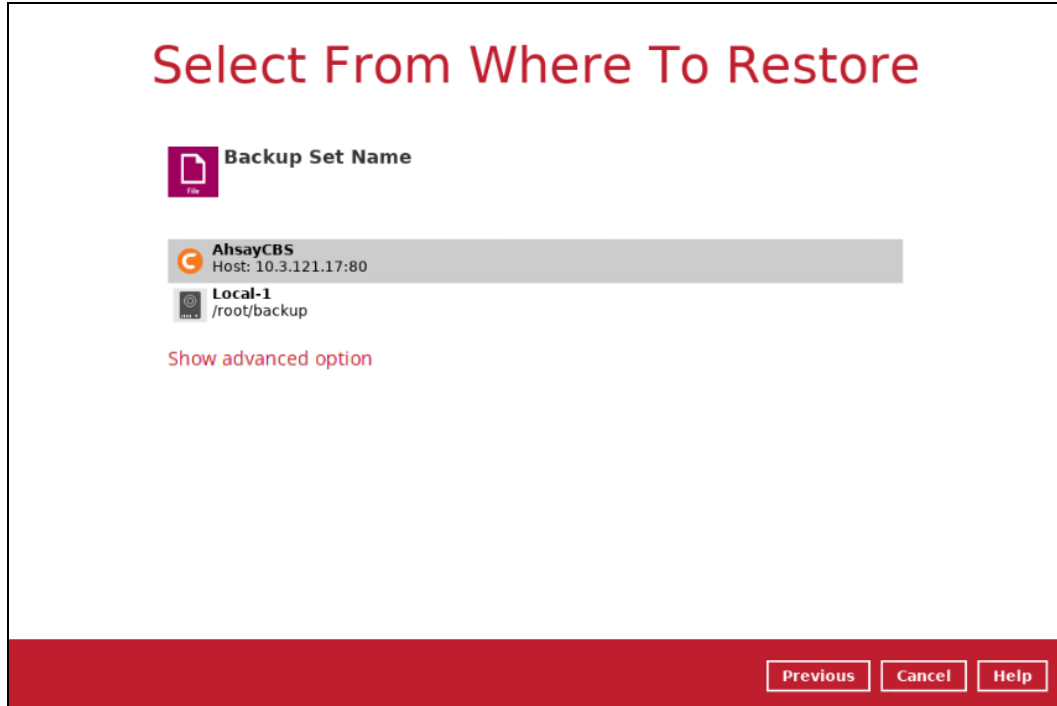
1. Click **Restore** on the AhsayOBM main interface.




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.



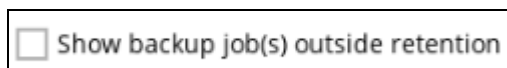
3. Click on the location from which you would like to restore the data from.



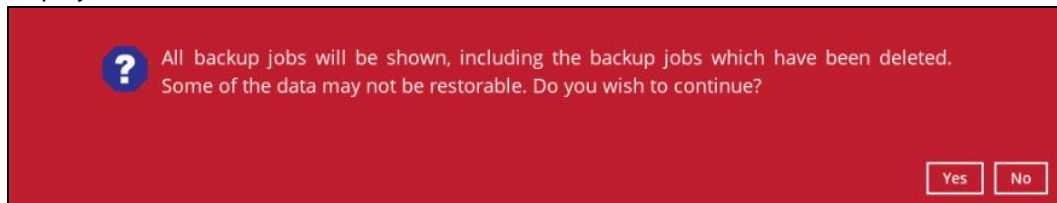
You may configure the **Temporary directory for storing restore files** by clicking **Show advanced option**. By default, the temporary files are stored under the temp directory of the user profile directory. In case the same directory path does not exist in the computer where AhsayOBM is running, you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



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



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



5. 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.

Select what to restore

Choose from files as of job ▼ 27/09/2022 ▼ Latest ▼ ☒ Show backup job(s) outside retention

Choose from files as of job

Choose from ALL files

backup file

Name	Size
backup file	

Select what to restore

Choose from files as of job ▼ 27/09/2022 ▼ Latest ▼ ☒ Show backup job(s) outside retention

27/09/2022

Folders

Name	Size
------	------

Select what to restore

Choose from files as of job ▼ 27/09/2022 ▼ Latest ▼ ☒ Show backup job(s) outside retention

Folders

- AhsayCBS
 - backup file
 - Archive
 - Documents
 - Excel

16:33

16:31

15:45

Name	Size
------	------

NOTE

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

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

Select Your Files To Be Restored

Select what to restore

Choose from ALL files ▼

Show filter

Folders

- AhsayCBS
 - /
 - root
 - Documents

Name	Size	Date modified
testfiles		
sample1.pdf	567KB	09/12/2021 18:28
sample1.ppt	891KB	09/12/2021 18:29
sample1.rtf	116KB	15/12/2021 17:34
sample1.txt	14KB	05/01/2022 12:00
sample1.txt	14KB	05/01/2022 11:53
sample1.txt	4KB	15/12/2021 17:33
sample1.xls	16KB	09/12/2021 18:30
sample2.pdf	64KB	09/12/2021 18:29
sample2.ppt	518KB	09/12/2021 18:29
sample2.rtf	1KB	09/12/2021 18:31
sample2.txt	2KB	09/12/2021 18:25
sample2.xls	7KB	09/12/2021 18:30
sample3.txt	3KB	09/12/2021 18:25
sample3.xls	13KB	09/12/2021 18:30
sample_640x360.avi	569KB	09/12/2021 18:26
sample_960x540.mkv	1.26MB	09/12/2021 18:27

Search

Items per page 50 Page 1 / 1

Previous Next Cancel Help

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.

	Name	Size	Date modified
<input type="checkbox"/>	testfiles		
<input type="checkbox"/>	sample1.pdf	567KB	09/12/2021 18:28
<input type="checkbox"/>	sample1.ppt	891KB	09/12/2021 18:29
<input type="checkbox"/>	sample1.rtf	116KB	15/12/2021 17:34
<input checked="" type="checkbox"/>	sample1.txt	14KB	05/01/2022 12:00
<input checked="" type="checkbox"/>	sample1.txt	14KB	05/01/2022 11:53
<input type="checkbox"/>	sample1.txt	4KB	15/12/2021 17:33
<input type="checkbox"/>	sample1.xls	16KB	09/12/2021 18:30
<input type="checkbox"/>	sample2.pdf	64KB	09/12/2021 18:29

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.

6. 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.

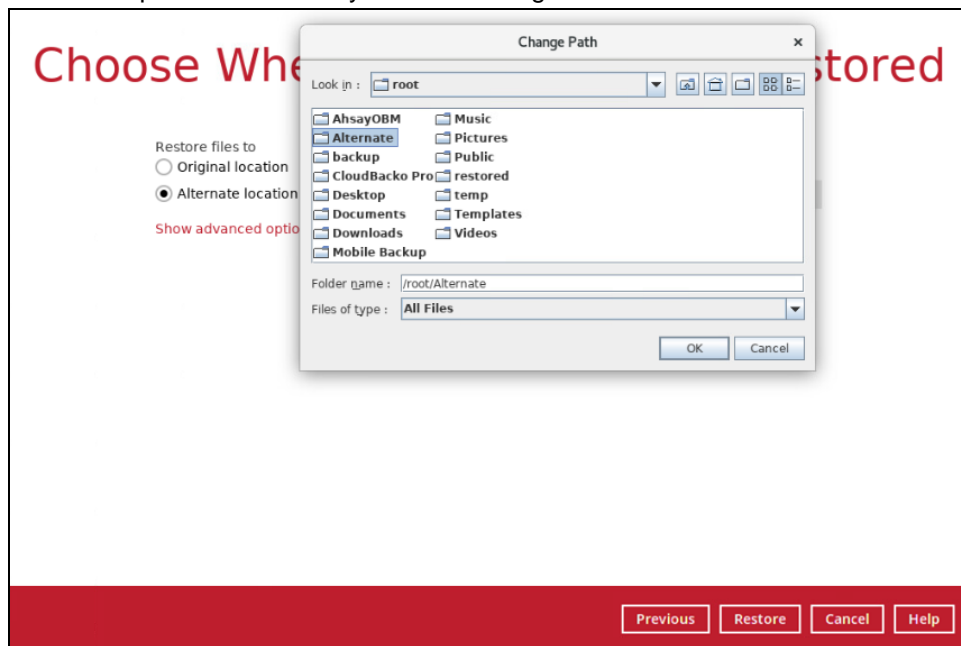
Choose Where The Files To Be Restored

Restore files to

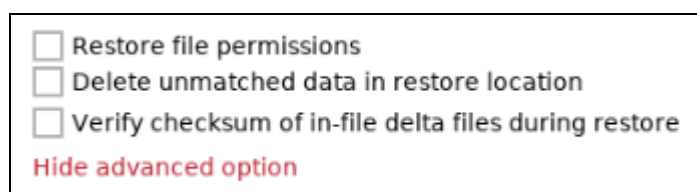
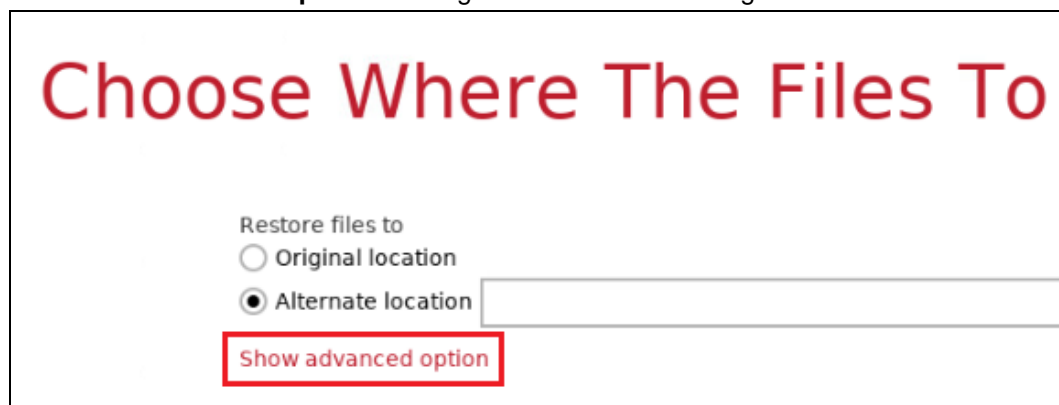
☒ Original location
 ☐ Alternate location

[Show advanced option](#)

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



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.



