Ahsay Backup

# Ahsay Online Backup Manager v9

## Quick Start Guide for Synology NAS

Ahsay Systems Corporation Limited

21 March 2023

www.ahsay.com

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

# Copyright Notice

# 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. 6.6 – added Deduplication<br>▪ Ch. 9.2 – added Migrate Data | 9.1.0.0 |
| 7 March 2022 | ▪ Ch. 9.2 – updated note for Migrate Data | 9.1.0.0 |
| 8 August 2022 | ▪ 2.12 – added non-compressible file list | 9.1.0.0 |
| 3 November 2022 | ▪ Ch. 5 – added how to register device in 2FA<br>▪ Ch. 6 – added how to login with 2FA using different authenticators<br>▪ Ch. 7 – added unable to login using 2FA<br>▪ Ch. 8.6 – added Recycle Bin instructions<br>▪ Ch. 8.10.1 – added Rebuild index and Delete corrupted data blocks permanently<br>▪ Appendix C – added removal of Scheduler in Settings | 9.5.0.0 |
| 22 November 2022 | ▪ Ch.8.6 – fixed typo in Recycle Bin | 9.5.0.0 |
| 21 March 2023 | ▪ Ch. 2.1 – changed description of hardware requirements<br>▪ Ch. 4 – updated download and installation instructions | 9.5.4.0 |

# Table of Contents

# 1 Overview

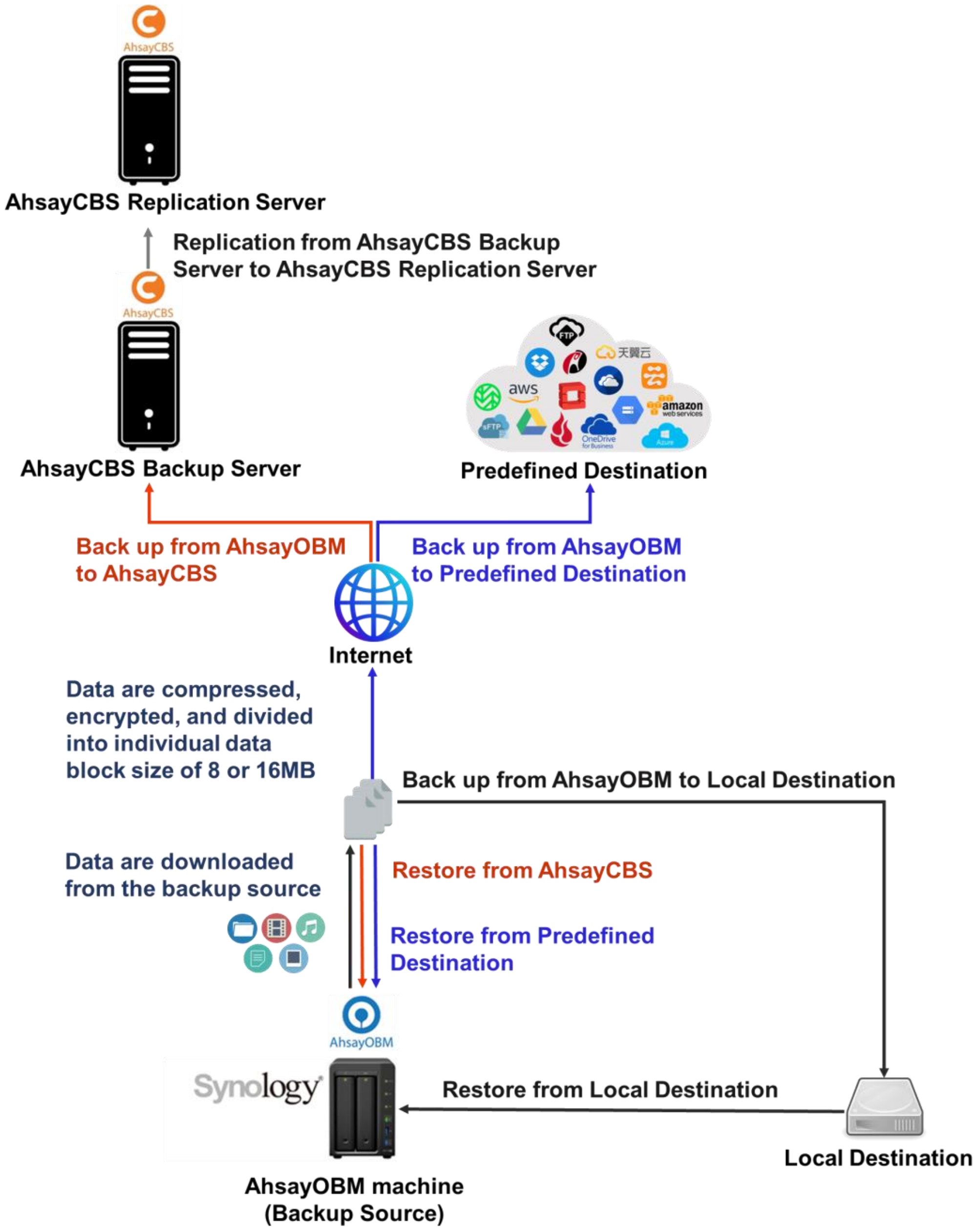
## 1.1 What is this software?

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

## 1.2 System Architecture

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

In this user guide, we will focus on the software installation, as well as the end-to-end backup and restore process using the AhsayOBM as a client backup software.


AhsayCBS
AhsayCBS Replication Server
Replication from AhsayCBS Backup Server to AhsayCBS Replication Server
AhsayCBS
AhsayCBS Backup Server
Predefined Destination
Back up from AhsayOBM to AhsayCBS
Back up from AhsayOBM to Predefined Destination
Internet
Data are compressed, encrypted, and divided into individual data block size of 8 or 16MB
Back up from AhsayOBM to Local Destination
Data are downloaded from the backup source
Restore from AhsayCBS
Restore from Predefined Destination
AhsayOBM
Synology
Restore from Local Destination
Local Destination
AhsayOBM machine (Backup Source)

# 2 Requirements for AhsayOBM on Synology NAS

## 2.1 Hardware Requirements

Refer to the following article for the list of supported CPU Model/Series for Synology NAS:

FAQ: Ahsay Hardware Compatibility List (HRL) for AhsayOBM on Synology NAS

## 2.2 Software Requirements

Refer to the following article on the supported DiskStation Manager (DSM) versions for Synology NAS:

FAQ: Ahsay Hardware Compatibility List (HRL) for AhsayOBM on Synology NAS

## 2.3 AhsayOBM Installation

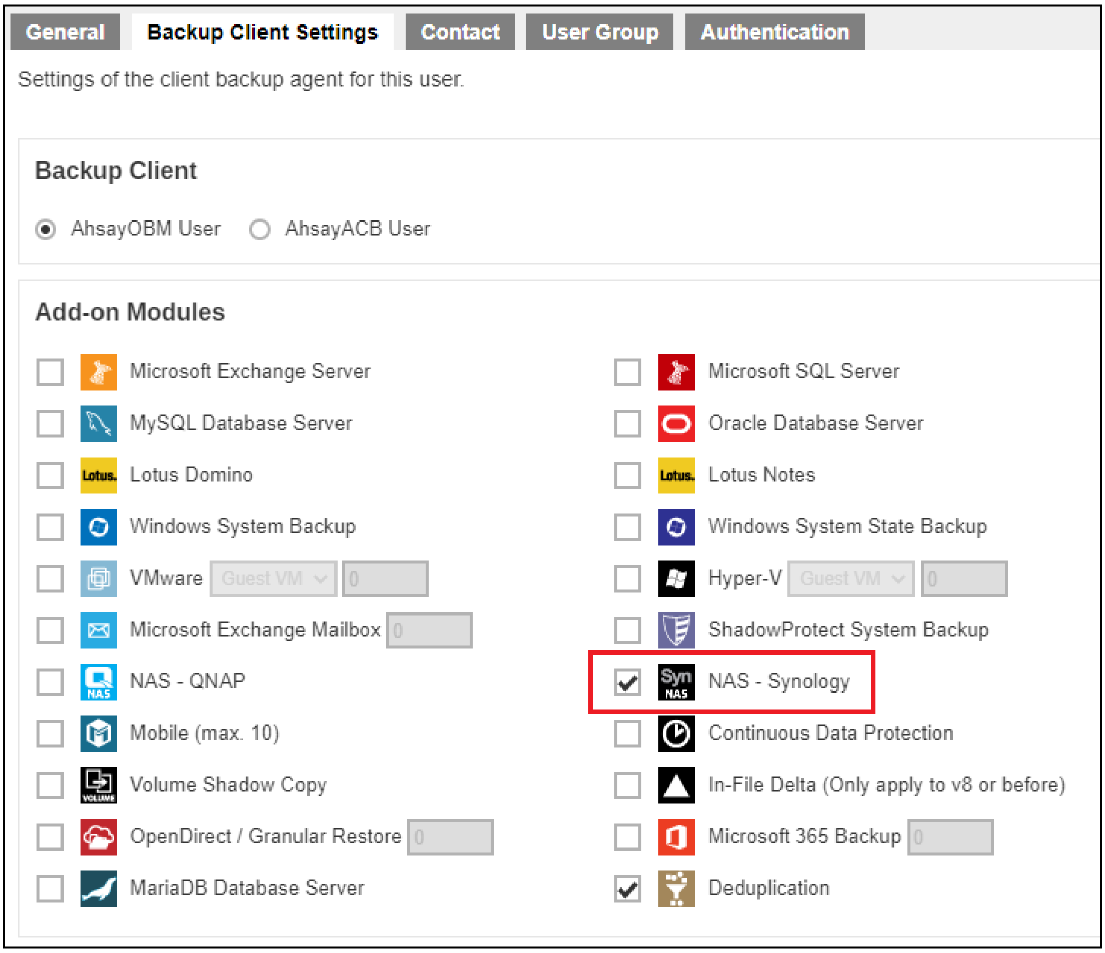
The latest version of AhsayOBM must be installed on the Synology NAS.

## 2.4 NAS-Synology Add-on Module

Make sure the NAS-Synology add-on module in your AhsayOBM user account covers the backup of your Synology NAS.

**NOTE**

The NAS-Synology add-on module allows for the backup of unlimited number of Synology NAS devices. However, each new AhsayOBM installation on a Synology NAS device will require an additional AhsayOBM device license. Please contact your backup service provider for more details.



Settings of the client backup agent for this user.

Backup Client

● AhsayOBM User ○ AhsayACB User

Add-on Modules

☐ Microsoft Exchange Server
☐ MySQL Database Server
☐ Lotus Domino
☐ Windows System Backup
☐ VMware Guest VM 0
☐ Microsoft Exchange Mailbox 0
☐ NAS - QNAP
☐ Mobile (max. 10)
☐ Volume Shadow Copy
☐ OpenDirect / Granular Restore 0
☐ MariaDB Database Server

☐ Microsoft SQL Server
☐ Oracle Database Server
☐ Lotus Notes
☐ Windows System State Backup
☐ Hyper-V Guest VM 0
☐ ShadowProtect System Backup
☑ NAS - Synology
☐ Continuous Data Protection
☐ In-File Delta (Only apply to v8 or before)
☐ Microsoft 365 Backup 0
☑ Deduplication

## 2.5 Backup Quota Storage

Please ensure there is sufficient storage quota allocated on your AhsayOBM user account to accommodate the data from the Synology NAS device.

Please contact your backup service provider for more details.

## 2.6 Java Requirement

In v9, the Oracle Java JDK files are already included and deployed as part of the AhsayOBM installation.

## 2.7 Memory Requirement

The default Java heap size of AhsayOBM installation on Synology NAS is 256 MB. It is recommended that 1 GB RAM or more is installed for stability and better backup / restore performance.

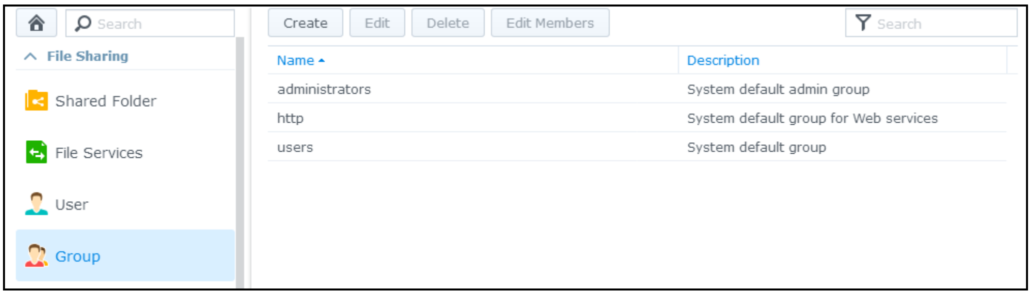
## 2.8 TCP Port Requirement

By default, the Synology NAS machine uses TCP port 32168 for the WuiService.

TCP port 32168 must be free on the machine. Otherwise, the AhsayOBM client will not start and its backup and/or restore functions will not work.

## 2.9 Synology NAS User Account Permission

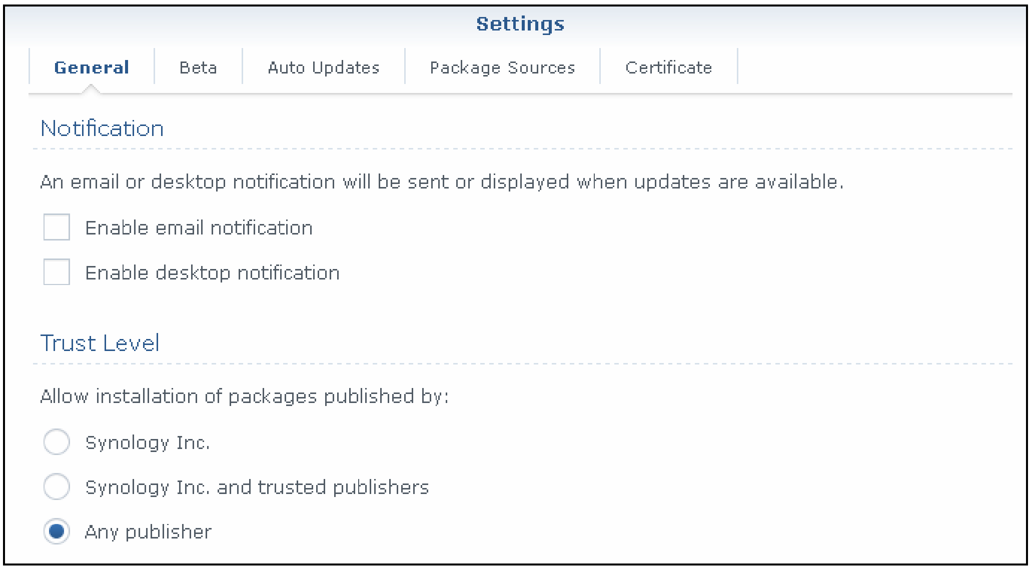
The Synology NAS user account used for the AhsayOBM installation and application must be a member of "**administrators**" user group.



| Name | Description |
|---|---|
| administrators | System default admin group |
| http | System default group for Web services |
| users | System default group |

## 2.10 Synology NAS Trust Level

In the **General** tab, modify the Trust Level setting by choosing **Any publisher**.



Settings

Notification

An email or desktop notification will be sent or displayed when updates are available.

□ Enable email notification

□ Enable desktop notification

Trust Level

Allow installation of packages published by:

○ Synology Inc.

○ Synology Inc. and trusted publishers

● Any publisher

## 2.11 Network Bandwidth

10 Mbps or above connection speed.

## 2.12 Limitations

These are the unsupported features of AhsayOBM on Synology NAS devices.

- **Auto Upgrade**
- **Backup of Network Drives**
- **Command Line Tool**
- **Decrypt Backup Data**
- **OpenDirect**
- **Restore Filter**
- **Space Freeing Up**

The following is a list of non-compressible files:

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

## 2.13 Best Practices and Recommendations

### Periodic Backup Schedule

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

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

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

- Hardware – to achieve optimal performance, compatible hardware requirements is a must. Ensure you have the backup machine's appropriate hardware specifications to accommodate frequency of backups,
    - so that the data is always backed up within the periodic backup interval
    - so that the backup frequency does not affect the performance of the production server
- Storage – ensure you have enough storage quota allocated based on the amount of new data and changed data you will back up.
- Retention Policy – also make sure to consider the Retention Policy settings and Retention Area storage management which can grow because of the changes in the backup data for each backup job.

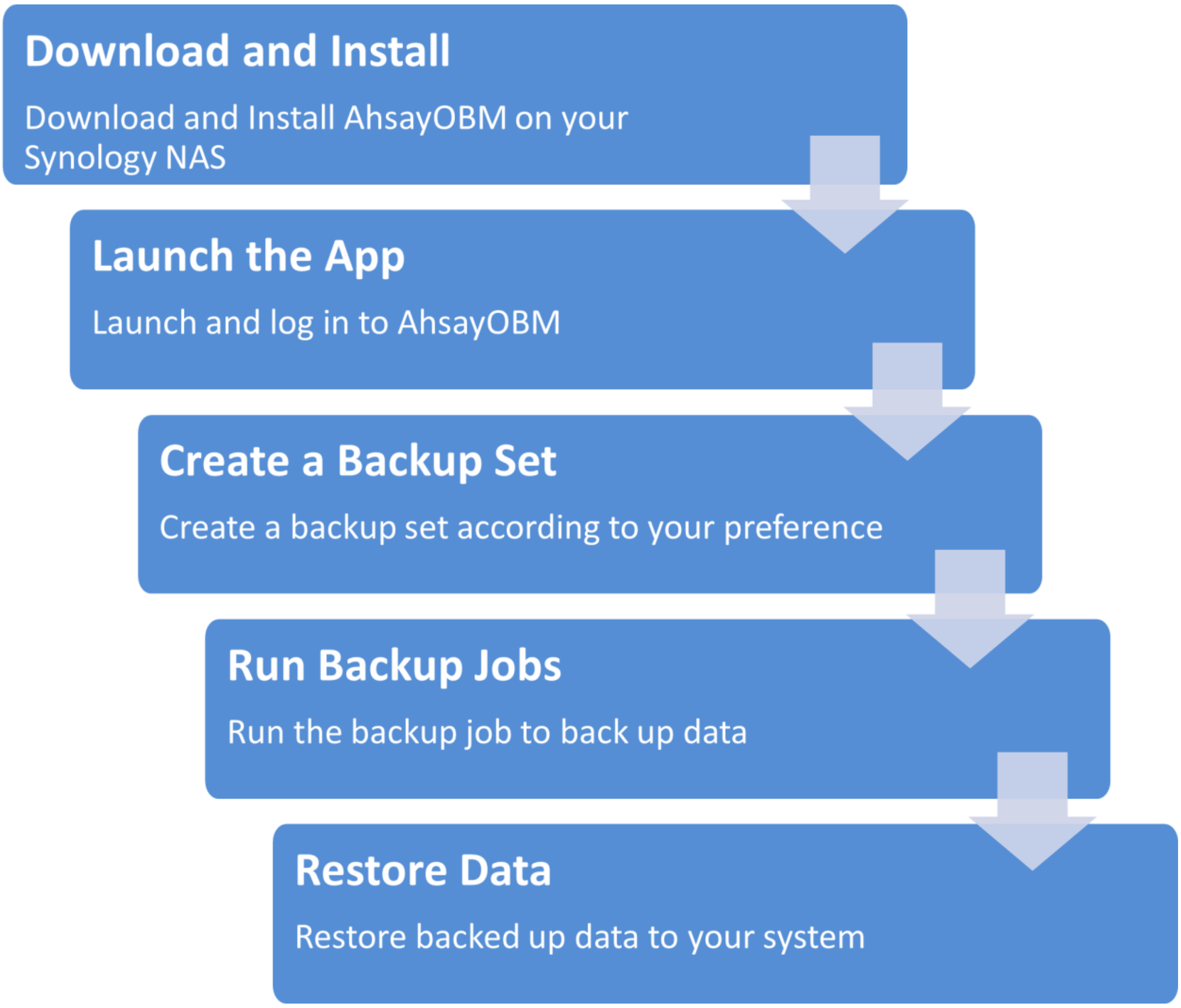
## 2.14 Supported Features from AhsayCBS Web Console

The following features of AhsayOBM on Synology NAS devices but not displayed on the AhsayOBM GUI. These features can only be accessed or configured using AhsayCBS Web Console:

- **Backup Source Filter**
- **In-File Delta**
- **Advanced Retention Policy Type**
- **Command Line Tool**
- **Bandwidth Control**
- **Follow Link**
- **Compression**
- **Usage Statistics Report**

# 3 Get started with AhsayOBM

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 Synology NAS

**Launch the App**

Launch and log in to AhsayOBM

**Create a Backup Set**

Create a backup set according to your preference

**Run Backup Jobs**

Run the backup job to back up data

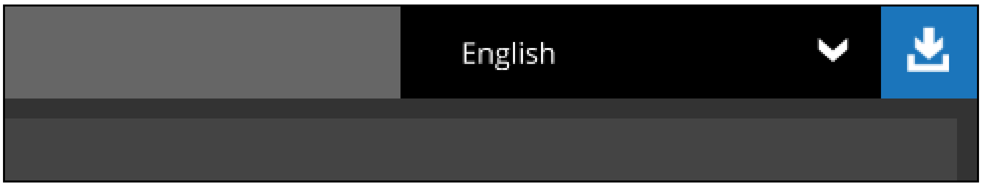
**Restore Data**

Restore backed up data to your system

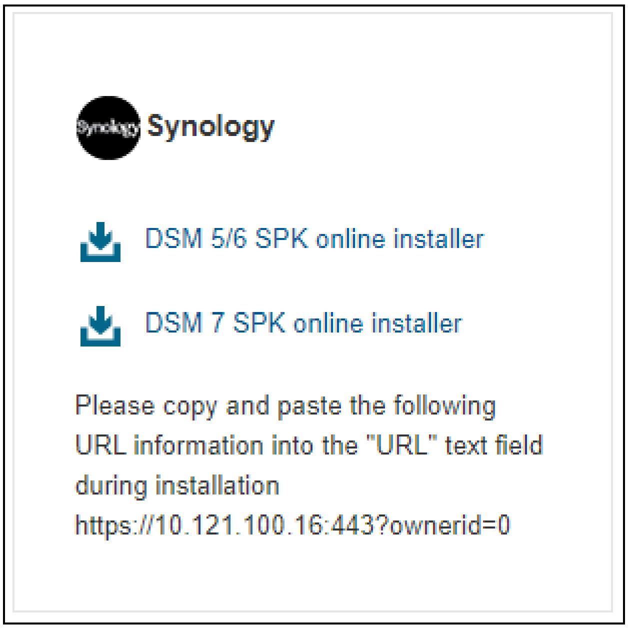
# 4 Download and Install AhsayOBM

## 4.1 Download AhsayOBM

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



2. In the **Synology** section under the **AhsayOBM** tab of the download page, download the AhsayOBM **SPK online installer** for the DSM version you are using.



Please copy and paste the following URL information into the "URL" text field during installation https://10.121.100.16:443?ownerid=0

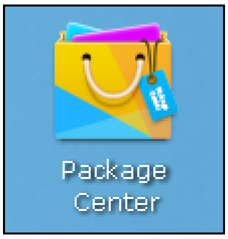
## 4.2 Install AhsayOBM using SPK online installer

1. Sign in to DiskStation Manager (DSM) with the admin account. In a web browser, enter the Synology NAS device IP address, followed by 5000

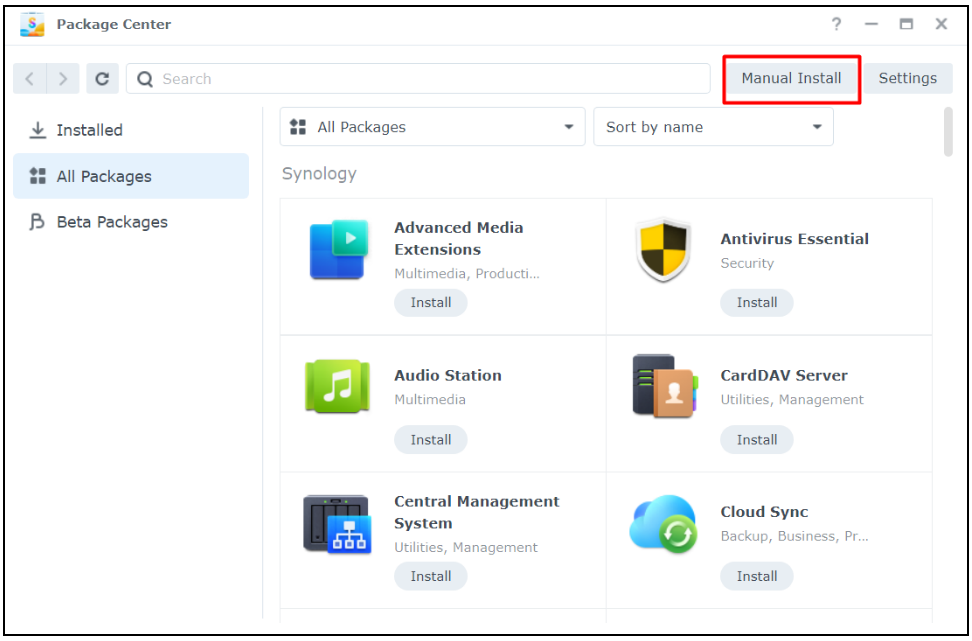
   https://nas_hostname:5000

> **NOTE**
>
> Refer to the following Synology article for information on how to sign into DSM: https://www.synology.com/en-us/knowledgebase/DSM/help/DSM/MainMenu/get_started.

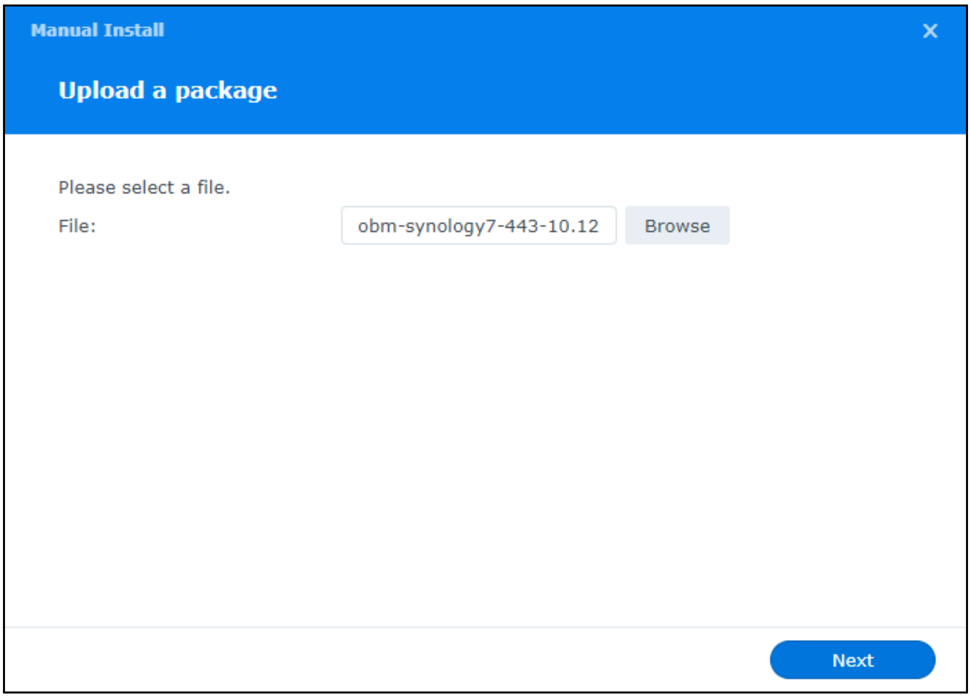
2. To install AhsayOBM on Synology NAS, click the Package Center icon from the desktop.



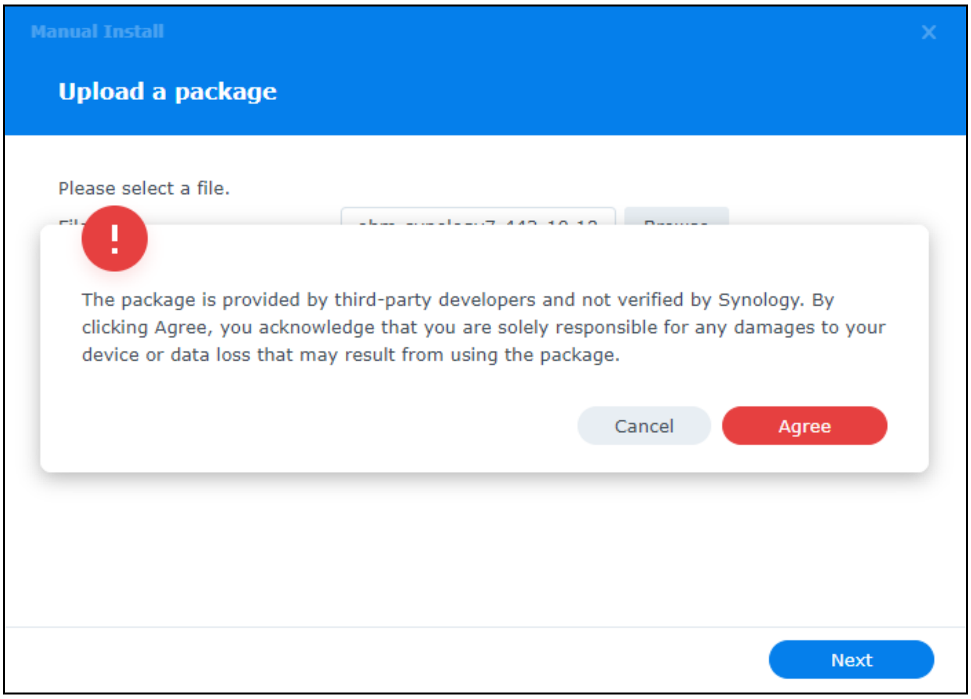
3. When the Package Center window appears, select **Manual Install**.



4. When the Manual Install window appears, click **Browse** to select the AhsayOBM SPK file which you have downloaded (e.g., obm-synology-443-10.3.121.17-https-0O.spk). Then, click **Next** to proceed.

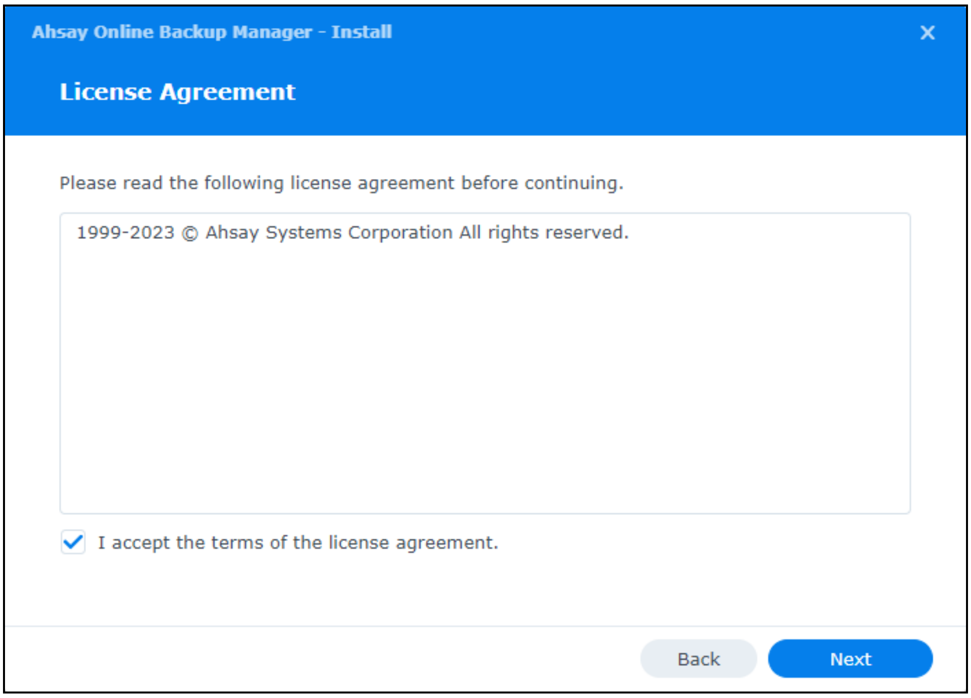


5. Click **Agree** in the confirmation message to proceed.



The package is provided by third-party developers and not verified by Synology. By clicking Agree, you acknowledge that you are solely responsible for any damages to your device or data loss that may result from using the package.

6. After reading the License Agreement carefully, tick the checkbox next to **I accept the terms of the license agreement**. Then, click **Next** to proceed.

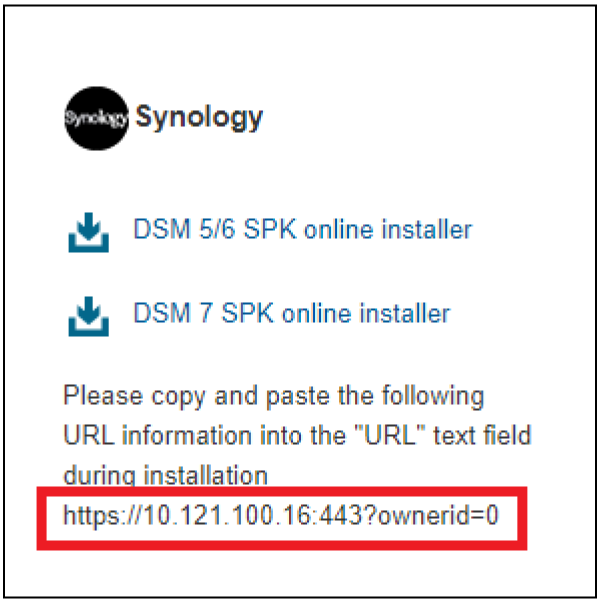


Please read the following license agreement before continuing.

1999-2023 © Ahsay Systems Corporation All rights reserved.

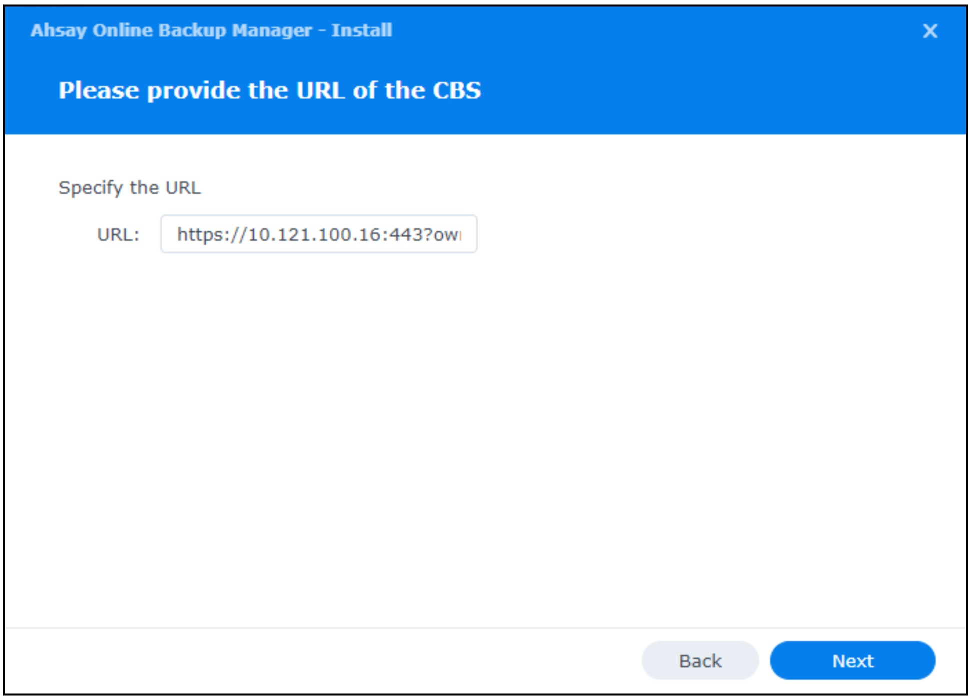
☑ I accept the terms of the license agreement.

7. From the download page of your backup service provider's website, copy and paste the URL on the Ahsay Online Backup Manager – Install window, then click **Next** to proceed.



Please copy and paste the following URL information into the "URL" text field during installation

https://10.121.100.16:443?ownerid=0



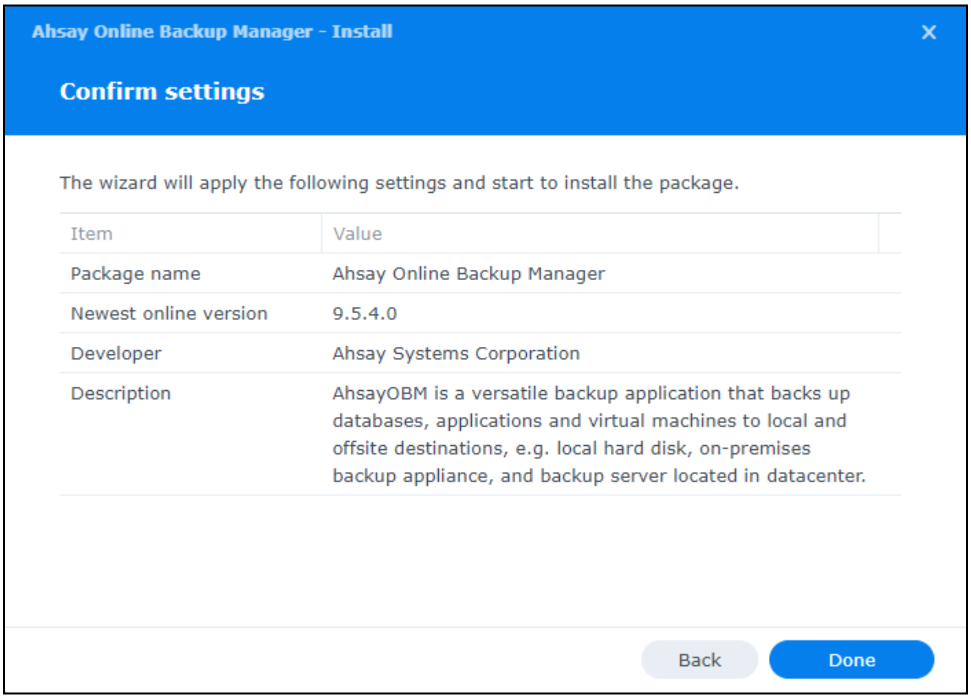
Ahsay Online Backup Manager - Install

Please provide the URL of the CBS

Specify the URL

URL: https://10.121.100.16:443?ow

8. Review the following information on the screen, then click **Done** to start the installation of AhsayOBM.

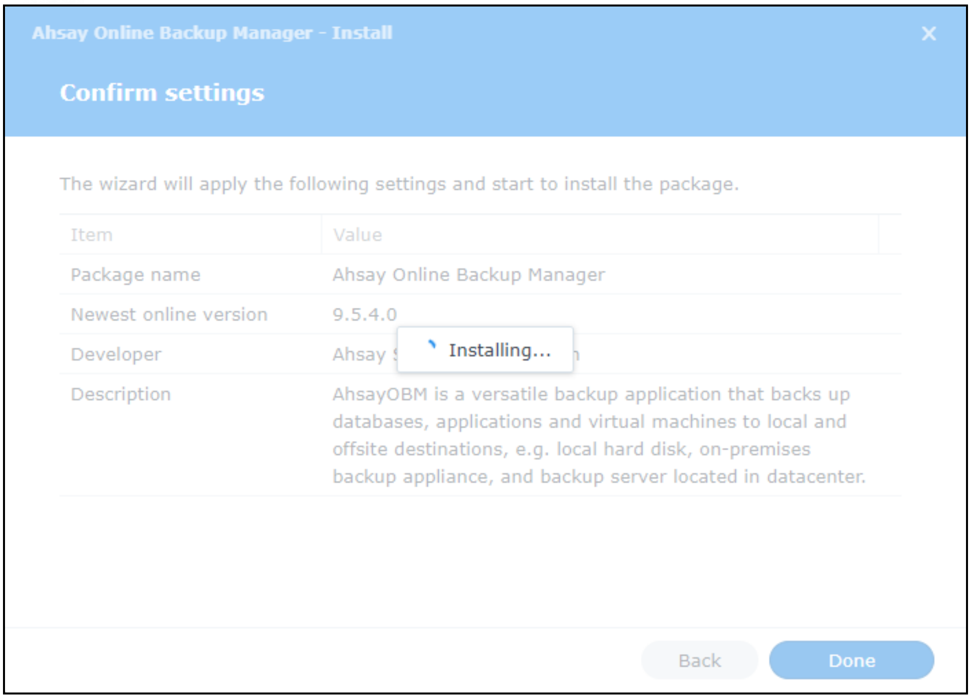


Ahsay Online Backup Manager - Install

Confirm settings

The wizard will apply the following settings and start to install the package.

| Item | Value |
|---|---|
| Package name | Ahsay Online Backup Manager |
| Newest online version | 9.5.4.0 |
| Developer | Ahsay Systems Corporation |
| Description | AhsayOBM is a versatile backup application that backs up databases, applications and virtual machines to local and offsite destinations, e.g. local hard disk, on-premises backup appliance, and backup server located in datacenter. |



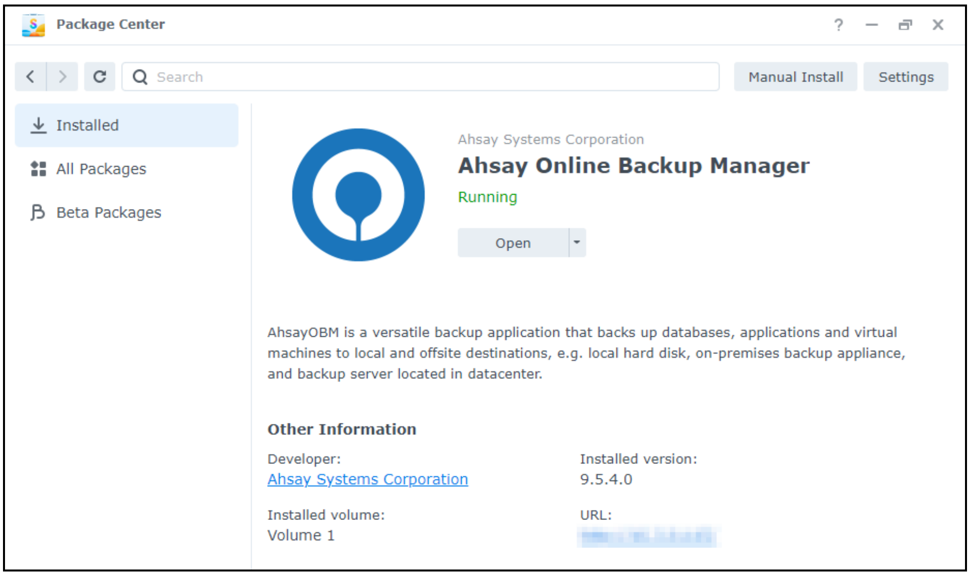
Ahsay Online Backup Manager - Install

Confirm settings

The wizard will apply the following settings and start to install the package.

| Item | Value |
|---|---|
| Package name | Ahsay Online Backup Manager |
| Newest online version | 9.5.4.0 |
| Developer | Ahsay S Installing... n |
| Description | AhsayOBM is a versatile backup application that backs up databases, applications and virtual machines to local and offsite destinations, e.g. local hard disk, on-premises backup appliance, and backup server located in datacenter. |

9. After a successful installation, AhsayOBM will be listed in the Installed packages.



Ahsay Systems Corporation

Ahsay Online Backup Manager

Running

AhsayOBM is a versatile backup application that backs up databases, applications and virtual machines to local and offsite destinations, e.g. local hard disk, on-premises backup appliance, and backup server located in datacenter.

Other Information

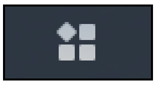
Developer: Ahsay Systems Corporation

Installed version: 9.5.4.0

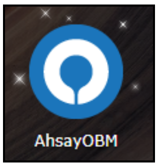
Installed volume: Volume 1

URL: [redacted]

10. Click the Main Menu icon on the top left corner of your desktop.



11. You can click the AhsayOBM icon to launch the application.



12. Revert the Trust Level to the previous setting in Package Center afterward. Refer to Pre-install Requirement for instructions.

## 4.3 AhsayOBM Scheduler Service Check

This option is used to kick automated or scheduled backup jobs. To start, login to Synology NAS device using ssh client, i.e., putty.

Go to the ***/volume1/@appstore/AhsayOBM/obm/bin*** directory.

To **check** if the AhsayOBM scheduler service is running, use the **ps** command.

Scheduler service is running, highlighted in red.

```
login as: admin

admin@10.3.0.116's password:

admin@dev-ds215j:~$ cd /volume1/@appstore/AhsayOBM/obm/bin

admin@dev-ds215j:/volume1/@appstore/AhsayOBM/obm/bin$ ps -ef|grep java

root 15083 1 0 May14 ? 00:03:05
/volume1/@appstore/AhsayOBM/obm/jvm/bin/java -Xrs -Xms64m -Xmx373m -
Dsun.nio.PageAlignDirectMemory=true -Djava.library.path=. -cp .:./cb.jar
WuiService
/volume1/@appstore/AhsayOBM/obm/volume1/@appstore/AhsayOBM/.obm --
port=32168

admin 16343 15411 0 08:56 pts/3 00:00:00 grep --color=auto java

admin 20925 1 1 May14 ? 00:11:46
/volume1/@appstore/AhsayOBM/obm/jvm/bin/java -Xms64m -Xmx256m -
Dsun.nio.PageAlignDirectMemory=true -Djava.library.path=. -cp .:./cbs.jar
cbs /volume1/@appstore/AhsayOBM/obm
```

To manually **stop** the scheduler service, use the **touch /volume1/@appstore/AhsayOBM/obm/ipc/Scheduler/stop** script.