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

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

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

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

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

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

WARNING

Please exercise extra caution when enabling this feature. Consider what data in the restore 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.

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

Choose Where The Files To Be Restored

Restore files to


☒ Original location


☐ Alternate location

[Show advanced option](#)

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

Restore

 **Backup Set Name**

 **AhsayCBS (Host: 10.3.121.17:80)**

✓ Restore Completed Successfully

Estimated time left 0 sec

Restored 9.43MB (33 files)

Elapsed time 2 sec

Transfer rate 8.66Mbit/s

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.

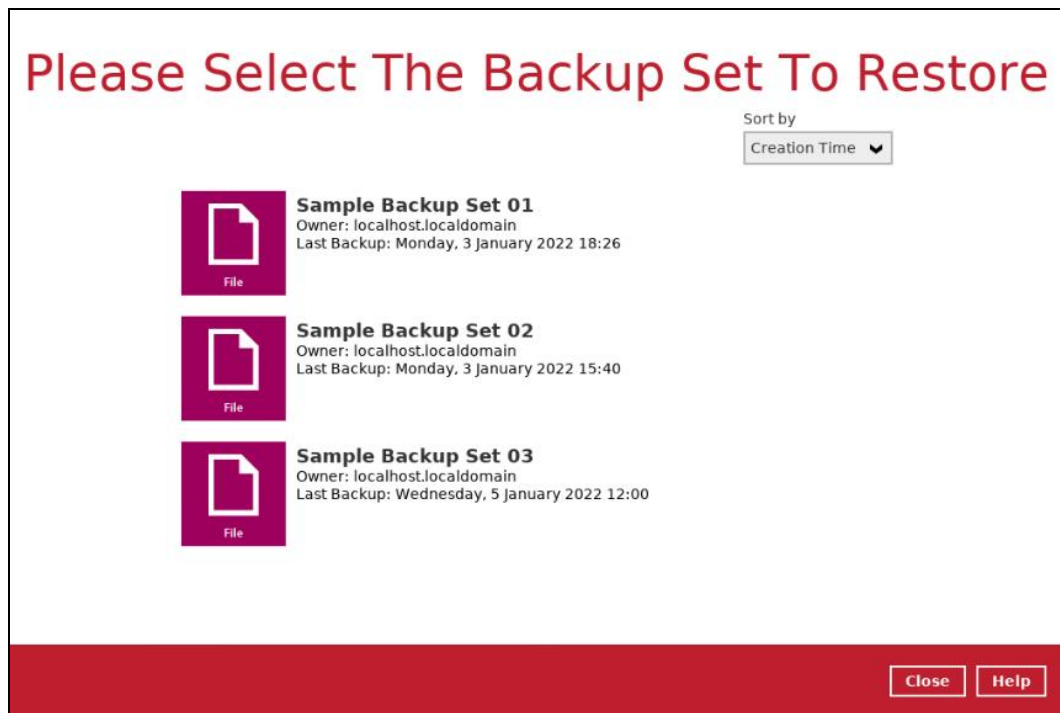
- ▶ **Ends With**

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

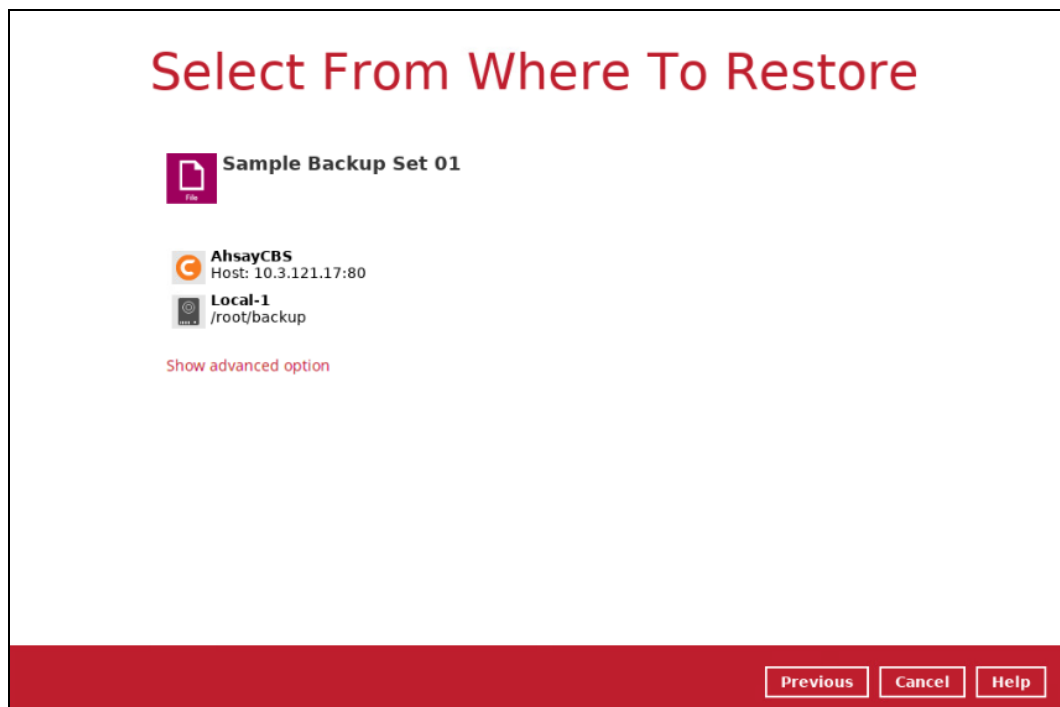
It also has the **Match Case** function, which serves as an additional accuracy when searching for any specific directories, files, folders, and mails.

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.

Select Your Files To Be Restored

Select what to restore

Choose from files as of job 03/01/2022 Latest ☒ Show backup job(s) outside retention

Show filter

Folders

AhsayCBS

/

root

Name Size Date modified

/

Search

Items per page 50 Page 1 / 1

Previous Next Cancel Help

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

Search

Look in

Change

☒ Search subfolders

Kind Type Pattern

Files and Directories contains

Match case

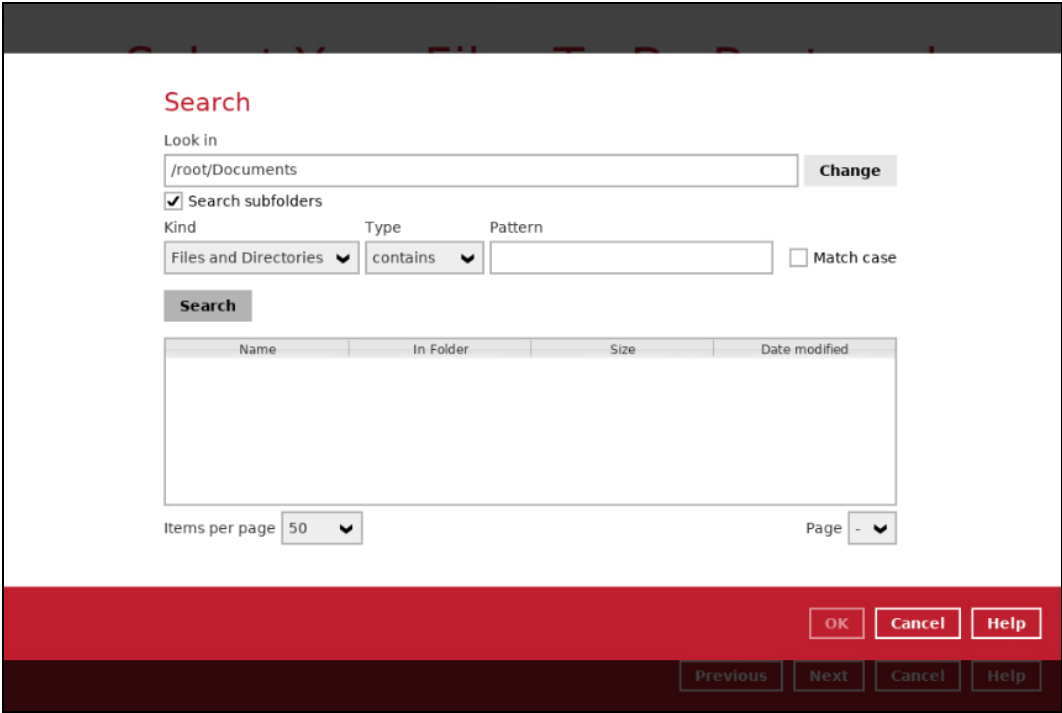
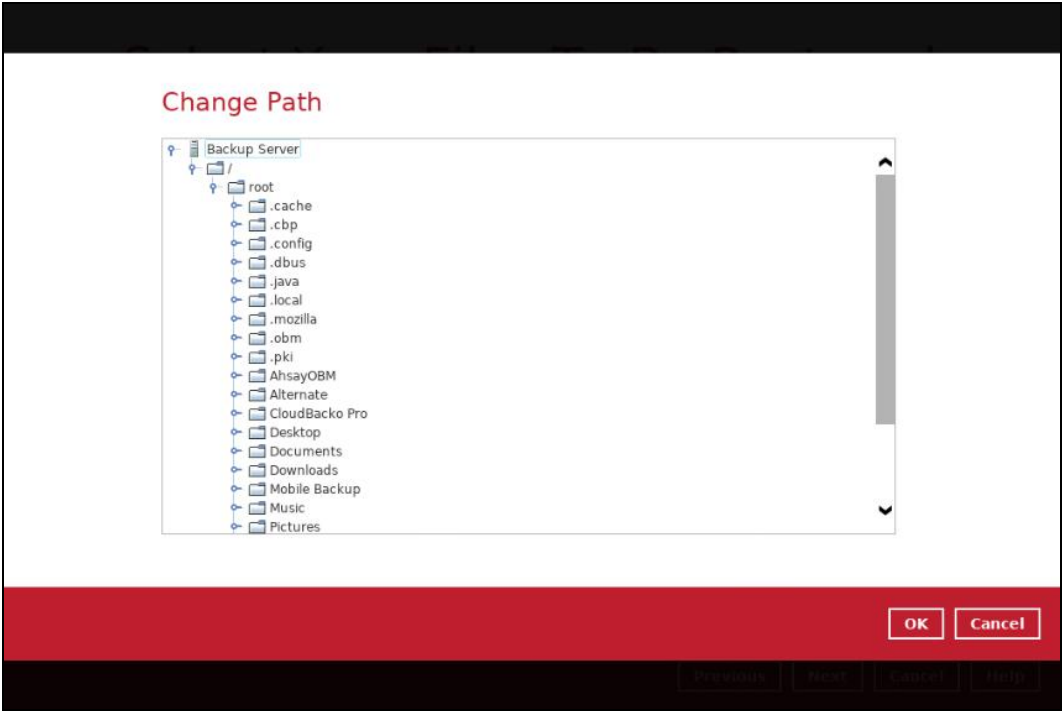
Search

Name In Folder Size Date modified

Items per page 50 Page -

OK Cancel Help

Previous Next Cancel Help



7. Tick “Search subfolders” to include available subfolders upon searching.

☒ Search subfolders

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

- Files and Directories
- Files only
- Directories

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

- Contains
- Exact
- Starts With
- Ends With

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

Pattern

☒ Match case

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.

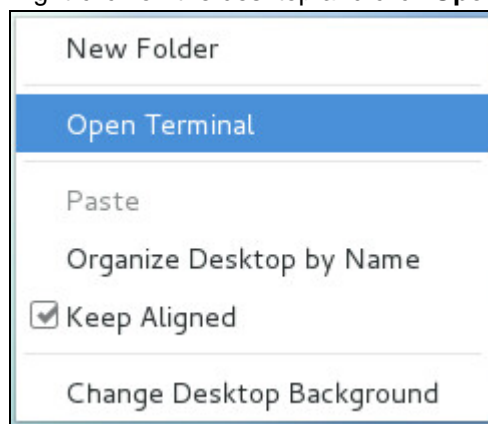
Appendix

Appendix A: Uninstall AhsayOBM (SH online installer)

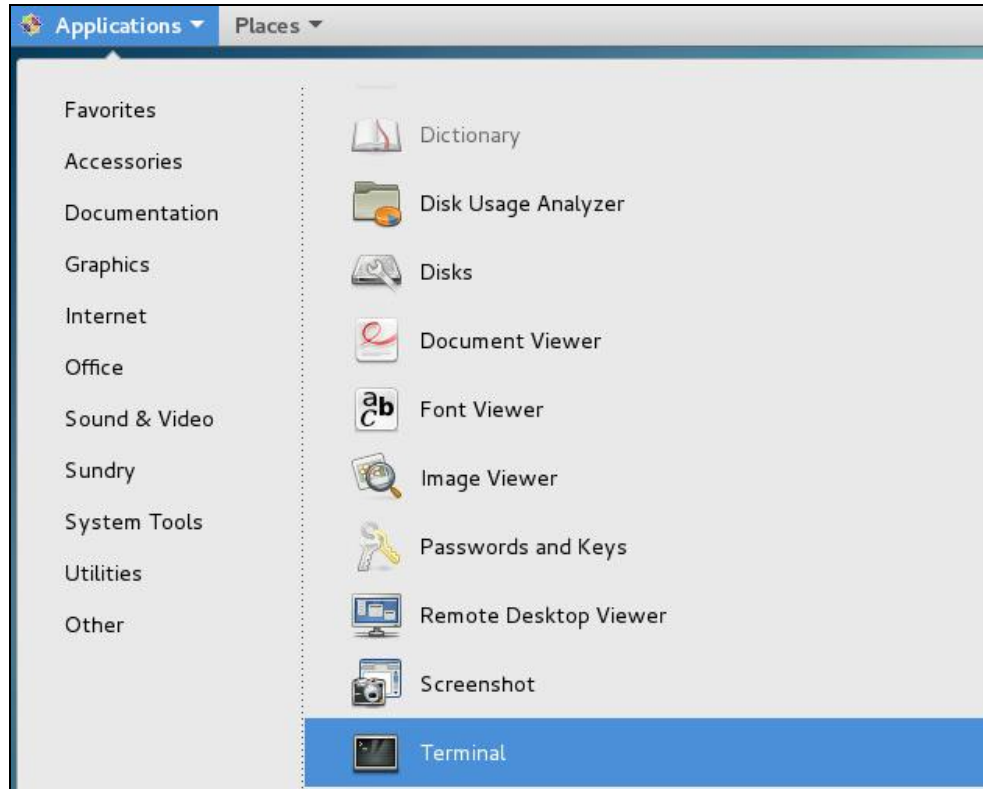
1. Log in to a Linux machine using the root account. (Alternatively, you can remotely invoke the GUI of another Linux machine using SSH client.)