Use the **ps** command again.

```
admin@dev-ds215j:/volume1/@appstore/AhsayOBM/obm/bin$ touch
/volume1/@appstore/AhsayOBM/obm/ipc/Scheduler/stop

admin@dev-ds215j:/volume1/@appstore/AhsayOBM/obm/bin$ ps -ef|grep java

root 15083 1 0 May14 ? 00:03:05
/volume1/@appstore/AhsayOBM/obm/jvm/bin/java -Xrs -Xms64m -Xmx373m -
Dsun.nio.PageAlignDirectMemory=true -Djava.library.path=. -cp .:./cb.jar
WuiService /volume1/@appstore/AhsayOBM/obm
/volume1/@appstore/AhsayOBM/.obm --port=32168

admin 16479 15411 0 08:58 pts/3 00:00:00 grep --color=auto java
```

To manually **start** the scheduler service, use **/volume1/@appstore/AhsayOBM/bin/Scheduler.sh** script and use the **ps** command.

Scheduler service is running, highlighted in red.

```
admin@dev-ds215j:/volume1/@appstore/AhsayOBM/obm/bin$
/volume1/@appstore/AhsayOBM/obm/bin/Scheduler.sh

admin@dev-ds215j:/volume1/@appstore/AhsayOBM/obm/bin$ ps -ef|grep java

root 15083 1 0 May14 ? 00:03:05
/volume1/@appstore/AhsayOBM/obm/jvm/bin/java -Xrs -Xms64m -Xmx373m -
Dsun.nio.PageAlignDirectMemory=true -Djava.library.path=. -cp .:./cb.jar
WuiService /volume1/@appstore/AhsayOBM/obm
/volume1/@appstore/AhsayOBM/.obm --port=32168

admin 16583 1 8 08:58 pts/3 00:00:16
/volume1/@appstore/AhsayOBM/obm/jvm/bin/java -Xms64m -Xmx256m -
Dsun.nio.PageAlignDirectMemory=true -Djava.library.path=. -cp .:./cbs.jar
cbs /volume1/@appstore/AhsayOBM/obm

admin 16962 15411 0 09:02 pts/3 00:00:00 grep --color=auto java
```

# 5 Register device for 2FA in AhsayOBM

There are two types of authenticators 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.)

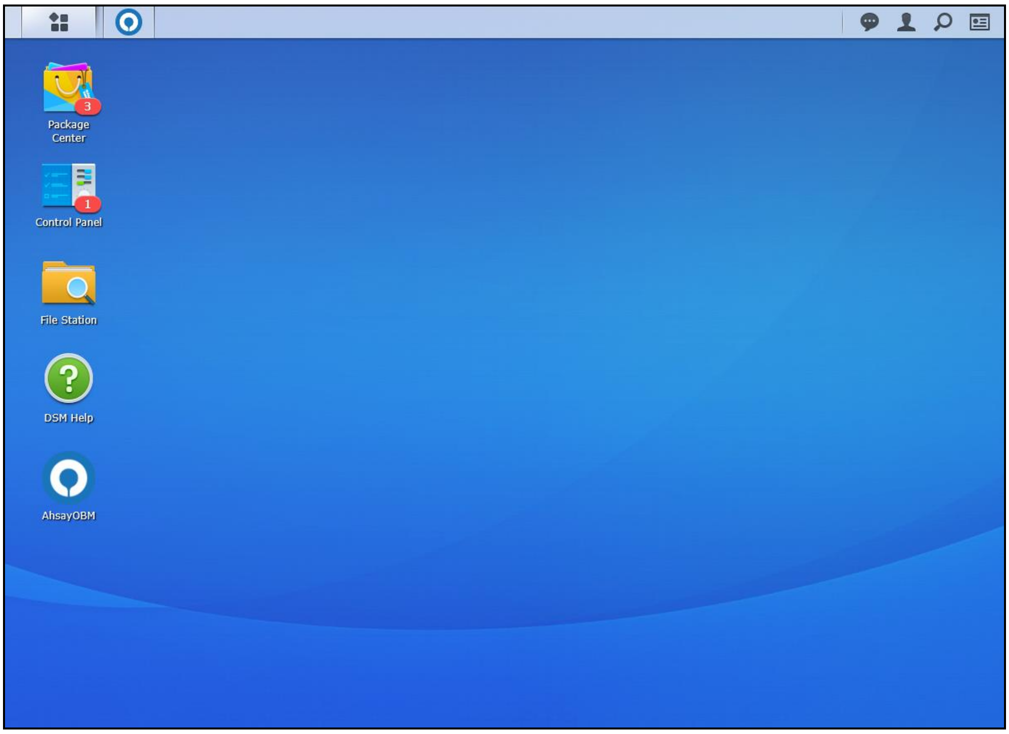
The 2FA registration steps using the different types of authenticators will be discussed in this chapter.

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

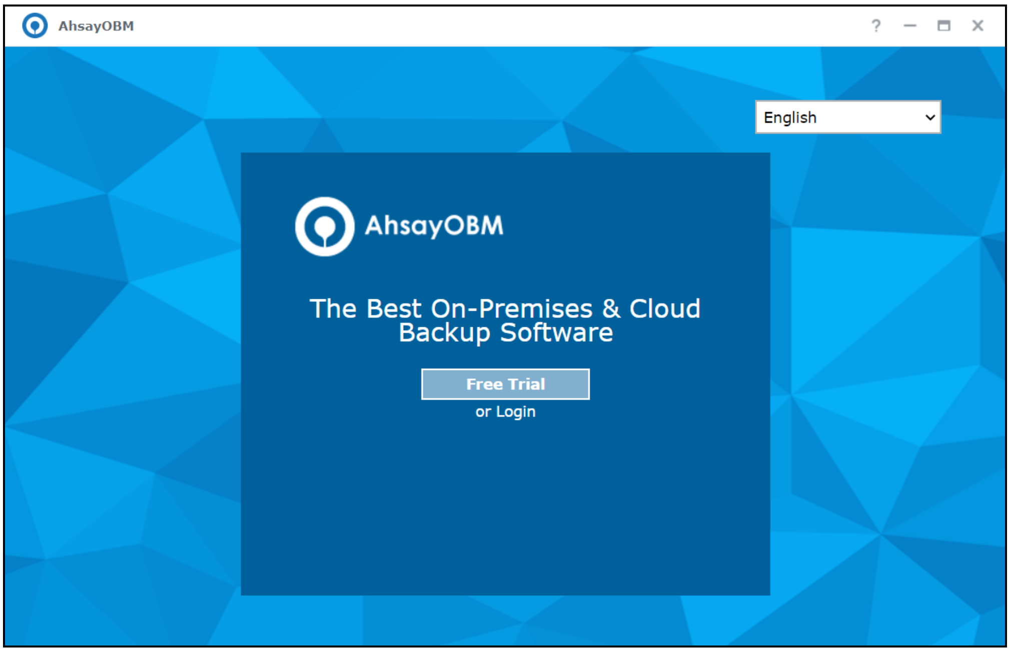
## 5.1 Using Ahsay Mobile Authenticator

To register a device for 2FA in AhsayOBM using Ahsay Mobile, please follow the steps below:

1. Click the AhsayOBM icon on the desktop to launch the application.



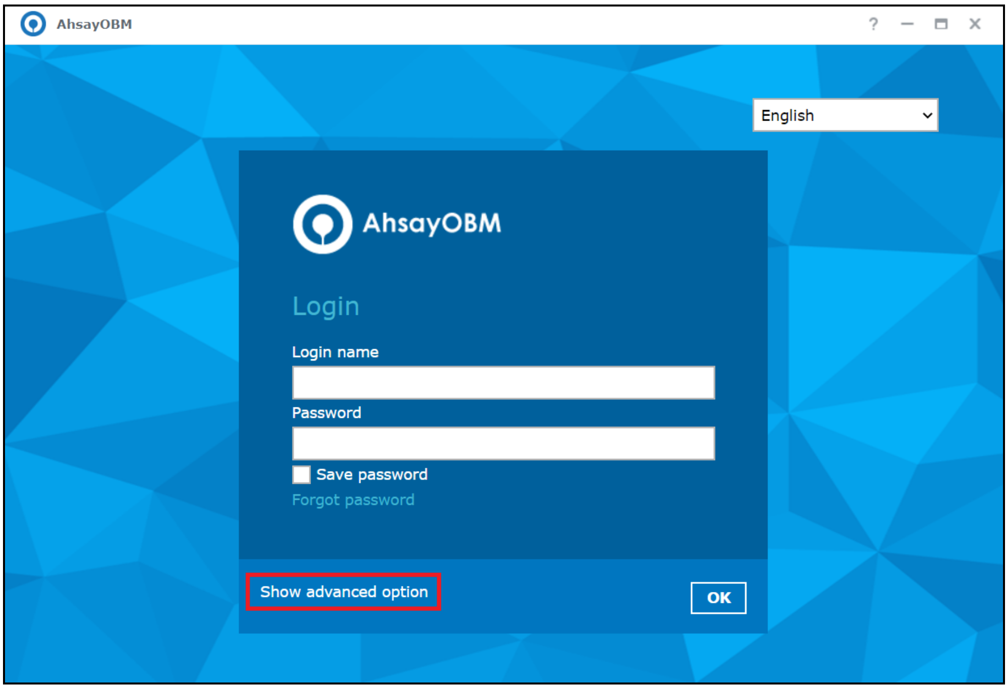
2. The Free Trial registration menu may be displayed when you login for the first time. Click **Login** if you already have an AhsayOBM account or click **Free Trial** to register for a trial backup account. For more details, refer to Appendix D: Create Free Trial Account in AhsayOBM.



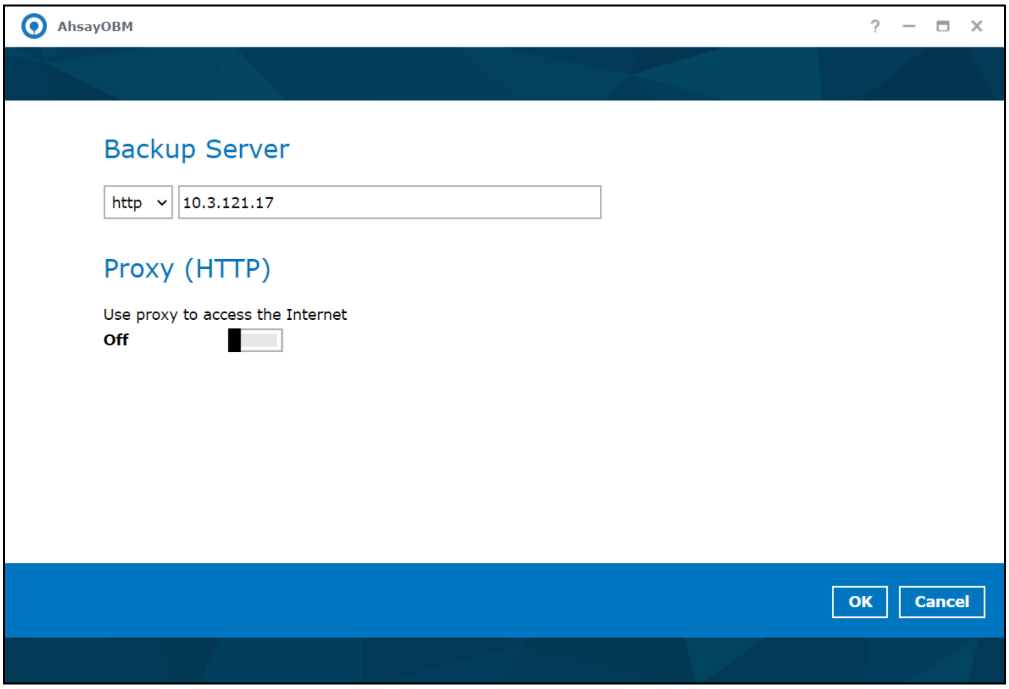
**NOTE**

The Free Trial registration option will only be displayed if your backup service provider has enabled free trial registration on the backup server.

3. In case you want to enter the backup server setting provided by your backup service provider, click **Show advanced option**.



4. Click **OK** after typing in the backup server information. You can turn on the Proxy feature if needed.



Backup Server

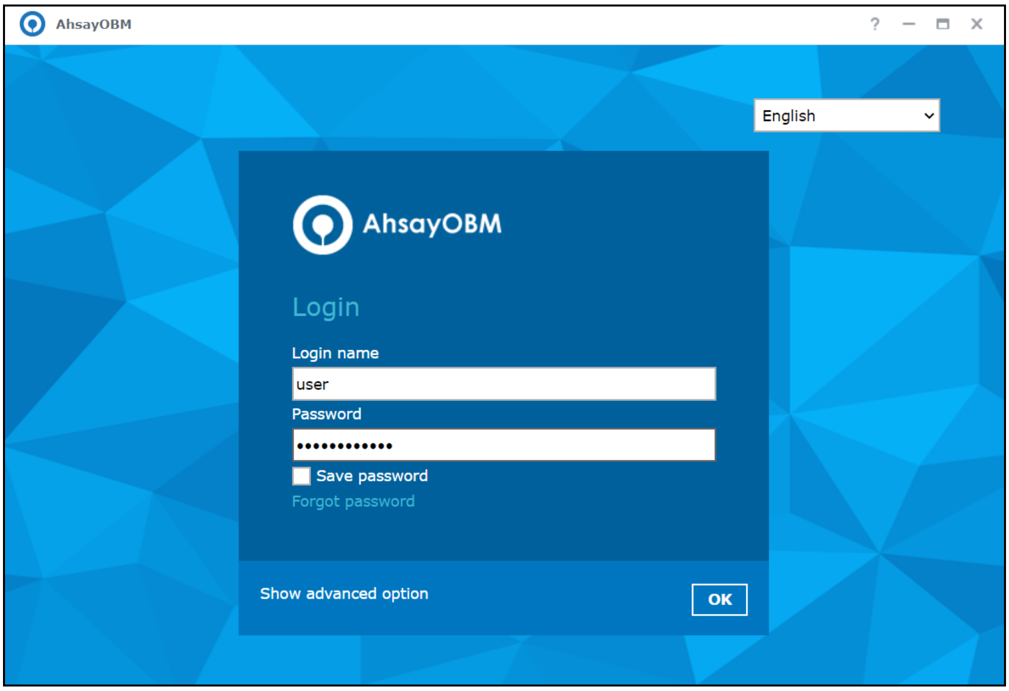
http 10.3.121.17

Proxy (HTTP)

Use proxy to access the Internet

Off

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



Login

Login name

user

Password

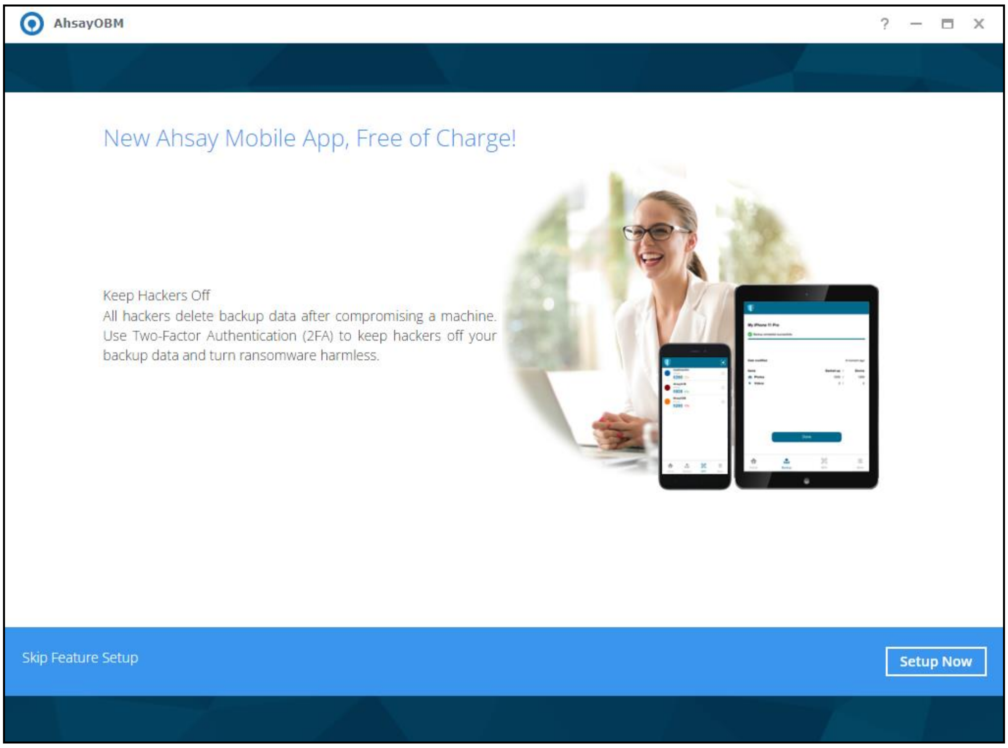
••••••••••••

□ Save password

**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.

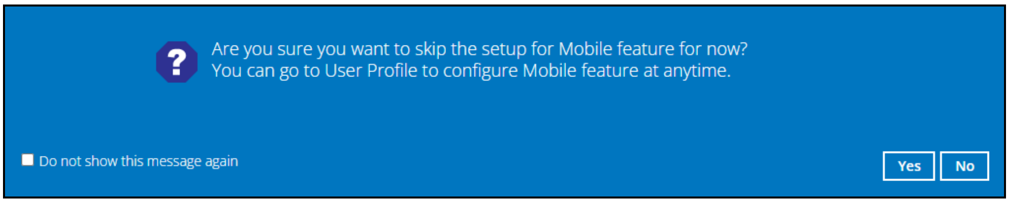
6. You will have the option to set up your 2FA. Click **Setup Now**.



New Ahsay Mobile App, Free of Charge!

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

If you do not want to setup 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 9. Otherwise, click **No** to continue with the setup of the 2FA feature.


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

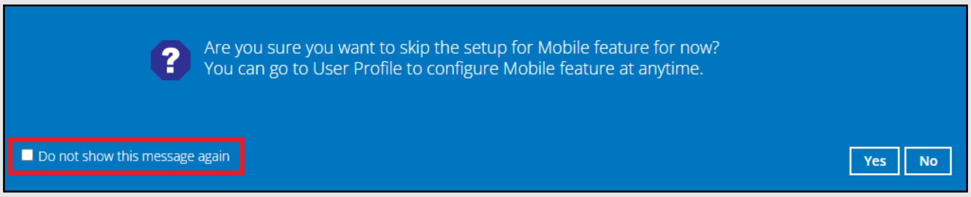
□ Do not show this message again

**NOTE**

The 2FA reminder screen will be displayed every time the user logs in if:

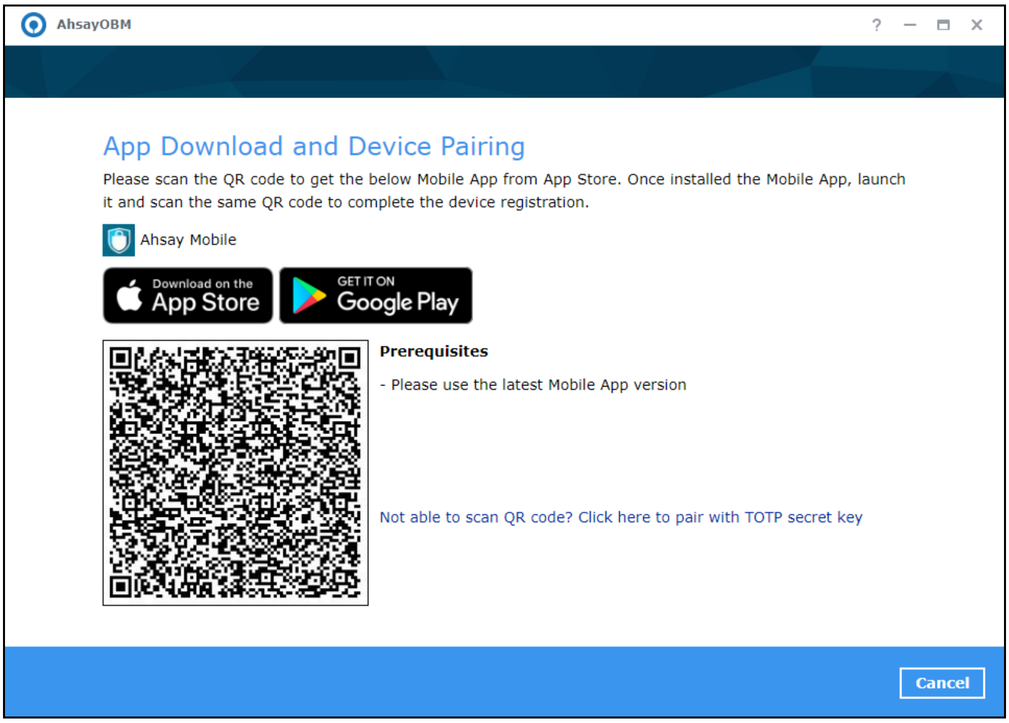
- 2FA is enabled
- the user does not have a paired device for 2FA

To stop the 2FA reminder screen from being displayed again upon login, tick the **Do not show this message again** checkbox.


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

□ Do not show this message again

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



App Download and Device Pairing

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

Ahsay Mobile

**Prerequisites**

- Please use the latest Mobile App version

Not able to scan QR code? Click here to pair with TOTP secret key

8. Ahsay Mobile supports two types of authentication method:

   ➢ Push Notification

   ➢ TOTP

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

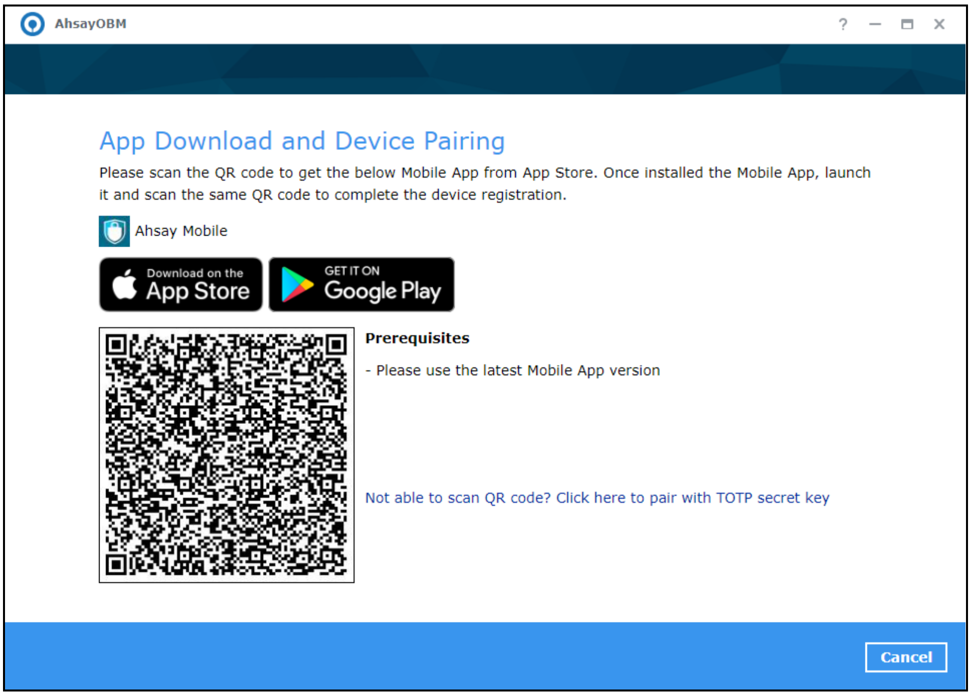
   ➢ Push Notification and TOTP (default mode)

   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.



App Download and Device Pairing

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

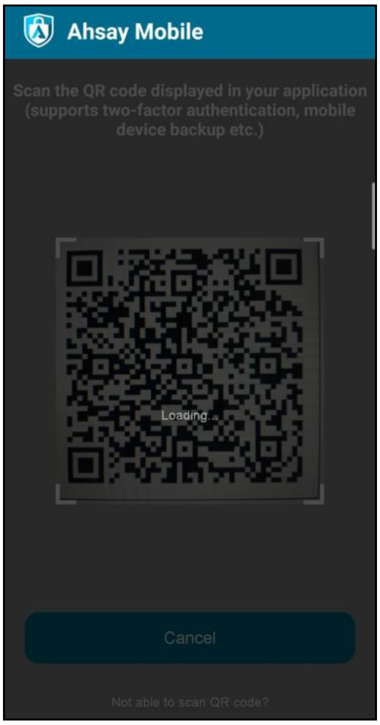
Ahsay Mobile

**Prerequisites**

- Please use the latest Mobile App version

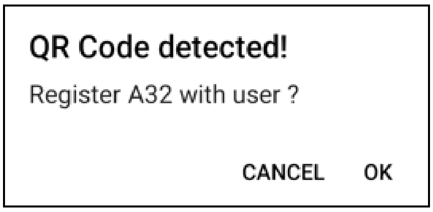
Not able to scan QR code? Click here to pair with TOTP secret key

ii. In this example, the Ahsay Mobile app is installed on a mobile device named “A32”.



Scan the QR code displayed in your application (supports two-factor authentication, mobile device backup etc.)

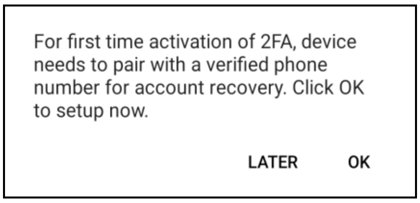
Tap **OK** to continue.



QR Code detected!

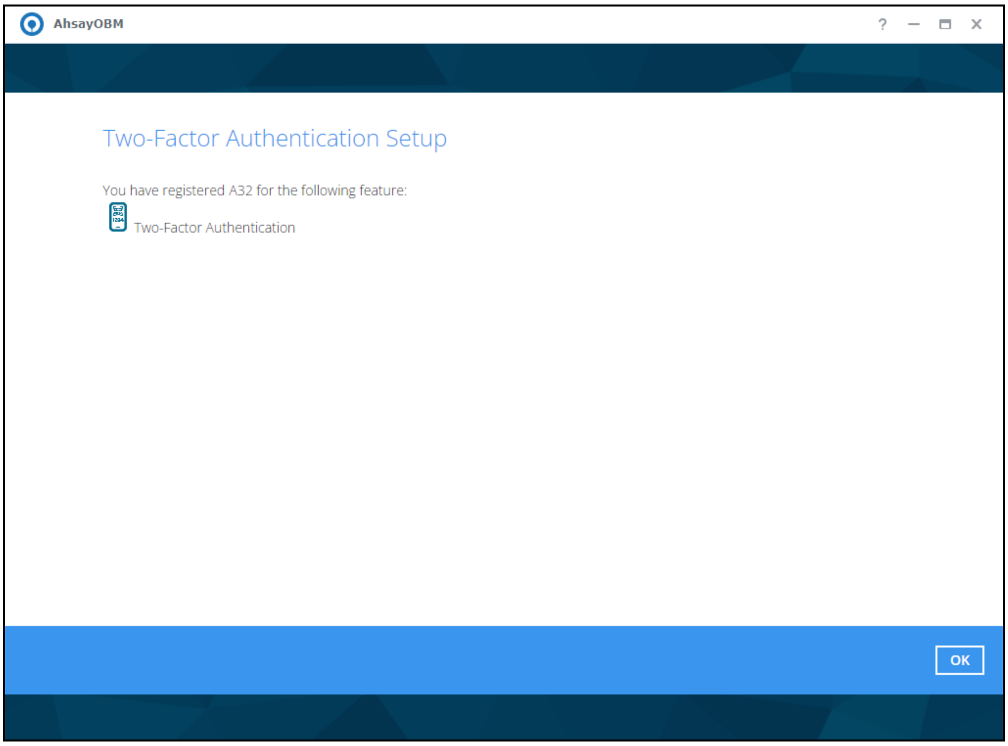
Register A32 with user ?

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



For first time activation of 2FA, device needs to pair with a verified phone number for account recovery. Click OK to setup now.

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



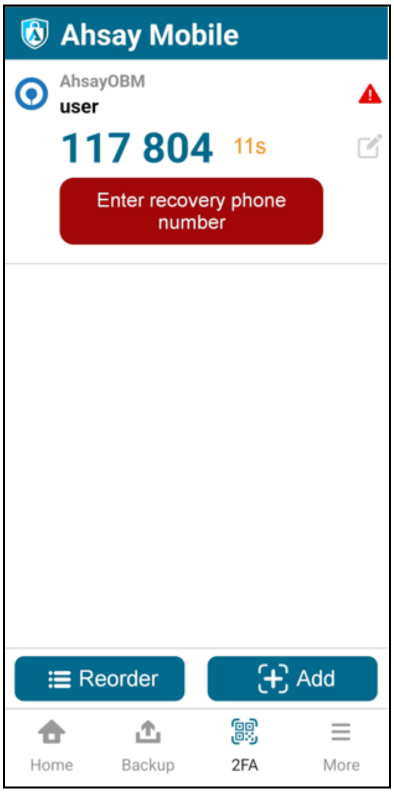
Two-Factor Authentication Setup

You have registered A32 for the following feature:

Two-Factor Authentication

**Phone number verification for account recovery**

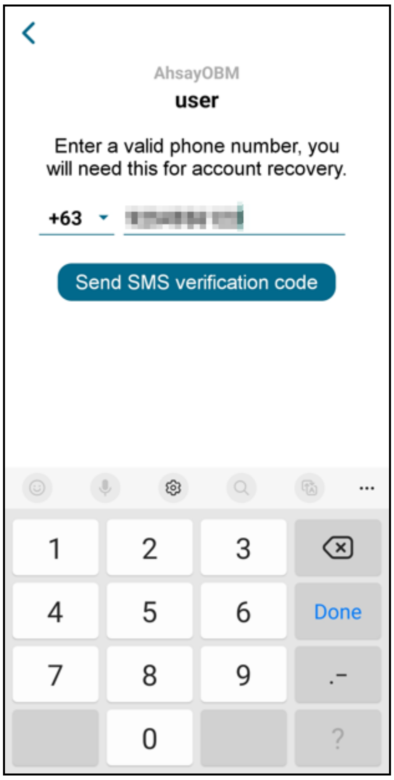
iv. In the Ahsay Mobile app, go to 2FA then enter the phone number for account recovery. Tap **Enter recovery phone number**.



**NOTE**

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

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



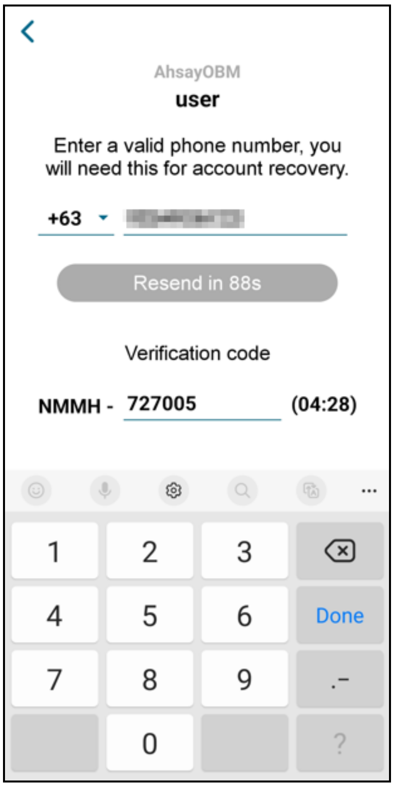
AhsayOBM

user

Enter a valid phone number, you will need this for account recovery.

+63 [redacted]

vi. Enter the verification code sent to your mobile device.



AhsayOBM

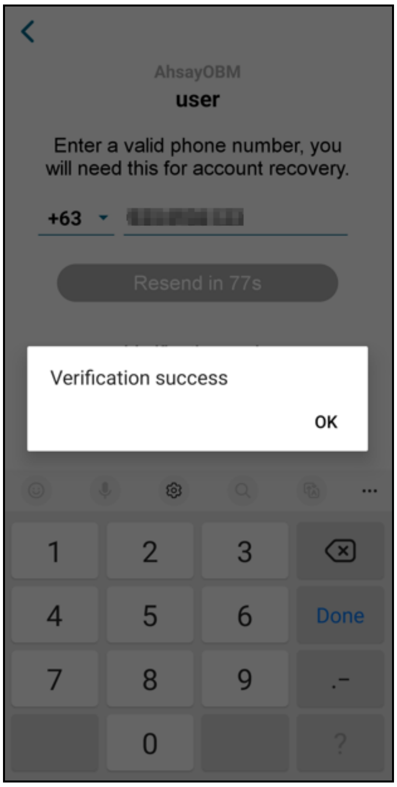
user

Enter a valid phone number, you will need this for account recovery.

+63 [redacted]

Verification code

NMMH - 727005 (04:28)



AhsayOBM

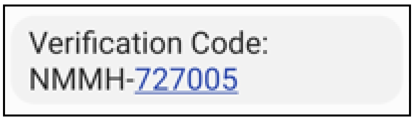
user

Enter a valid phone number, you will need this for account recovery.

+63 [redacted]

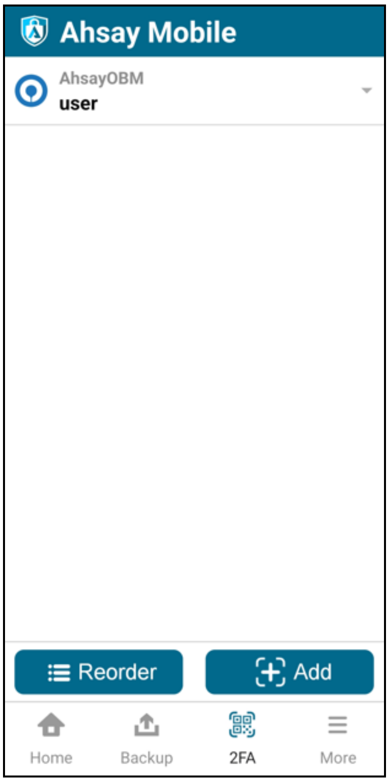
Verification success

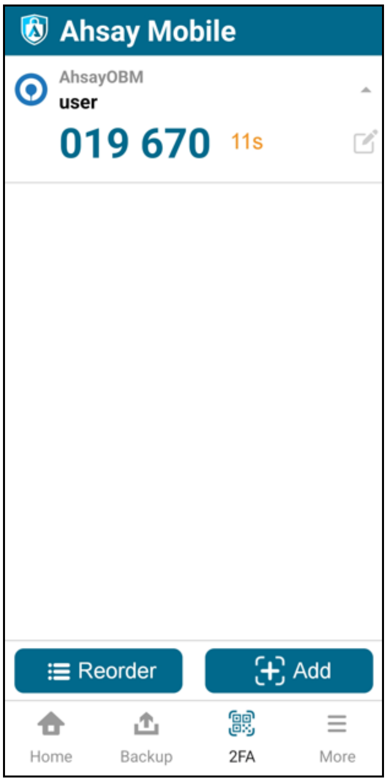
Example of verification code:



Verification Code:
NMMH-727005

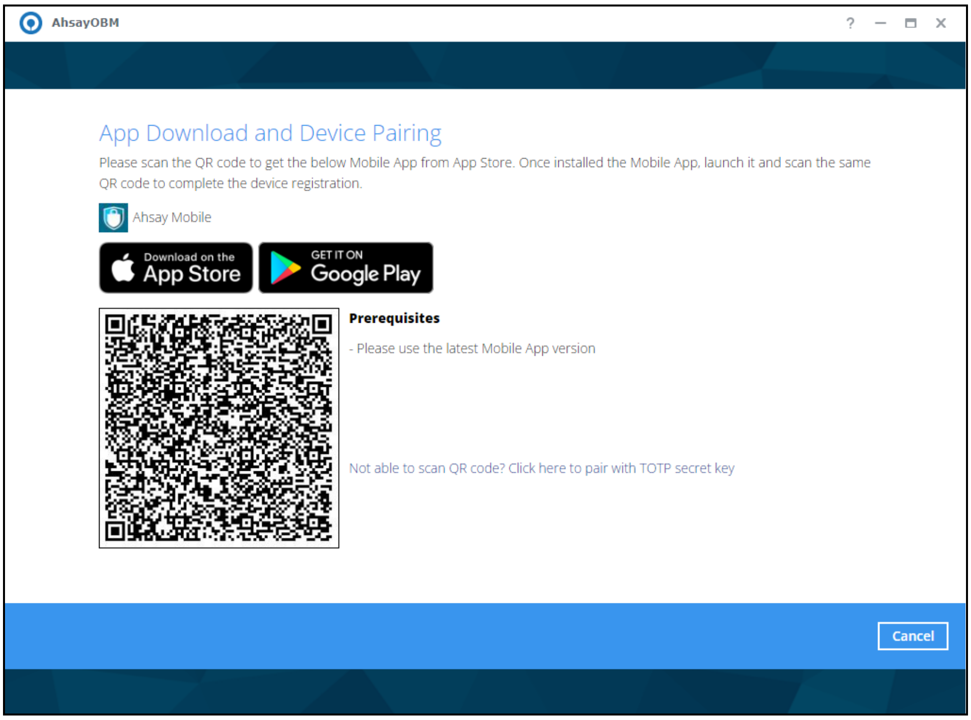
vii. Your phone number for account recovery is successfully verified.





**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.



App Download and Device Pairing

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

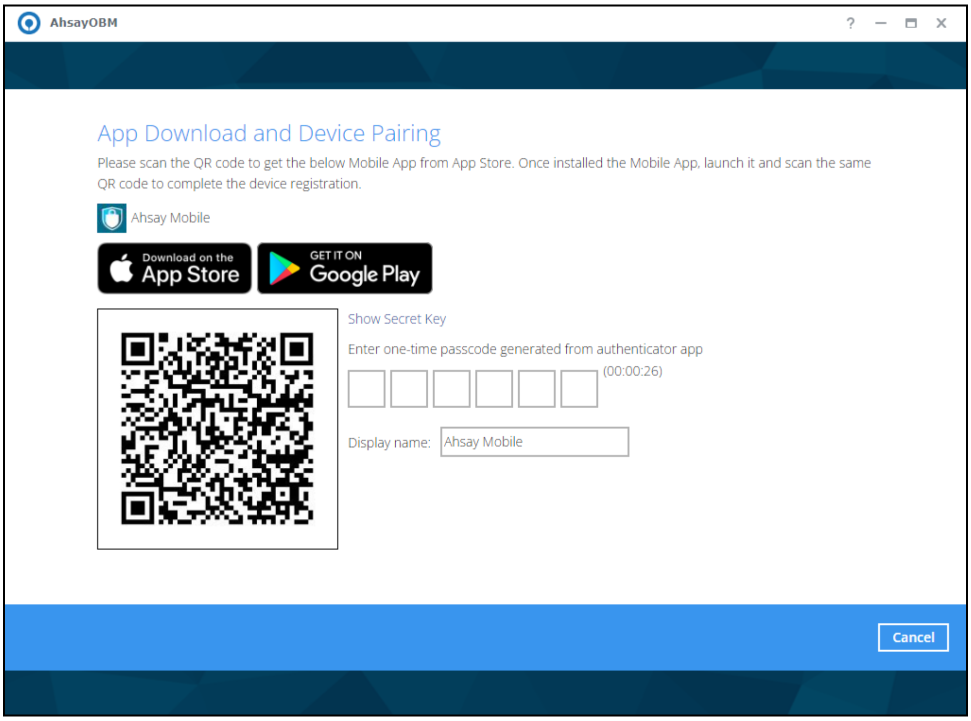
Ahsay Mobile

**Prerequisites**

- Please use the latest Mobile App version

Not able to scan QR code? Click here to pair with TOTP secret key

ii. The QR code for the TOTP only authenticator will be displayed.



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.

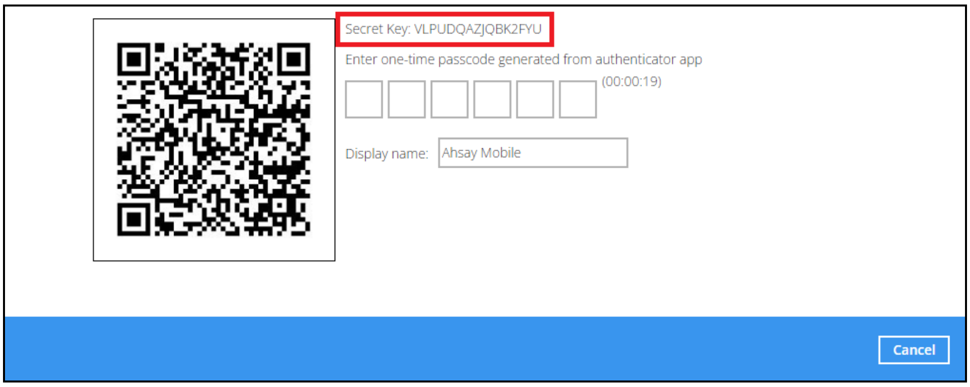
Ahsay Mobile

Enter one-time passcode generated from authenticator app

(00:00:26)

Display name: Ahsay Mobile

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.



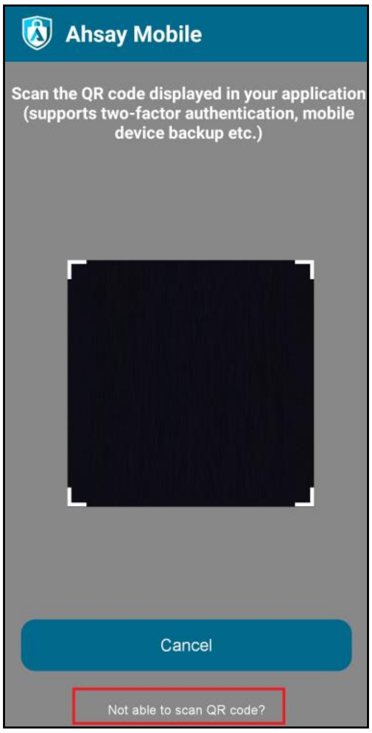
Secret Key: VLPUDQAZJQBK2FYU

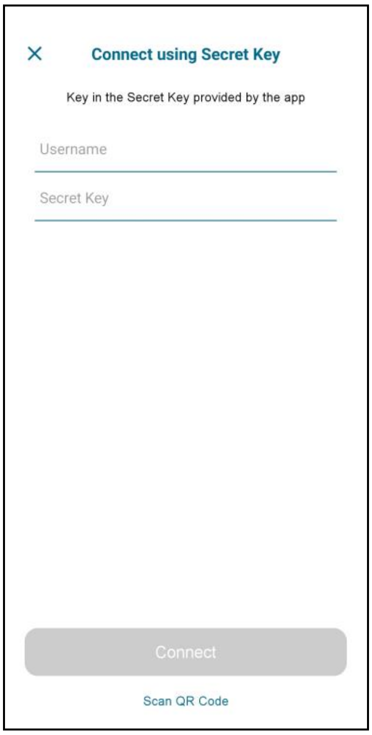
Enter one-time passcode generated from authenticator app

(00:00:19)

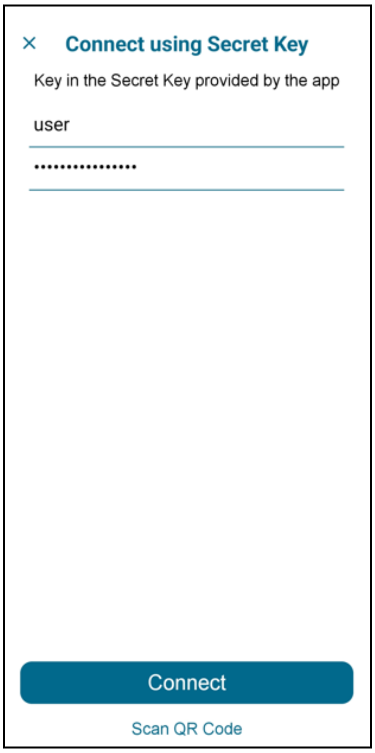
Display name: Ahsay Mobile

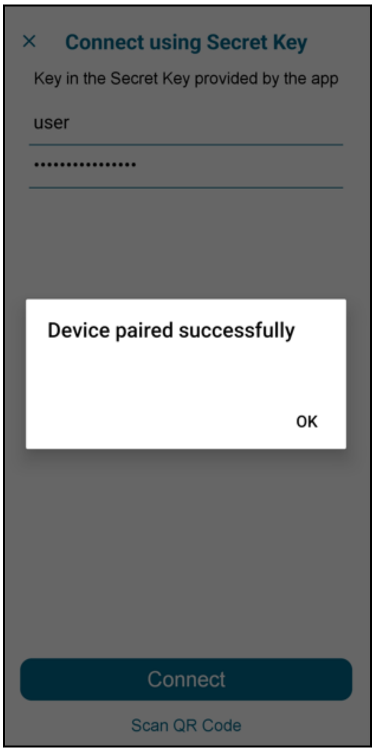
iii. In the Ahsay Mobile app, go to 2FA. Tap the **Not able to scan QR code?** Link.


Ahsay Mobile
Scan the QR code displayed in your application (supports two-factor authentication, mobile device backup etc.)
Cancel
Not able to scan QR code?