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

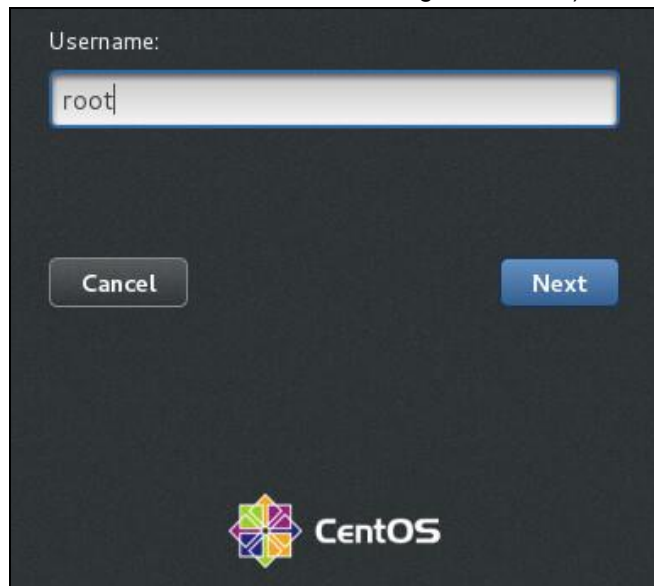
Shutting down Scheduler
Wait 5 seconds before Scheduler exits
Kill running Ahsay Online Backup Manager
Kill Process by Image Name: /usr/local/obm/jvm/bin/bJW
Ignore Process by Image Name:
Kill Process by Image Name: /usr/local/obm/jvm/bin/bschJW
Ignore Process by Image Name:
Kill Process by Image Name: /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
```

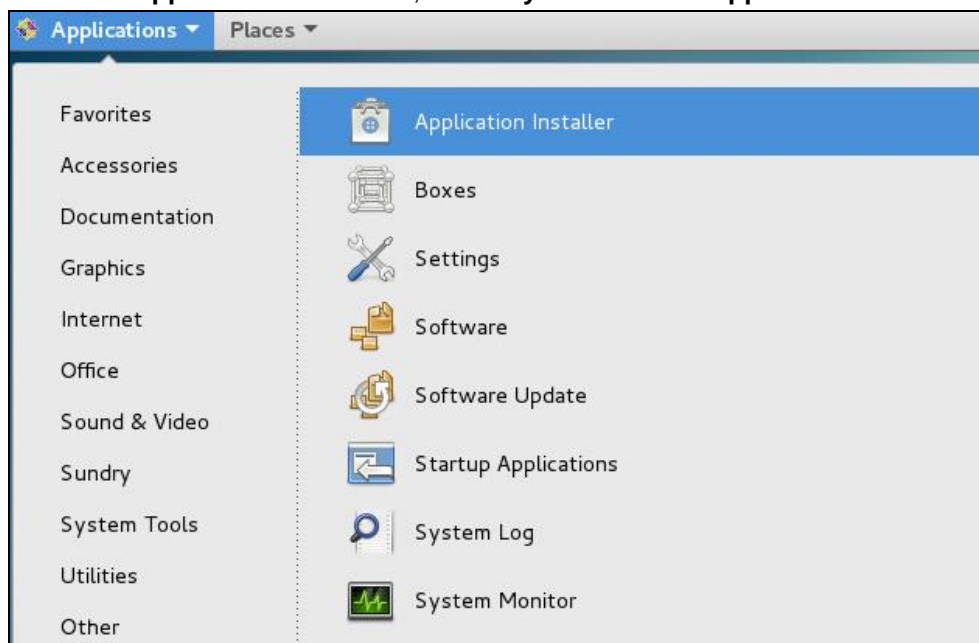
5. After successful uninstallation, AhsayOBM will be removed from the **Applications**.

Appendix B: Uninstall AhsayOBM (RPM online installer)

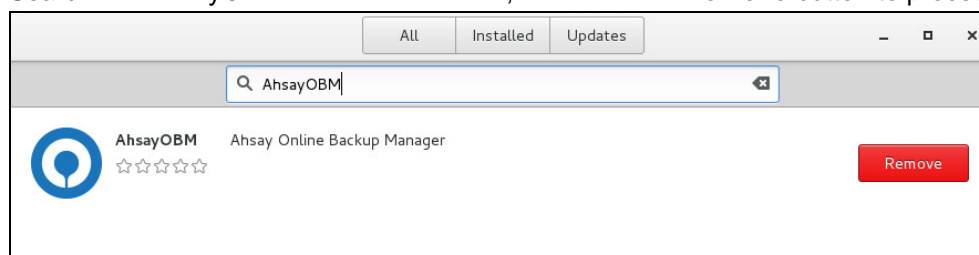
1. Log in to a Linux machine using the root account. (Alternatively, you can remotely invoke the GUI of another Linux machine using SSH client.)



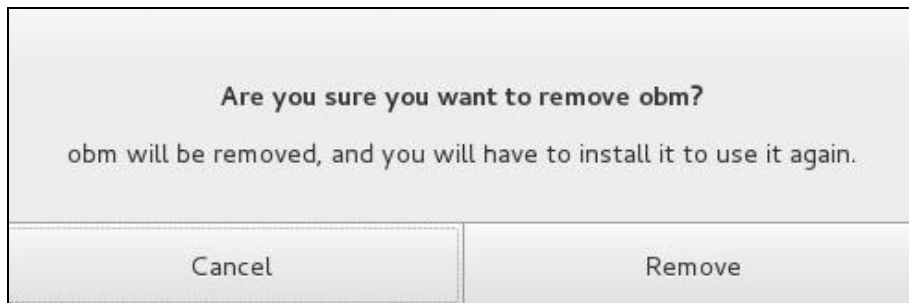
2. Under the **Applications** menu bar, select **System Tools > Application Installer**.



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



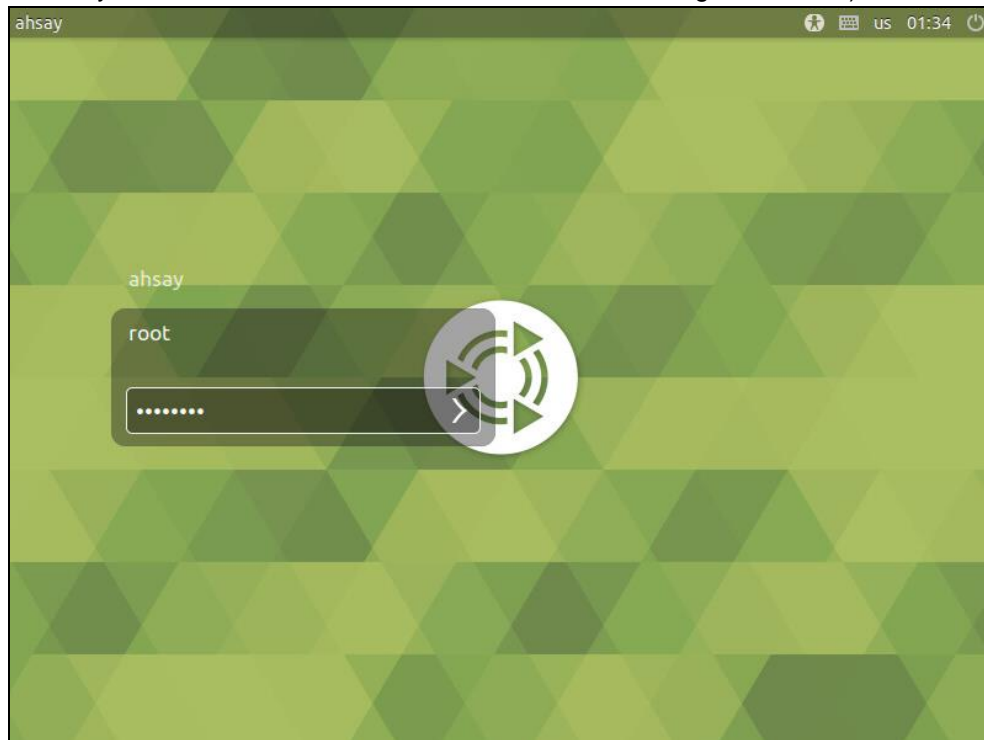
4. Click **Remove** to uninstall AhsayOBM.



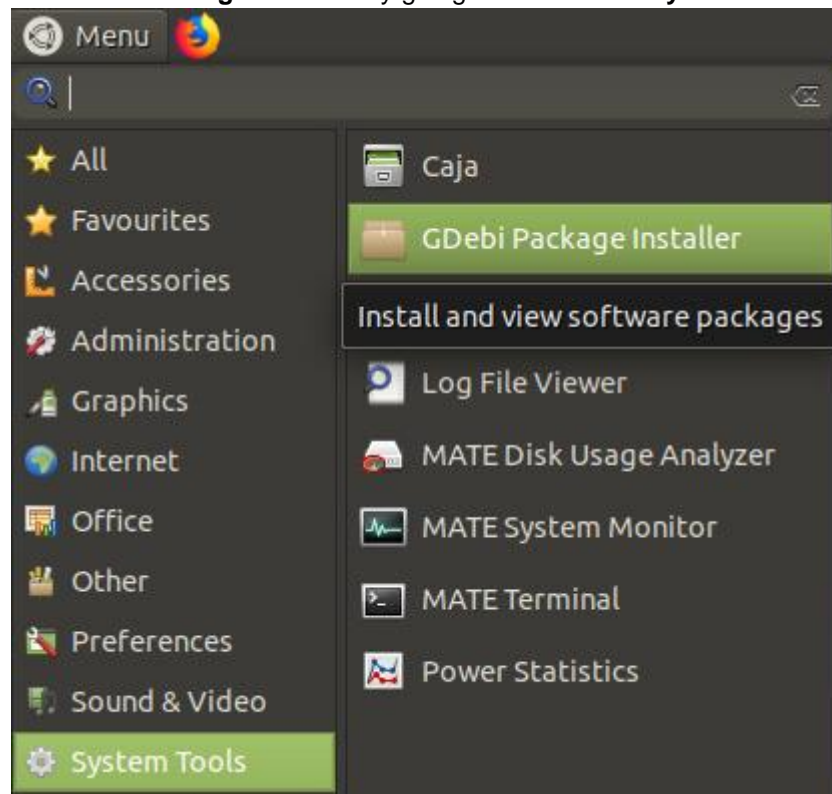
5. After successful uninstallation, AhsayOBM will be removed from the **Applications**.

Appendix C: Uninstall AhsayOBM (DEB online installer)

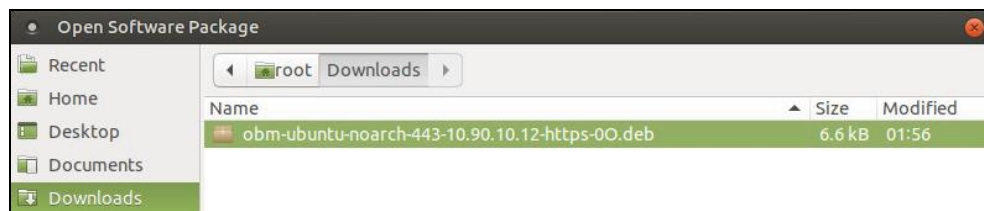
1. Log in to a Debian or Ubuntu machine using the root account. (Alternatively, you can remotely invoke the GUI of another Debian or Ubuntu using SSH client.)



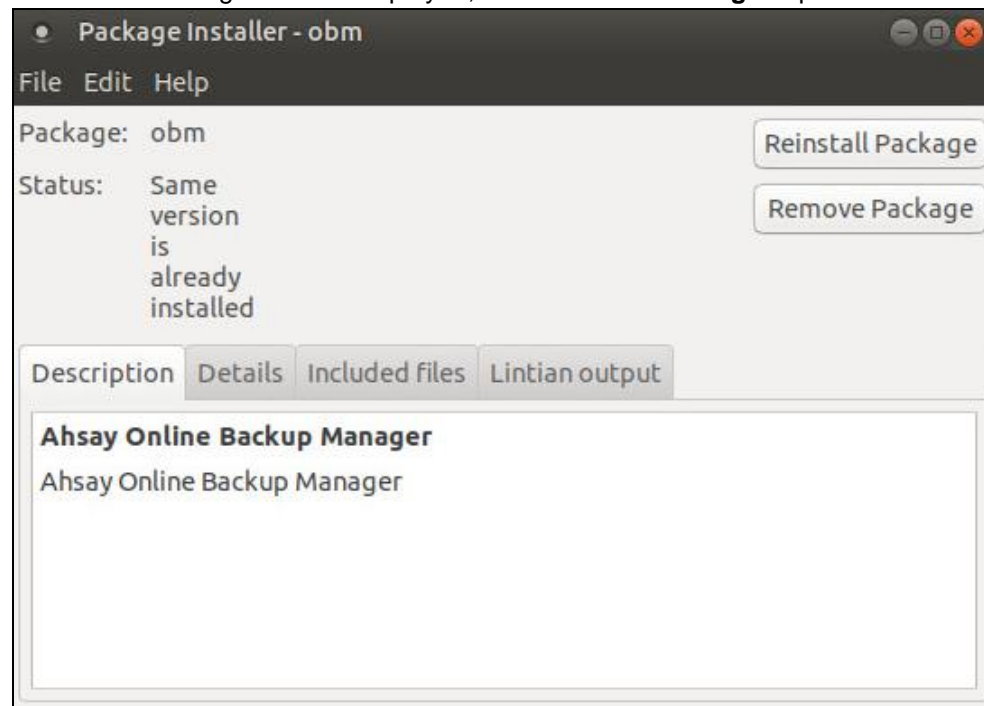
2. Locate the **Package Installer** by going to the **Menu > System Tools > Package Installer**.



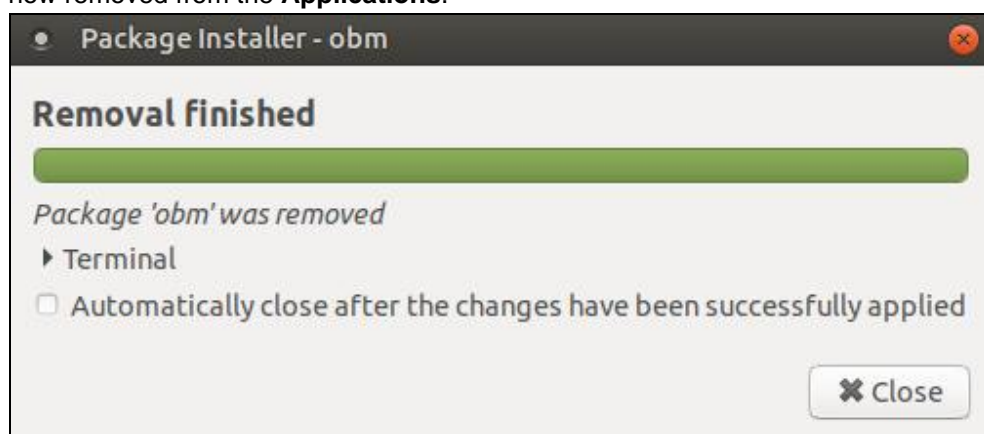
3. Go to **Downloads** and select the AhsayOBM **DEB** installation package file.



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:

- ❶ **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"

- ❷ **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:

- ❶ **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
    fi
fi
```

```

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:

- ❶ **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"

- ❷ **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"

- ❸ **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;
    fi
done

```

```

        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:

- ❶ **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"
- ❷ **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"
- ❸ **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
- ❹ **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"
- ❺ **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
- ❻ **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"
- ❼ **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:

- ❶ **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"
- ❷ **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"
- ❸ **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"
- ❹ **RESTORE_FROM** – this is the file or directory that you would like to restore.

e.g. RESTORE_FROM="/Data"
- ❺ **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"
- ❻ **RESTORE_PERMISSION** – you can set the file permission here.

e.g. RESTORE_PERMISSION="N" or RESTORE_PERMISSION="Y"
- ❼ **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"
- ❽ **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
- ❾ **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

- ❶ **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"

- ❷ **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*, *startsWith*, *startsWithMatchCase*, *endsWith* and *endsWithMatchCase*.

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"

- ❸ **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"

- ❹ **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
```

```

        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:

- ❶ **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"`
- ❷ **ENCRYPT_KEY** – this is the encryption key of the backup set. You can leave this blank if you backup set is not encrypted.
e.g. `ENCRYPT_KEY="RU5DUIIQVF9LRVk="`
- ❸ **DECRYPT_TO** – this is the directory where you want to store the decrypted backup file.
e.g. `DECRYPT_TO="/tmp"`
- ❹ **DECRYPT_FROM** – this is the file or directory that you would like to decrypt.
e.g. `DECRYPT_FROM="/Data"`
- ❺ **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"`
- ❻ **RESTORE_PERMISSION** – you can set the file permission here.
e.g. `RESTORE_PERMISSION="N"` or `RESTORE_PERMISSION="Y"`
- ❼ **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"`
- ❽ **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
- ❾ **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

- ❶ **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"

- ❷ **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*, *startsWith*, *startsWithMatchCase*, *endsWith* and *endsWithMatchCase*.

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"

- ❸ **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"

- ❹ **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="RU5DU1lQVF9LRVk="
# |
# |
# | 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}"

#####
#####

```

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

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:

- ❶ **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"

- ❷ **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"

- ❸ **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"

- ❹ **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

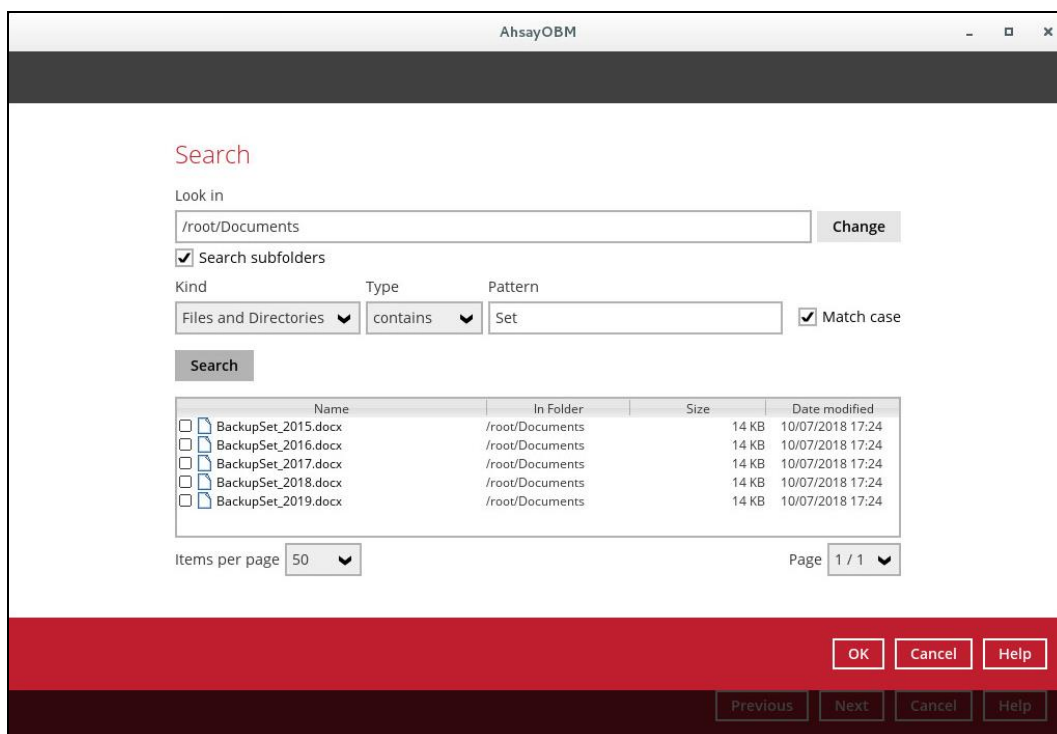
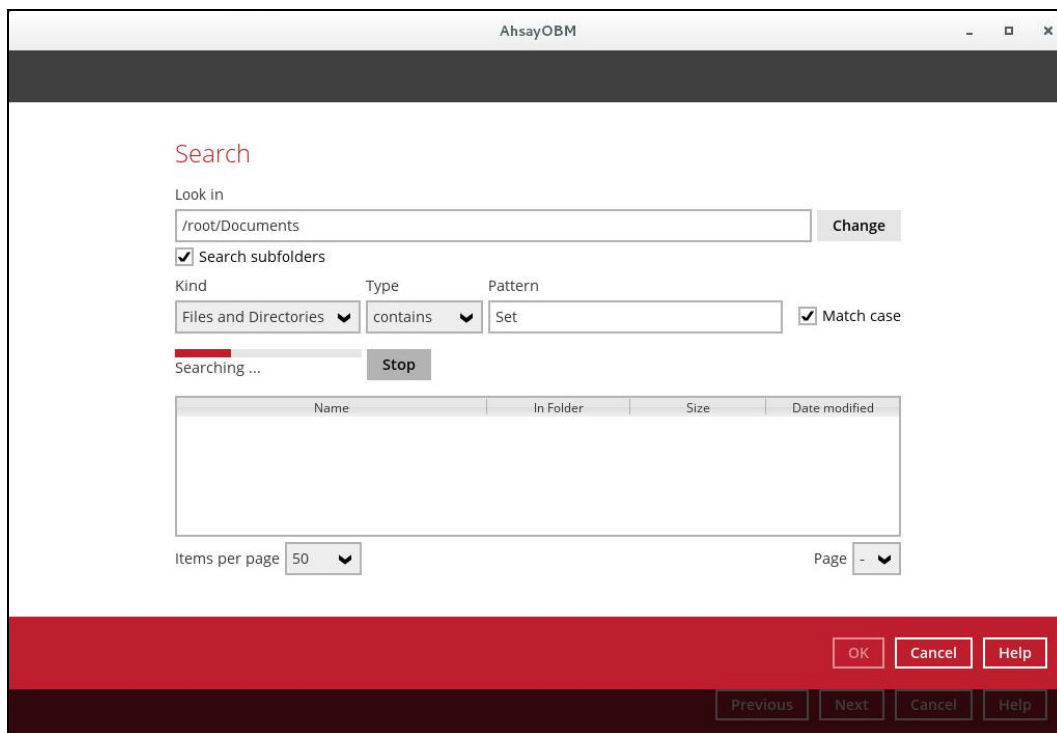
Location:	/root/Documents
Search subfolders:	True
Kind:	Files and Directories
Type:	Contains
Pattern:	Set
Match Case:	True

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

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

- "Look in" field with the value "/root/Documents" and a "Change" button.
- A checked checkbox for "Search subfolders".
- "Kind" dropdown menu set to "Files and Directories".
- "Type" dropdown menu set to "contains".
- "Pattern" text field with the value "Set".
- A checked checkbox for "Match case".
- A "Search" button.

Below these settings is a table with the following headers: "Name", "In Folder", "Size", and "Date modified". The table is currently empty. At the bottom of the dialog, there are two dropdown menus: "Items per page" set to "50" and "Page" set to "-". At the very bottom, there are four buttons: "OK", "Cancel", "Help", and "Previous".



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](#).