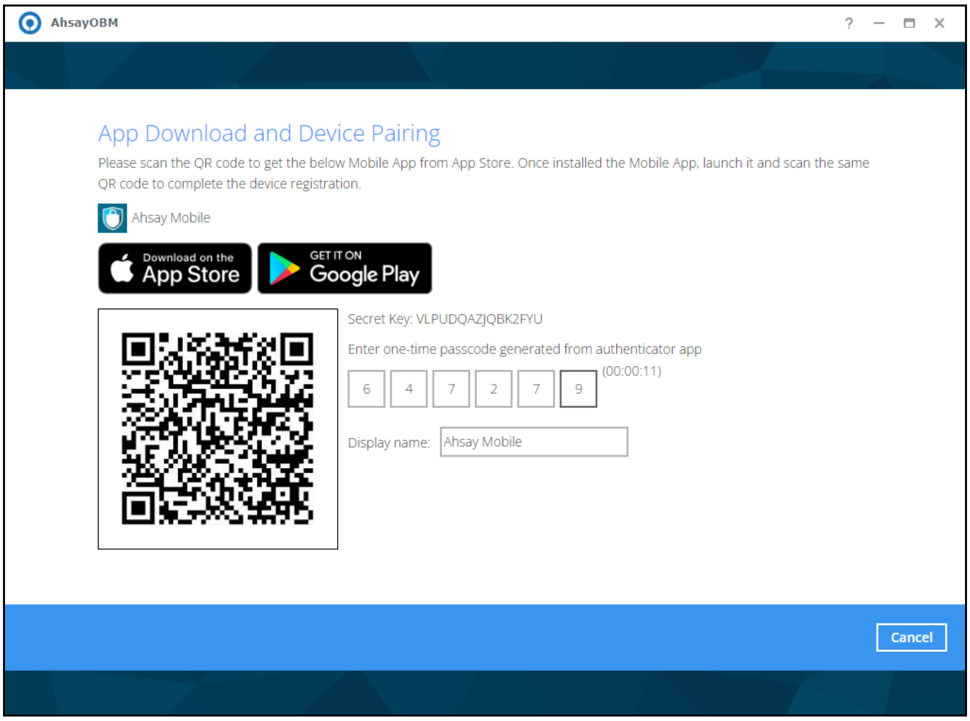


iv. Enter the Username and Secret Key shown in AhsayOBM then tap **Connect**. Once the device is paired successfully, tap **OK** to continue.




Connect using Secret Key
Key in the Secret Key provided by the app
user
••••••••••••••••
Device paired successfully
OK
Connect
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.

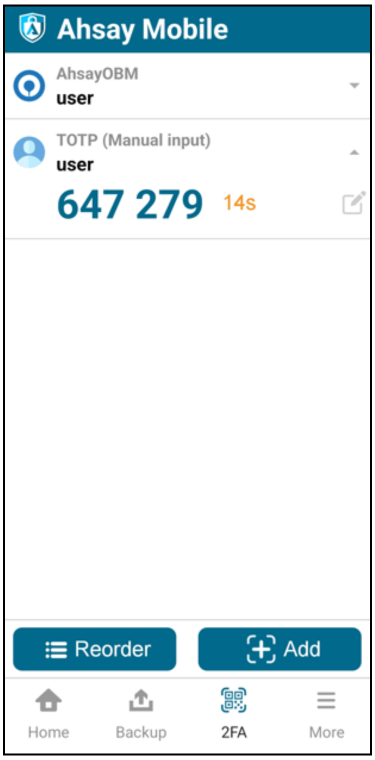
Secret Key: VLPUDQAZJQBK2FYU

Enter one-time passcode generated from authenticator app

6 4 7 2 7 9 (00:00:11)

Display name: Ahsay Mobile

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

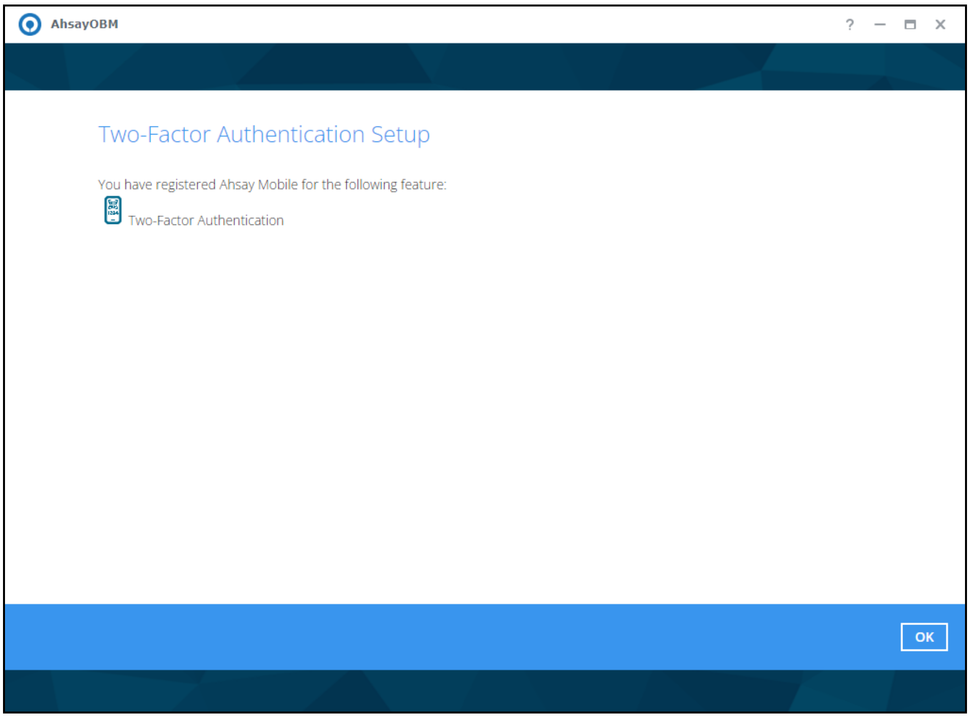


AhsayOBM
user

TOTP (Manual input)
user

647 279 14s

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



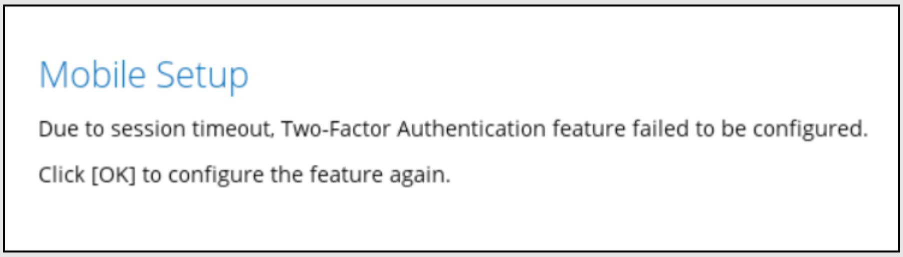
Two-Factor Authentication Setup

You have registered Ahsay Mobile for the following feature:

Two-Factor Authentication

**NOTE**

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

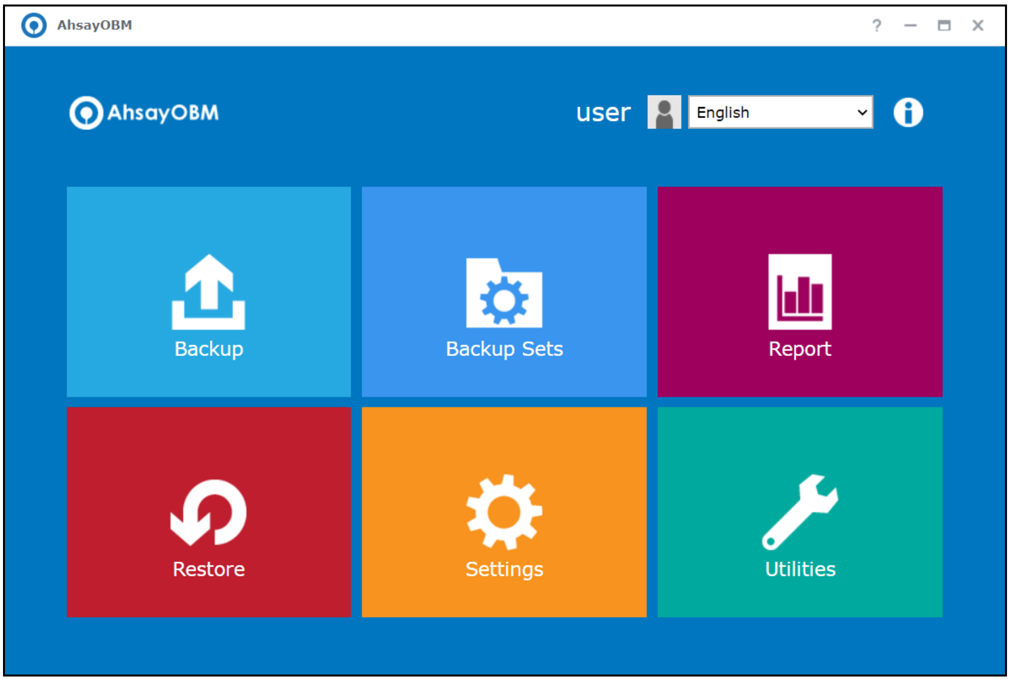


Mobile Setup

Due to session timeout, Two-Factor Authentication feature failed to be configured.

Click [OK] to configure the feature again.

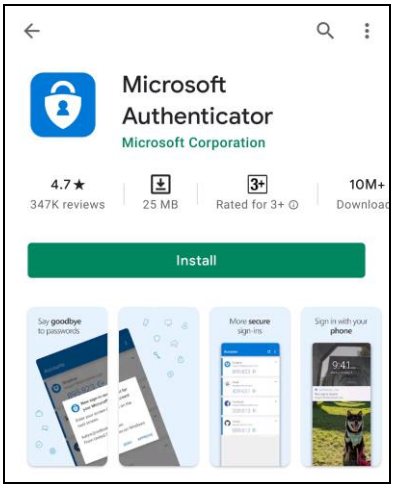
9. After successful pairing, the following screen will be displayed.



## 5.2 Using Microsoft Authenticator

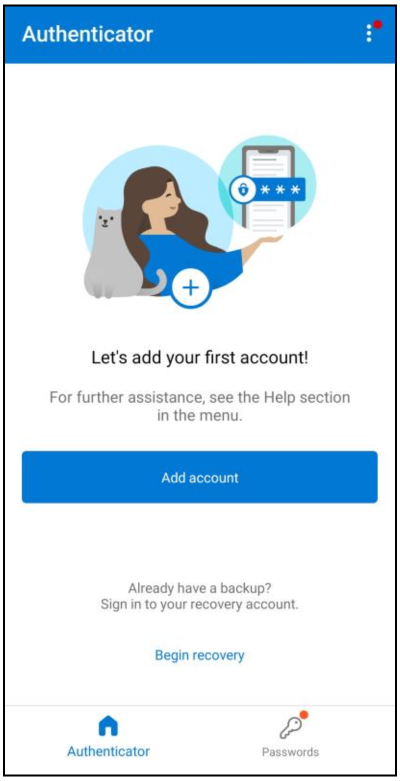
To register a device for TOTP 2FA in AhsayOBM using Microsoft Authenticator, please follow the steps below:

1. Download and install 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**.

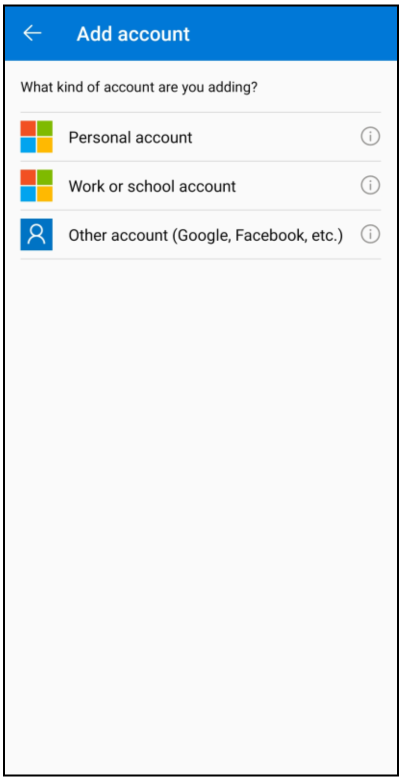


Let's add your first account!

For further assistance, see the Help section in the menu.

Already have a backup?
Sign in to your recovery account.

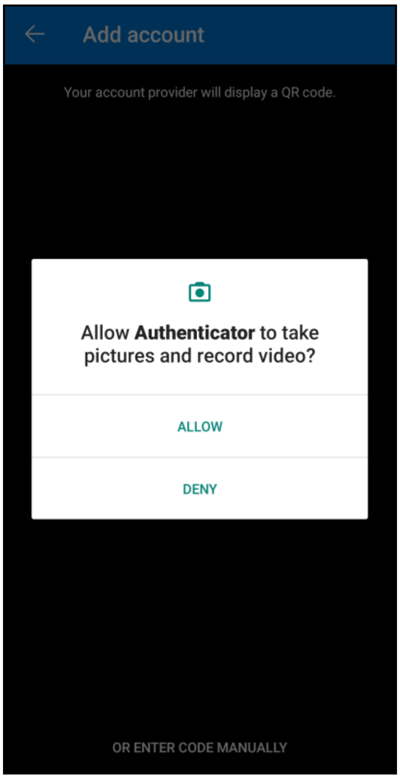
4. Select **Other account (Google, Facebook, etc.)**.



Add account

What kind of account are you adding?

5. Allow permission to take pictures and record video.



Add account

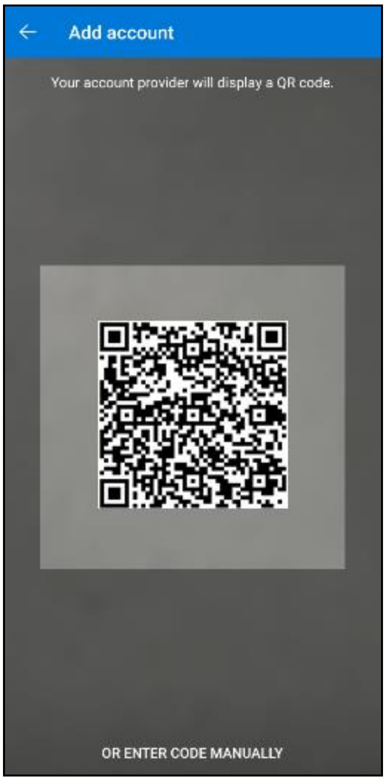
Your account provider will display a QR code.

Allow **Authenticator** 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**

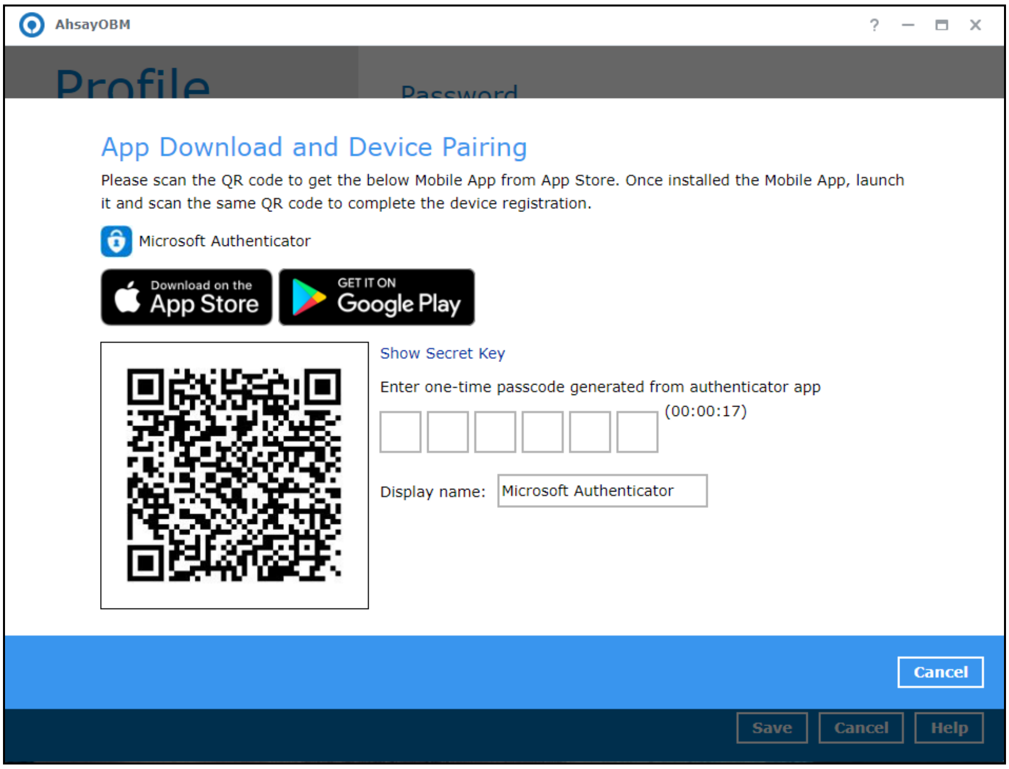
i. Scan the QR code on AhsayOBM.



Add account

Your account provider will display a QR code.

Example of the displayed QR code:



App Download and Device Pairing

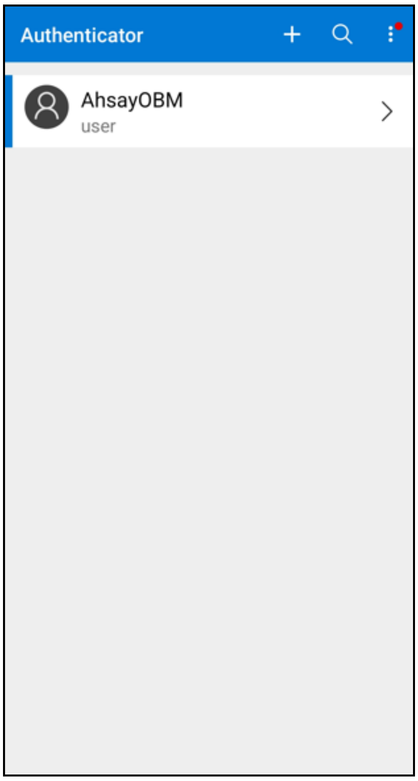
Please scan the QR code to get the below Mobile App from App Store. Once installed the Mobile App, launch it and scan the same QR code to complete the device registration.

Microsoft Authenticator

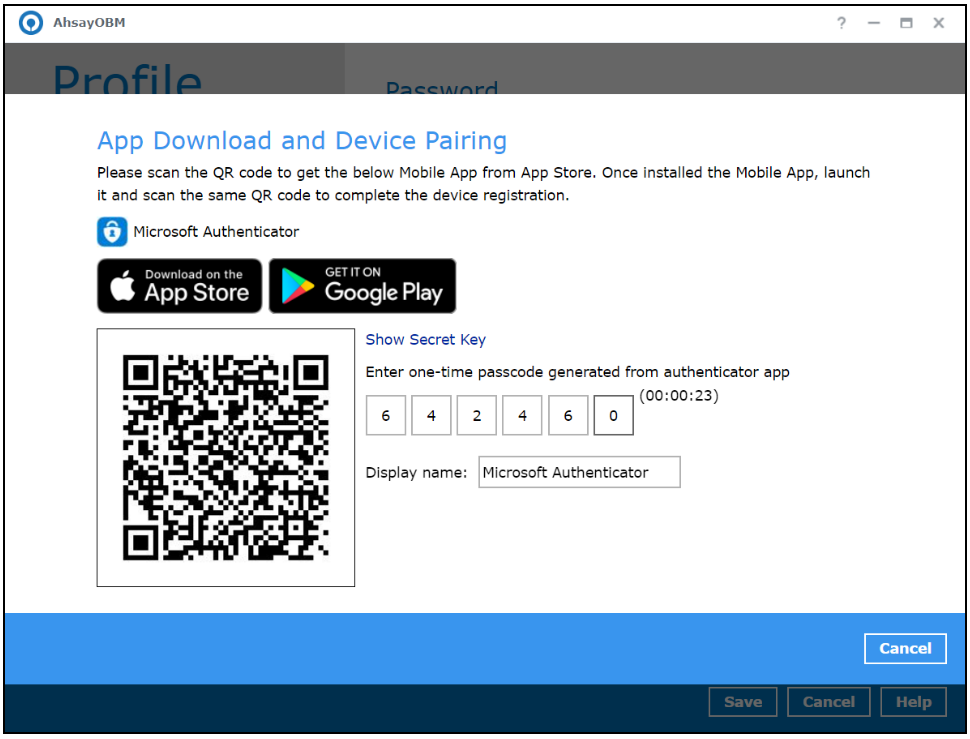
Enter one-time passcode generated from authenticator app (00:00:17)

Display name: Microsoft Authenticator

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



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

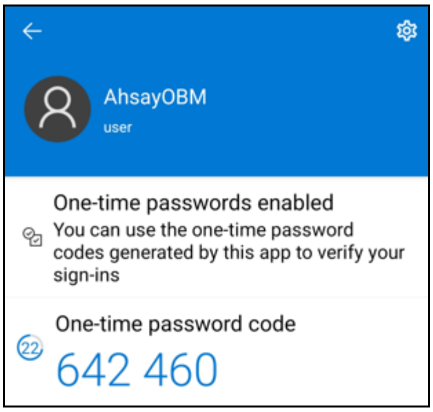
Microsoft Authenticator

Enter one-time passcode generated from authenticator app

6 4 2 4 6 0 (00:00:23)

Display name: Microsoft Authenticator

Example of the one-time passcode generated:

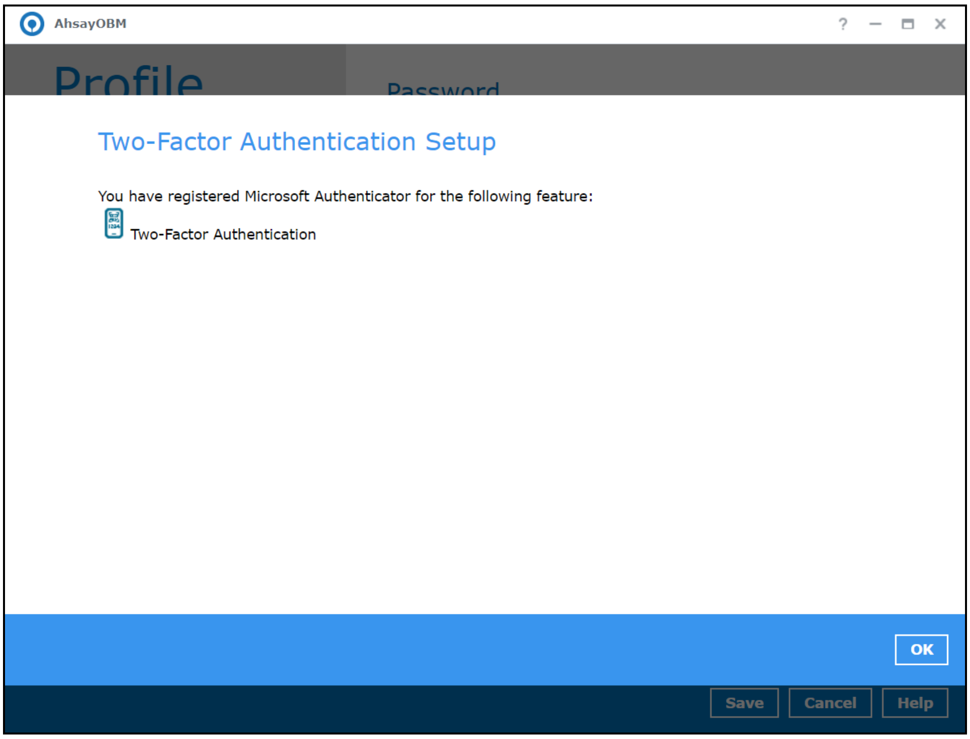


AhsayOBM
user

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

One-time password code
642 460

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



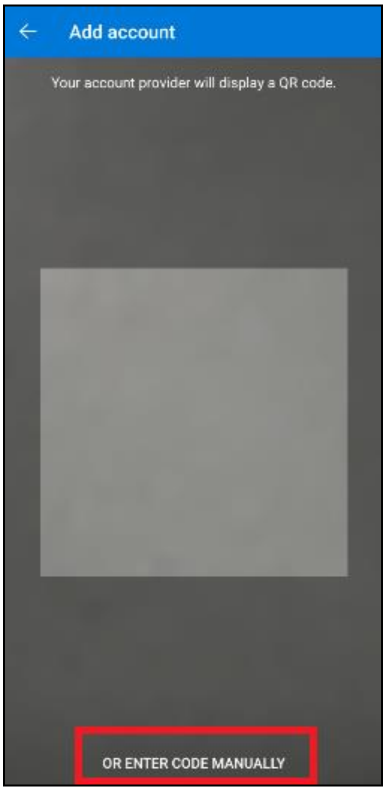
Two-Factor Authentication Setup

You have registered Microsoft Authenticator for the following feature:

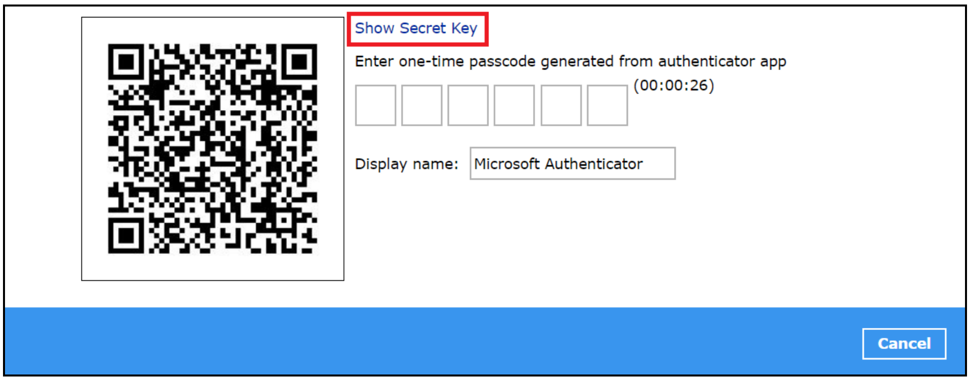
Two-Factor Authentication

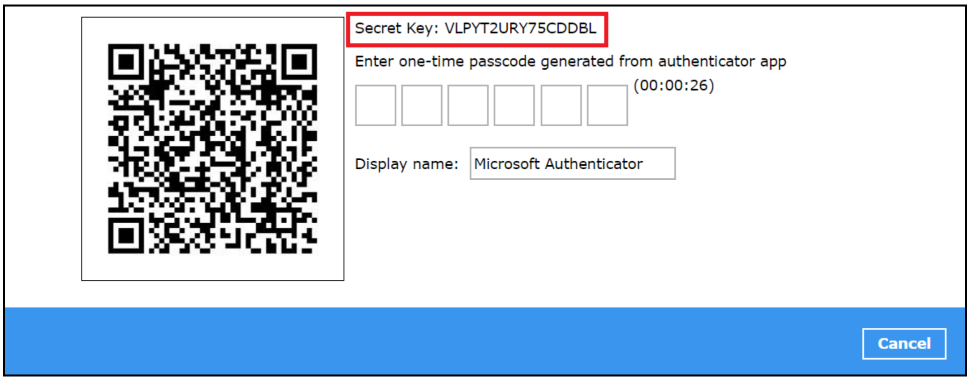
### Method 2: Enter Code Manually

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

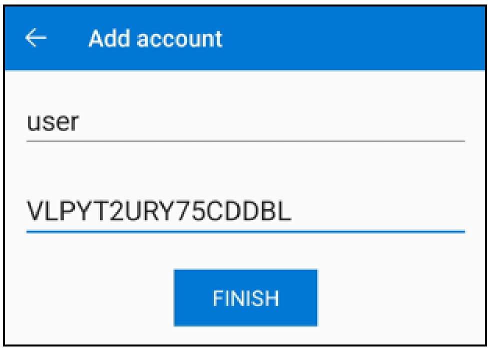


ii. Click the **Show Secret Key** link in AhsayOBM to display the Secret Key which must be entered manually in Microsoft Authenticator.


Show Secret Key
Enter one-time passcode generated from authenticator app
(00:00:26)
Display name: Microsoft Authenticator
Cancel


Secret Key: VLPYT2URY75CDDBL
Enter one-time passcode generated from authenticator app
(00:00:26)
Display name: Microsoft Authenticator
Cancel

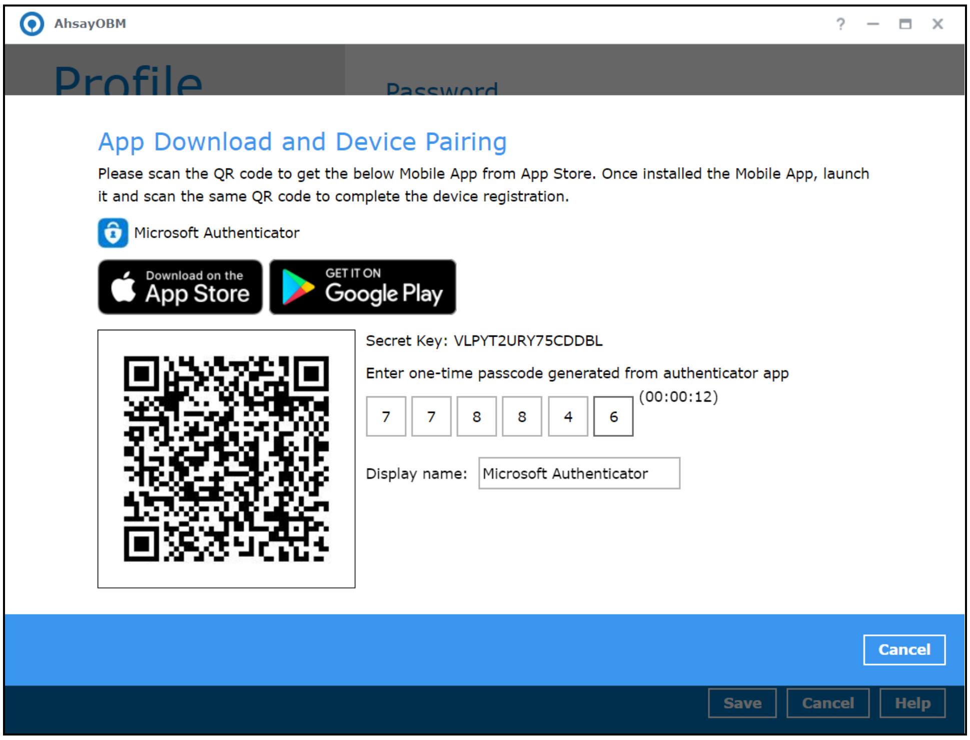
iii. On the Microsoft Authenticator app, input an account name, then enter the displayed Secret Key in AhsayOBM. Tap **FINISH** to proceed.



user

VLPYT2URY75CDDBL

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

Microsoft Authenticator

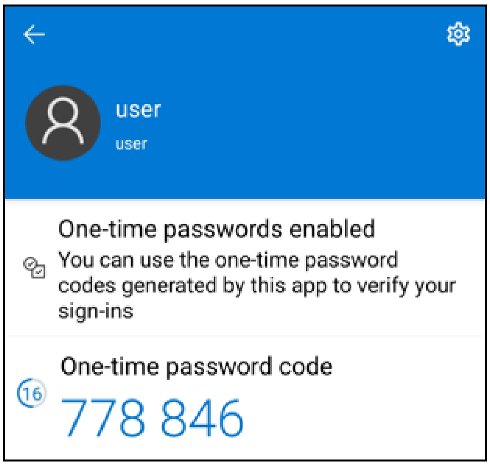
Secret Key: VLPYT2URY75CDDBL

Enter one-time passcode generated from authenticator app

7 7 8 8 4 6 (00:00:12)

Display name: Microsoft Authenticator

Example of the one-time passcode generated:



user

user

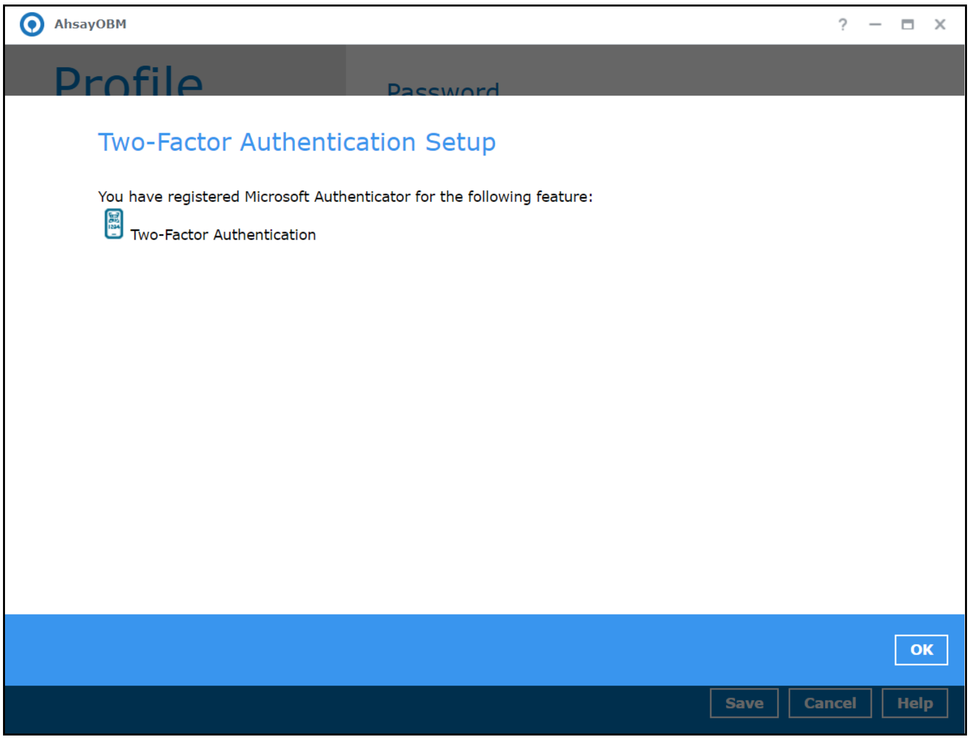
One-time passwords enabled

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

One-time password code

778 846

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

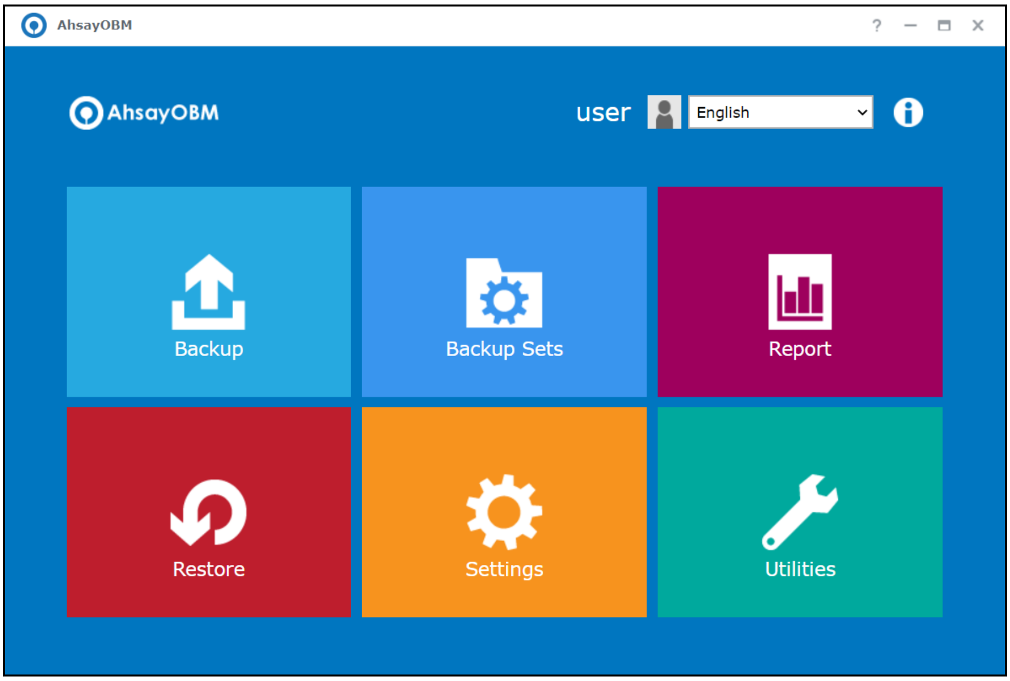


Two-Factor Authentication Setup

You have registered Microsoft Authenticator for the following feature:

Two-Factor Authentication

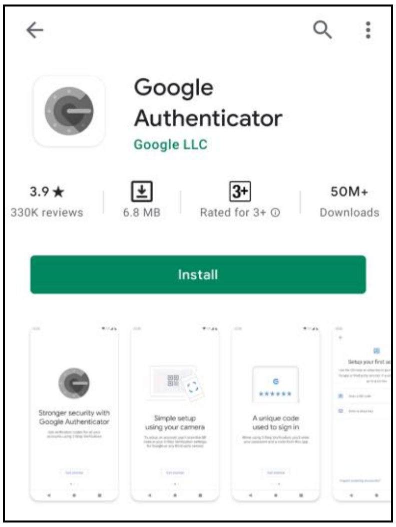
7. After successful pairing, the following screen will be displayed.



## 5.3 Using Google Authenticator

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

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



Google Authenticator

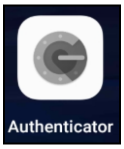
Google LLC

3.9★ 330K reviews | 6.8 MB | Rated for 3+ | 50M+ Downloads

Install

Stronger security with Google Authenticator
Simple setup using your camera
A unique code used to sign in

2. Launch the Google Authenticator app.

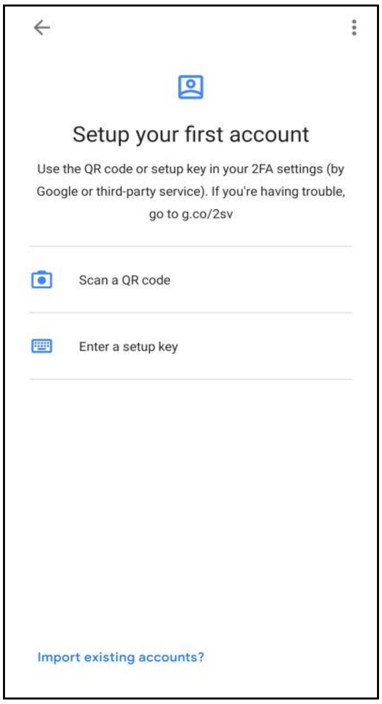


Authenticator

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**.



Setup your first account

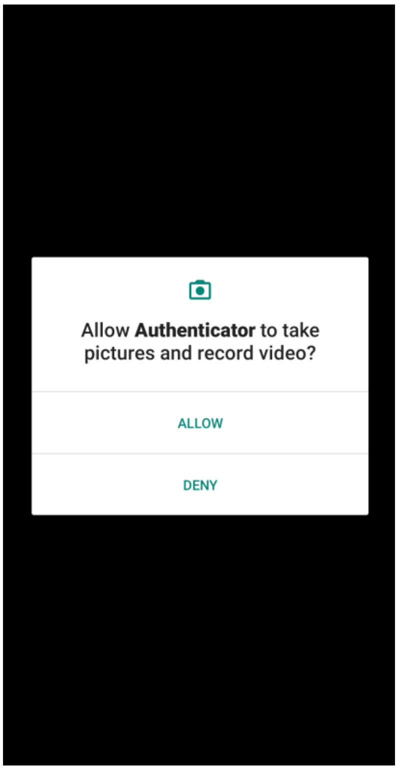
Use the QR code or setup key in your 2FA settings (by Google or third-party service). If you're having trouble, go to g.co/2sv

Scan a QR code

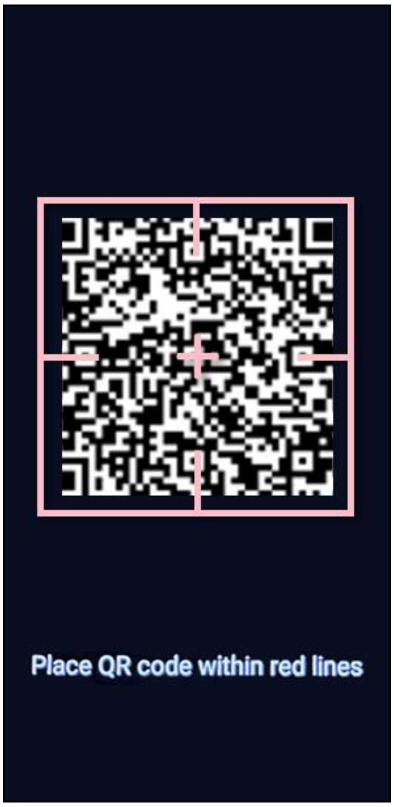
Enter a setup key

Import existing accounts?

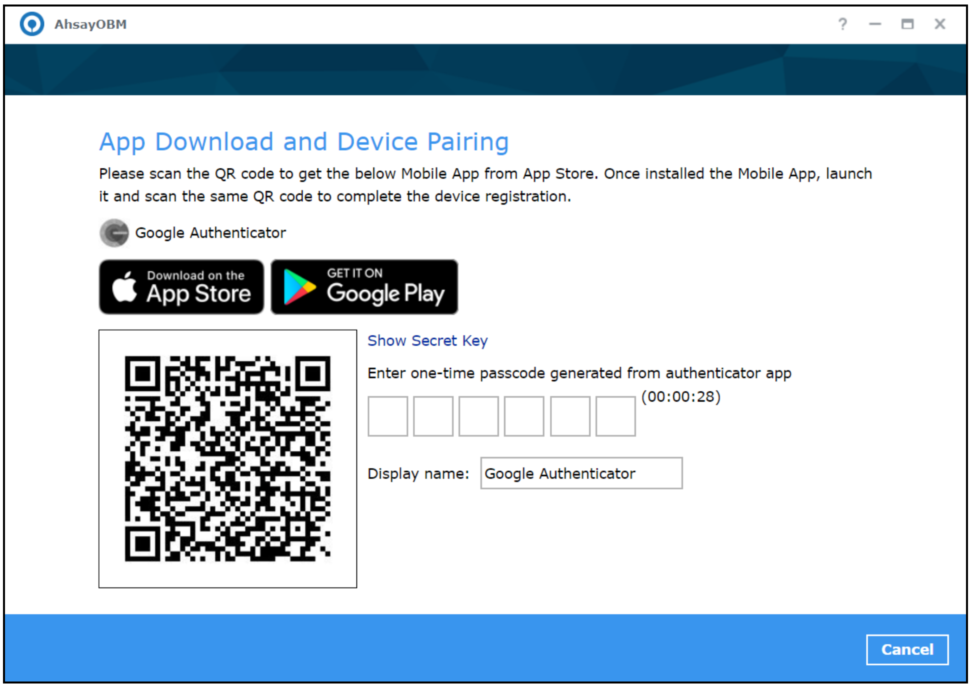
ii. Allow permission to take pictures and record video.


Allow **Authenticator** to take pictures and record video?

iii. Scan the QR code on AhsayOBM.


Place QR code within red lines

Example of the displayed QR code:



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.