AhsayOBM

Search

Look in
/root/Documents Change

☒ Search subfolders

Kind Type Pattern
Files only starts with A ☒ Match case

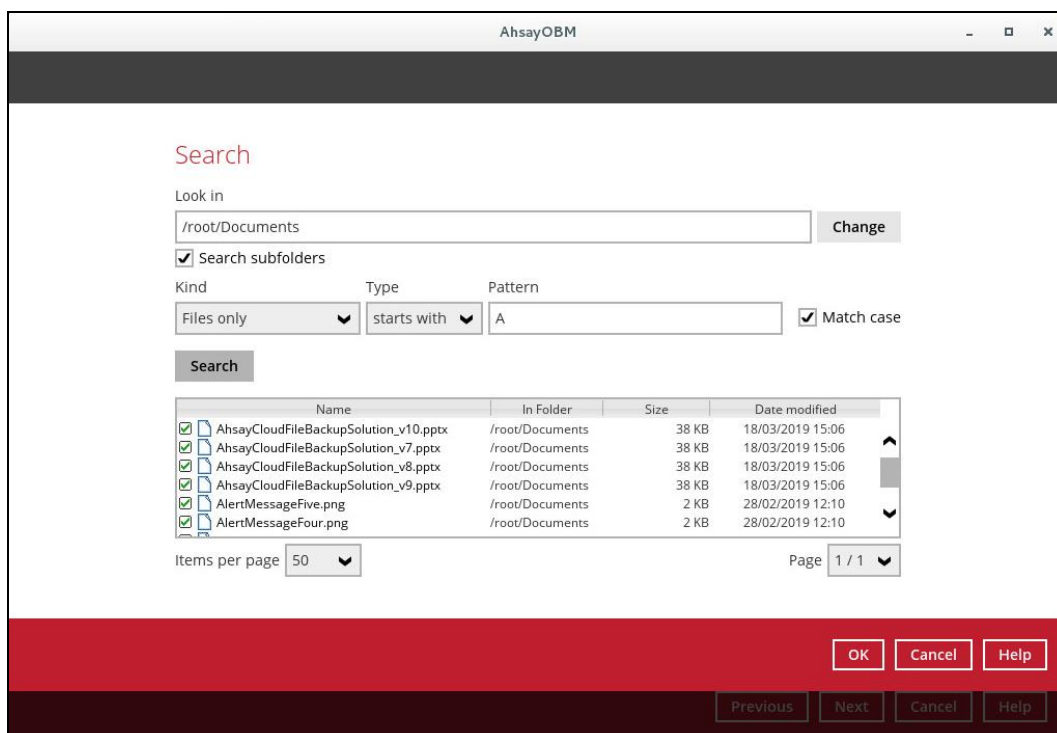
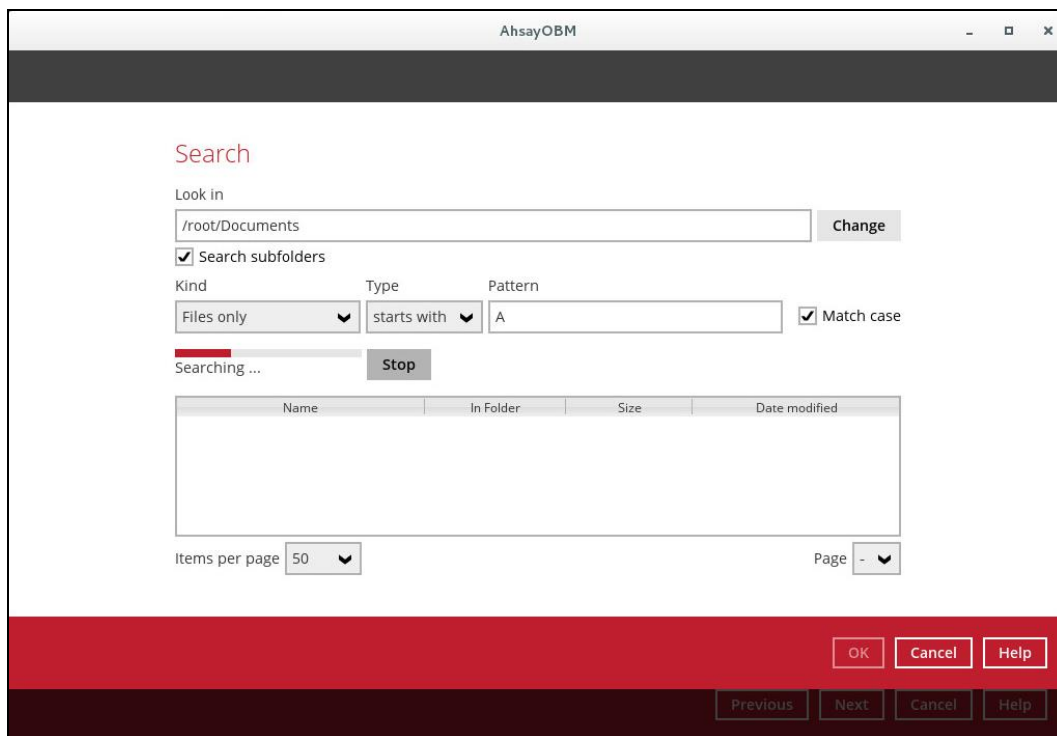
Search

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

Items per page 50 Page -

OK Cancel Help

Previous Next Cancel Help



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.

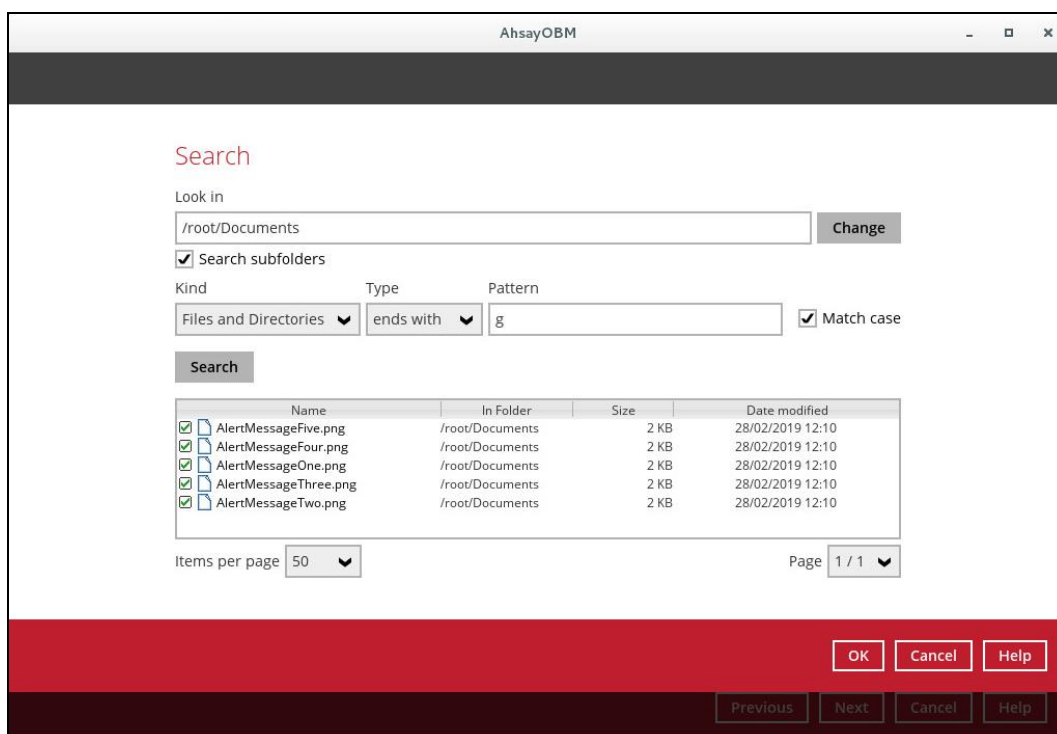
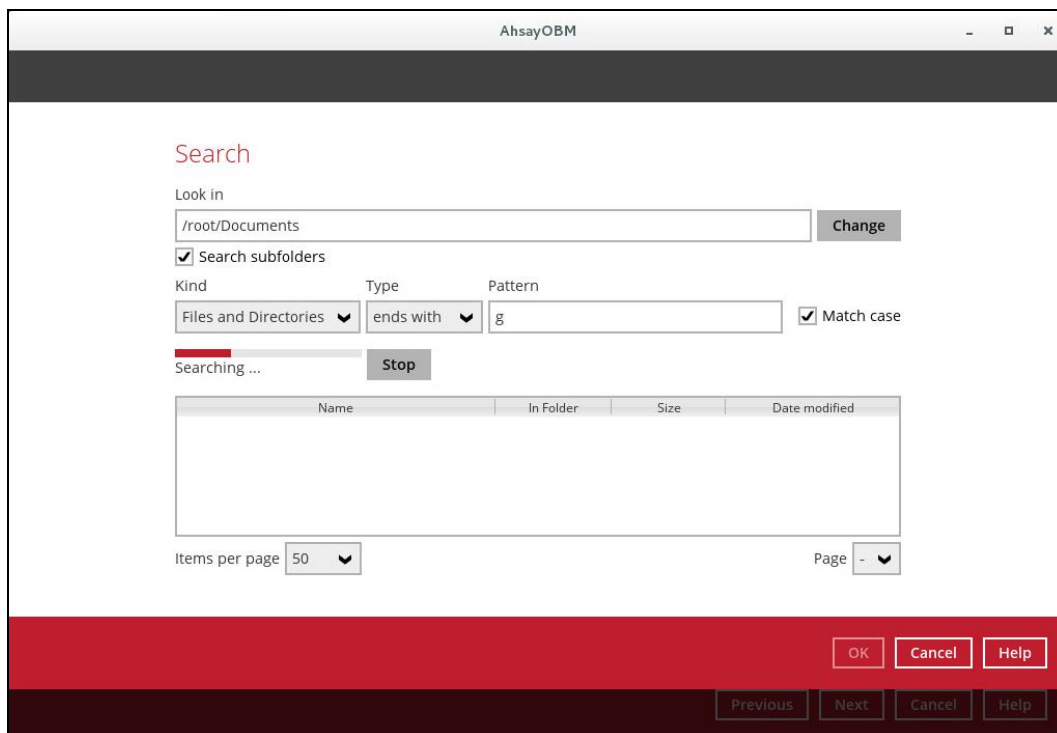
The restore filter setting includes the Search subfolder and Match case set to true. Meaning, the filter will include all available subfolders in \Documents upon searching. And it will strictly search only the specified pattern and case which starts with 'A'.