Google Authenticator

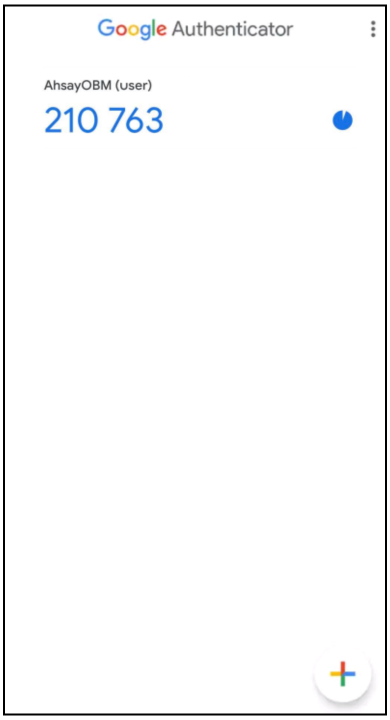
Show Secret Key

Enter one-time passcode generated from authenticator app

□□□□□□ (00:00:28)

Display name: Google Authenticator

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

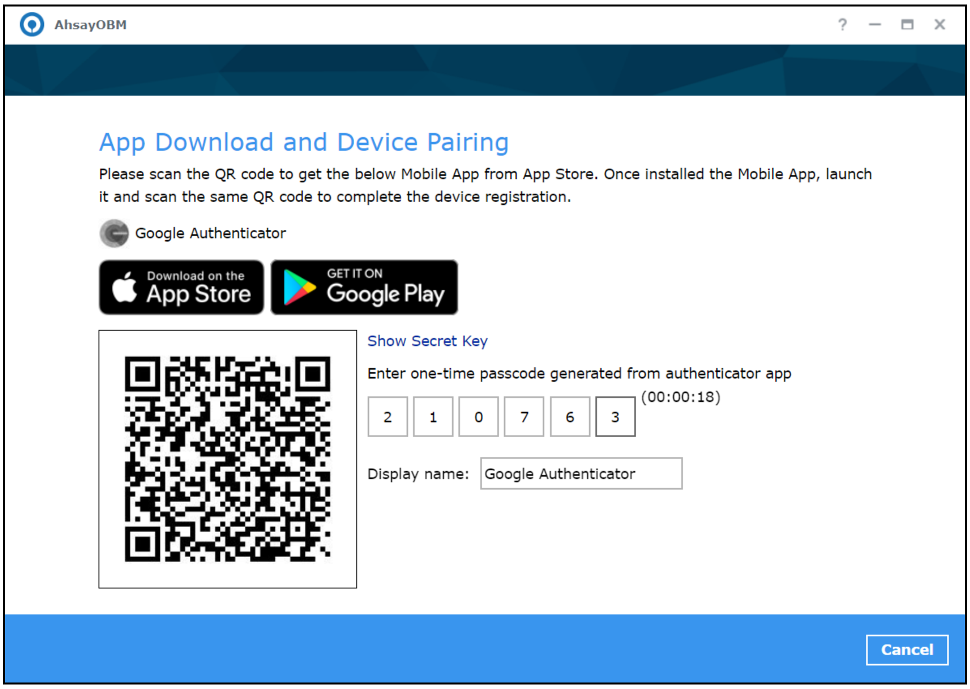


Google Authenticator

AhsayOBM (user)

210 763

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

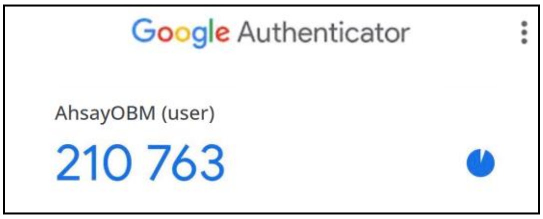
Google Authenticator

Enter one-time passcode generated from authenticator app

2 1 0 7 6 3 (00:00:18)

Display name: Google Authenticator

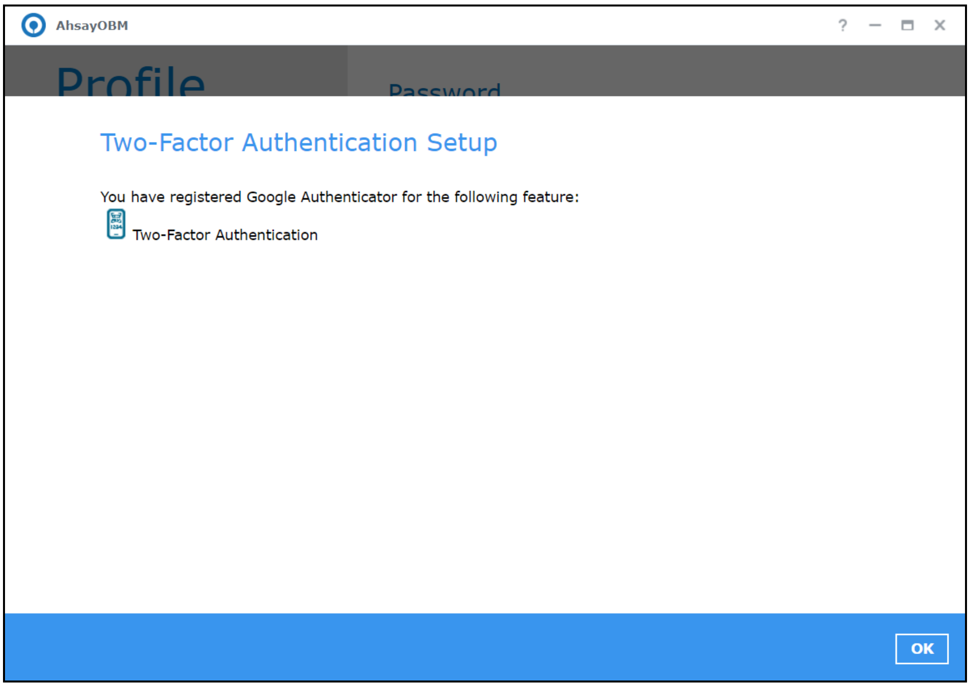
Example of the one-time passcode generated:



AhsayOBM (user)

210 763

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



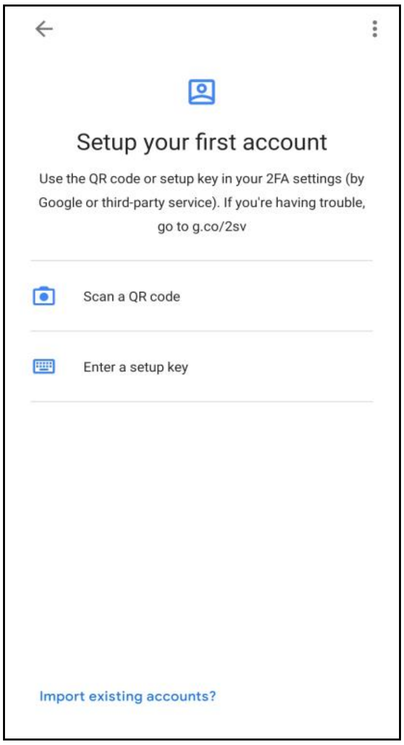
Two-Factor Authentication Setup

You have registered Google Authenticator for the following feature:

Two-Factor Authentication

**Method 2: Enter a setup key manually**

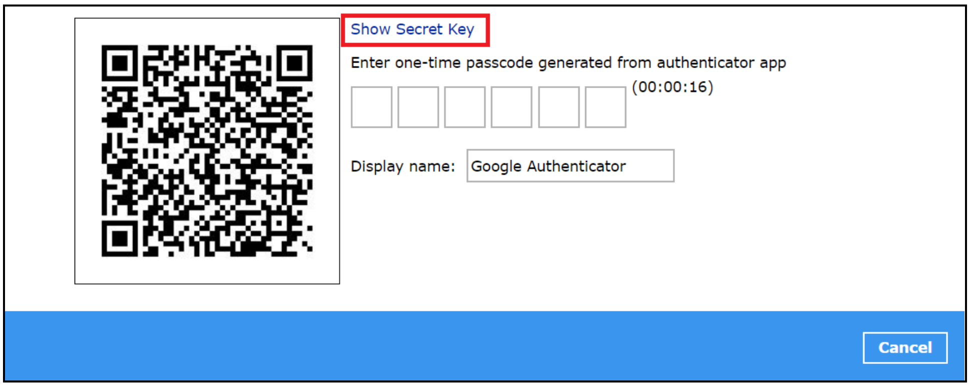
i. Tap **Enter a setup key**.



Setup your first account

Use the QR code or setup key in your 2FA settings (by Google or third-party service). If you're having trouble, go to g.co/2sv

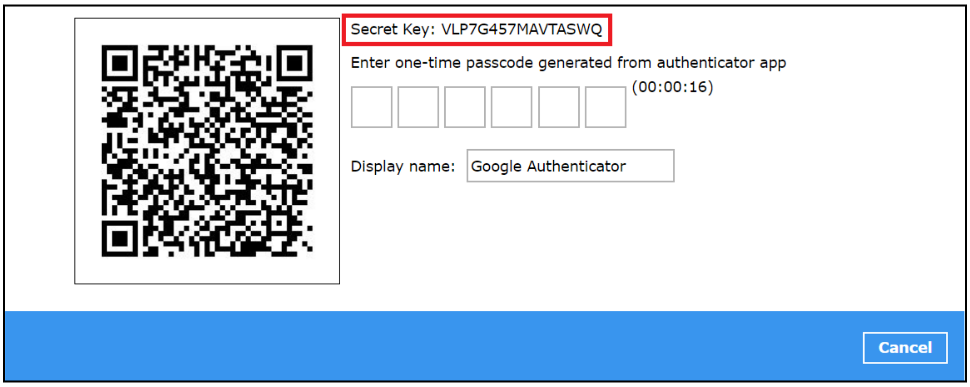
ii. Click the **Show Secret Key** link in AhsayOBM to display the Secret Key which must be entered manually in Google Authenticator.



Enter one-time passcode generated from authenticator app

(00:00:16)

Display name: Google Authenticator



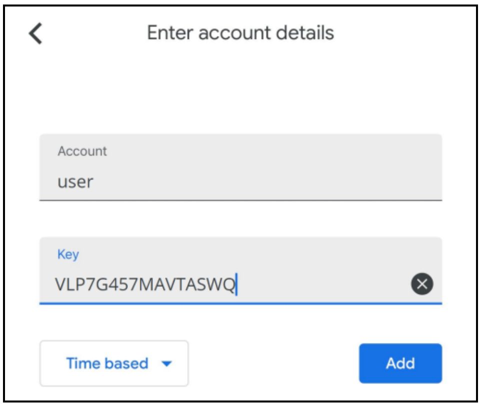
Secret Key: VLP7G457MAVTASWQ

Enter one-time passcode generated from authenticator app

(00:00:16)

Display name: Google Authenticator

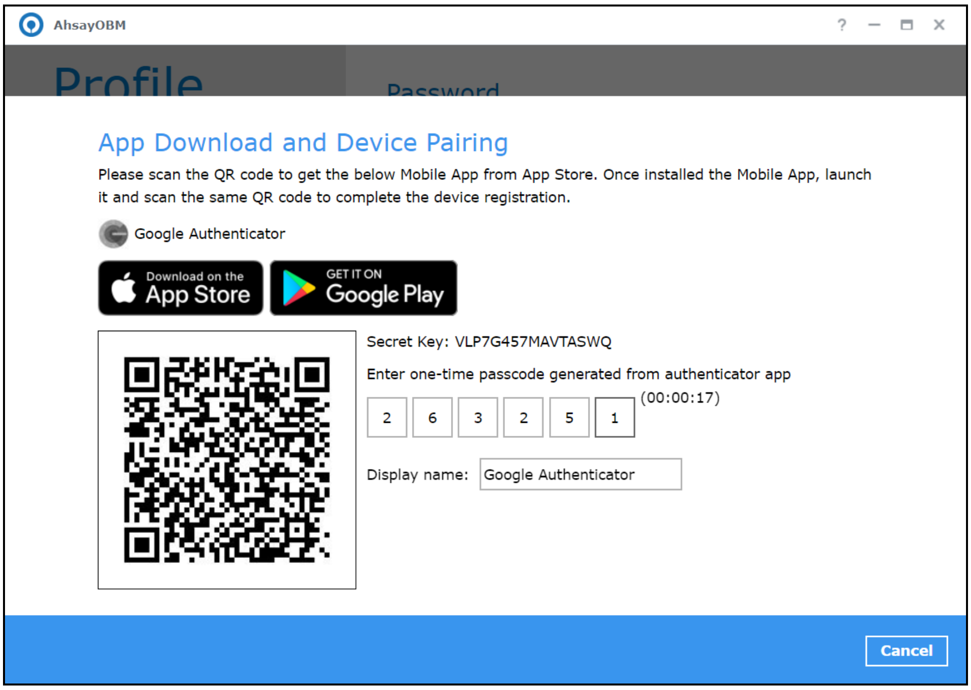
iii. On the Google Authenticator app, input an account name, then enter the displayed Secret Key in AhsayOBM. Tap **Add** to proceed.



Account: user

Key: VLP7G457MAVTASWQ

iv. Once the account is added to Google 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.

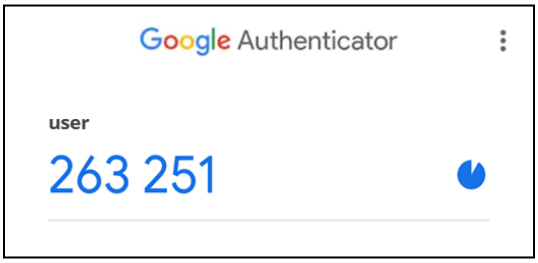
Secret Key: VLP7G457MAVTASWQ

Enter one-time passcode generated from authenticator app

2 6 3 2 5 1 (00:00:17)

Display name: Google Authenticator

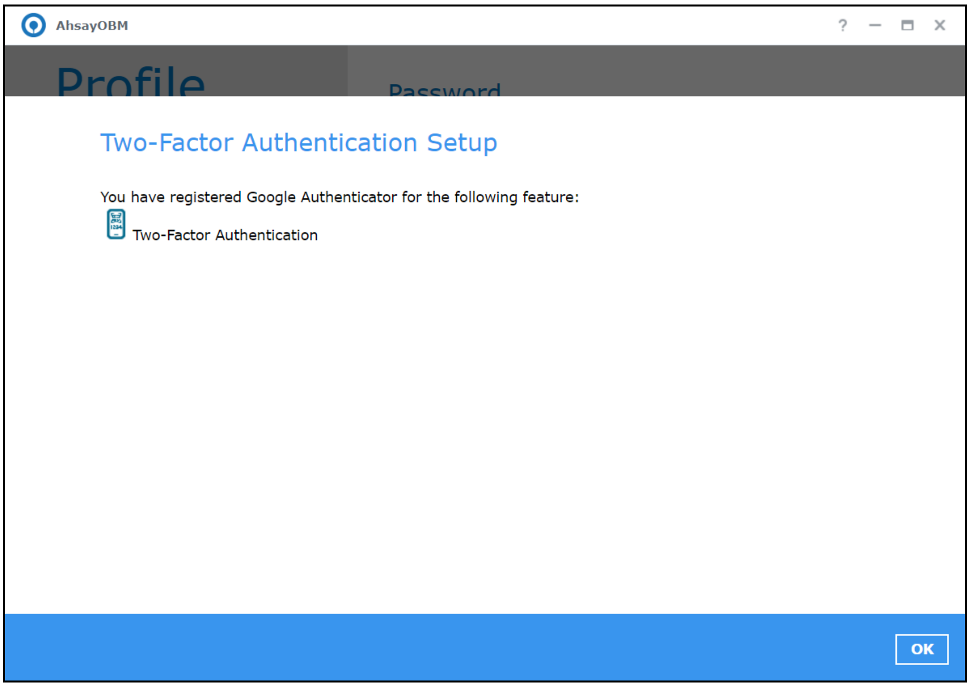
Example of the one-time passcode generated:



user

263 251

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

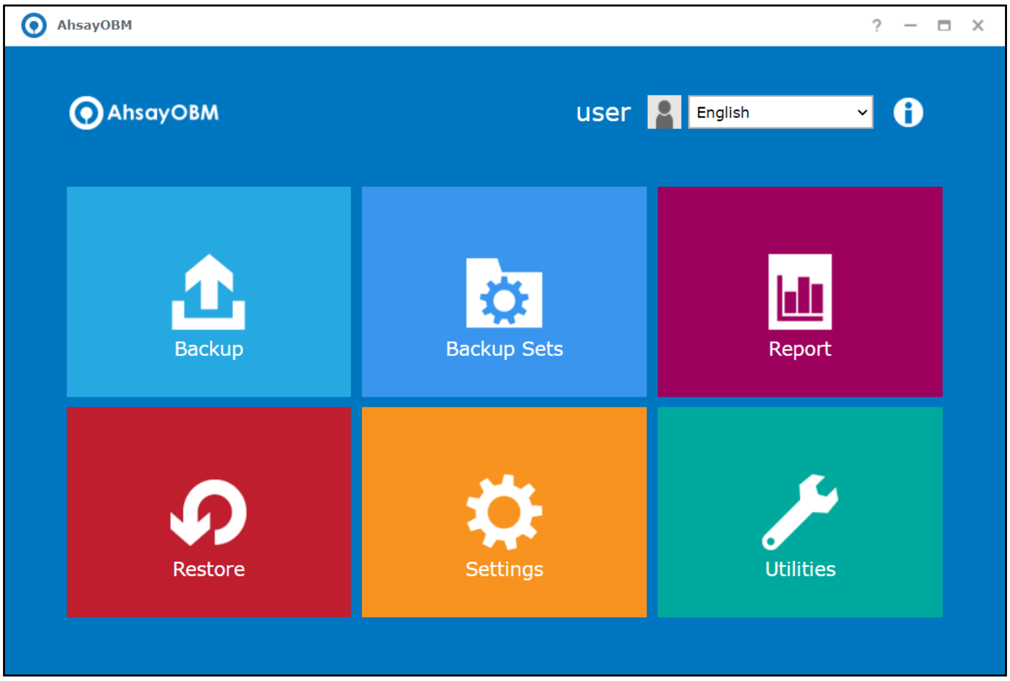


Two-Factor Authentication Setup

You have registered Google Authenticator for the following feature:

Two-Factor Authentication

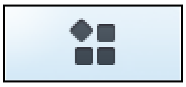
4. After successful pairing, the following screen will be displayed.



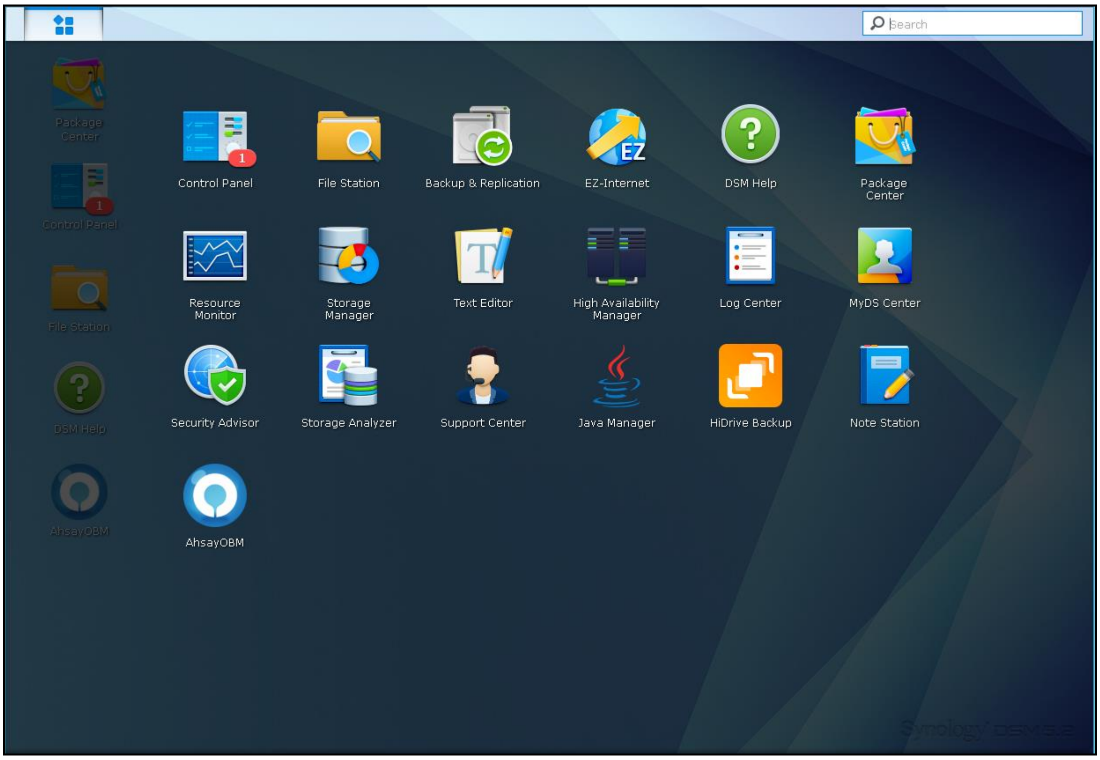
# 6 Start AhsayOBM

## 6.1 Add an AhsayOBM Shortcut Icon to the Desktop

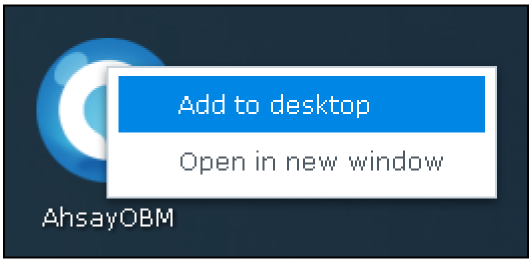
1. In the DiskStation Manager (DSM) console, click the **Main Menu** icon on the top left corner of the desktop to open it.



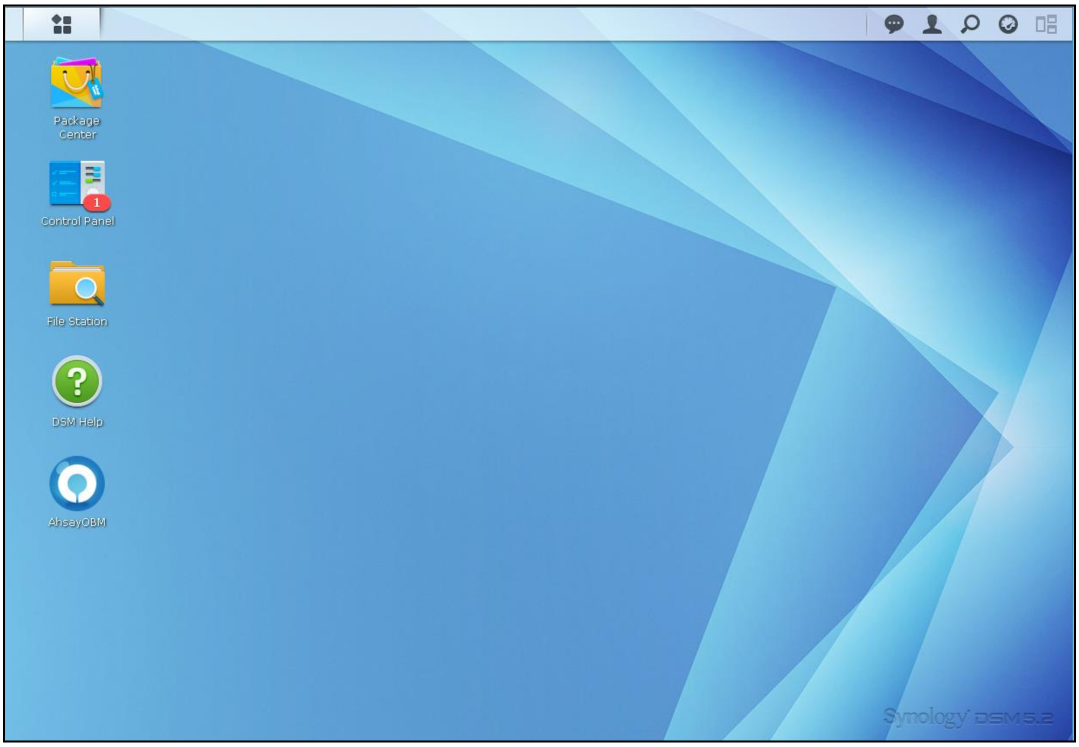
2. All application icons will be shown. Look for the **AhsayOBM** icon.



3. Right-click the **AhsayOBM** icon and select **Add to desktop**.



4. The AhsayOBM shortcut icon will be added to the desktop.



## 6.2 Login to AhsayOBM

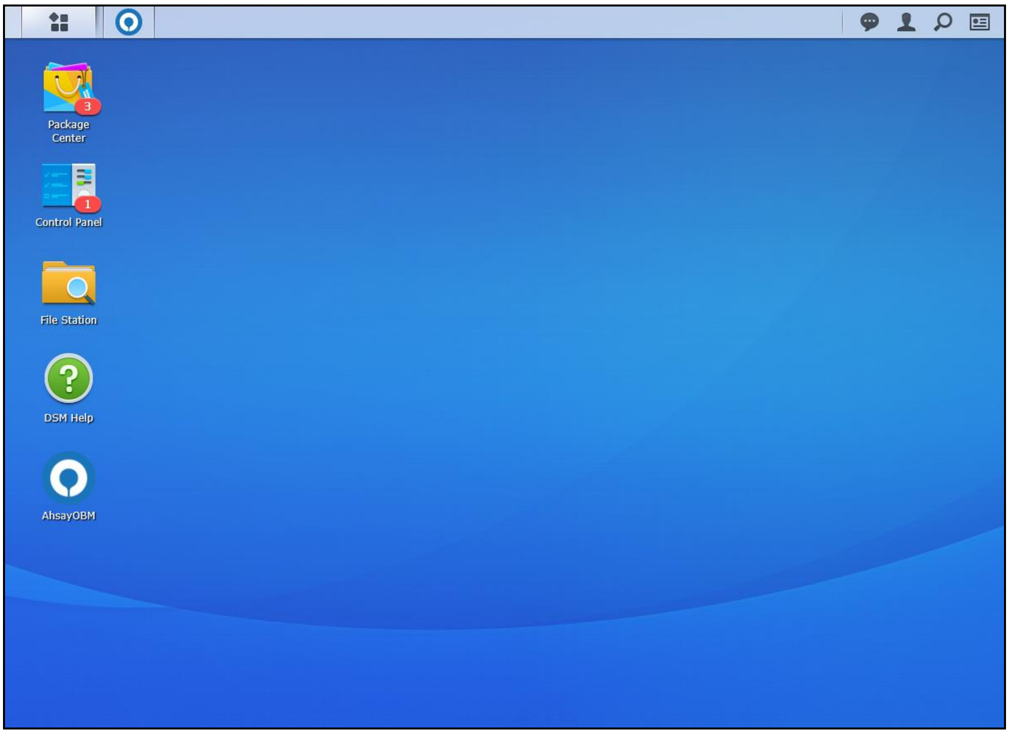
Login steps without 2FA and with 2FA using the different types of authenticators will be discussed in this chapter.

- Login to AhsayOBM without 2FA
- Login to AhsayOBM with 2FA using Ahsay Mobile
- Login to AhsayOBM with 2FA using third-party TOTP authenticator
- Login to AhsayOBM with 2FA using Twilio

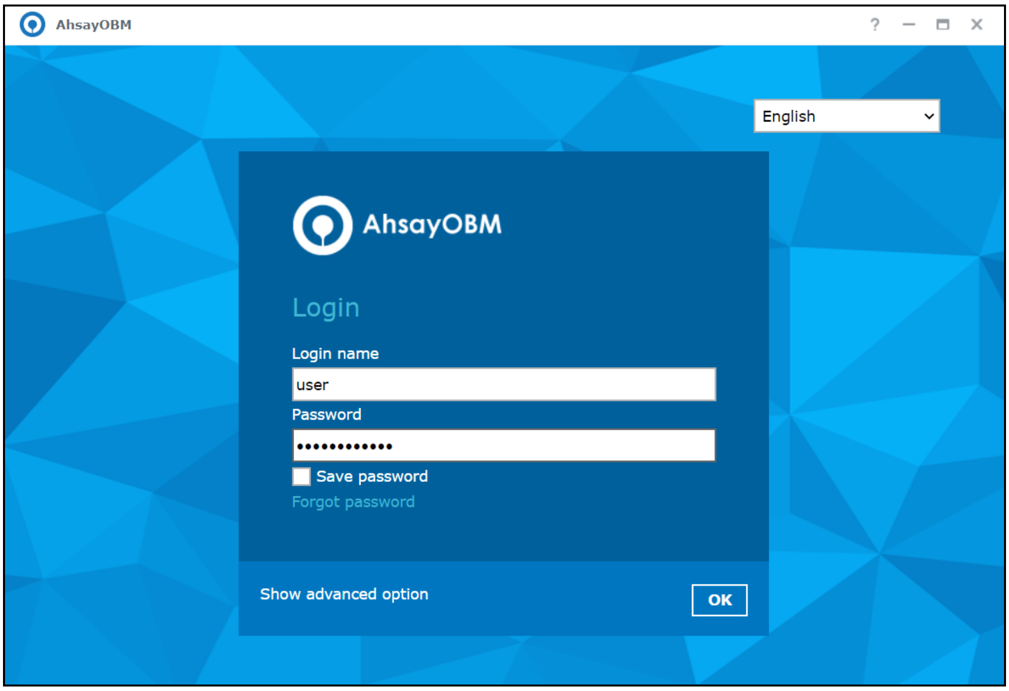
### 6.2.1 Login to AhsayOBM without 2FA

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

1. Click the AhsayOBM icon on the desktop to launch the application.



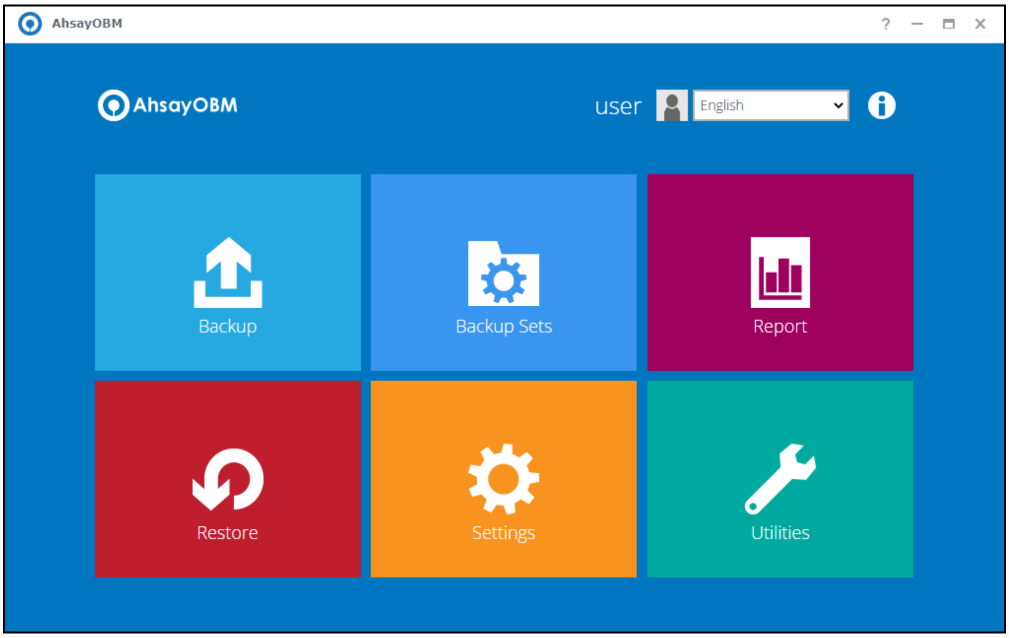
2. Enter the Login name and Password of your AhsayOBM account provided by your backup service provider. Then, click **OK** to login.



**NOTE**

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

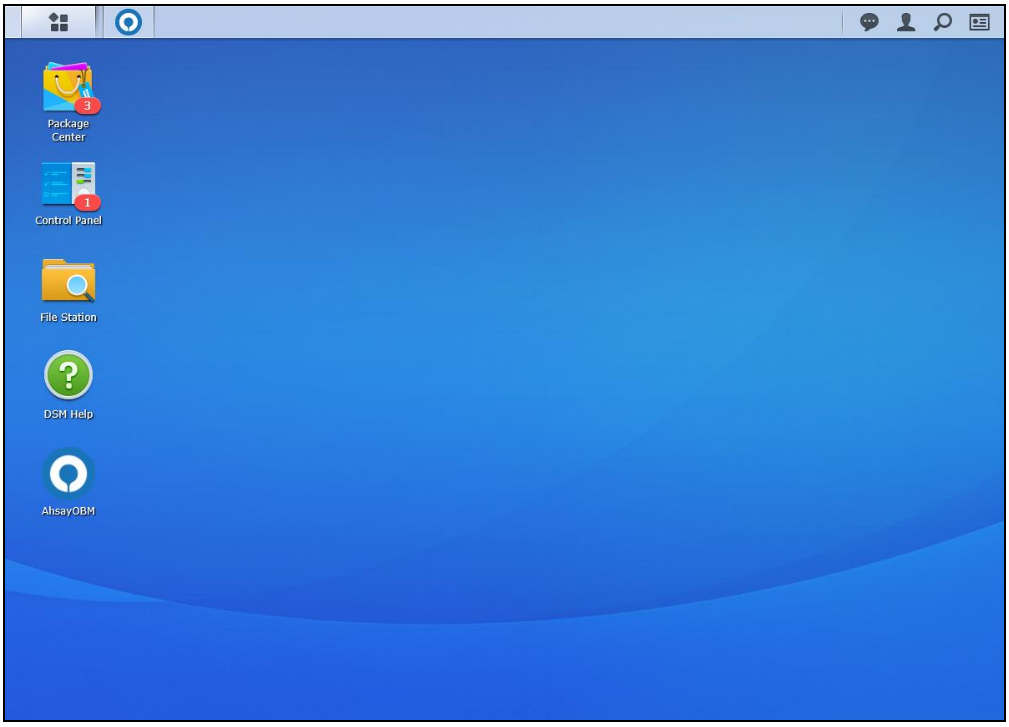
3. After successful login, the following screen will be displayed.



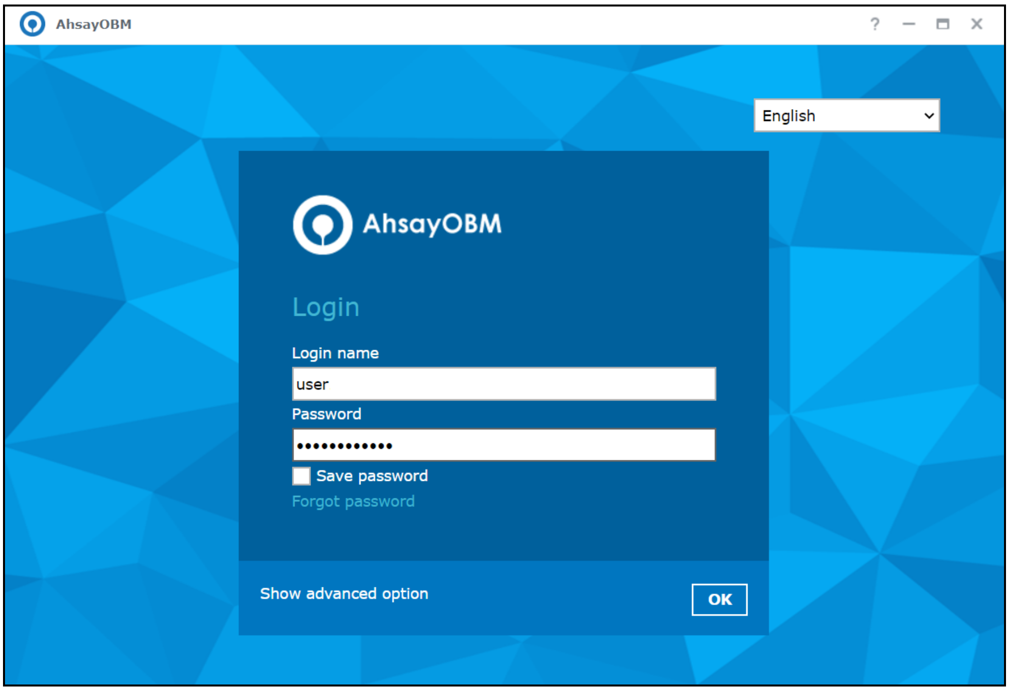
### 6.2.2 Login to AhsayOBM with 2FA using Ahsay Mobile

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

1. Click the AhsayOBM icon on the desktop 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.



Login name: user

Password: ••••••••••••

□ Save password

**NOTE**

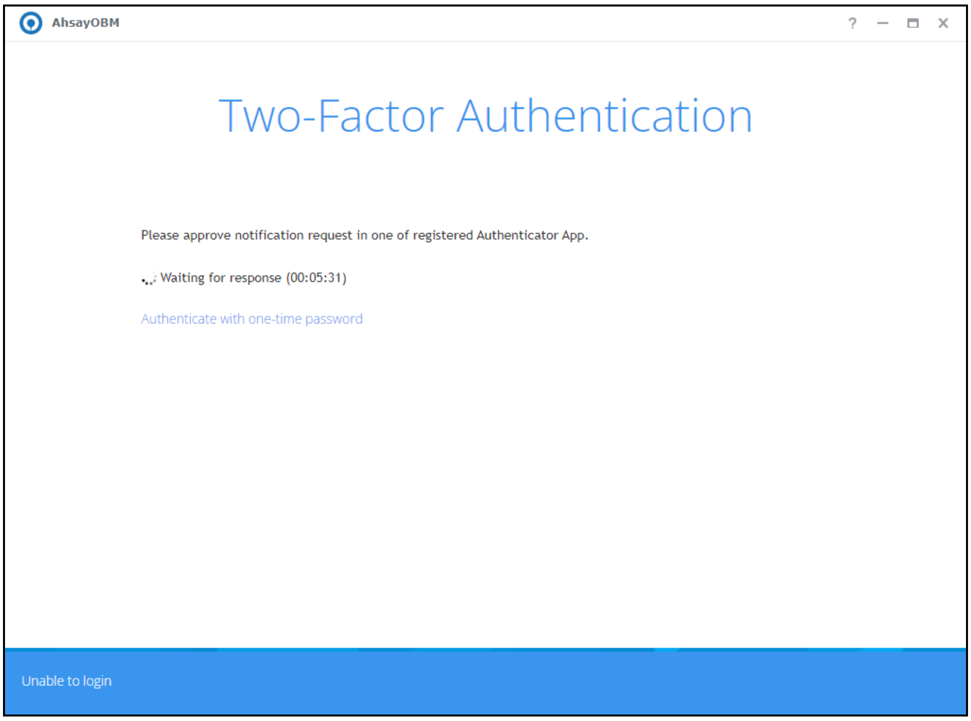
The Save password option may not be available. This depends on the settings of your backup service provider. Please contact your backup service provider for more information.

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

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

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

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



AhsayOBM
? — ▭ ✕
Two-Factor Authentication

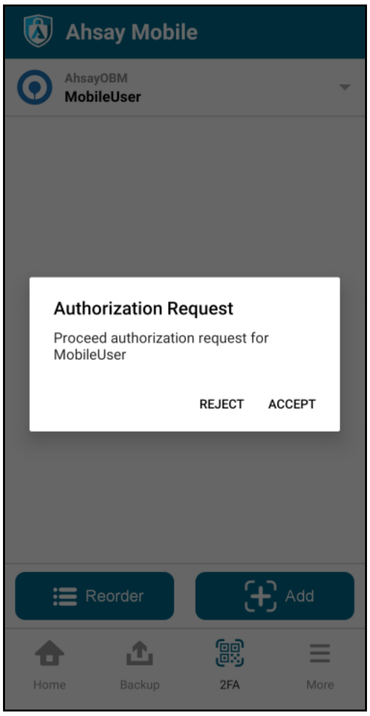
Please approve notification request in one of registered Authenticator App.

Waiting for response (00:05:31)

Authenticate with one-time password
Unable to login

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

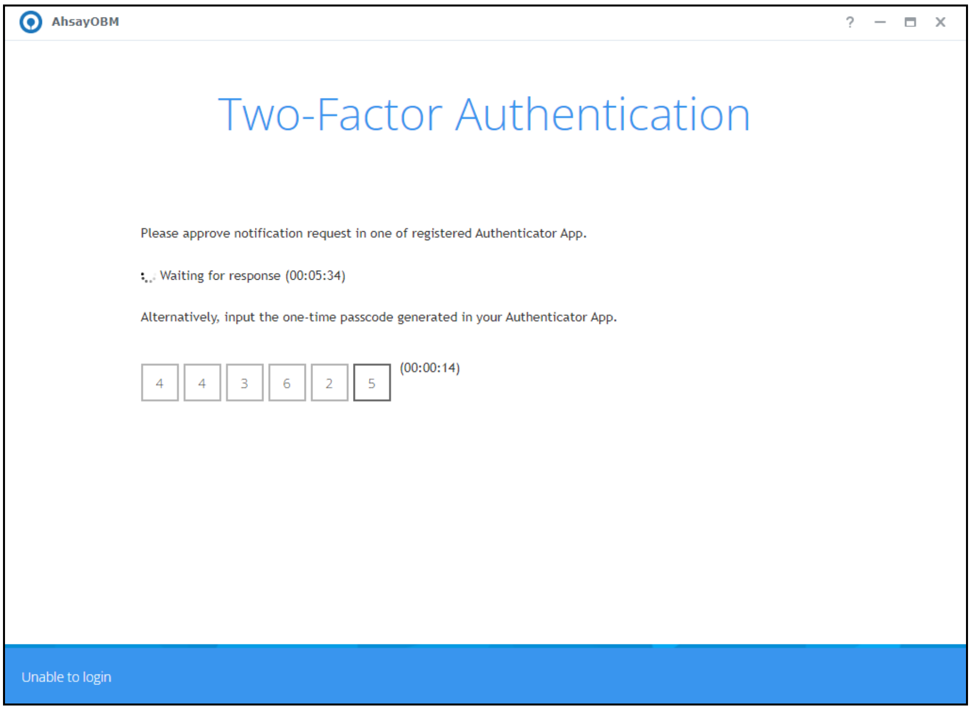
Example of the login request sent to Ahsay Mobile:



Authorization Request

Proceed authorization request for MobileUser

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

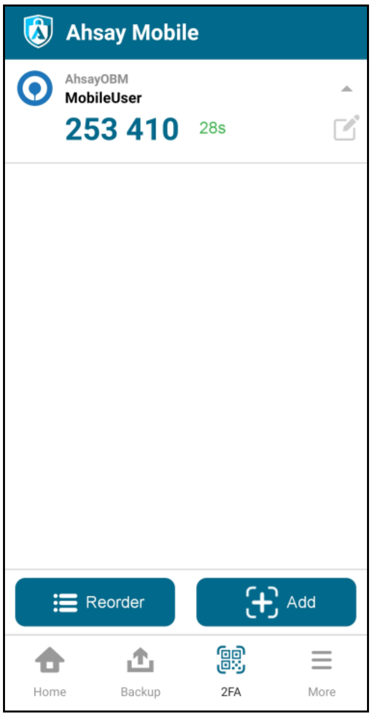
Please approve notification request in one of registered Authenticator App.

Waiting for response (00:05:34)

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

4 4 3 6 2 5 (00:00:14)

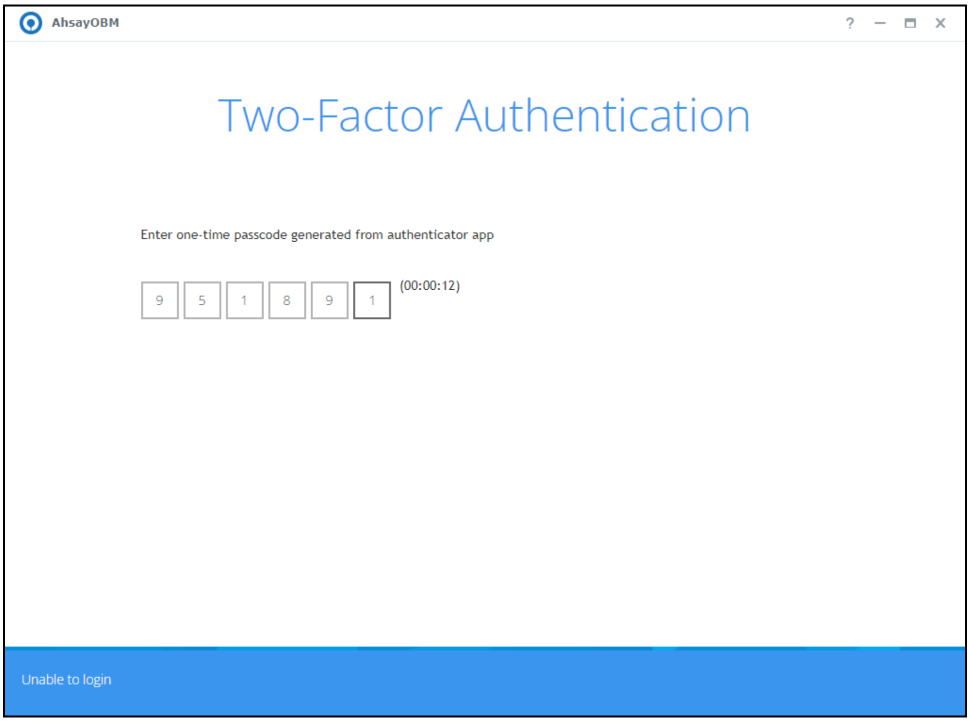
Example of the one-time password generated by Ahsay Mobile:



- **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.



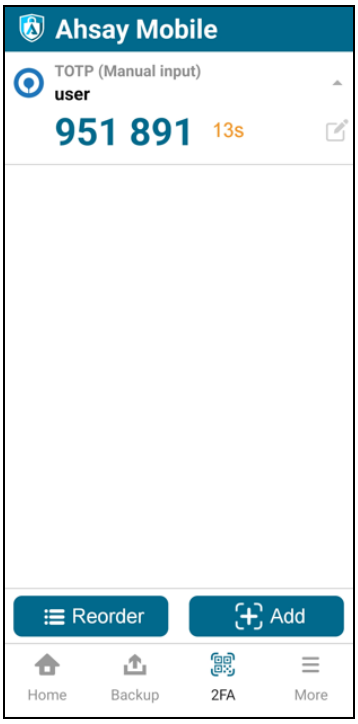
Two-Factor Authentication

Enter one-time passcode generated from authenticator app

9 5 1 8 9 1 (00:00:12)

Unable to login

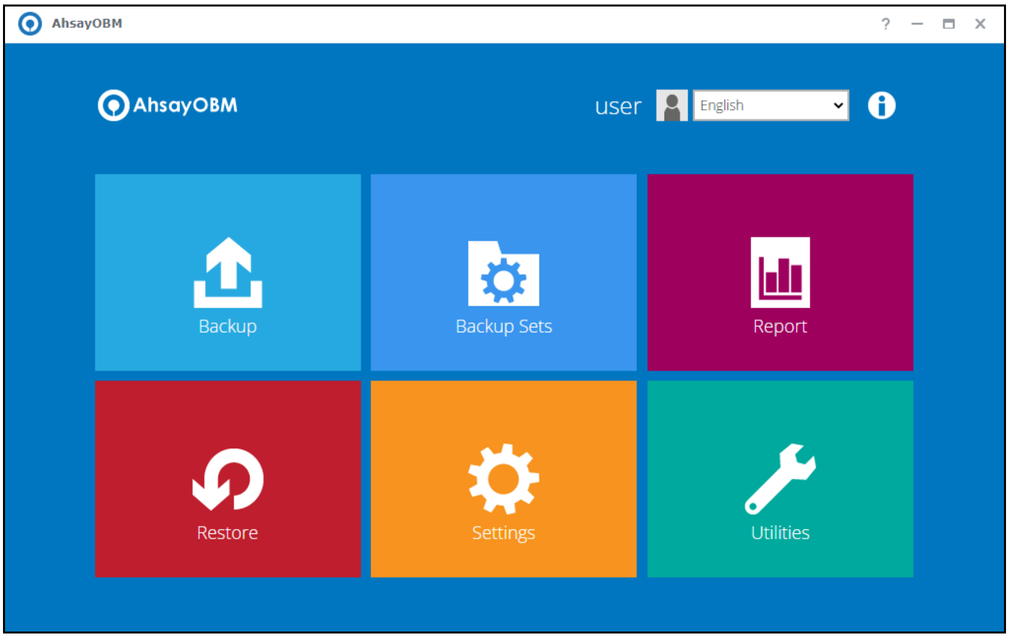
Example of the one-time password generated by Ahsay Mobile:



**NOTE**

If you are unable to login using any of the authentication method, refer to Chapter 7 Unable to login to AhsayOBM with 2FA.