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](#).

The screenshot shows the AhsayOBM Search dialog box. The title bar reads "AhsayOBM". The main area is titled "Search" in red. Below the title, there is a "Look in" field with the value "/root/Documents" and a "Change" button. A checkbox labeled "Search subfolders" is checked. Below this, there are three fields: "Kind" with a dropdown menu showing "Files and Directories", "Type" with a dropdown menu showing "ends with", and "Pattern" with a text field containing "g". A "Match case" checkbox is also checked. A "Search" button is located below these fields. Below the search fields is a table with four columns: "Name", "In Folder", "Size", and "Date modified". The table is currently empty. At the bottom left, there is a label "Items per page" with a dropdown menu showing "50". At the bottom right, there is a label "Page" with a dropdown menu showing "-". At the very bottom, there is a red bar containing "OK", "Cancel", and "Help" buttons. Below the red bar, there is a dark bar containing "Previous", "Next", "Cancel", and "Help" buttons.



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.

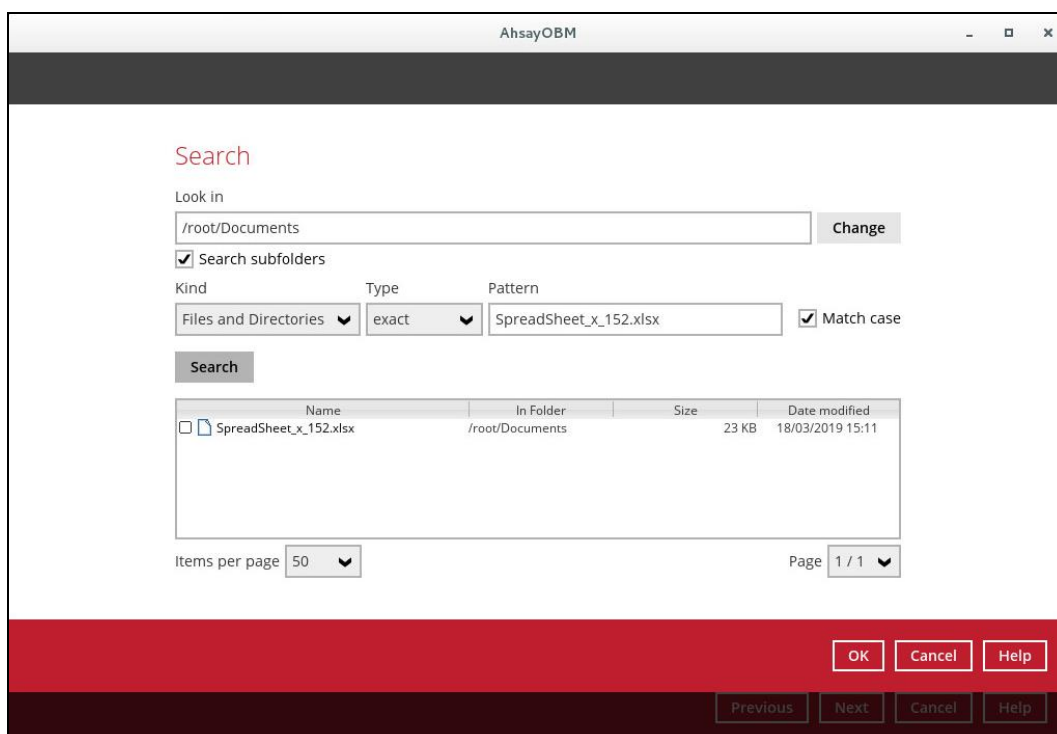
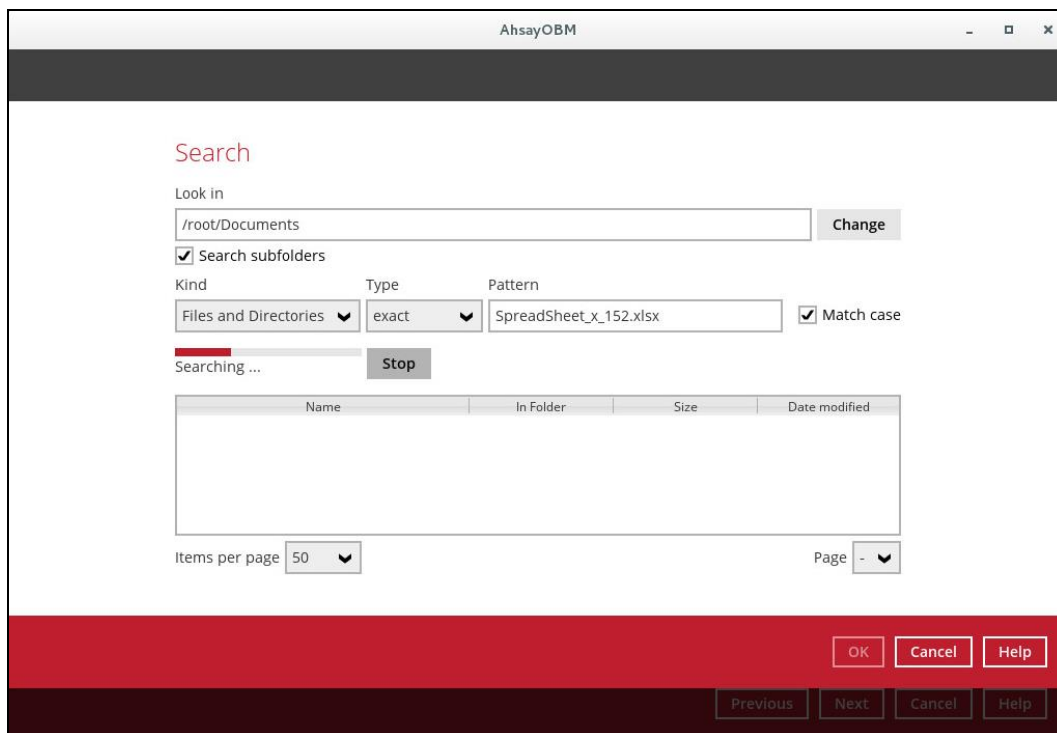
The restore filter setting includes the Search subfolder and Match case set to true. Meaning, the filter will include all available subfolders in \Documents upon searching. And it will strictly search only the specified pattern and case which starts with 'g'.

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](#).

The screenshot shows the AhsayOBM Search dialog box. The title bar reads "AhsayOBM". The main area is titled "Search" in red. Below the title, there is a "Look in" text box containing "/root/Documents" and a "Change" button to its right. Below this is a checked checkbox labeled "Search subfolders". Further down are three labels: "Kind", "Type", and "Pattern". Under "Kind" is a dropdown menu showing "Files and Directories". Under "Type" is a dropdown menu showing "exact". Under "Pattern" is a text box containing "SpreadSheet_x_152.xlsx". To the right of the "Pattern" text box is a checked checkbox labeled "Match case". Below these settings is a "Search" button. Under the "Search" button is a table with four columns: "Name", "In Folder", "Size", and "Date modified". The table is currently empty. Below the table are two dropdown menus: "Items per page" set to "50" and "Page" set to "-". At the bottom of the dialog, there is a red bar containing "OK", "Cancel", and "Help" buttons. Below the red bar is a dark bar containing "Previous", "Next", "Cancel", and "Help" buttons.



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:

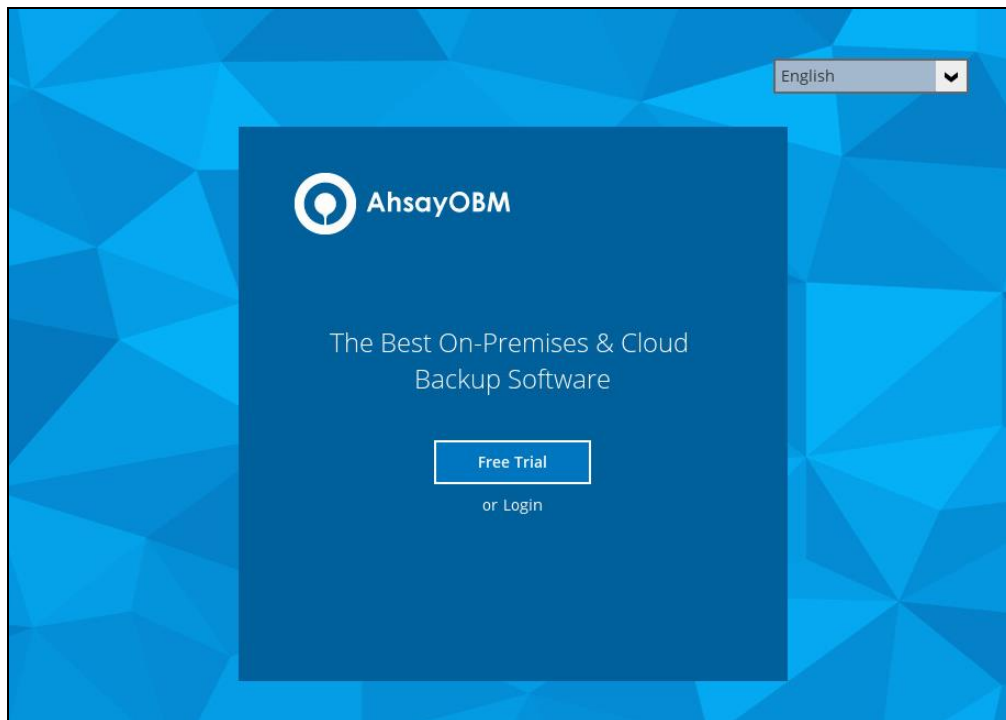
- The Free Trial button will only be displayed once when the user login for the first time. If you cannot create a free trial account kindly contact your backup service provider.
- Only alphanumeric characters and selected special characters, A to Z, 0 to 9, @, - and _, are allowed to be used for the 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

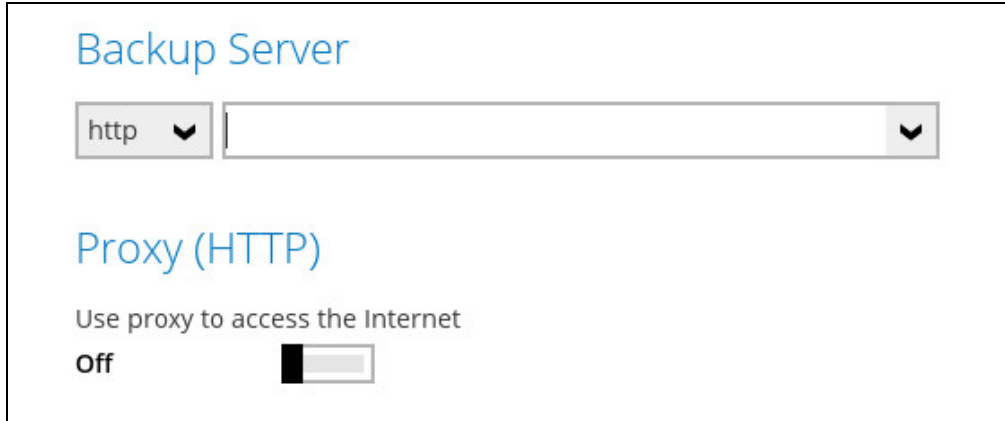
The Free Trial Registration option may not be available. This depends on the settings of your backup service provider. Please contact your backup service provider for more information.

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

1. Click on **Free Trial**.

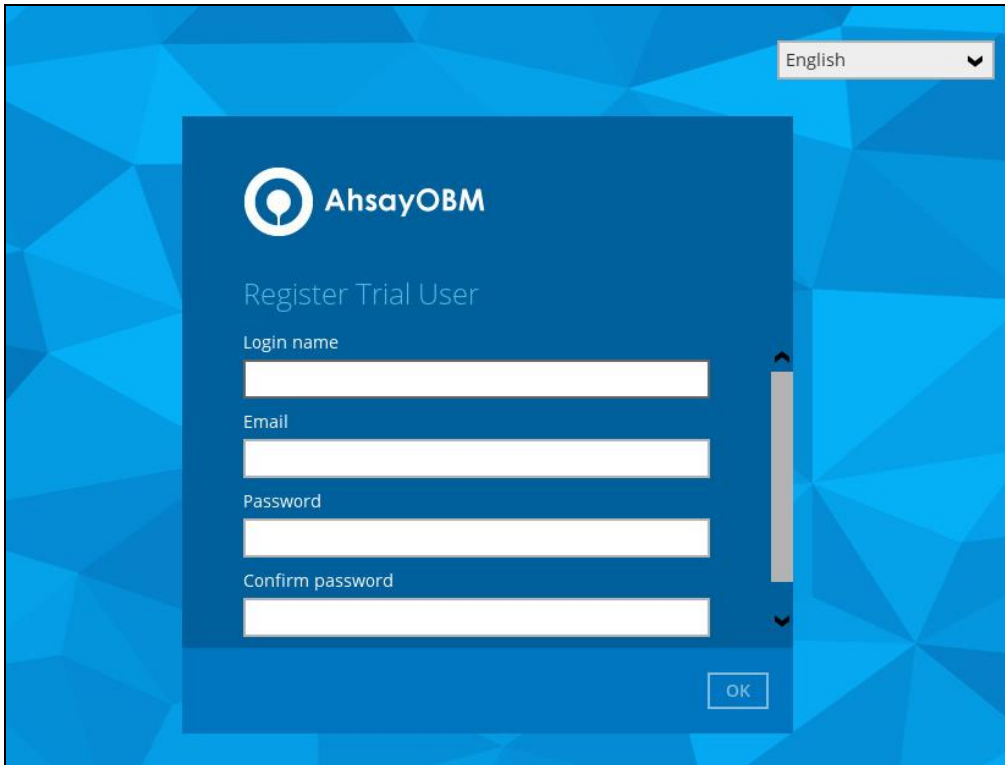


1. Configure your Backup Server settings.



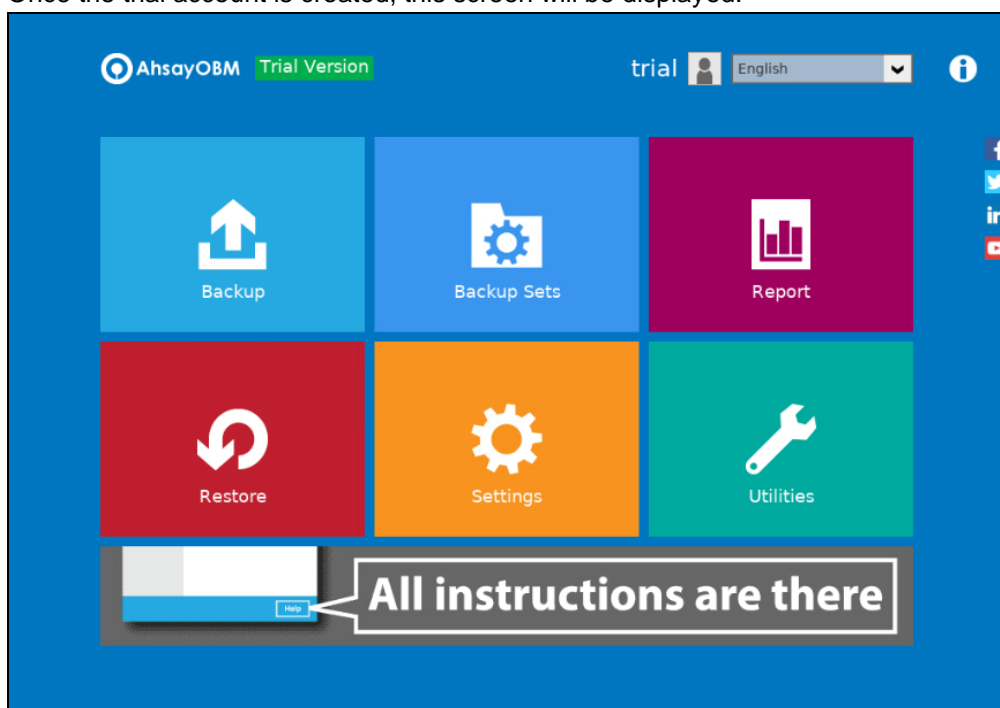
The screenshot shows a window titled "Backup Server". It contains a dropdown menu set to "http" followed by a text input field and another dropdown menu. Below this is a section titled "Proxy (HTTP)" with the text "Use proxy to access the Internet" and a toggle switch labeled "Off".

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



The screenshot shows a window titled "Register Trial User" with the AhsayOBM logo. It features four input fields labeled "Login name", "Email", "Password", and "Confirm password". A vertical scrollbar is visible on the right side of the input fields. At the bottom right, there is an "OK" button. In the top right corner, there is a language dropdown menu set to "English".

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



4. 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](#).

User Profile	General	Backup Client Settings	Contact	User Group	Authentication	Mobile Backup
Backup Set	Suspend At <input type="text" value="04-02-2022"/> (dd-mm-yyyy)					
Settings	Status <input checked="" type="radio"/> Enable <input type="radio"/> Suspended <input type="radio"/> Locked					
Report	Upload Encryption Key <input checked="" type="checkbox"/> Upload encryption key after running backup for recovery					
Statistics	Language <input type="text" value="English"/>					
Effective Policy	Timezone <input type="text" value="GMT+08:00 (HKT)"/>					

- You also need to check the available add-on modules and quota by going to the **Backup Client Settings** tab.

Settings of the client backup agent for this user.

Backup Client

☒ AhsayOBM User ☐ AhsayACB User

Add-on Modules

<input checked="" type="checkbox"/> Microsoft Exchange Server	<input checked="" type="checkbox"/> Microsoft SQL Server
<input checked="" type="checkbox"/> MySQL Database Server	<input checked="" type="checkbox"/> Oracle Database Server
<input checked="" type="checkbox"/> Lotus Domino	<input checked="" type="checkbox"/> Lotus Notes
<input checked="" type="checkbox"/> Windows System Backup	<input checked="" type="checkbox"/> Windows System State Backup
<input checked="" type="checkbox"/> VMware <input type="text" value="Guest VM"/> 0	<input checked="" type="checkbox"/> Hyper-V <input type="text" value="Guest VM"/> 0
<input checked="" type="checkbox"/> Microsoft Exchange Mailbox <input type="text" value="0"/>	<input checked="" type="checkbox"/> ShadowProtect System Backup
<input checked="" type="checkbox"/> NAS - QNAP	<input checked="" type="checkbox"/> NAS - Synology
<input checked="" type="checkbox"/> Mobile (max. 10)	<input checked="" type="checkbox"/> Continuous Data Protection
<input checked="" type="checkbox"/> Volume Shadow Copy	<input checked="" type="checkbox"/> In-File DeltaOnly apply to v8 or before
<input checked="" type="checkbox"/> OpenDirect / Granular Restore <input type="text" value="0"/>	<input checked="" type="checkbox"/> Office 365 Backup <input type="text" value="0"/>
<input checked="" type="checkbox"/> MariaDB Database Server	<input checked="" type="checkbox"/> Deduplication

Quota

Unlimited storage space for the destination not shown in the following table

Destination	Quota

- 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.

Contact information for this user.

Manage Contact Information

Name	Email	Encrypt Email
trial	name@email.com	No

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](#).