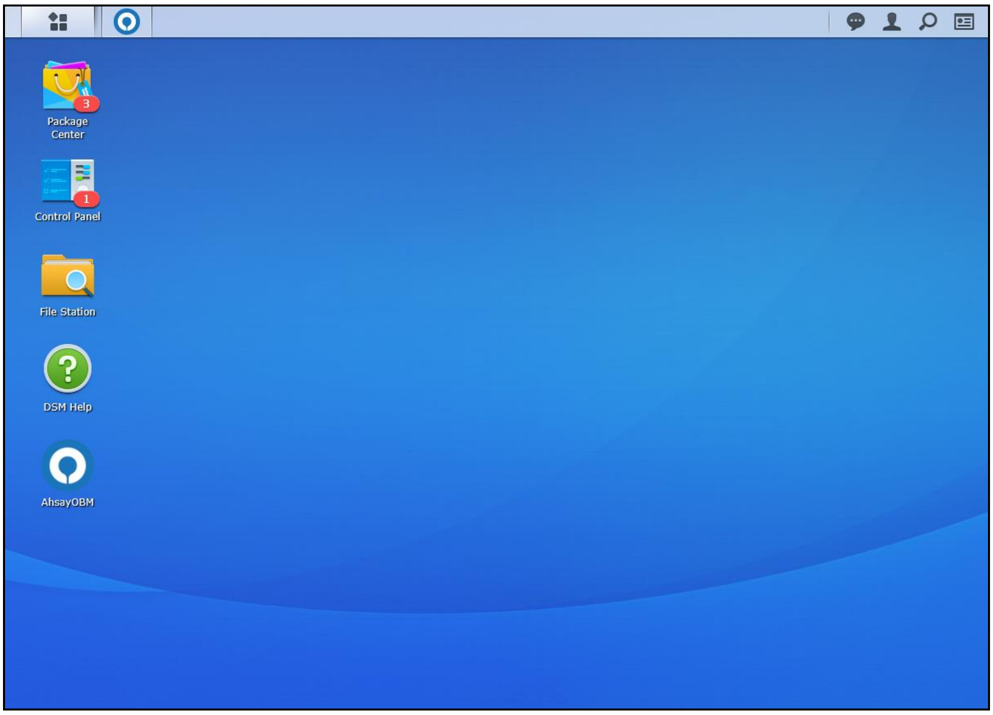
4. After successful login, the following screen will be displayed.



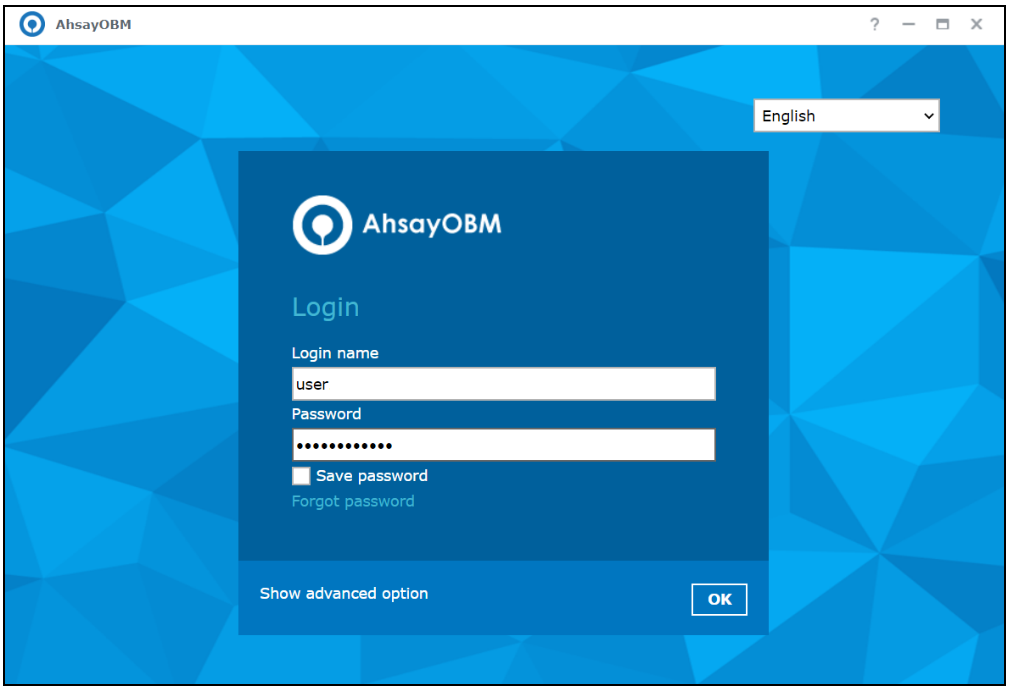
### 6.2.3 Login to AhsayOBM with 2FA using third-party TOTP authenticator

When logging in to AhsayOBM with Two-Factor Authentication using third-party TOTP authenticator, please follow the steps below:

1. Click the AhsayOBM icon on the desktop 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.



Login name: user

Password: ••••••••••••

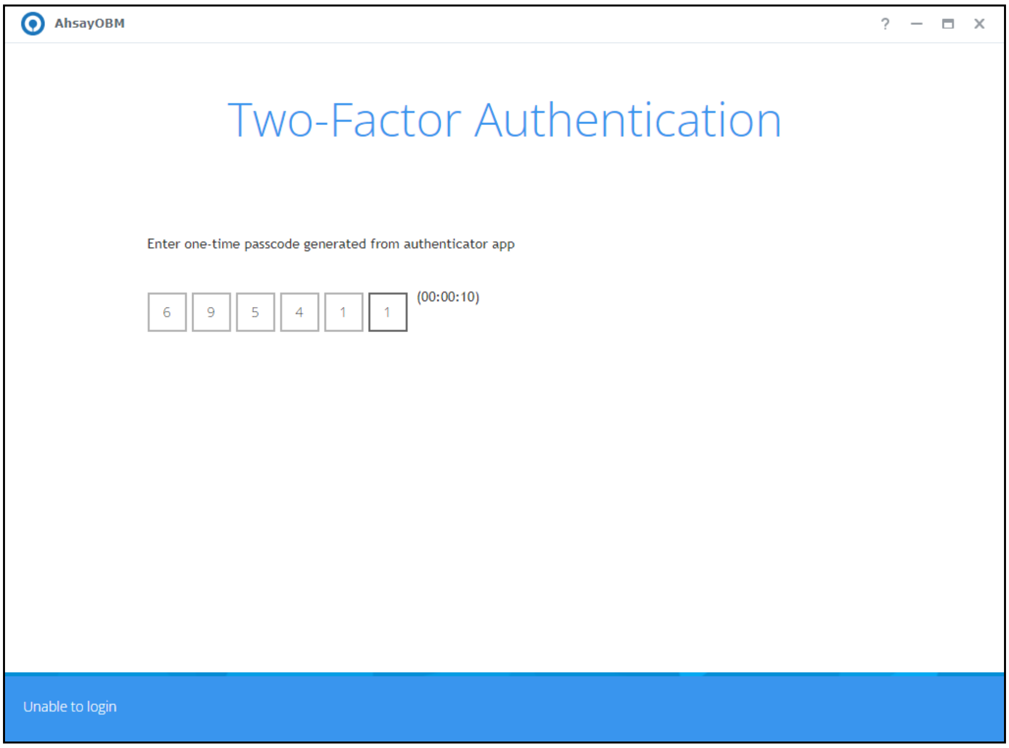
□ Save password

Forgot password

**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 third-party TOTP authenticator.

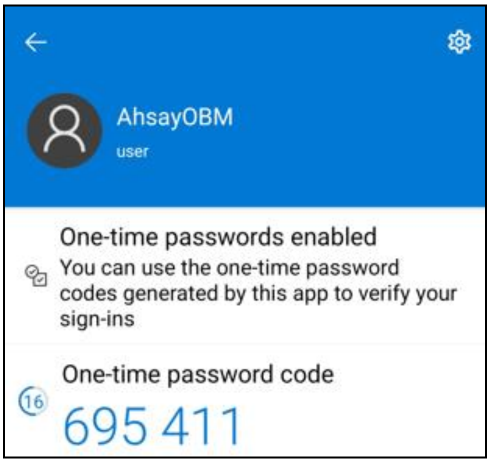


Two-Factor Authentication

Enter one-time passcode generated from authenticator app

6 9 5 4 1 1 (00:00:10)

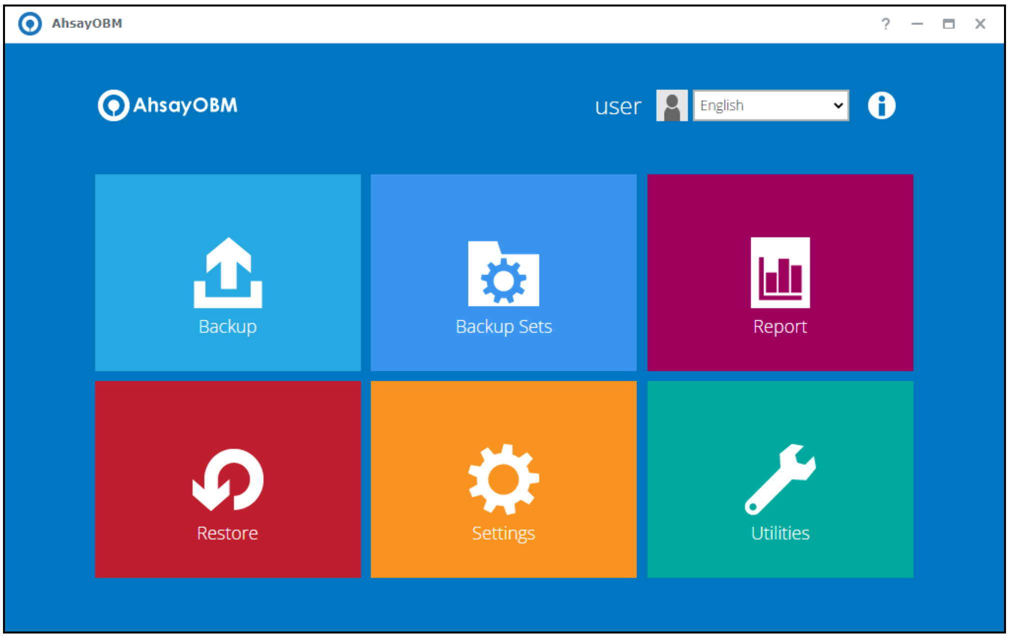
Example of the one-time passcode generated.



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

One-time password code
695 411

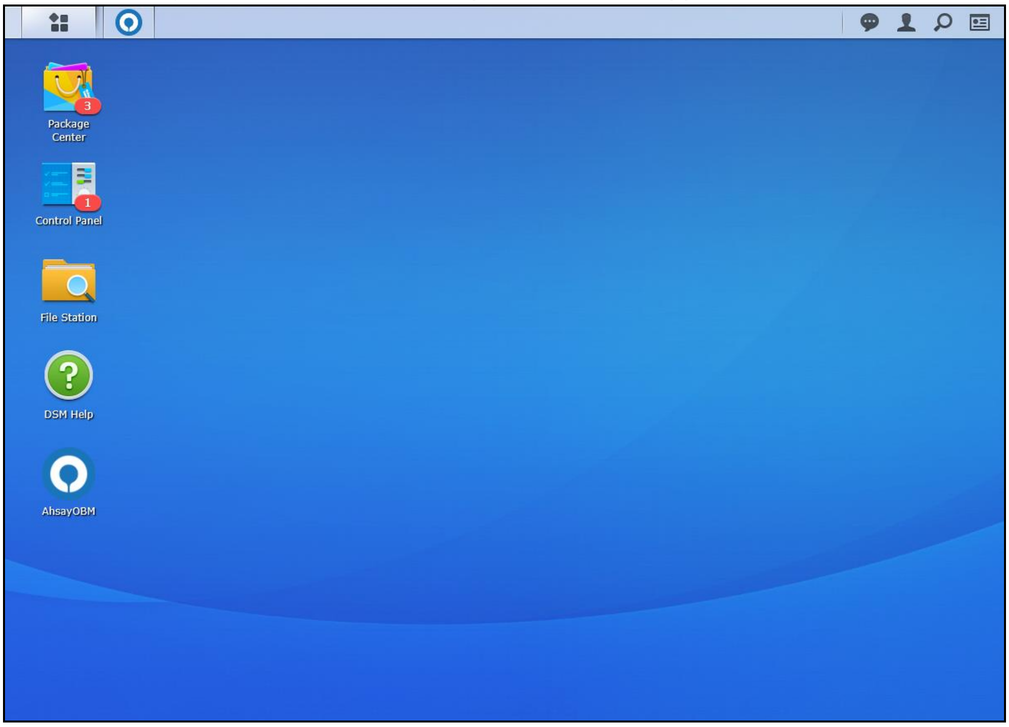
4. After successful login, the following screen will be displayed.



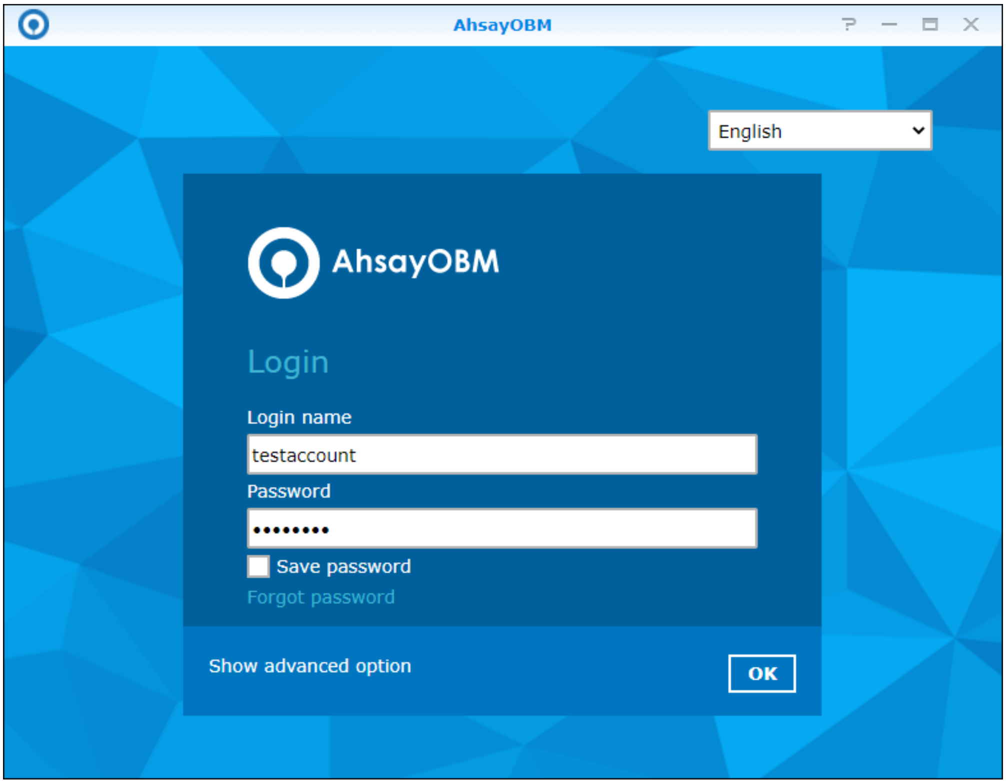
### 6.2.4 Login to AhsayOBM with 2FA using Twilio

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

1. Click the AhsayOBM icon on the desktop 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.



English

Login

Login name: testaccount

Password: ••••••••

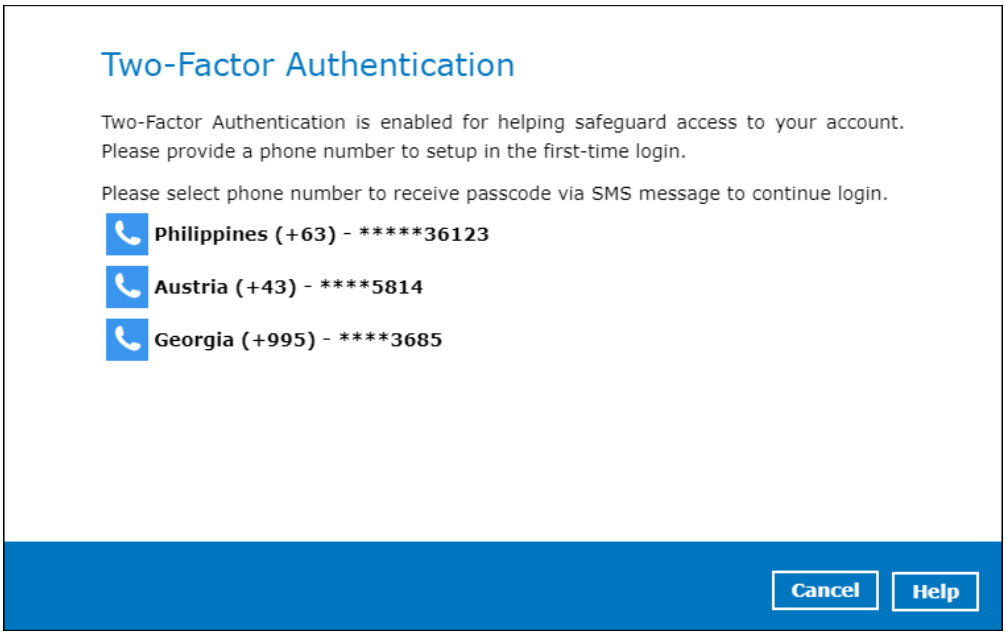
□ Save password

Forgot password

**NOTE**

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

3. Select your phone number to receive the passcode.



## Two-Factor Authentication

Two-Factor Authentication is enabled for helping safeguard access to your account. Please provide a phone number to setup in the first-time login.

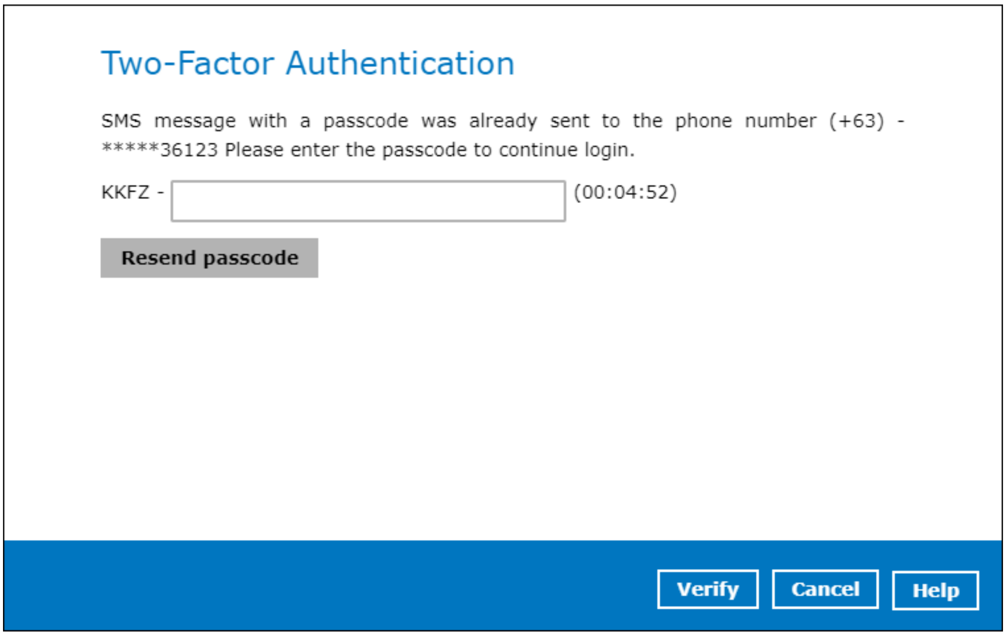
Please select phone number to receive passcode via SMS message to continue login.

☎ **Philippines (+63) - *****36123**

☎ **Austria (+43) - ****5814**

☎ **Georgia (+995) - ****3685**

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

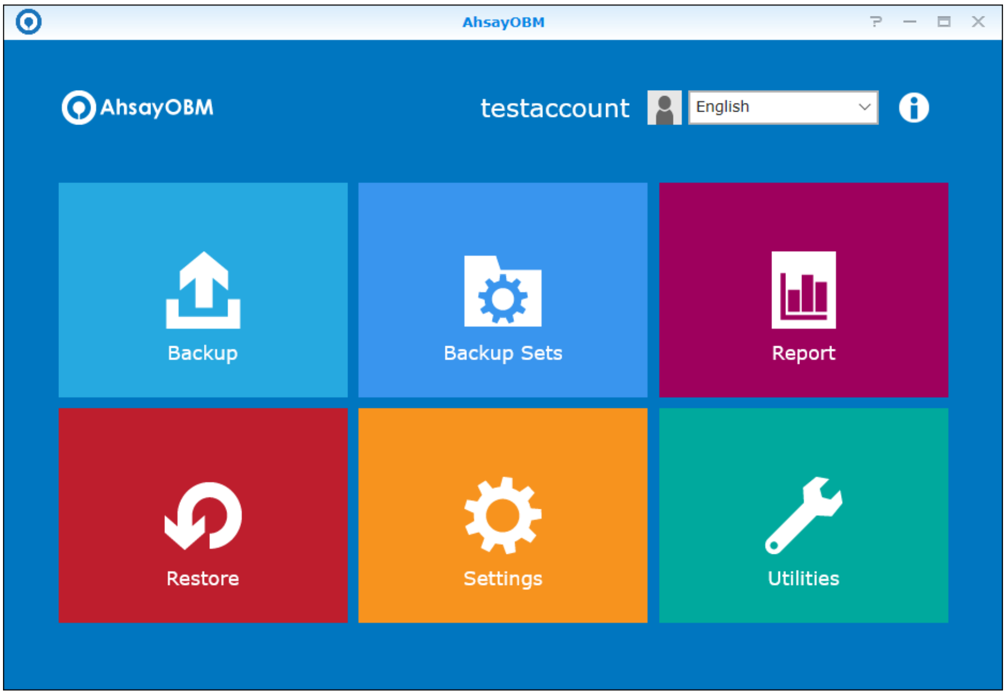


## Two-Factor Authentication

SMS message with a passcode was already sent to the phone number (+63) - *****36123 Please enter the passcode to continue login.

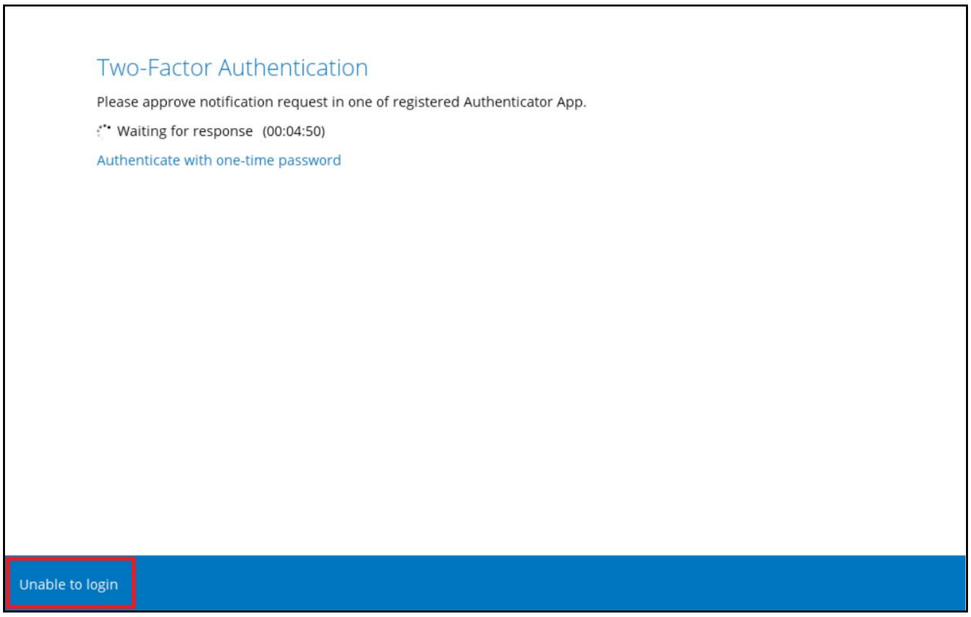
KKFZ - (00:04:52)

5. After successful login, the following screen will be displayed.



# 7 Unable to login to AhsayOBM with 2FA

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



Two-Factor Authentication

Please approve notification request in one of registered Authenticator App.

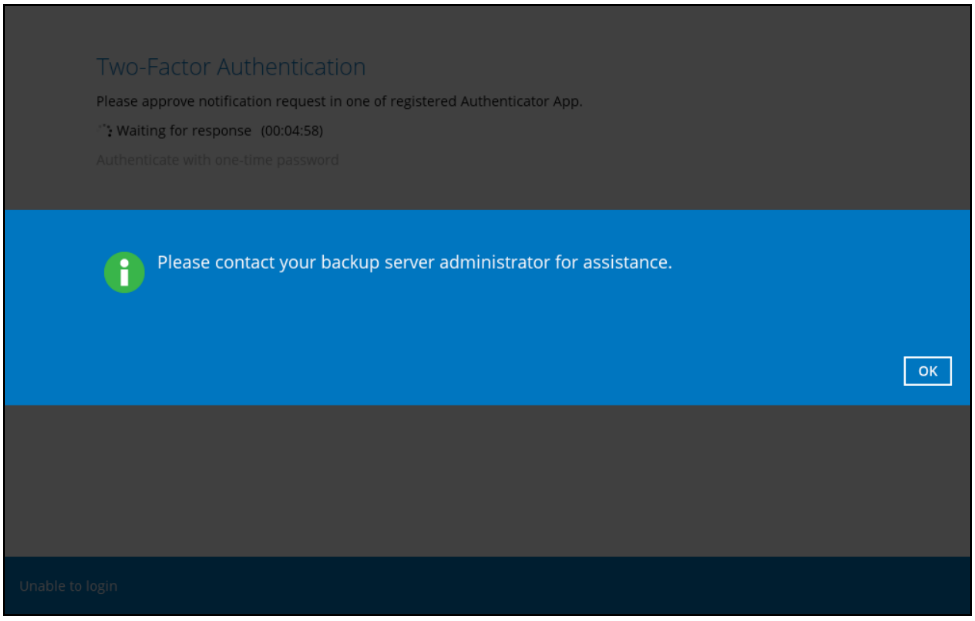
Waiting for response (00:04:50)

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.



Two-Factor Authentication

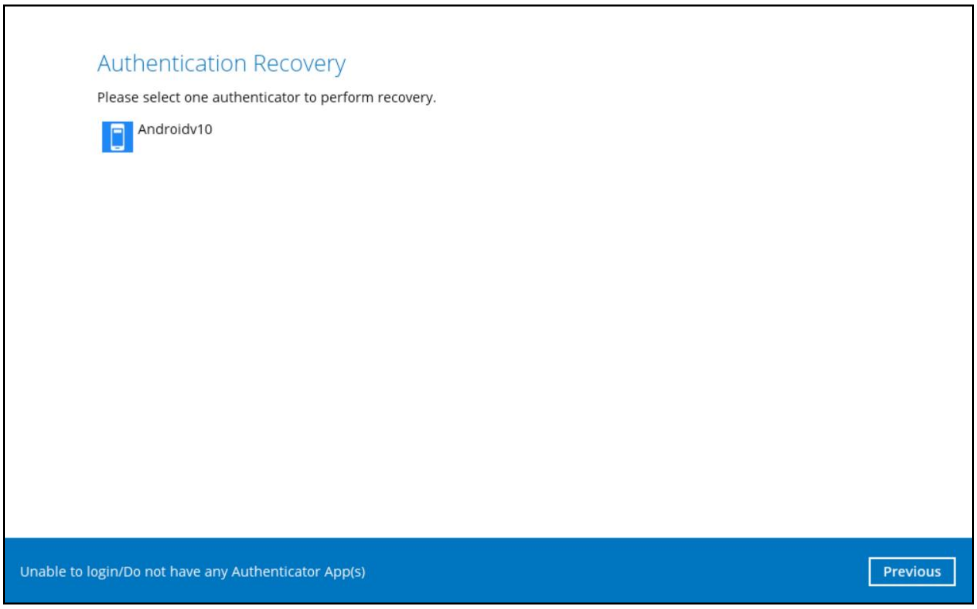
Please approve notification request in one of registered Authenticator App.

Waiting for response (00:04:58)

Please contact your backup server administrator for assistance.

**“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 "Authentication Recovery" procedure.

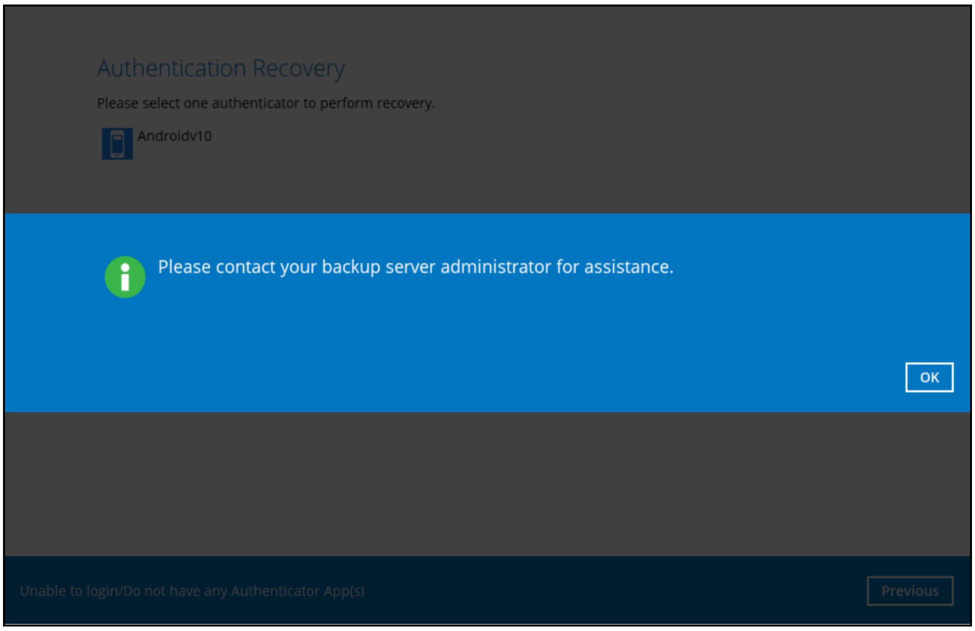


Authentication Recovery

Please select one authenticator to perform recovery.

**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.

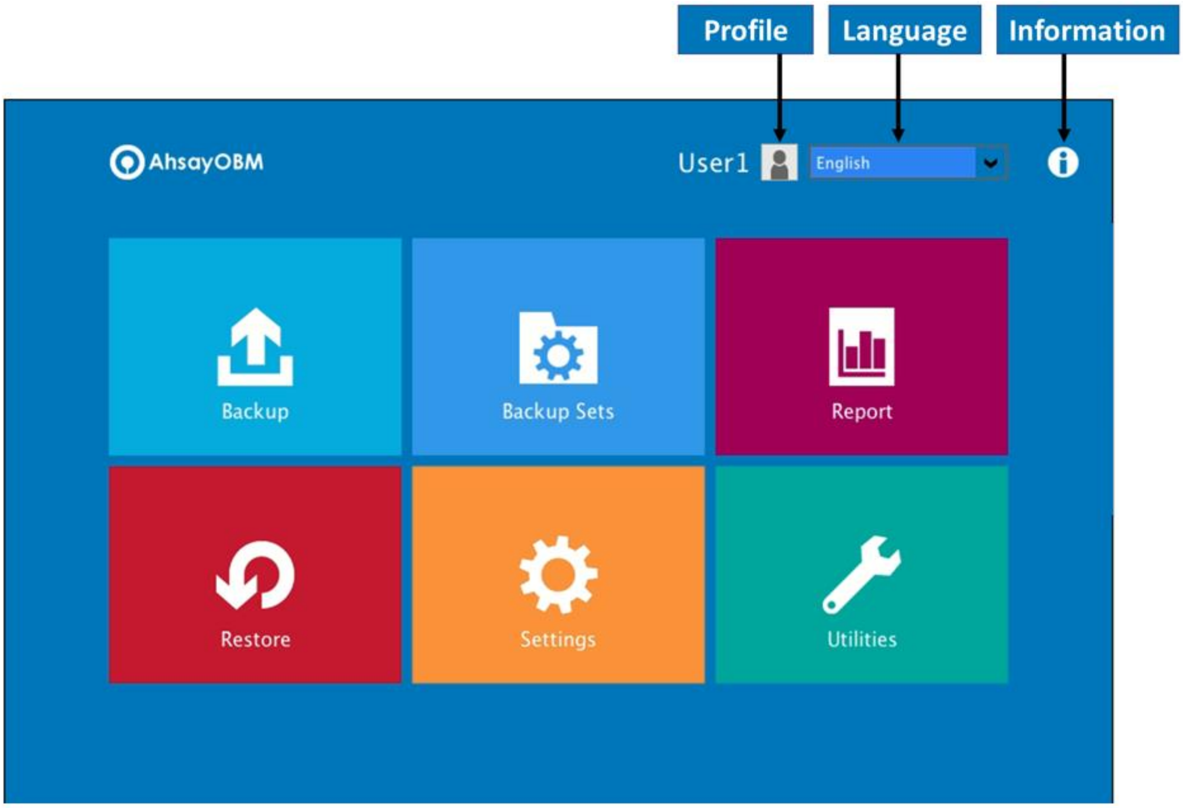


Authentication Recovery

Please select one authenticator to perform recovery.

Please contact your backup server administrator for assistance.

# 8 AhsayOBM Overview

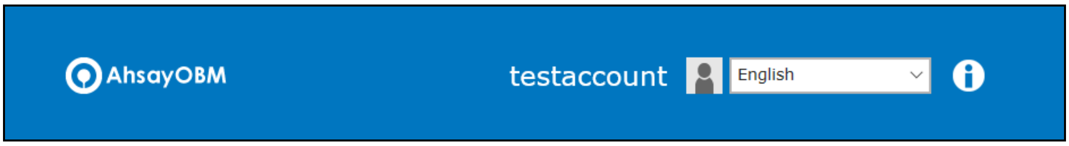


**AhsayOBM** main interface has nine (9) icons that can be accessed by the user:

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

## 8.1 Profile

The **Profile** icon shows the profile settings that can be modified by the user.

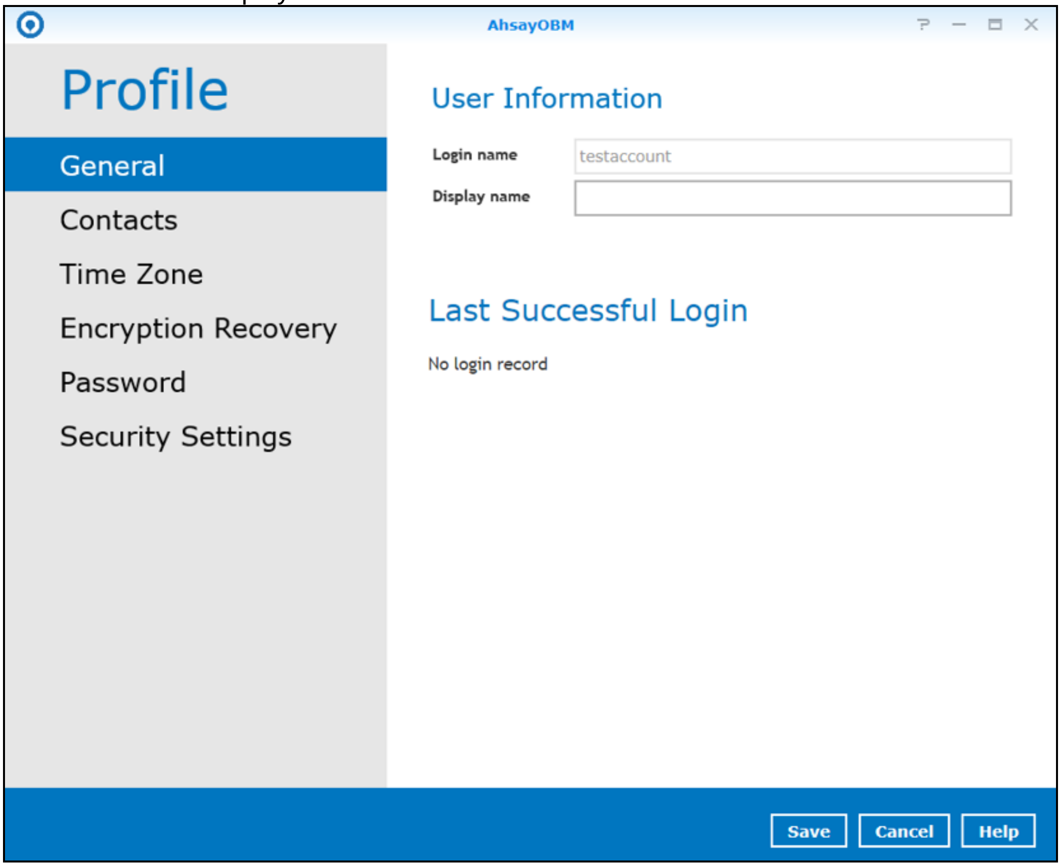


**Profile** has five (5) features:

- **General**
- **Contacts**
- **Time Zone**
- **Encryption Recovery**
- **Password**
- **Security Settings** (Only shown for backup accounts created prior to AhsayOBM v8.5.0.0 and using Twilio for Two-Factor Authentication.)

### 8.1.1 General

The **General** tab displays the user's information.



User Information

Login name: testaccount

Display name:

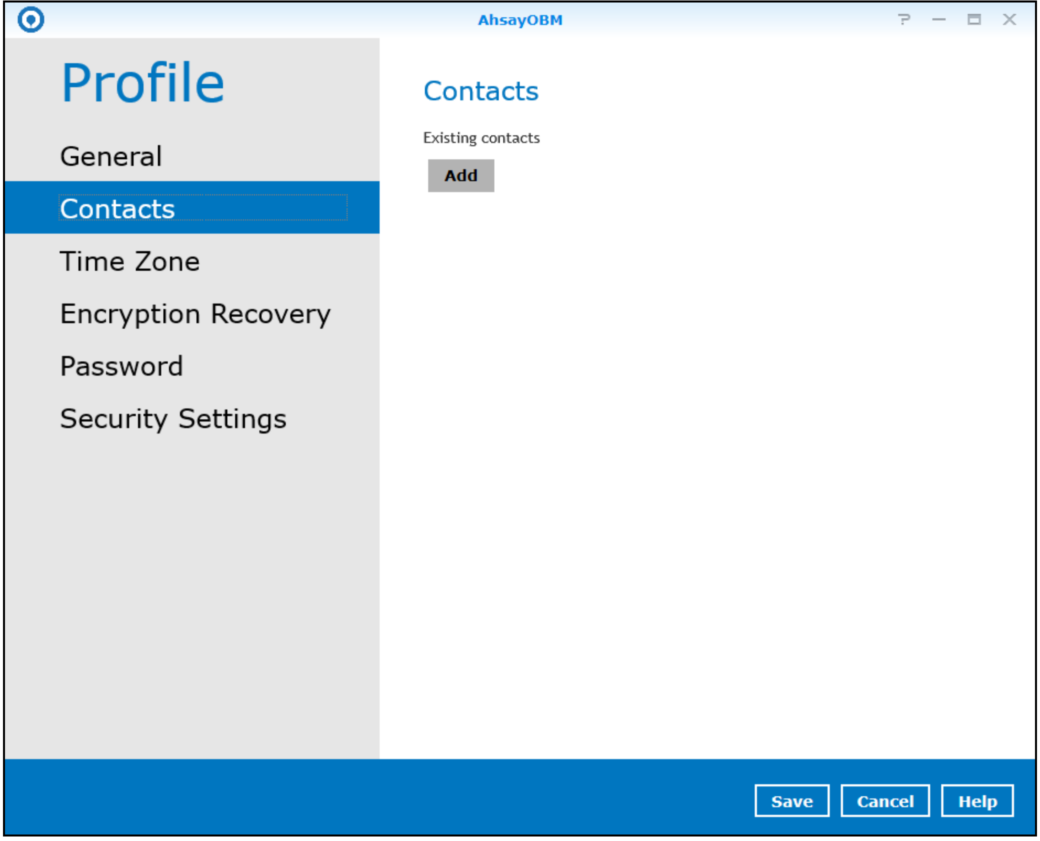
Last Successful Login

No login record

- The **Login name** is the name of your backup account.
- The **Display name** is the display name of your backup account as you log on to the AhsayCBS management console.
- The **Last Successful Login** displays the user's last login information such as the Date, Time, IP address, and Browser.

### 8.1.2 Contacts

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

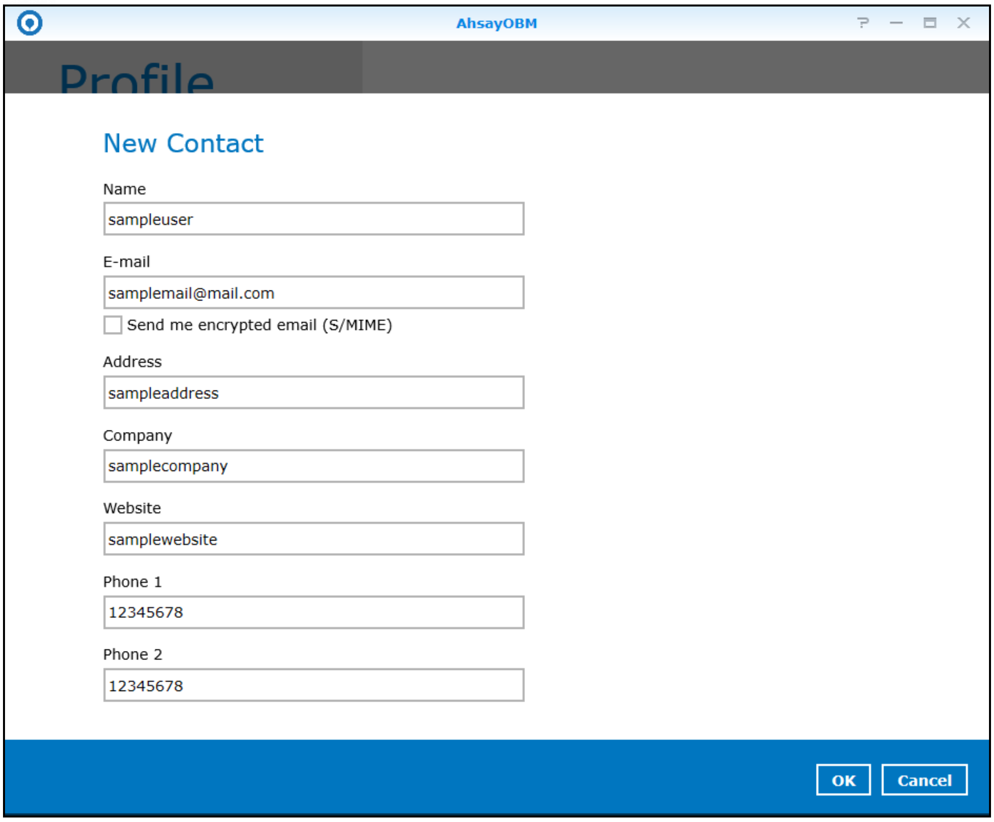


To add a new contact, follow the instructions below:

1. Click the **Add** button.

2. Complete the following fields then click the **OK** button to return to the main screen.

   - Name
   - Email
   - Address
   - Company
   - Website
   - Phone 1
   - Phone 2



New Contact

Name
sampleuser

E-mail
samplemail@mail.com

□ Send me encrypted email (S/MIME)

Address
sampleaddress

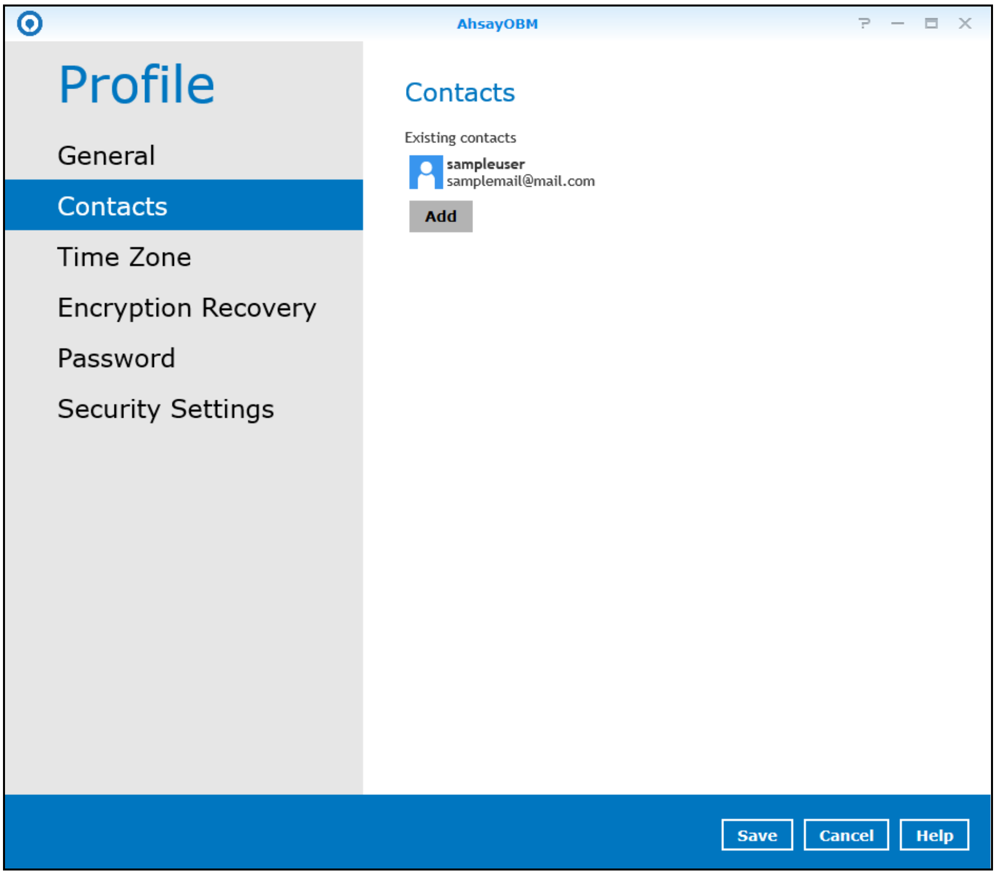
Company
samplecompany

Website
samplewebsite

Phone 1
12345678

Phone 2
12345678

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



Contacts

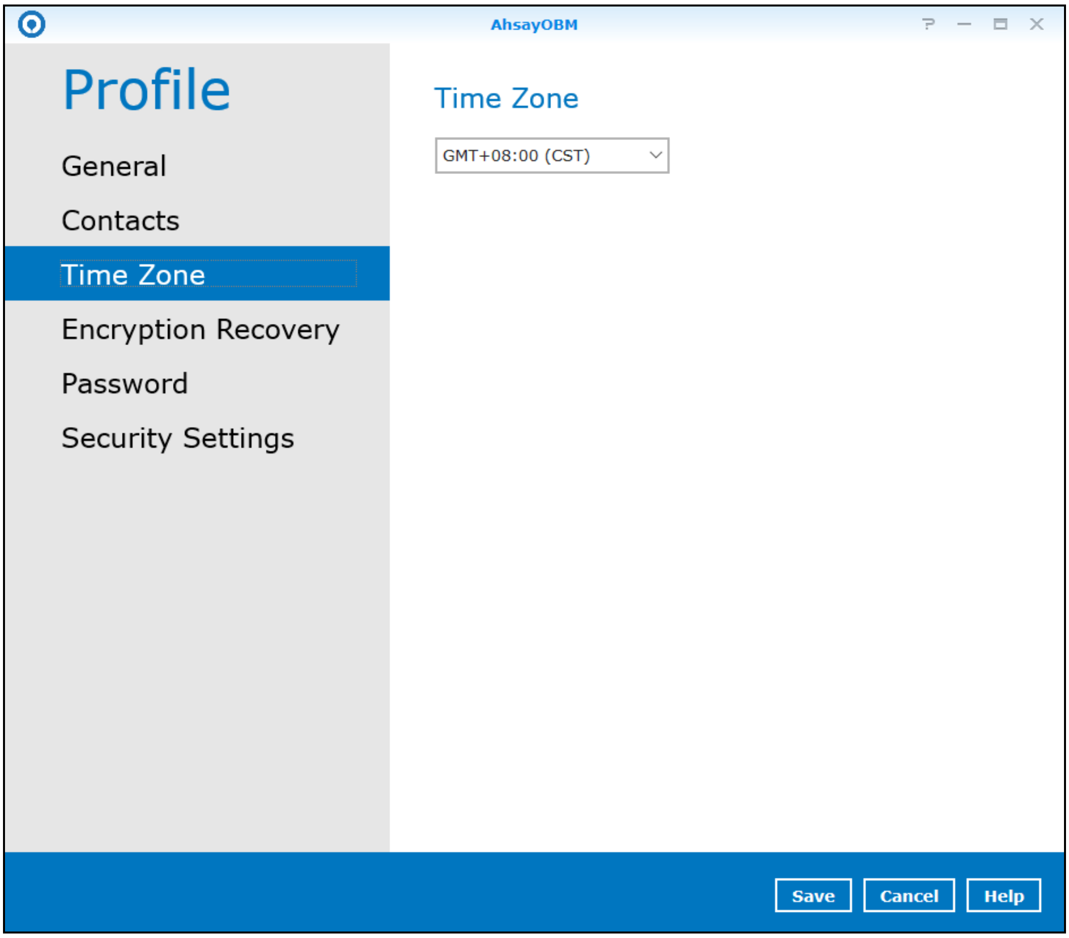
Existing contacts

sampleuser
samplemail@mail.com

**NOTE:** You can add multiple contacts here

### 8.1.3 Time Zone

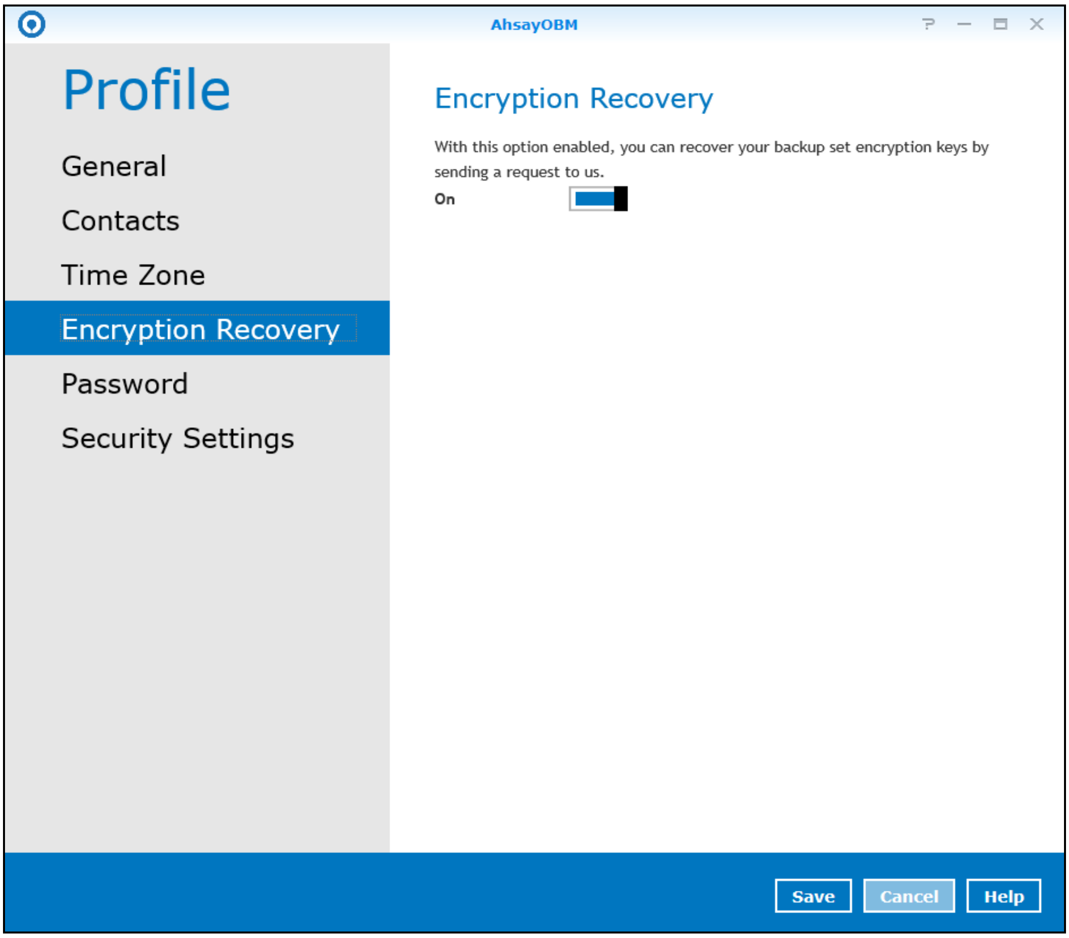
This is the **time zone** of the machine where the AhsayOBM is installed. To ensure that the backup will run accurately at your specified time, set up the correct time.



GMT+08:00 (CST)

### 8.1.4 Encryption Recovery

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



Encryption Recovery

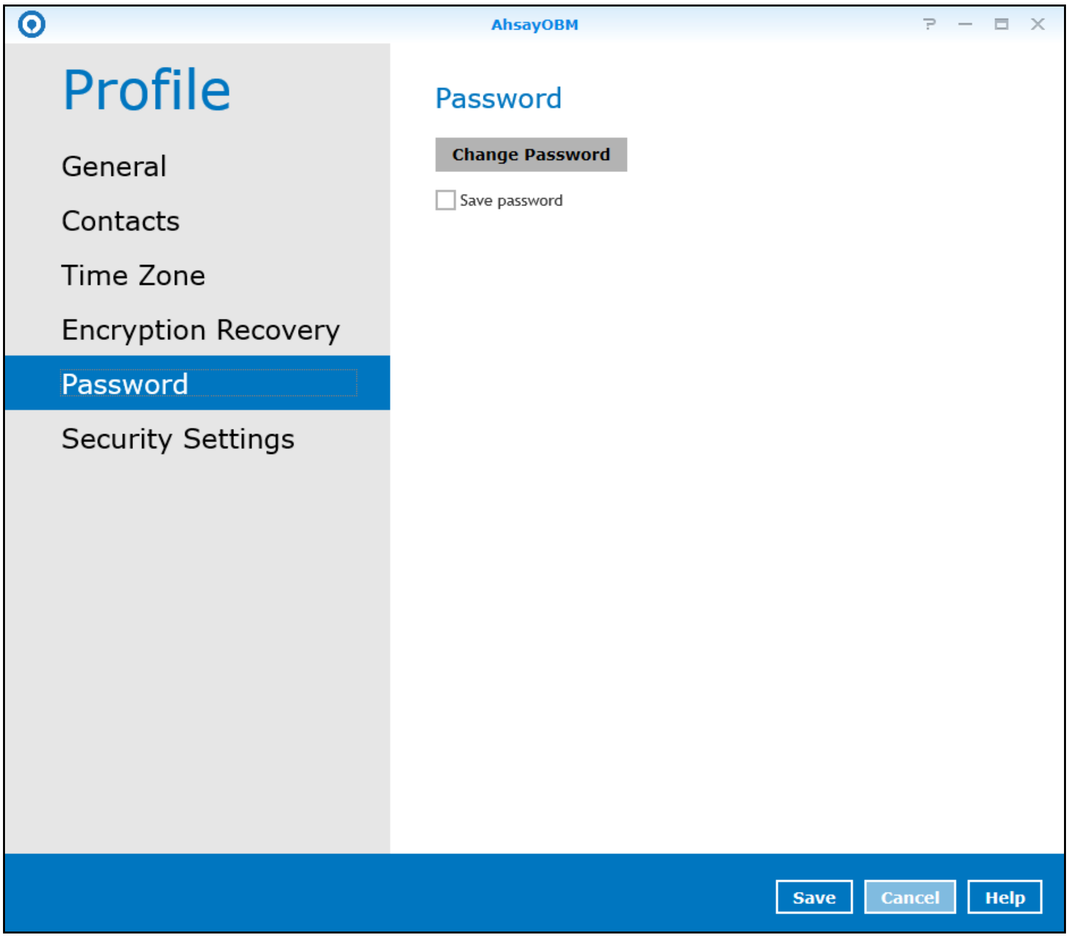
With this option enabled, you can recover your backup set encryption keys by sending a request to us.

On

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

### 8.1.5 Password

Login password can be modified anytime. You can also tick the **Save password** box to bypass the password entry when opening the AhsayOBM interface.



AhsayOBM

Profile

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

Password

Change Password

□ Save password

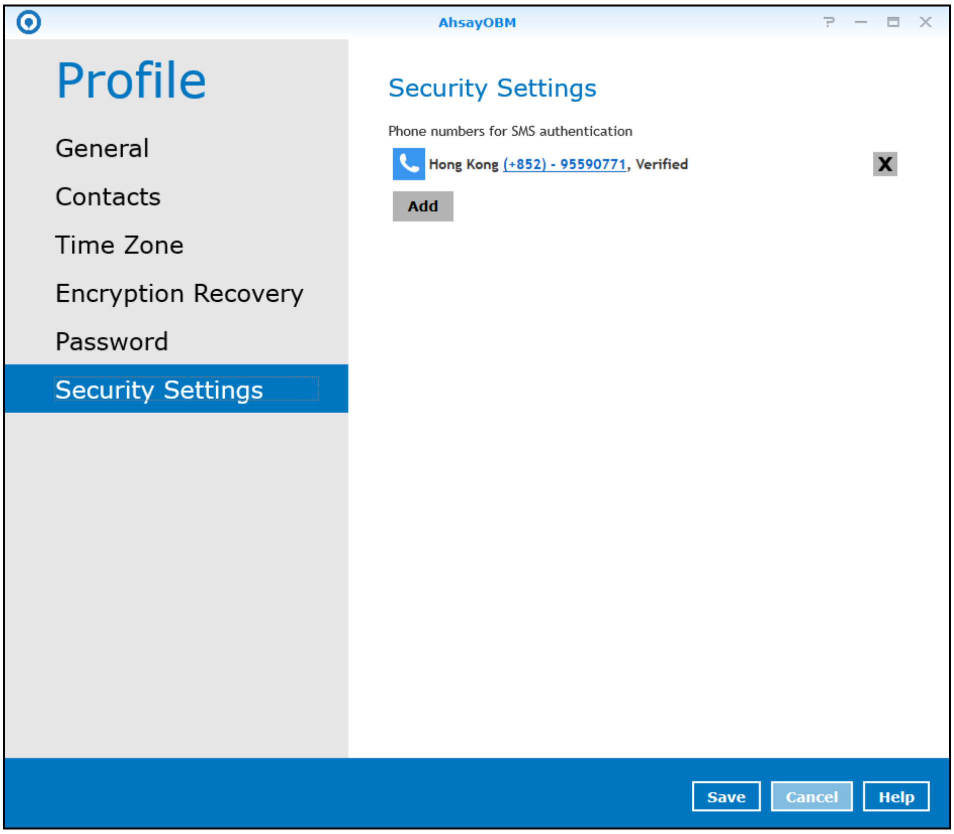
Save Cancel Help

**NOTE**

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

### 8.1.7 Security Settings

The **Security Settings** tab will only be visible if multi-factor authentication is enabled. The 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.



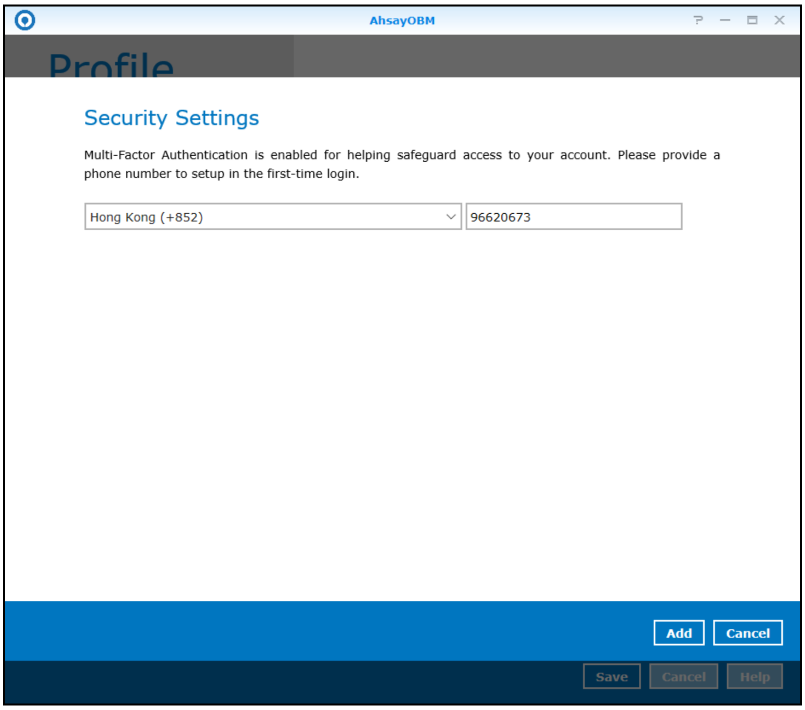
Security Settings

Phone numbers for SMS authentication

☎ Hong Kong (+852) - 95590771, Verified ☒

Add

1. Click the **Add** button.
2. Select the country and enter the phone number, then click **Add**.



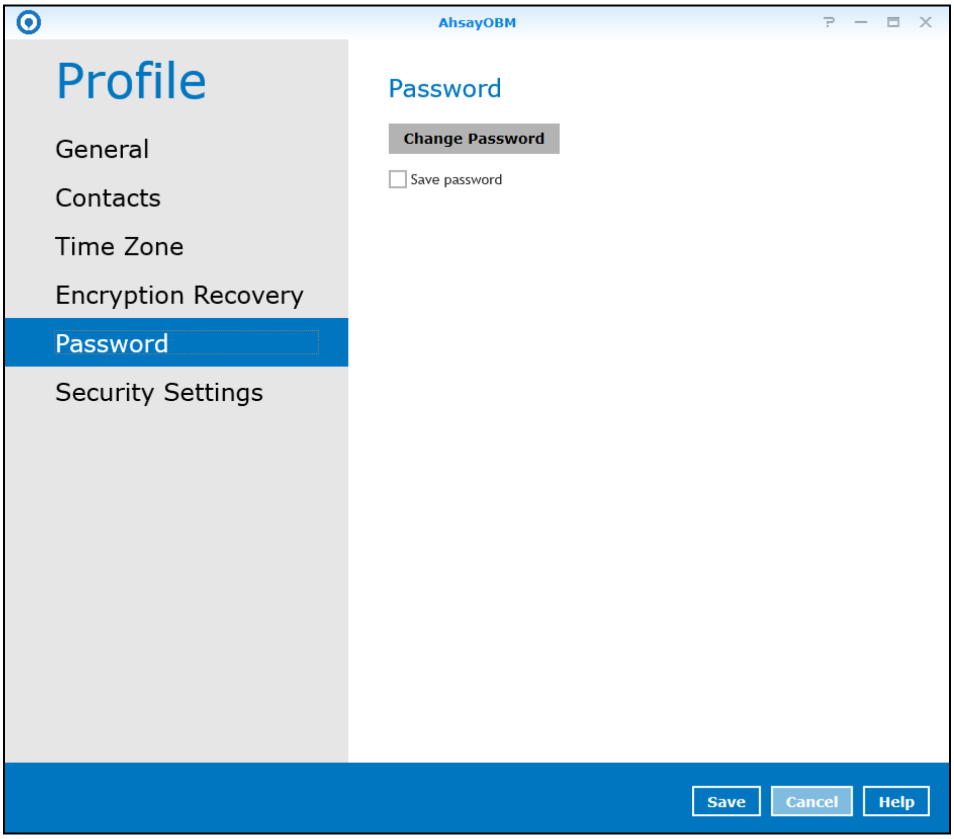
Security Settings

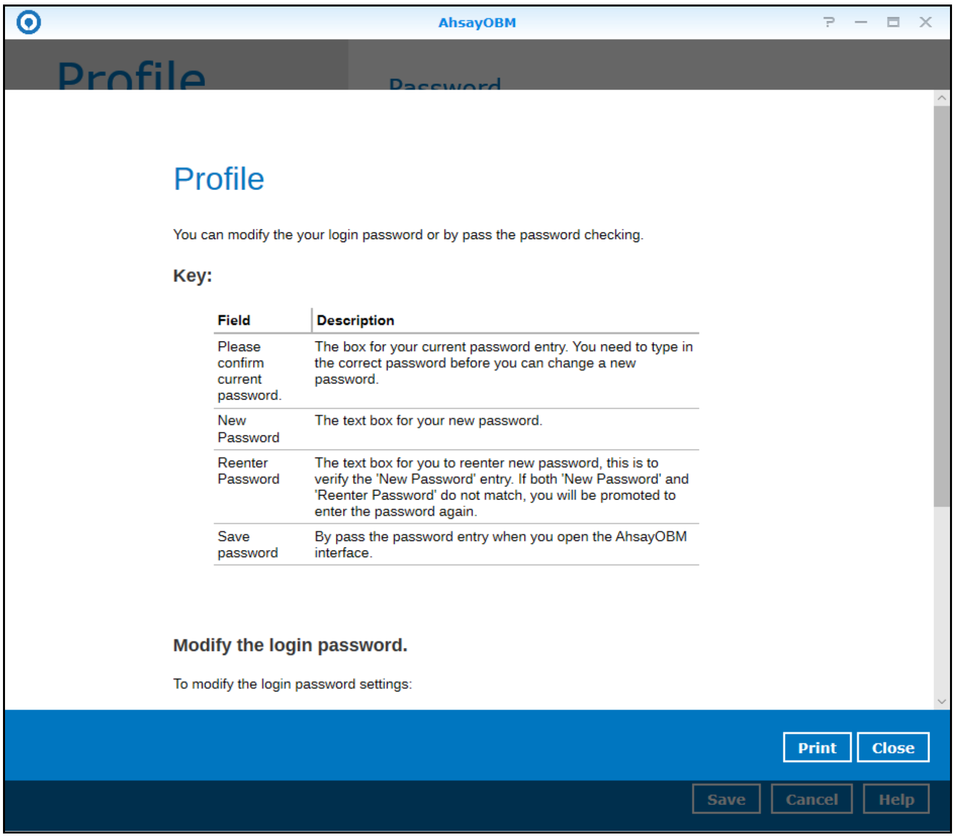
Multi-Factor Authentication is enabled for helping safeguard access to your account. Please provide a phone number to setup in the first-time login.

Hong Kong (+852) | 96620673

## 8.2 Online Help

Clicking the **Help** button will show you the information and instructions you may need.





Profile

You can modify the your login password or by pass the password checking.

**Key:**

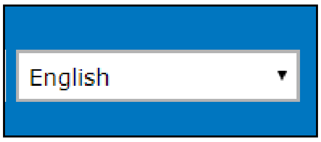
| Field | Description |
|---|---|
| Please confirm current password. | The box for your current password entry. You need to type in the correct password before you can change a new password. |
| New Password | The text box for your new password. |
| Reenter Password | The text box for you to reenter new password, this is to verify the 'New Password' entry. If both 'New Password' and 'Reenter Password' do not match, you will be promoted to enter the password again. |
| Save password | By pass the password entry when you open the AhsayOBM interface. |

**Modify the login password.**

To modify the login password settings:

## 8.3 Language

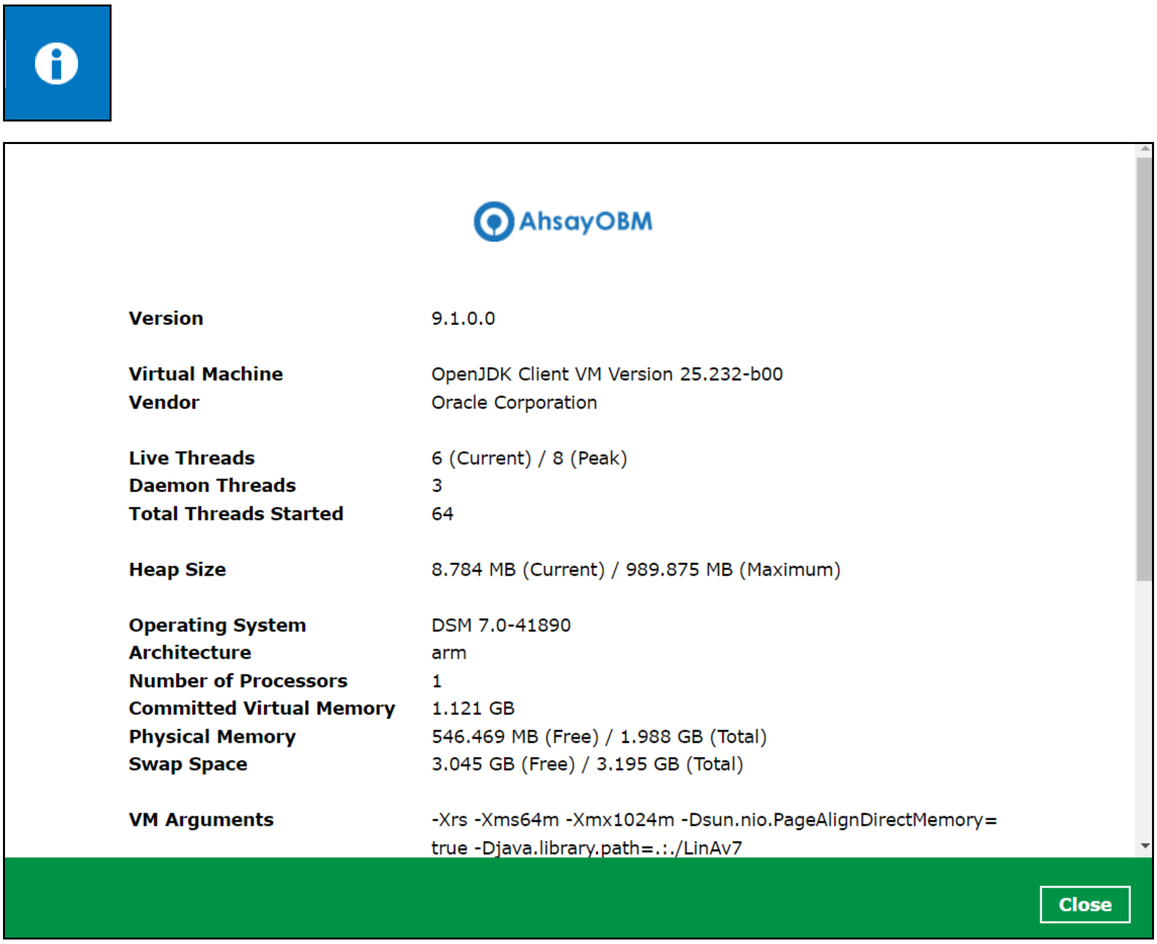
This option is used to change the language of the user interface. The list of available languages depends on the backup service provider.



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

## 8.4 Information

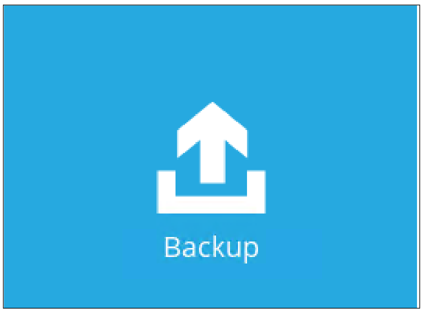
The **information** icon displays the product version and system information of the machine where AhsayOBM is installed.



| | |
|---|---|
| **Version** | 9.1.0.0 |
| **Virtual Machine** | OpenJDK Client VM Version 25.232-b00 |
| **Vendor** | Oracle Corporation |
| **Live Threads** | 6 (Current) / 8 (Peak) |
| **Daemon Threads** | 3 |
| **Total Threads Started** | 64 |
| **Heap Size** | 8.784 MB (Current) / 989.875 MB (Maximum) |
| **Operating System** | DSM 7.0-41890 |
| **Architecture** | arm |
| **Number of Processors** | 1 |
| **Committed Virtual Memory** | 1.121 GB |
| **Physical Memory** | 546.469 MB (Free) / 1.988 GB (Total) |
| **Swap Space** | 3.045 GB (Free) / 3.195 GB (Total) |
| **VM Arguments** | -Xrs -Xms64m -Xmx1024m -Dsun.nio.PageAlignDirectMemory=true -Djava.library.path=.:./LinAv7 |

## 8.5 Backup

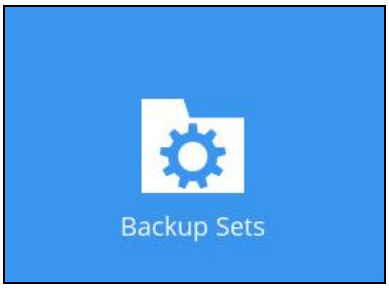
This feature is used to run your backup set(s).



For instructions on how to start a backup, refer to Chapter 11.2 Start a Manual Backup.

## 8.6 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 7 Create a Backup Set.

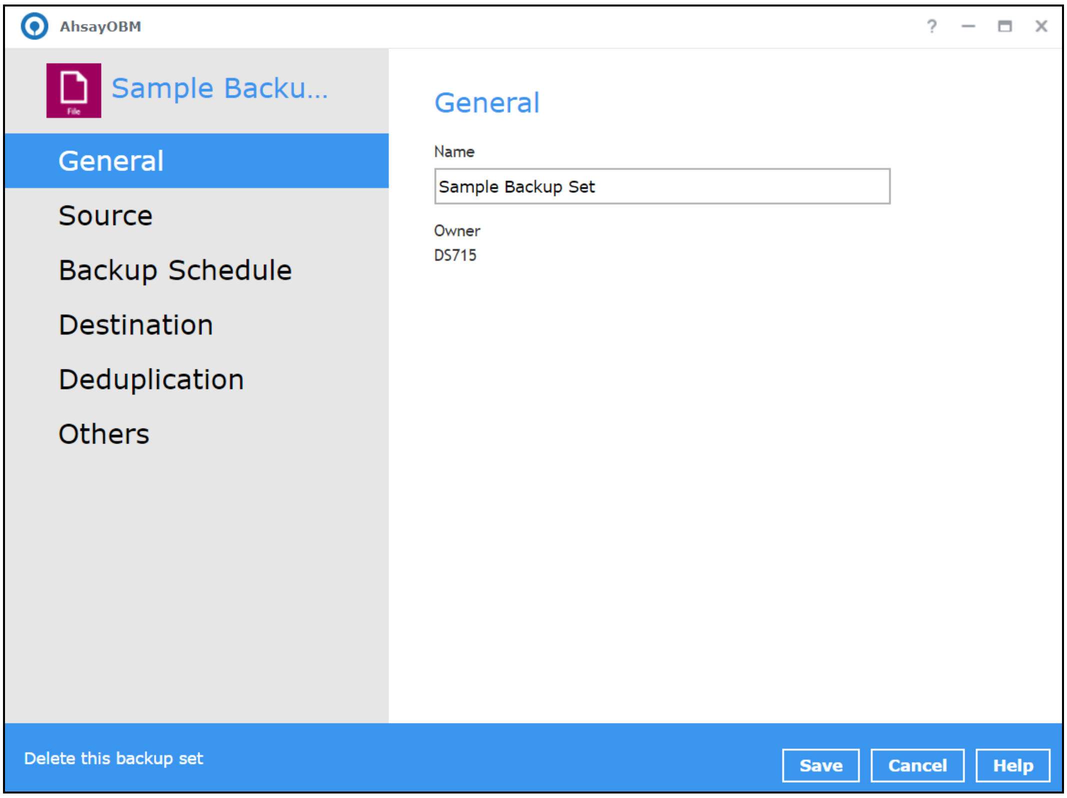
### Backup Set Settings

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

- General
- Source
- Backup Schedule
- Destination
- Deduplication
- Others

### General

This allows the user to modify the name of the backup set and displays the Owner which is the name of the machine where the backup set was created on.



General

Name

Sample Backup Set

Owner

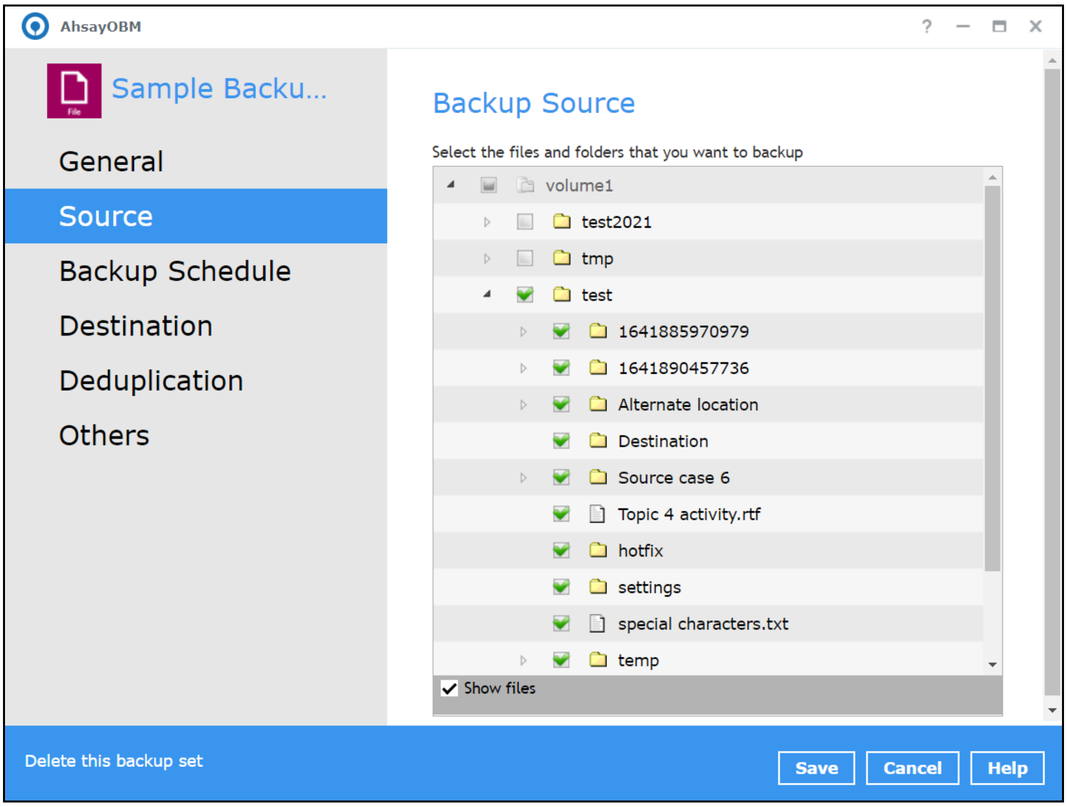
DS715

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

1. Select the **General** tab.
2. Enter a new backup set name on the **Name** field.
3. Click the **Save** button to save the new backup set name.

## Source

This allows the user to select from the available files and/or folders to back up from the NAS device.

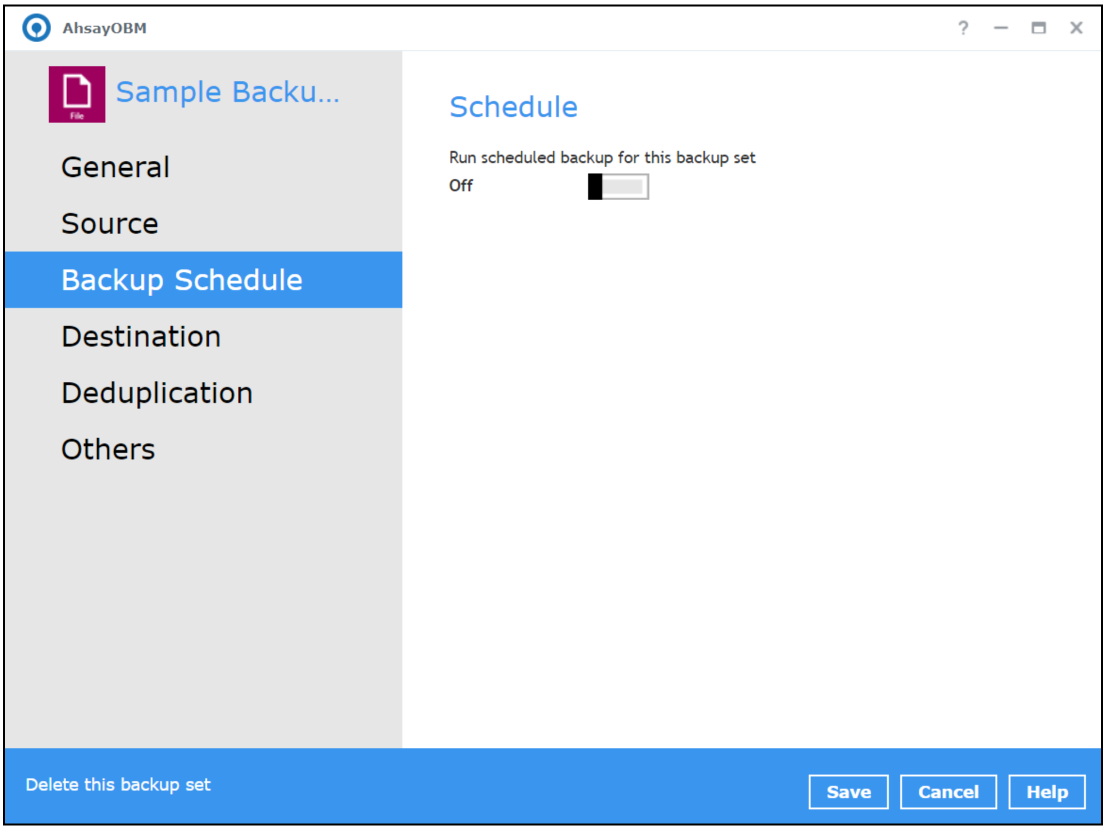


To add backup source, follow the instructions below:

1. Select the **Source** tab.
2. On the right side of the screen, select the files and/or folders that you want to back up.
3. Tick the **Show files** checkbox to show the files under a specific folder.
4. Click the **Save** button to save the settings made.

### Backup Schedule

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



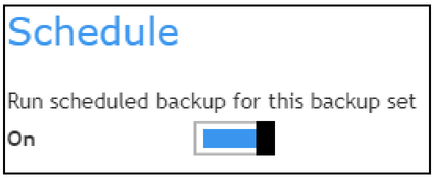
Schedule

Run scheduled backup for this backup set

Off

To configure a backup schedule, follow the steps below:

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

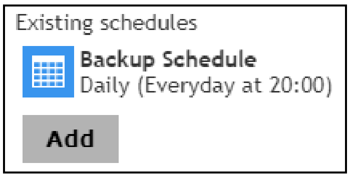


Schedule

Run scheduled backup for this backup set

On

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



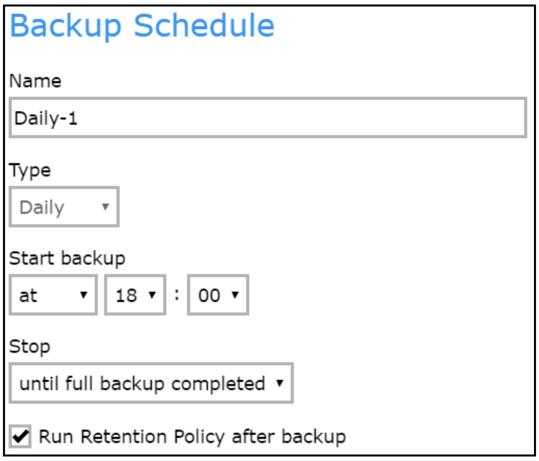
Existing schedules

Backup Schedule
Daily (Everyday at 20:00)

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 when the backup job will run.



Backup Schedule

Name

Daily-1

Type

Daily ▾

Start backup

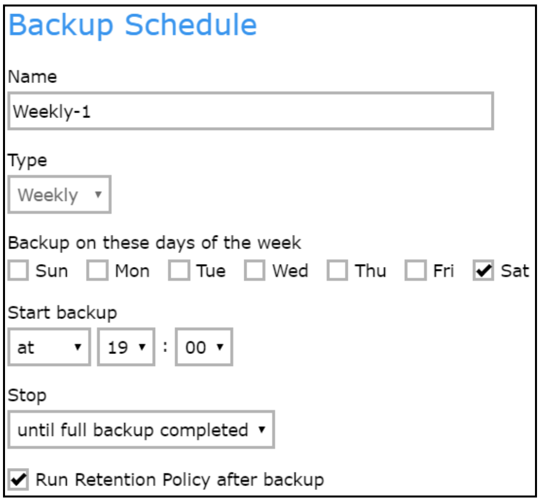
at ▾ 18 ▾ : 00 ▾

Stop

until full backup completed ▾

☑ Run Retention Policy after backup

- **Weekly** – the day of the week and the time of the day when the backup job will run.



Backup Schedule

Name

Weekly-1

Type

Weekly ▾

Backup on these days of the week

□ Sun □ Mon □ Tue □ Wed □ Thu □ Fri ☑ Sat

Start backup

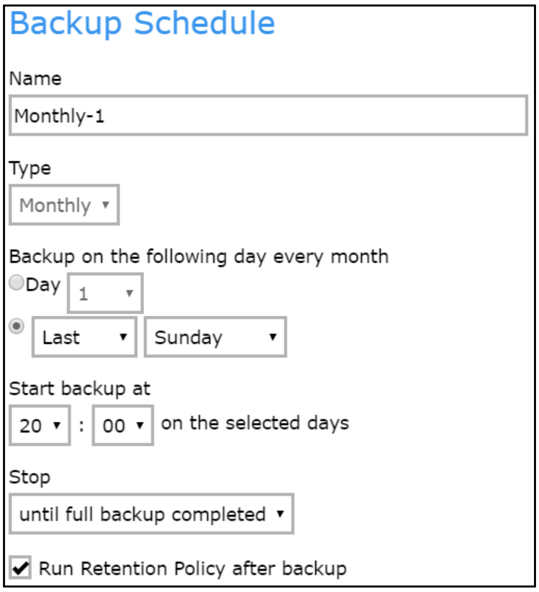
at ▾ 19 ▾ : 00 ▾

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.



Backup Schedule

Name

Monthly-1

Type

Monthly ▾

Backup on the following day every month

○ Day 1 ▾

● Last ▾ Sunday ▾

Start backup at

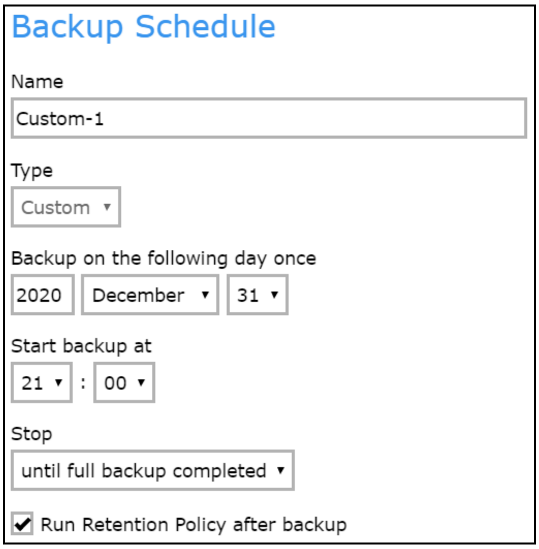
20 ▾ : 00 ▾ on the selected days

Stop

until full backup completed ▾

☑ Run Retention Policy after backup

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



Backup Schedule

Name

Custom-1

Type

Custom

Backup on the following day once

2020 December 31

Start backup at

21 : 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.
- **Stop** – the stop **time** of the backup job.
  - **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.

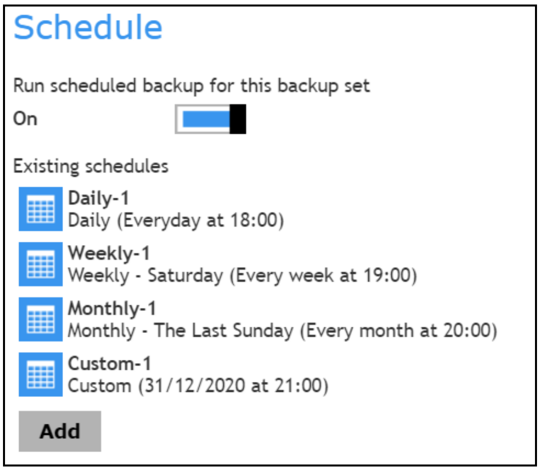
    The partially backed up data will have to be removed by running the Data Integrity Check.

    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.

5. Click the **OK** button to save the configured backup schedule settings.

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

**NOTE:** Multiple backup schedules can be created.



## Schedule

Run scheduled backup for this backup set

On

Existing schedules

Daily-1
Daily (Everyday at 18:00)

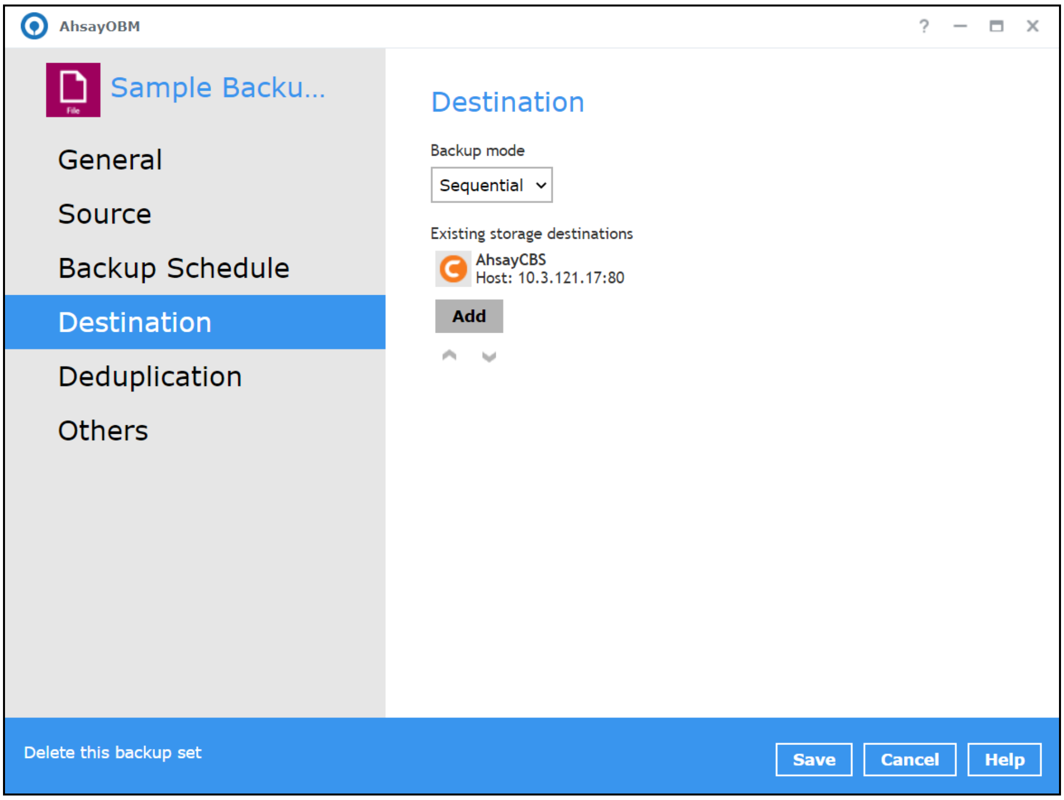
Weekly-1
Weekly - Saturday (Every week at 19:00)

Monthly-1
Monthly - The Last Sunday (Every month at 20:00)

Custom-1
Custom (31/12/2020 at 21:00)

### Destination

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



Destination

Backup mode: Sequential

Existing storage destinations

AhsayCBS
Host: 10.3.121.17:80

To add a destination, follow the instructions below:

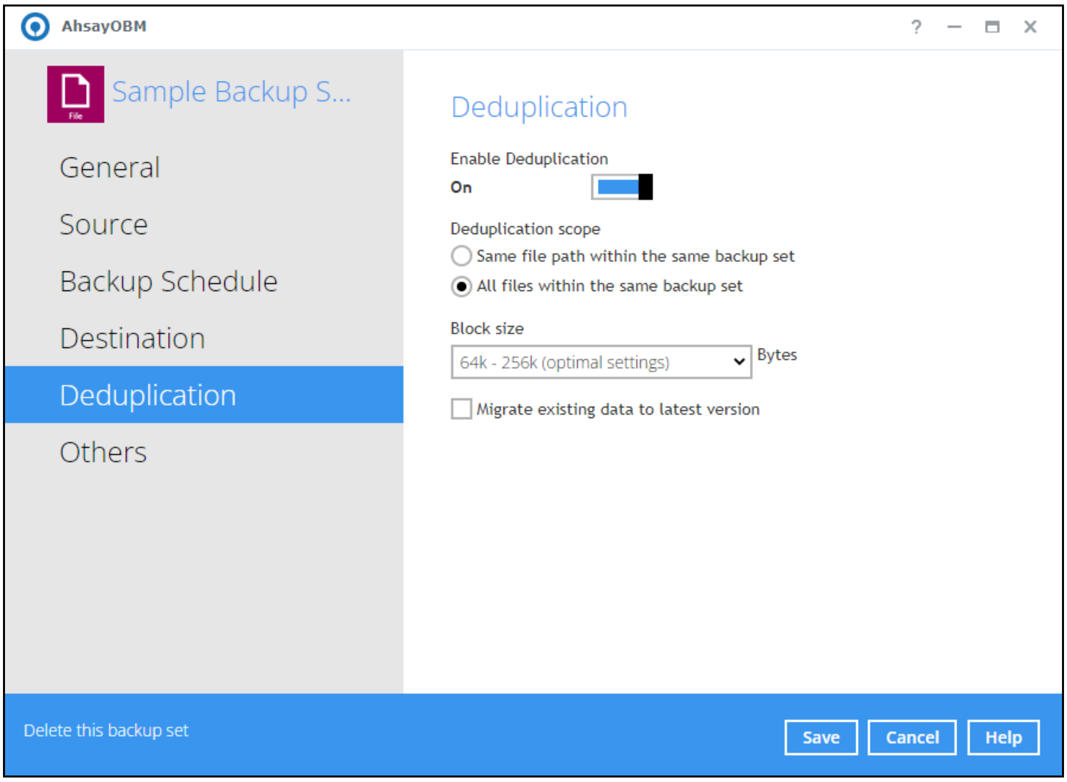
1. Select the **Destination** tab.
2. Click the **Add** button
3. Complete the following fields:
    - Name
    - Destination storage
4. Click the **OK** button to add the new destination.
5. Click the **Save** button to save the destination.

### 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.



Deduplication

Enable Deduplication
On

Deduplication scope
○ Same file path within the same backup set
● All files within the same backup set

Block size
64k - 256k (optimal settings) Bytes

□ Migrate existing data to latest version

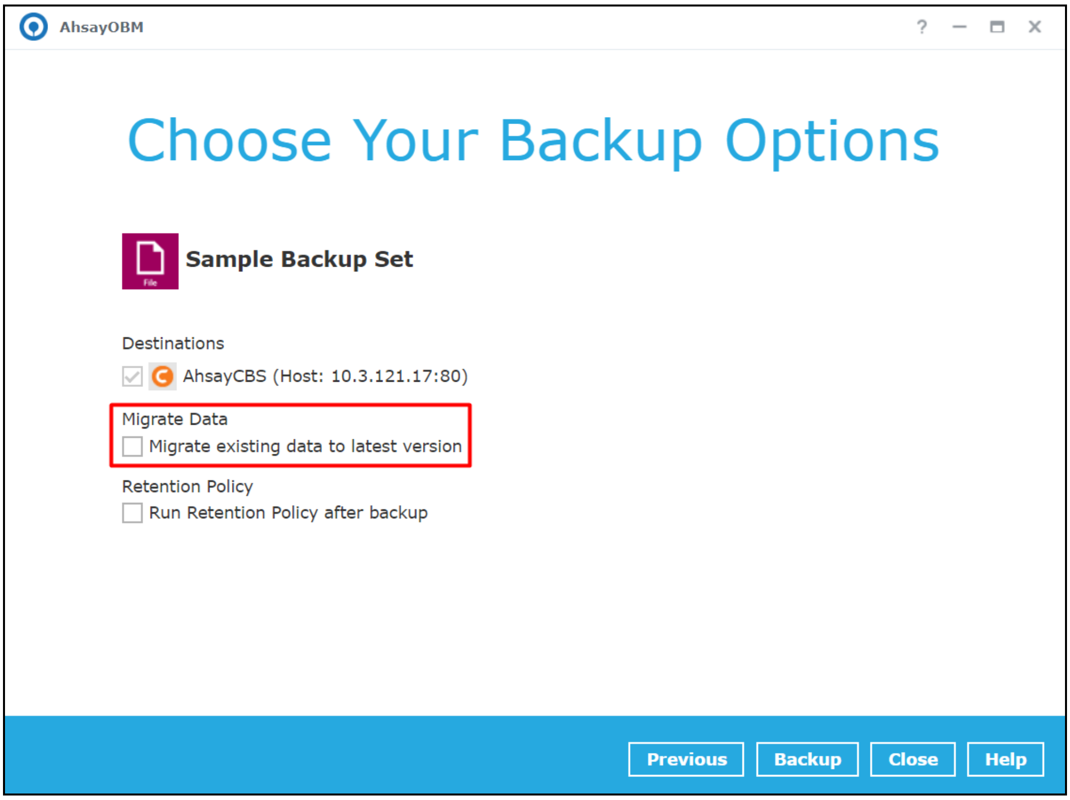
There are two (2) types of Deduplication scope:

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

**NOTE**
For more details about the **Deduplication** feature, refer to the AhsayCBS v9 New Features Supplemental document.

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.



Destinations

☑ AhsayCBS (Host: 10.3.121.17:80)

Migrate Data

□ Migrate existing data to latest version

Retention Policy

□ Run Retention Policy after backup

**Migrate Data**

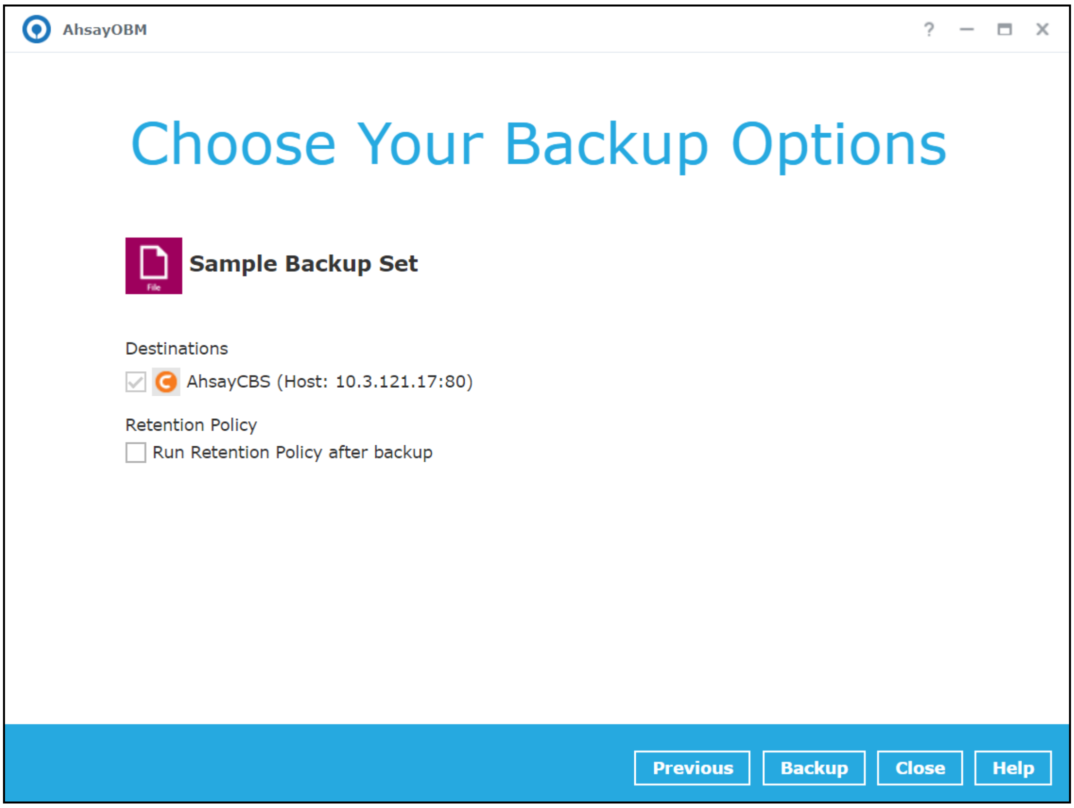
When this option is enabled, the existing data will be migrated to the latest version during a backup job. This option is disabled by default.

□ Migrate existing data to latest version

**NOTE**

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

Below is an example of a backup set with Deduplication setting **Off (disabled)**.



Choose Your Backup Options

Sample Backup Set

Destinations

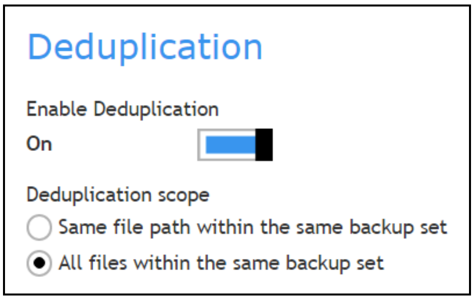
☑ AhsayCBS (Host: 10.3.121.17:80)

Retention Policy

□ Run Retention Policy after backup

To configure the Deduplication settings, follow the steps below:

1. Select a type of Deduplication scope.



Deduplication

Enable Deduplication

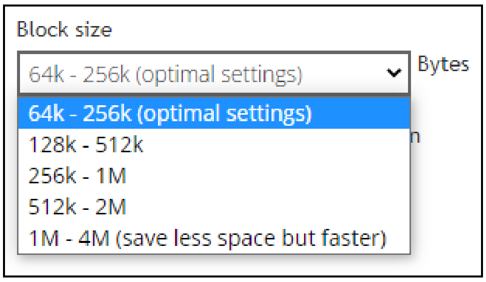
On

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 deduplicated data. 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.

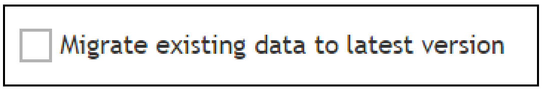


Block size

64k - 256k (optimal settings) Bytes

64k - 256k (optimal settings)
128k - 512k
256k - 1M
512k - 2M
1M - 4M (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.



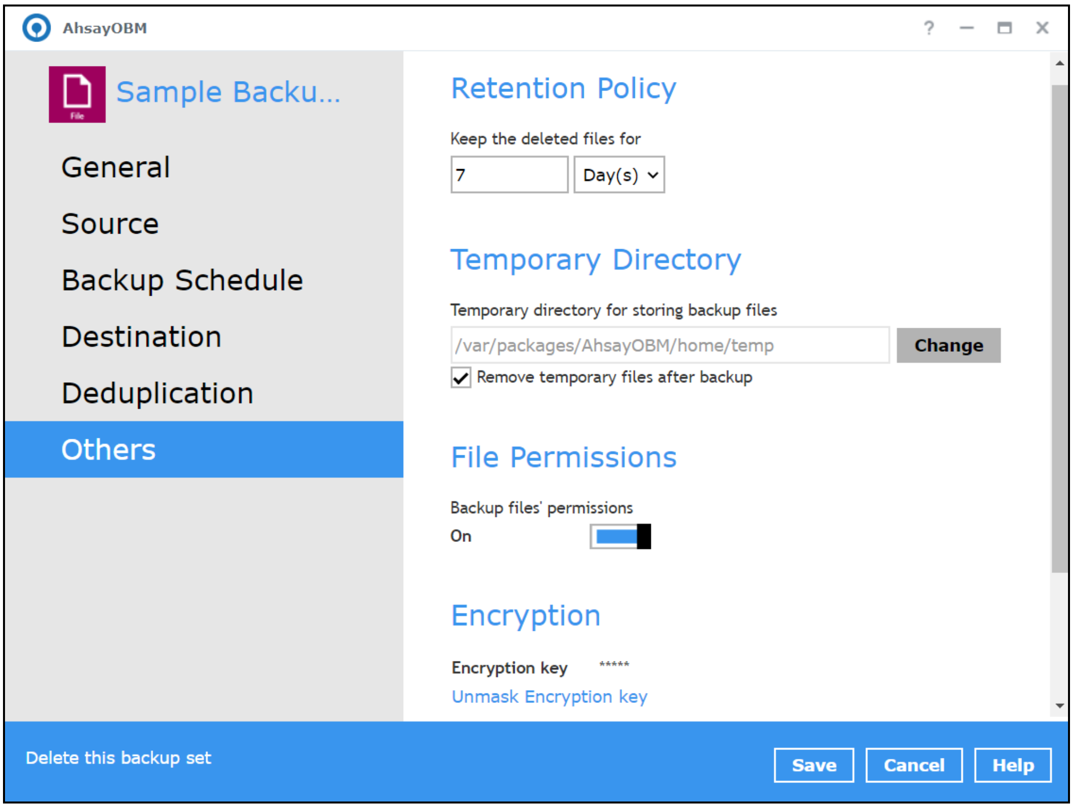
□ Migrate existing data to latest version

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

### Others

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

- Retention Policy
- Temporary Directory
- File Permissions
- Encryption
- Recycle Bin



Keep the deleted files for 7 Day(s)

Temporary directory for storing backup files /var/packages/AhsayOBM/home/temp

☑ Remove temporary files after backup

Backup files' permissions On

Encryption key *****

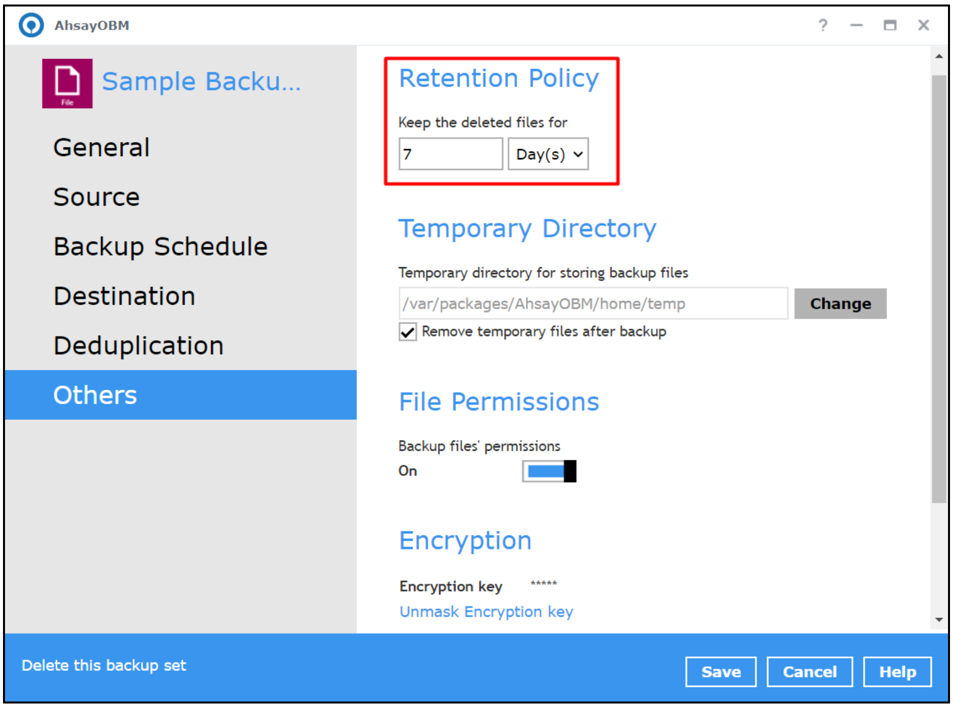
## Retention Policy

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

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

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

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



Retention Policy

Keep the deleted files for

7 Day(s)

Temporary Directory

Temporary directory for storing backup files

/var/packages/AhsayOBM/home/temp

☑ Remove temporary files after backup

File Permissions

Backup files' permissions

On

Encryption

Encryption key *****

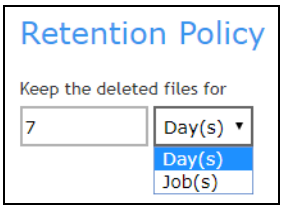
Unmask Encryption key

**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.

To modify the Retention Policy, follow the instructions below:

1. Select the **Others** tab.
2. Select from the two (2) options: Day(s) or Job(s).



Retention Policy

Keep the deleted files for

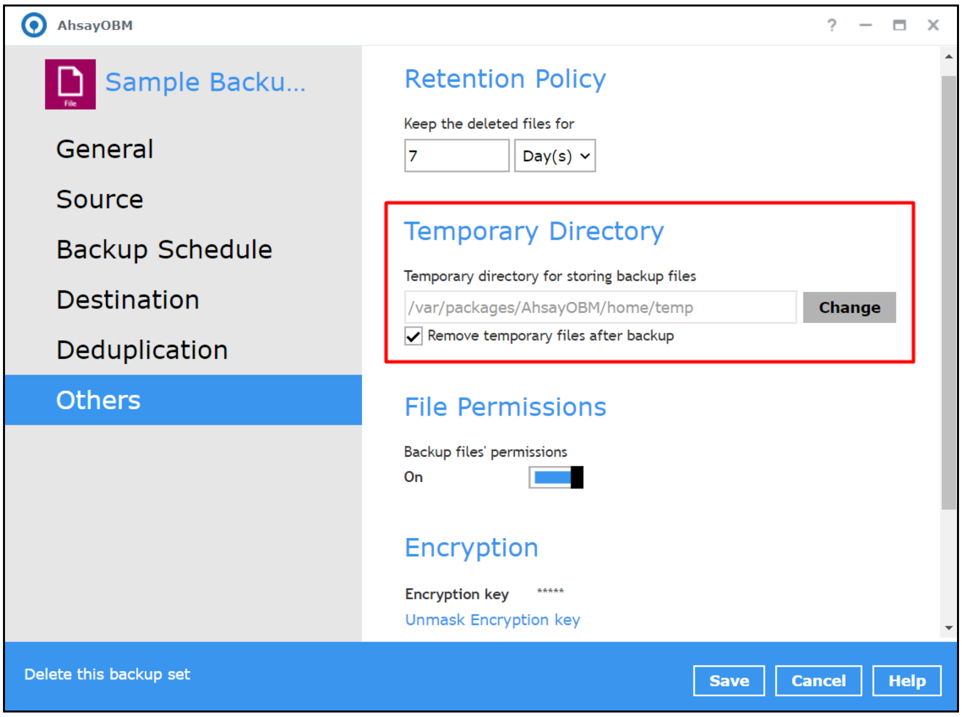
7 Day(s)

3. Input a valid number of Day(s) or Job(s), then click the **Save** button to save the Retention Policy settings.

## Temporary Directory

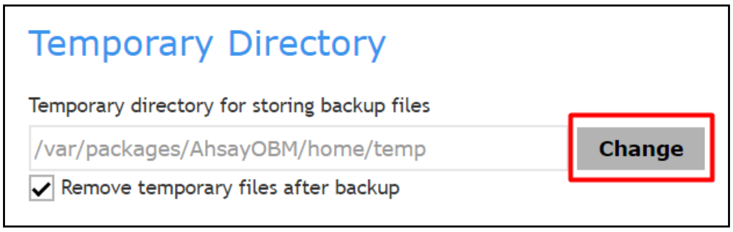
For a **backup job**, it is used to temporarily store backup set index files. An updated set of index files is generated after each backup job. The index files are synchronized to each individual backup destination at the end of each backup job.

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



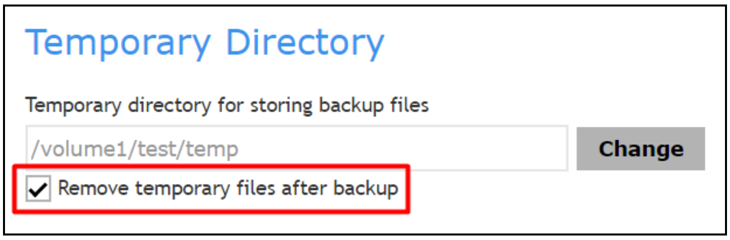
To configure the temporary directory, follow the instructions below:

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


Temporary Directory
Temporary directory for storing backup files
/var/packages/AhsayOBM/home/temp
Change
☑ Remove temporary files after backup

2. Locate the directory that you would like to use, then click **OK** to select the folder.

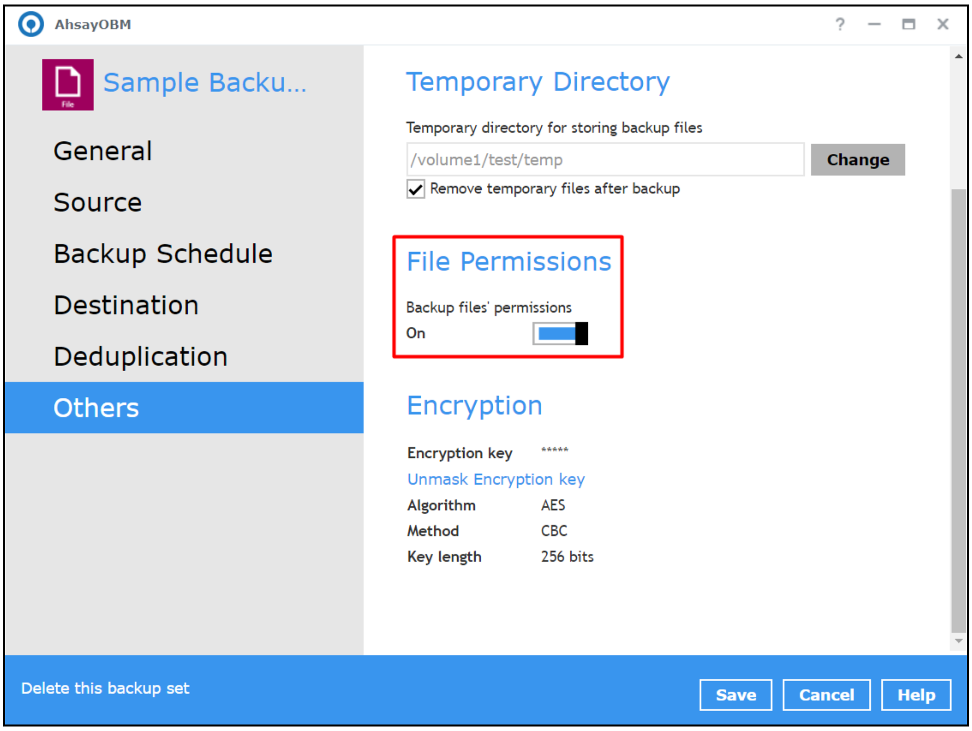
3. You also have an option to check or uncheck the **Remove temporary files after backup** checkbox.


Temporary Directory
Temporary directory for storing backup files
/volume1/test/temp
Change
☑ Remove temporary files after backup

4. Click the **Save** button to apply the settings.

## File Permissions

When this option is enabled, AhsayOBM will include to back up the operating system file permission of the data selected as backup source. This option is enabled by default.



Temporary Directory

Temporary directory for storing backup files

/volume1/test/temp

☑ Remove temporary files after backup

File Permissions

Backup files' permissions

On

Encryption

Encryption key *****

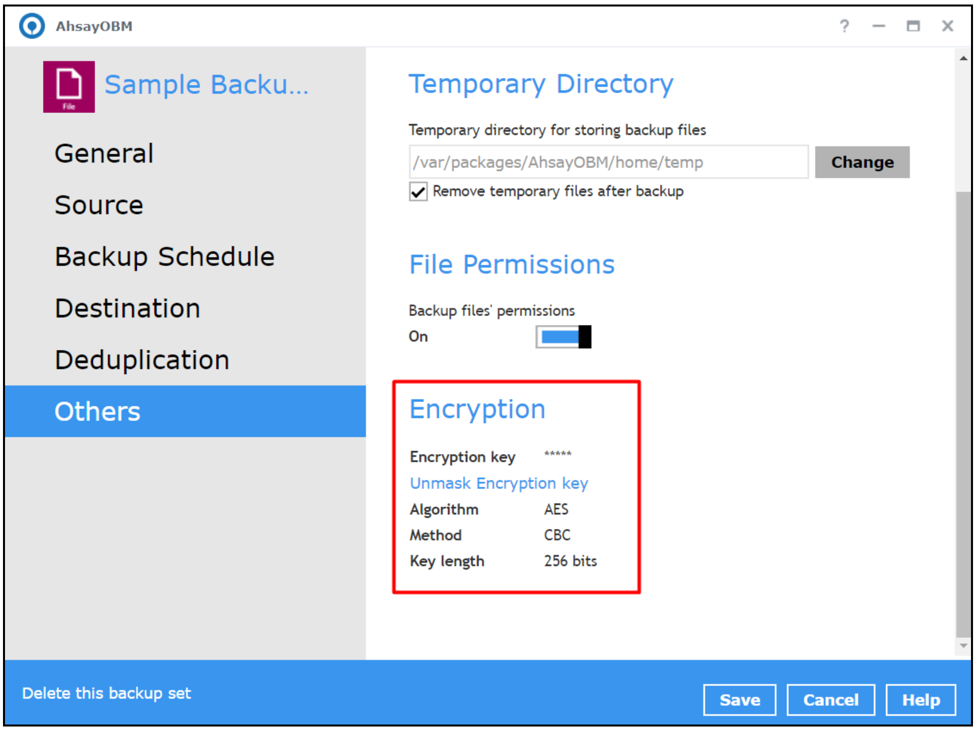
Algorithm AES

Method CBC

Key length 256 bits

## Encryption

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



Temporary Directory

Temporary directory for storing backup files

/var/packages/AhsayOBM/home/temp

☑ Remove temporary files after backup

File Permissions

Backup files' permissions

On

Encryption

Encryption key *****

Unmask Encryption key

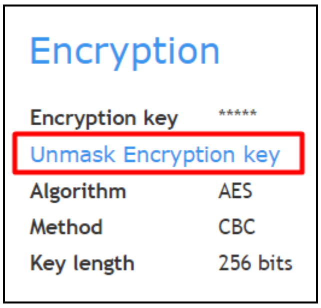
Algorithm AES

Method CBC

Key length 256 bits

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

1. Click the **Others** tab in the backup set settings.
2. In the Encryption section, click the 'Unmask encryption key' link to display the encryption key of the backup set.



Encryption

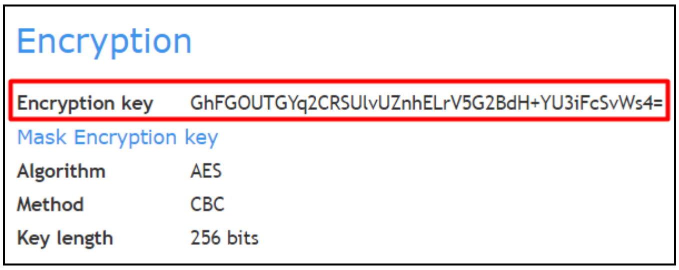
Encryption key *****

Unmask Encryption key

Algorithm AES

Method CBC

Key length 256 bits



Encryption

Encryption key GhFGOUTGYq2CRSUlvUZnhELrV5G2BdH+YU3iFcSvWs4=

Mask Encryption key

Algorithm AES

Method CBC

Key length 256 bits

**NOTE**

For more details about encryption settings, please refer to step no. **12** in Chapter 7 Create a Backup Set.

## Recycle Bin

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

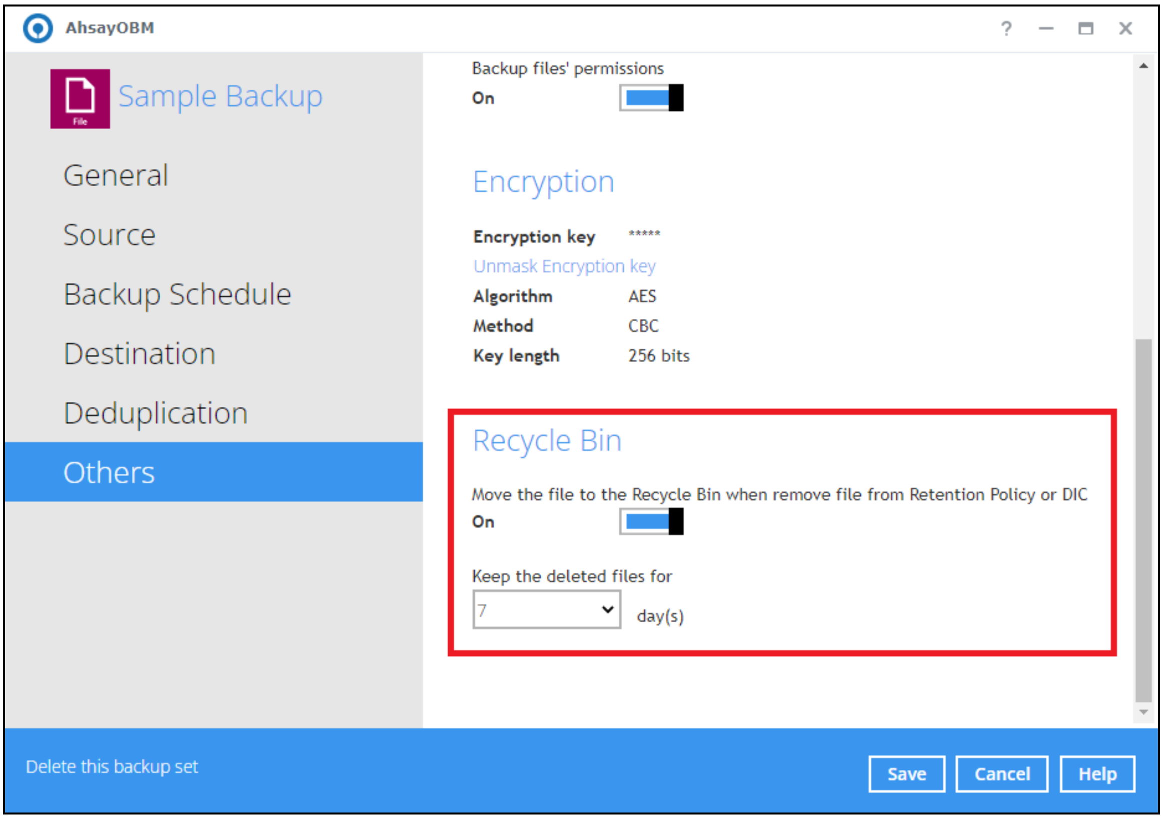
This is how the Recycle Bin will treat deleted data:

- Data in the Recycle Bin will consume Quota.
- It does not move the data in another location within the storage, instead the index tracks the xxxxxx.bak files and 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 set.
- 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.



Backup files' permissions
On

Encryption

Encryption key *****
Unmask Encryption key
Algorithm AES
Method CBC
Key length 256 bits

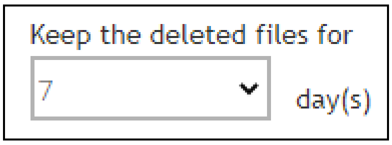
Recycle Bin

Move the file to the Recycle Bin when remove file from Retention Policy or DIC
On

Keep the deleted files for
7 day(s)

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

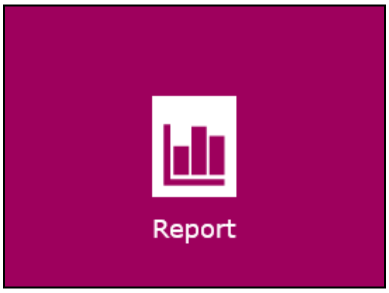
1. Go to Backup Sets, then select a backup set.
2. Click the **Others** tab in the backup set settings.
3. Under Recycle Bin, select the number of days or you can enter it manually.



Keep the deleted files for
7 day(s)

## 8.7 Report

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



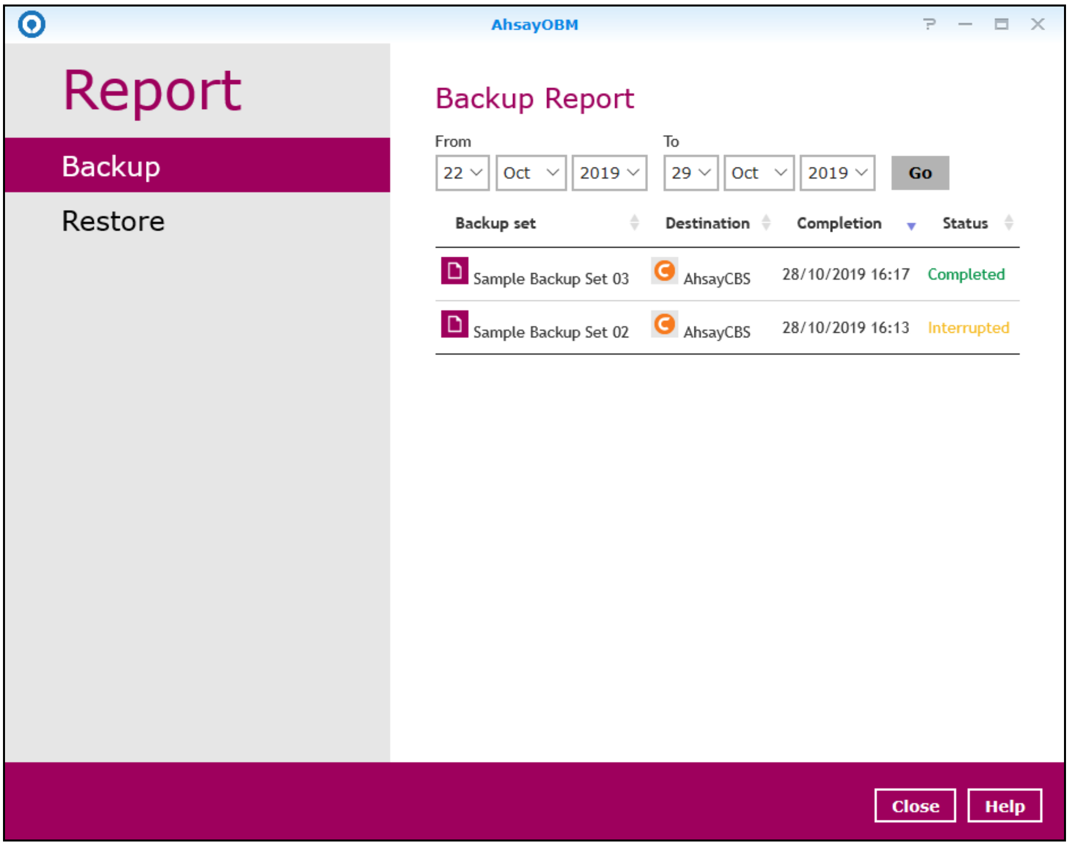
There are two (2) option available for this feature:

- Backup
- Restore

### 8.7.1 Backup

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

- Date
- Backup set
- Destination
- Status



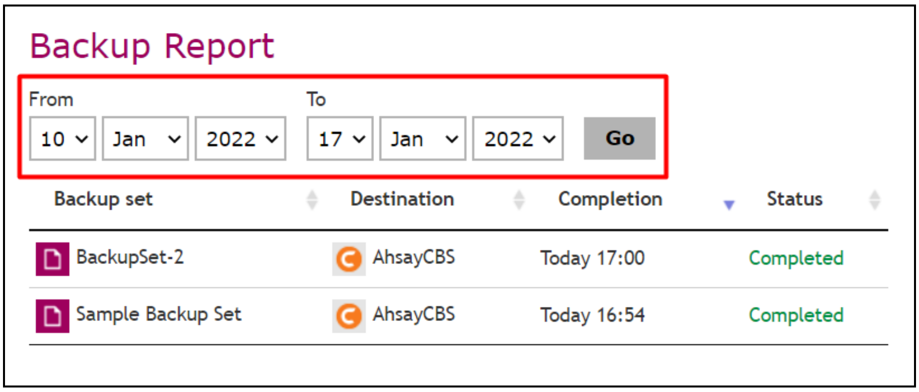
Backup Report

From 22 Oct 2019 To 29 Oct 2019 Go

| Backup set | Destination | Completion | Status |
|---|---|---|---|
| Sample Backup Set 03 | AhsayCBS | 28/10/2019 16:17 | Completed |
| Sample Backup Set 02 | AhsayCBS | 28/10/2019 16:13 | Interrupted |

### Date

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



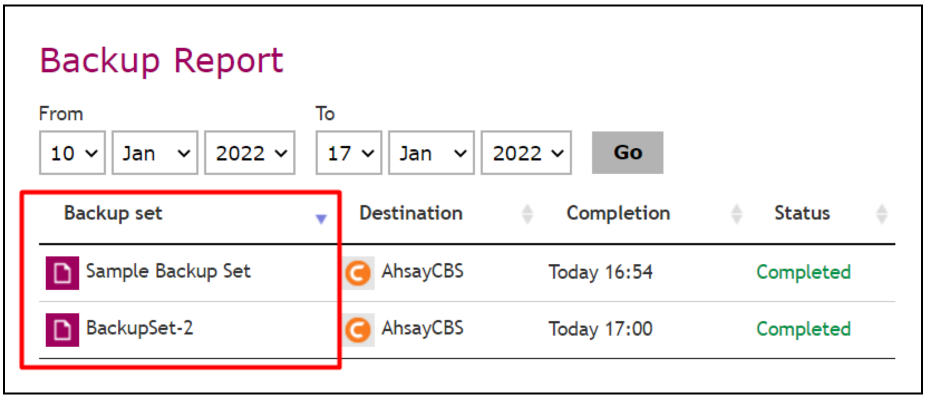
Backup Report

From 10 Jan 2022 To 17 Jan 2022 Go

| Backup set | Destination | Completion | Status |
|---|---|---|---|
| BackupSet-2 | AhsayCBS | Today 17:00 | Completed |
| Sample Backup Set | AhsayCBS | Today 16:54 | Completed |

### Backup set

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



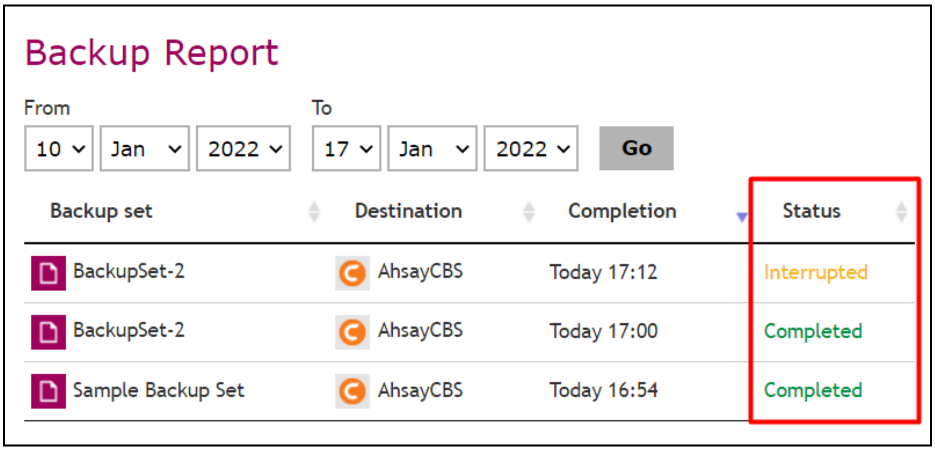
Backup Report

From 10 Jan 2022 To 17 Jan 2022 Go

| Backup set | Destination | Completion | Status |
|---|---|---|---|
| Sample Backup Set | AhsayCBS | Today 16:54 | Completed |
| BackupSet-2 | AhsayCBS | Today 17:00 | Completed |

### Status

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



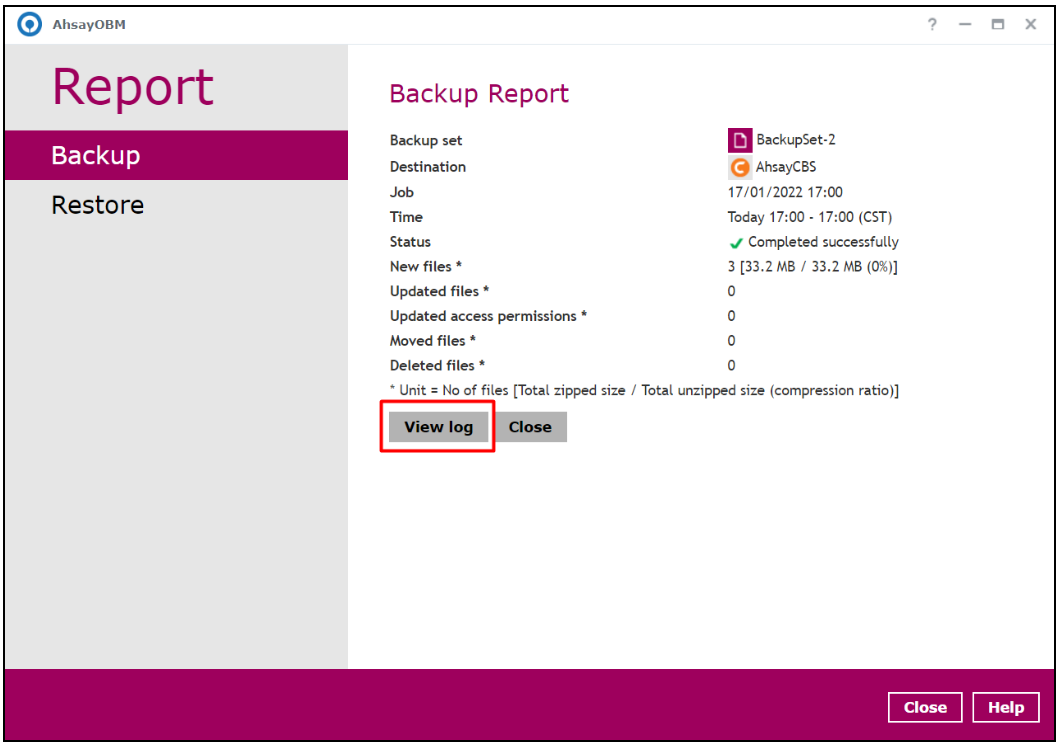
Backup Report

From 10 Jan 2022 To 17 Jan 2022 Go

| Backup set | Destination | Completion | Status |
|---|---|---|---|
| BackupSet-2 | AhsayCBS | Today 17:12 | Interrupted |
| BackupSet-2 | AhsayCBS | Today 17:00 | Completed |
| Sample Backup Set | AhsayCBS | Today 16:54 | Completed |

To view the backup log, follow the instructions below:

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

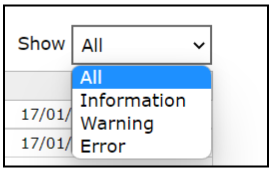


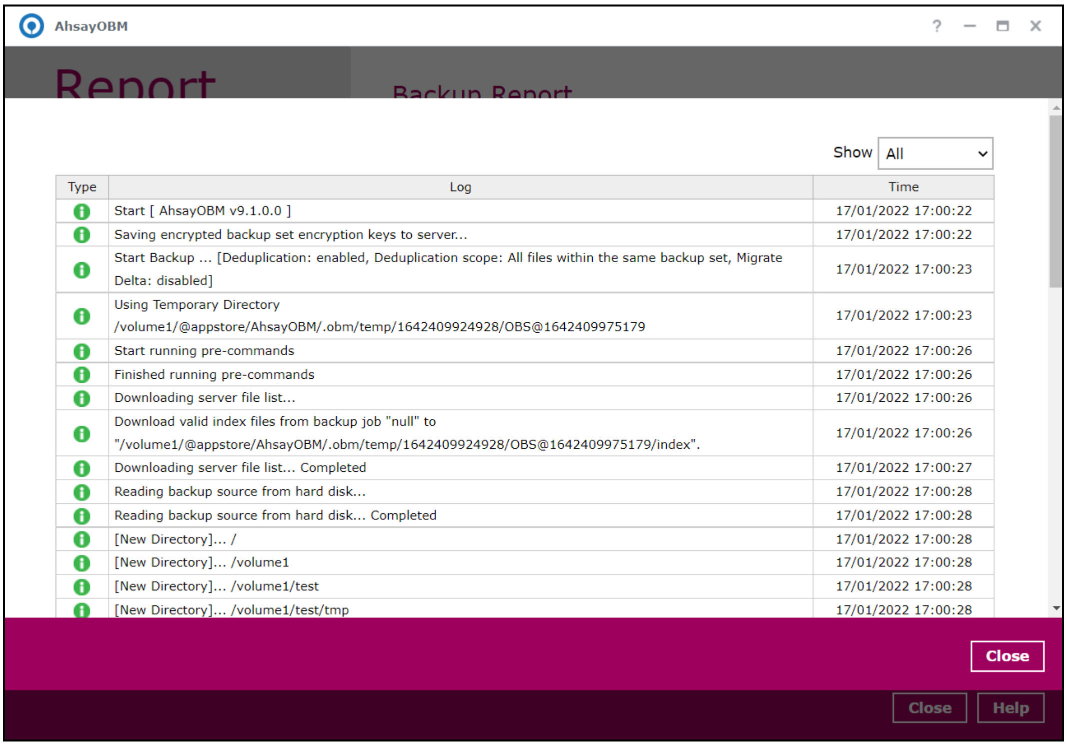
Backup Report

| | |
|---|---|
| Backup set | BackupSet-2 |
| Destination | AhsayCBS |
| Job | 17/01/2022 17:00 |
| Time | Today 17:00 - 17:00 (CST) |
| Status | ✓ Completed successfully |
| New files * | 3 [33.2 MB / 33.2 MB (0%)] |
| Updated files * | 0 |
| Updated access permissions * | 0 |
| Moved files * | 0 |
| Deleted files * | 0 |

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

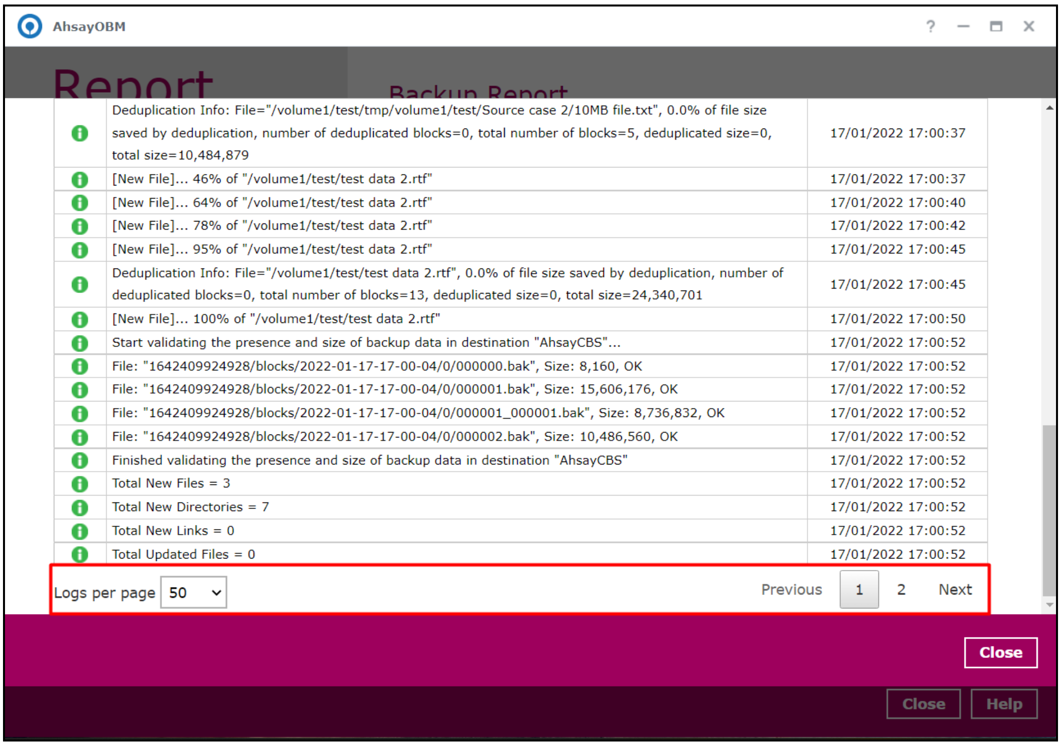
2. The status can be filtered when viewing the backup report.





| Type | Log | Time |
|---|---|---|
| ● | Start [ AhsayOBM v9.1.0.0 ] | 17/01/2022 17:00:22 |
| ● | Saving encrypted backup set encryption keys to server... | 17/01/2022 17:00:22 |
| ● | Start Backup ... [Deduplication: enabled, Deduplication scope: All files within the same backup set, Migrate Delta: disabled] | 17/01/2022 17:00:23 |
| ● | Using Temporary Directory /volume1/@appstore/AhsayOBM/.obm/temp/1642409924928/OBS@1642409975179 | 17/01/2022 17:00:23 |
| ● | Start running pre-commands | 17/01/2022 17:00:26 |
| ● | Finished running pre-commands | 17/01/2022 17:00:26 |
| ● | Downloading server file list... | 17/01/2022 17:00:26 |
| ● | Download valid index files from backup job "null" to "/volume1/@appstore/AhsayOBM/.obm/temp/1642409924928/OBS@1642409975179/index". | 17/01/2022 17:00:26 |
| ● | Downloading server file list... Completed | 17/01/2022 17:00:27 |
| ● | Reading backup source from hard disk... | 17/01/2022 17:00:28 |
| ● | Reading backup source from hard disk... Completed | 17/01/2022 17:00:28 |
| ● | [New Directory]... / | 17/01/2022 17:00:28 |
| ● | [New Directory]... /volume1 | 17/01/2022 17:00:28 |
| ● | [New Directory]... /volume1/test | 17/01/2022 17:00:28 |
| ● | [New Directory]... /volume1/test/tmp | 17/01/2022 17:00:28 |

3. You can also select the number of logs per page or navigate through the backup report by clicking the next page.

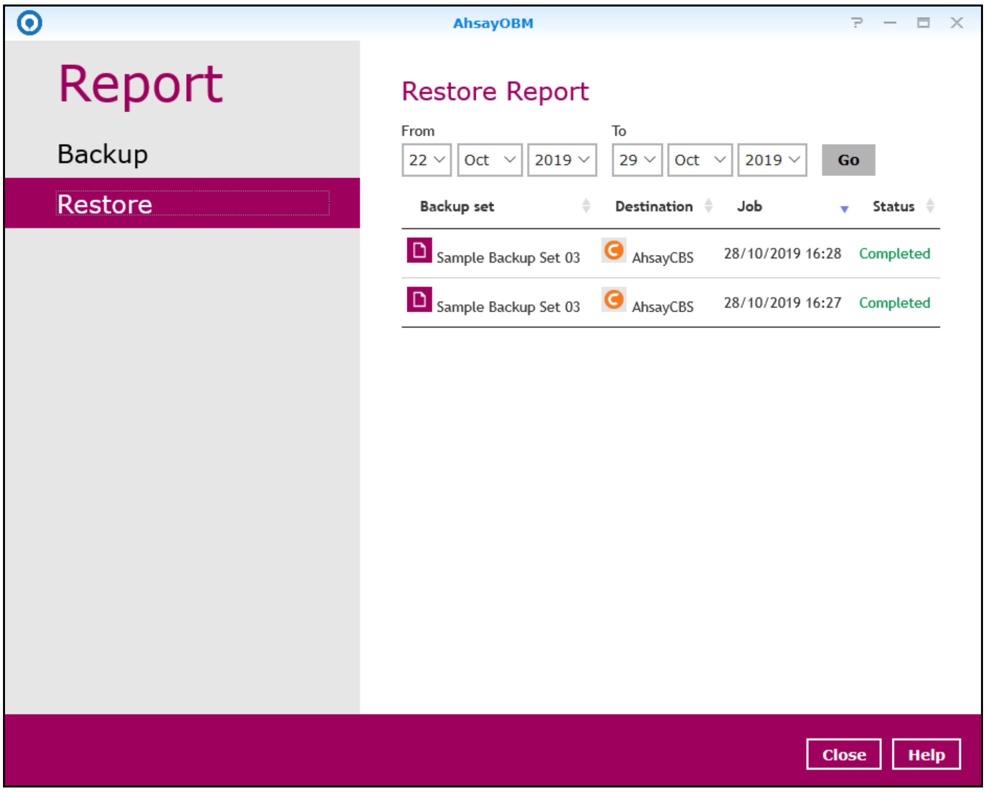


```
Deduplication Info: File="/volume1/test/tmp/volume1/test/Source case 2/10MB file.txt", 0.0% of file size
saved by deduplication, number of deduplicated blocks=0, total number of blocks=5, deduplicated size=0,
total size=10,484,879                                                                                        17/01/2022 17:00:37
[New File]... 46% of "/volume1/test/test data 2.rtf"                                                         17/01/2022 17:00:37
[New File]... 64% of "/volume1/test/test data 2.rtf"                                                         17/01/2022 17:00:40
[New File]... 78% of "/volume1/test/test data 2.rtf"                                                         17/01/2022 17:00:42
[New File]... 95% of "/volume1/test/test data 2.rtf"                                                         17/01/2022 17:00:45
Deduplication Info: File="/volume1/test/test data 2.rtf", 0.0% of file size saved by deduplication, number of
deduplicated blocks=0, total number of blocks=13, deduplicated size=0, total size=24,340,701                 17/01/2022 17:00:45
[New File]... 100% of "/volume1/test/test data 2.rtf"                                                        17/01/2022 17:00:50
Start validating the presence and size of backup data in destination "AhsayCBS"...                          17/01/2022 17:00:52
File: "1642409924928/blocks/2022-01-17-17-00-04/0/000000.bak", Size: 8,160, OK                              17/01/2022 17:00:52
File: "1642409924928/blocks/2022-01-17-17-00-04/0/000001.bak", Size: 15,606,176, OK                         17/01/2022 17:00:52
File: "1642409924928/blocks/2022-01-17-17-00-04/0/000001_000001.bak", Size: 8,736,832, OK                   17/01/2022 17:00:52
File: "1642409924928/blocks/2022-01-17-17-00-04/0/000002.bak", Size: 10,486,560, OK                         17/01/2022 17:00:52
Finished validating the presence and size of backup data in destination "AhsayCBS"                          17/01/2022 17:00:52
Total New Files = 3                                                                                          17/01/2022 17:00:52
Total New Directories = 7                                                                                    17/01/2022 17:00:52
Total New Links = 0                                                                                          17/01/2022 17:00:52
Total Updated Files = 0                                                                                      17/01/2022 17:00:52
```

### 8.7.2 Restore

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

- Date
- Backup set
- Destination
- Status



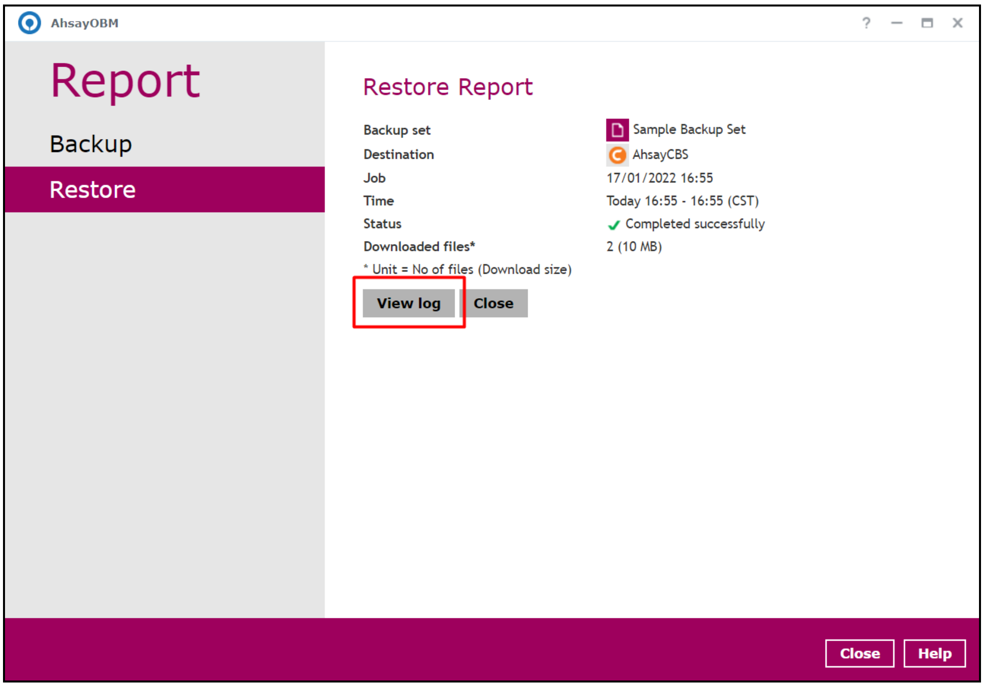
Restore Report

From 22 Oct 2019 To 29 Oct 2019 Go

| Backup set | Destination | Job | Status |
|---|---|---|---|
| Sample Backup Set 03 | AhsayCBS | 28/10/2019 16:28 | Completed |
| Sample Backup Set 03 | AhsayCBS | 28/10/2019 16:27 | Completed |

To view the restore log, follow the instructions below:

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

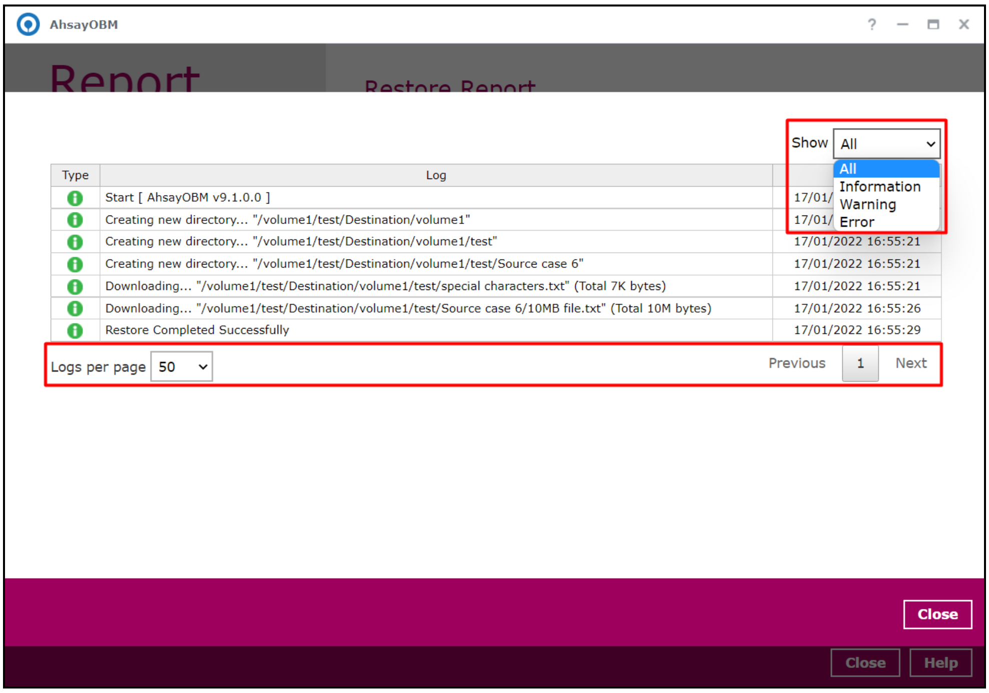


Restore Report

| | |
|---|---|
| Backup set | Sample Backup Set |
| Destination | AhsayCBS |
| Job | 17/01/2022 16:55 |
| Time | Today 16:55 - 16:55 (CST) |
| Status | ✓ Completed successfully |
| Downloaded files* | 2 (10 MB) |

* Unit = No of files (Download size)

2. The status can be filtered when viewing the restore report. You can also select the number of logs per page or navigate through the restore report by clicking the next page.



Show All

| Type | Log | |
|---|---|---|
| ⓘ | Start [ AhsayOBM v9.1.0.0 ] | 17/01/ |
| ⓘ | Creating new directory... "/volume1/test/Destination/volume1" | 17/01/ |
| ⓘ | Creating new directory... "/volume1/test/Destination/volume1/test" | 17/01/2022 16:55:21 |
| ⓘ | Creating new directory... "/volume1/test/Destination/volume1/test/Source case 6" | 17/01/2022 16:55:21 |
| ⓘ | Downloading... "/volume1/test/Destination/volume1/test/special characters.txt" (Total 7K bytes) | 17/01/2022 16:55:21 |
| ⓘ | Downloading... "/volume1/test/Destination/volume1/test/Source case 6/10MB file.txt" (Total 10M bytes) | 17/01/2022 16:55:26 |
| ⓘ | Restore Completed Successfully | 17/01/2022 16:55:29 |

Logs per page 50

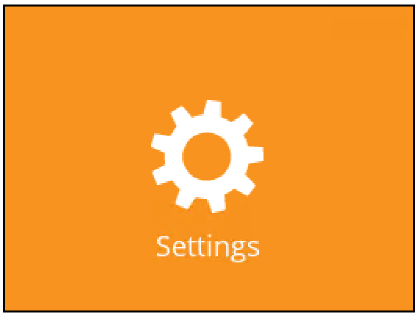
## 8.8 Restore

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 12 Restore Data.

## 8.9 Settings

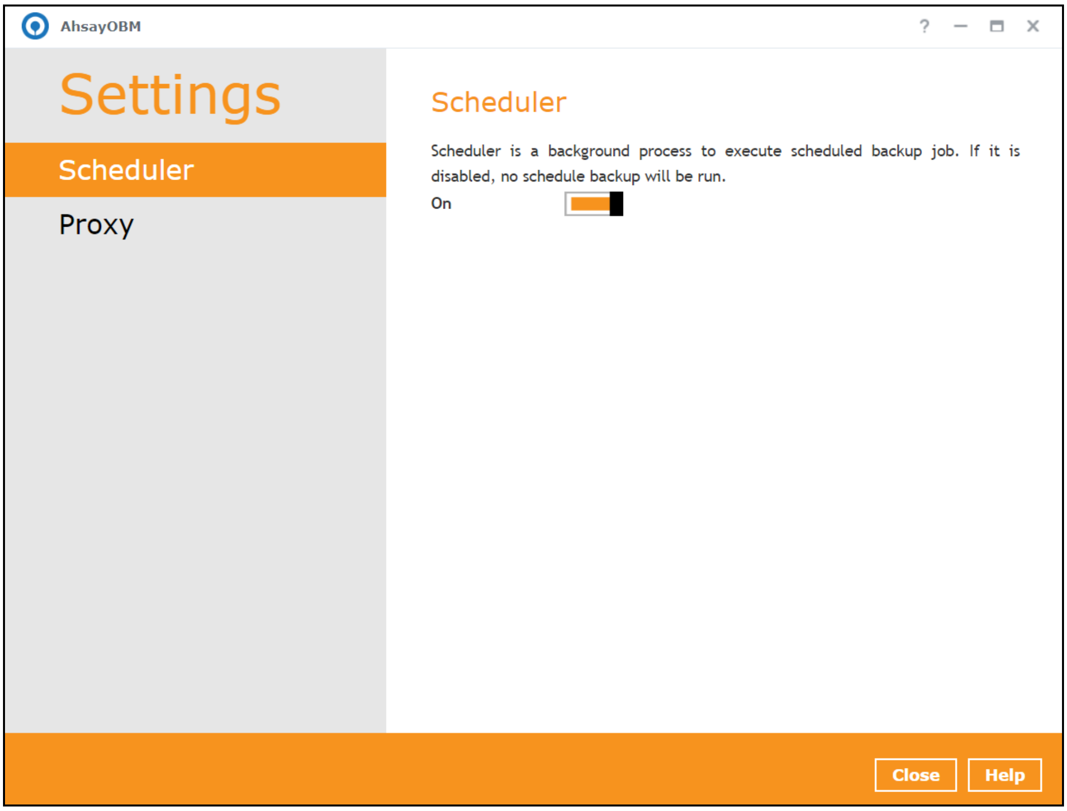
This feature allows the user to enable the **Scheduler** and **Proxy** settings.



### 8.9.1 Scheduler

The Scheduler setting was for AhsayOBM pre-v9.3.2.0 and has been removed.

When this feature is on, the user can execute a **scheduled backup** job. Otherwise, no scheduled backup will run.



Scheduler

Scheduler is a background process to execute scheduled backup job. If it is disabled, no schedule backup will be run.

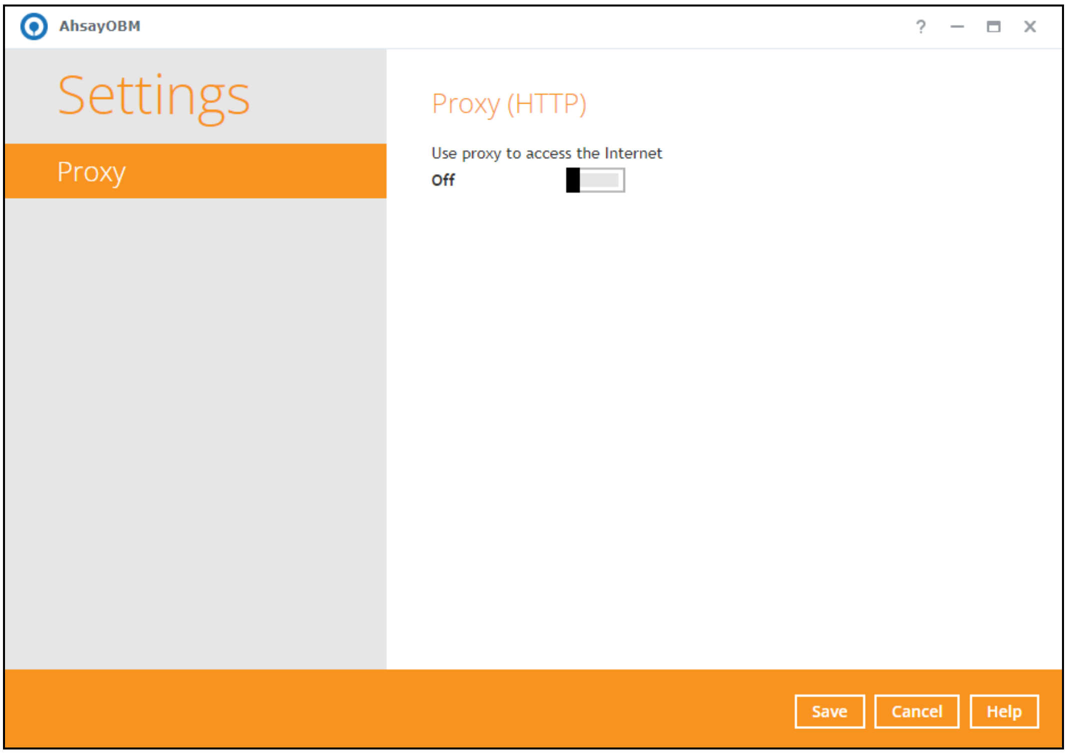
On

**NOTE**

For more details on the scenario for the Scheduler settings, refer to Appendix C: Scheduler Scenarios.

### 8.9.2 Proxy

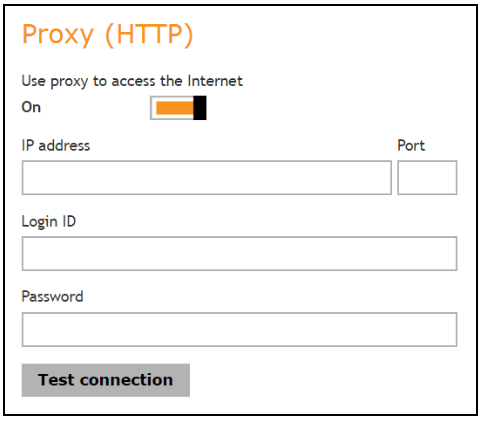
When this feature is on, AhsayOBM will use a proxy to gain access to the internet.



Use proxy to access the Internet
Off

To enable the Proxy Settings, follow the instructions below:

1. Slide the lever to the right to turn on this feature.
2. Complete the following fields:
   - IP address
   - Port
   - Login ID
   - Password



Use proxy to access the Internet
On

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

## 8.10 Utilities

This feature allows the user to perform quality check on the backed up data and/or delete backed up data.

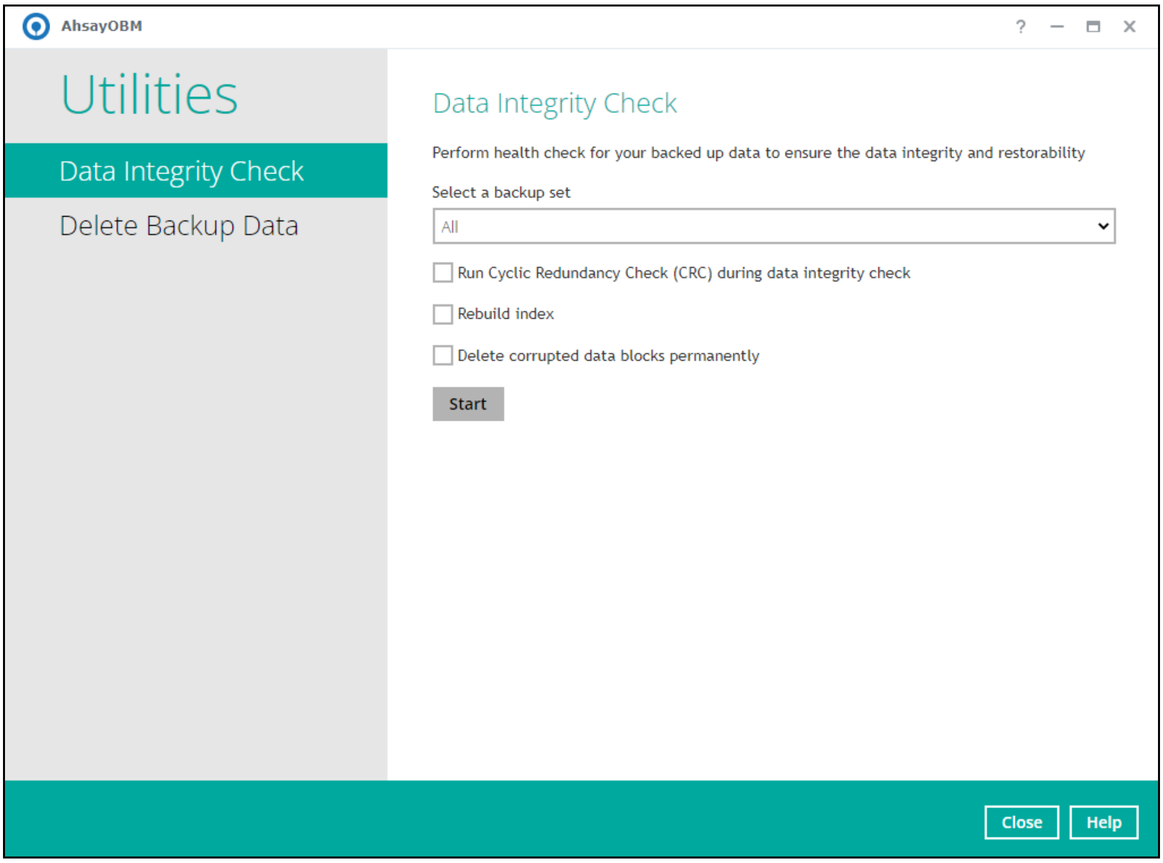
There are two (2) options available for this feature:

- Data Integrity Check
- Delete Backup Data

### 8.10.1 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 DIC 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).



Data Integrity Check

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

Select a backup set

All

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

□ Rebuild index

□ Delete corrupted data blocks permanently

Start

**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. 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. As the **backup**, **restore** and **Data Integrity Check** are using the same index for read and write operations which causes the error.

### 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 DIC depends on the number of factors such as:

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

**NOTE**

For user(s) with metered internet connection, additional data charges may be incurred if the Cyclic Redundancy Check (CRC) is enabled. As the Cyclic Redundancy Check data involves downloading the data from the backup destination(s) to the client machine in order to perform this check.

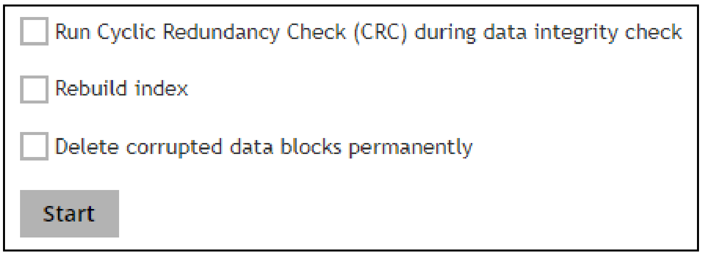
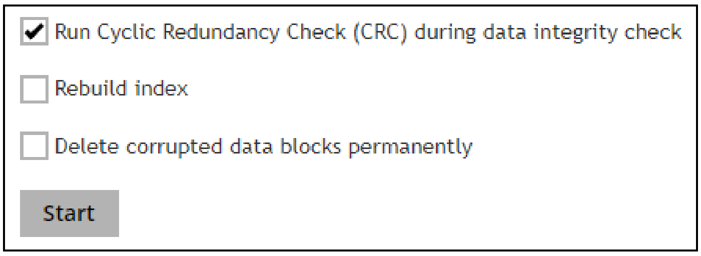
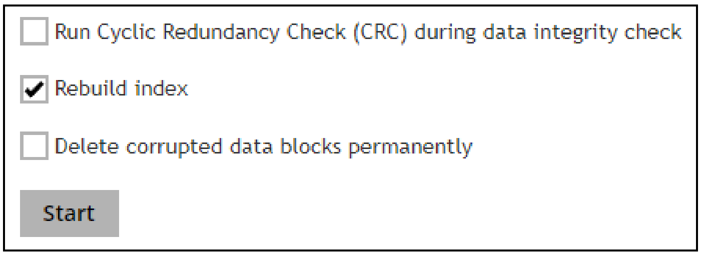
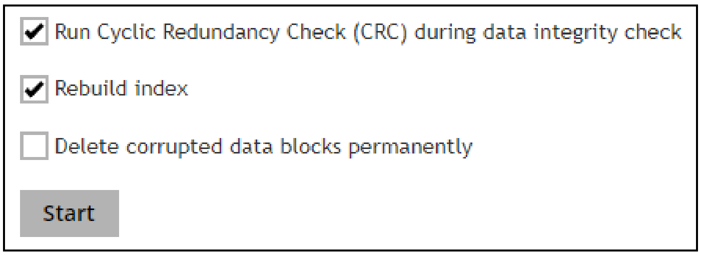
### Rebuild index

When this option is enabled, the DIC 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.

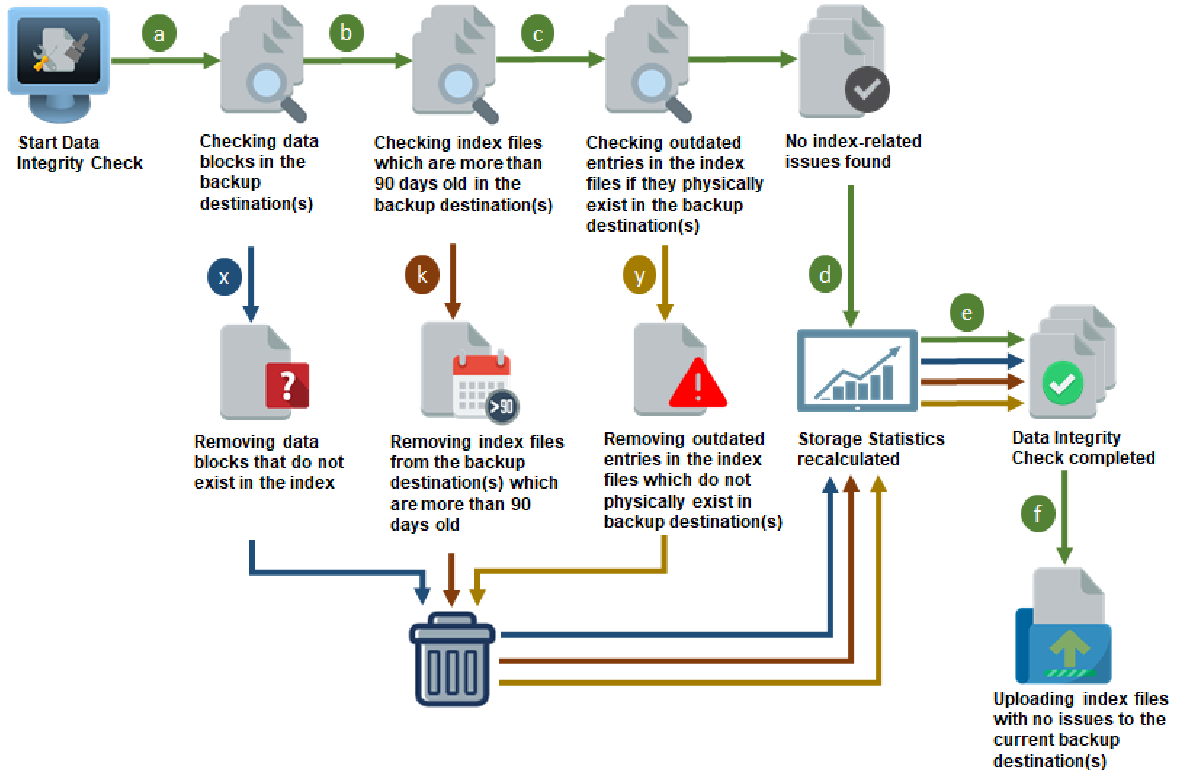
There are four (4) options in performing the DIC:

| Settings | Function |
|---|---|
| **Option 1**<br><br>□ Run Cyclic Redundancy Check (CRC) during data integrity check<br>□ Rebuild index<br>□ Delete corrupted data blocks permanently<br>Start | For checking of index and data. |
| **Option 2**<br><br>☑ Run Cyclic Redundancy Check (CRC) during data integrity check<br>□ Rebuild index<br>□ Delete corrupted data blocks permanently<br>Start | For checking of index and integrity of files against the checksum file generated at the time of the backup job. |
| **Option 3**<br><br>□ Run Cyclic Redundancy Check (CRC) during data integrity check<br>☑ Rebuild index<br>□ Delete corrupted data blocks permanently<br>Start | For checking and rebuilding of index. |
| **Option 4**<br><br>☑ Run Cyclic Redundancy Check (CRC) during data integrity check<br>☑ Rebuild index<br>□ Delete corrupted data blocks permanently<br>Start | For checking of index, integrity of files against the checksum file generated at the time of the backup job and rebuilding of index |

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

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

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


a
b
c
Start Data Integrity Check
Checking data blocks in the backup destination(s)
Checking index files which are more than 90 days old in the backup destination(s)
Checking outdated entries in the index files if they physically exist in the backup destination(s)
No index-related issues found
x
k
y
d
e
Removing data blocks that do not exist in the index
Removing index files from the backup destination(s) which are more than 90 days old
Removing outdated entries in the index files which do not physically exist in backup destination(s)
Storage Statistics recalculated
Data Integrity Check completed
f
Uploading index files with no issues to the current backup destination(s)

a Check the data blocks (.bak files) located in the backup destination(s) if they exist in the index.

➔If **YES**, proceed to b

➔ If **NO**, proceed to x

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

➔If **YES**, proceed to k

➔ If **NO**, proceed to c

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

➔If **YES**, proceed to d

➔ If **NO**, proceed to y

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

e Data integrity check is completed.

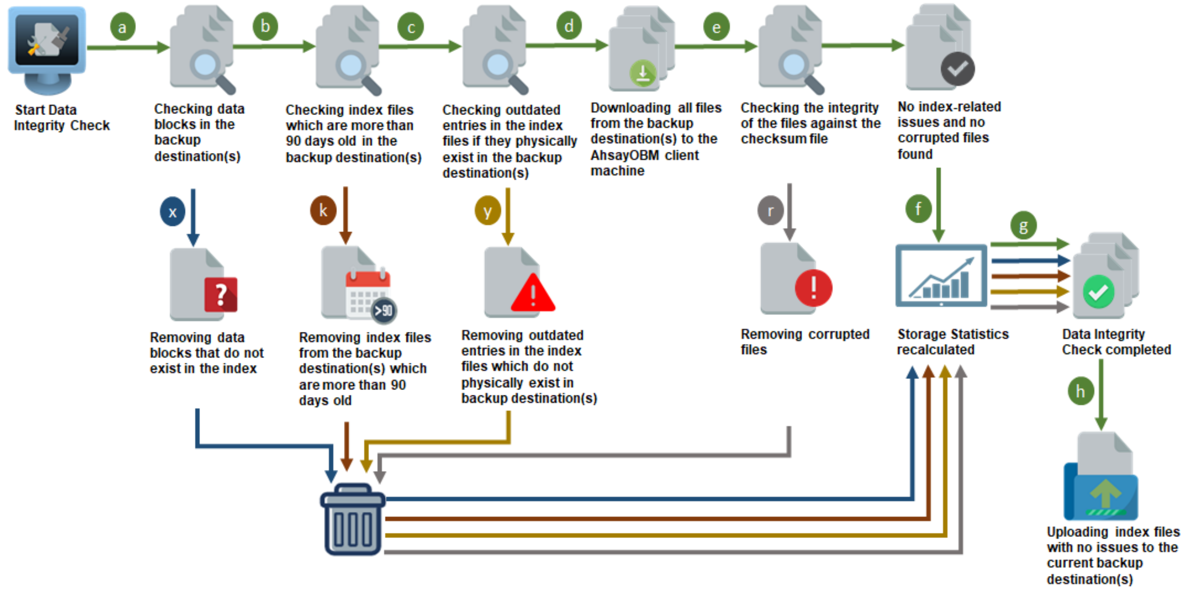
f Index files with no issues will be uploaded to the current backup destination(s).

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

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

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

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


Start Data Integrity Check
a
Checking data blocks in the backup destination(s)
b
Checking index files which are more than 90 days old in the backup destination(s)
c
Checking outdated entries in the index files if they physically exist in the backup destination(s)
d
Downloading all files from the backup destination(s) to the AhsayOBM client machine
e
Checking the integrity of the files against the checksum file
No index-related issues and no corrupted files found
x
k
y
r
f
g
Removing data blocks that do not exist in the index
>90
Removing index files from the backup destination(s) which are more than 90 days old
Removing outdated entries in the index files which do not physically exist in backup destination(s)
Removing corrupted files
Storage Statistics recalculated
Data Integrity Check completed
h
Uploading index files with no issues to the current backup destination(s)

a Check the data blocks (.bak files) located in the backup destination(s) if they exist in the index.

→ If **YES**, proceed to b

→ If **NO**, proceed to x

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

→ If **YES**, proceed to k

→ If **NO**, proceed to c

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

→ If **YES**, proceed to d

→ If **NO**, proceed to y

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

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

e Check the integrity of files in the backup destination(s) against the checksum file generated at the time of the backup job.

→ If any discrepancy is **FOUND**, proceed to r

→ If **NO** discrepancy is found, proceed to f

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

g Data integrity check is completed.

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

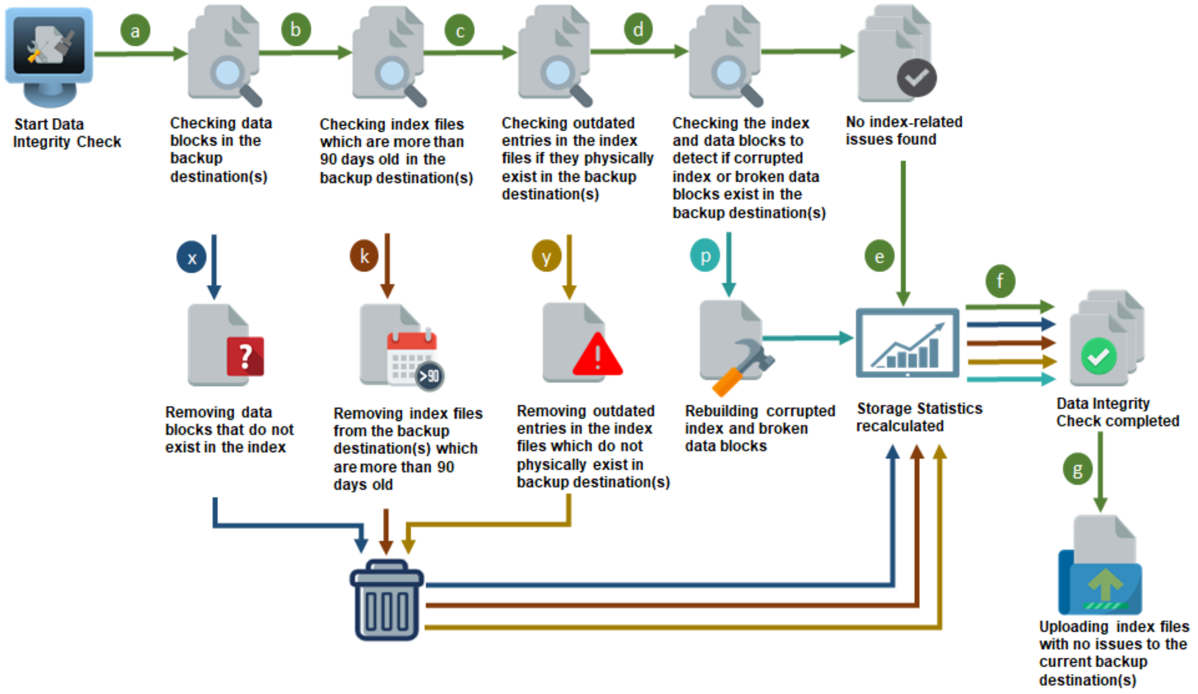
x Data blocks (.bak files) that do not exist in the index and partially uploaded orphan files will be automatically removed from the backup destination(s).

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

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

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

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


Start Data Integrity Check
a
Checking data blocks in the backup destination(s)
b
Checking index files which are more than 90 days old in the backup destination(s)
c
Checking outdated entries in the index files if they physically exist in the backup destination(s)
d
Checking the index and data blocks to detect if corrupted index or broken data blocks exist in the backup destination(s)
No index-related issues found
x
k
y
p
e
f
Removing data blocks that do not exist in the index
Removing index files from the backup destination(s) which are more than 90 days old
Removing outdated entries in the index files which do not physically exist in backup destination(s)
Rebuilding corrupted index and broken data blocks
Storage Statistics recalculated
Data Integrity Check completed
g
Uploading index files with no issues to the current backup destination(s)

a Check the data blocks (.bak files) located in the backup destination(s) if they exist in the index.

➔ If **YES**, proceed to b

➔ If **NO**, proceed to x

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

➔ If **YES**, proceed to k

➔ If **NO**, proceed to c

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

➔ If **YES**, proceed to d

➔ If **NO**, proceed to y

d Check the index and data blocks in the backup destination(s) to identify corrupted index and broken data blocks.

➔ If corrupted index and broken data blocks are **FOUND**, proceed to p

➔ If **NO** corrupted index and broken data blocks are **FOUND**, proceed to e

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

f Data integrity check is completed.

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

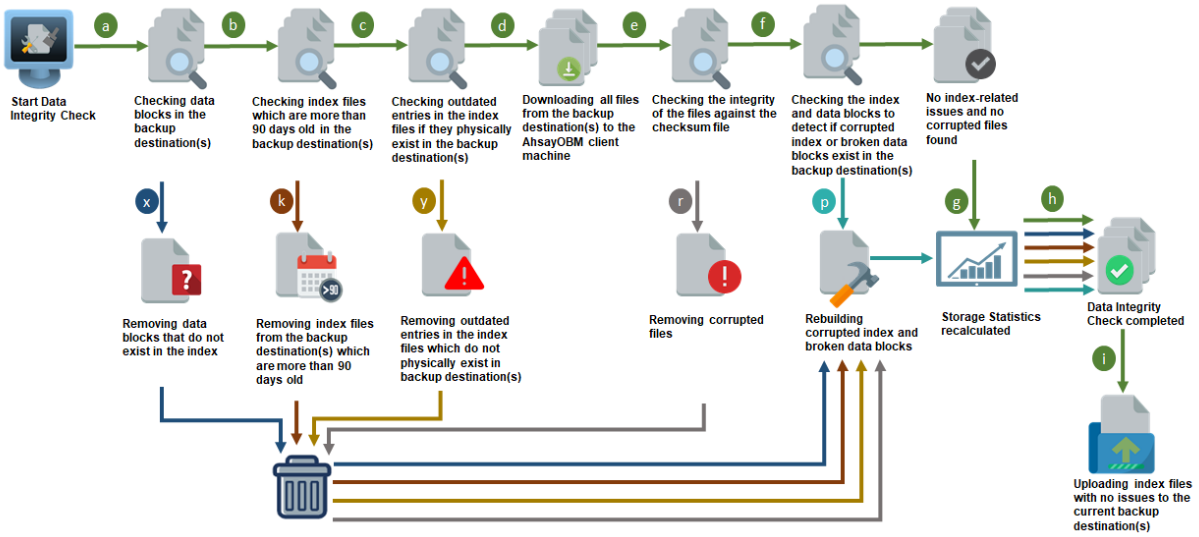
x Data blocks (.bak files) that do not exist in the index and partially uploaded orphan files will be automatically removed from the backup destination(s).

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

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

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

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


a
b
c
d
e
f
Start Data Integrity Check
Checking data blocks in the backup destination(s)
Checking index files which are more than 90 days old in the backup destination(s)
Checking outdated entries in the index files if they physically exist in the backup destination(s)
Downloading all files from the backup destination(s) to the AhsayOBM client machine
Checking the integrity of the files against the checksum file
Checking the index and data blocks to detect if corrupted index or broken data blocks exist in the backup destination(s)
No index-related issues and no corrupted files found
x
k
y
r
p
g
h
Removing data blocks that do not exist in the index
>90
Removing index files from the backup destination(s) which are more than 90 days old
Removing outdated entries in the index files which do not physically exist in backup destination(s)
Removing corrupted files
Rebuilding corrupted index and broken data blocks
Storage Statistics recalculated
Data Integrity Check completed
i
Uploading index files with no issues to the current backup destination(s)

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

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

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

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

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

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

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

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

h Data integrity check is completed.

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

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

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

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

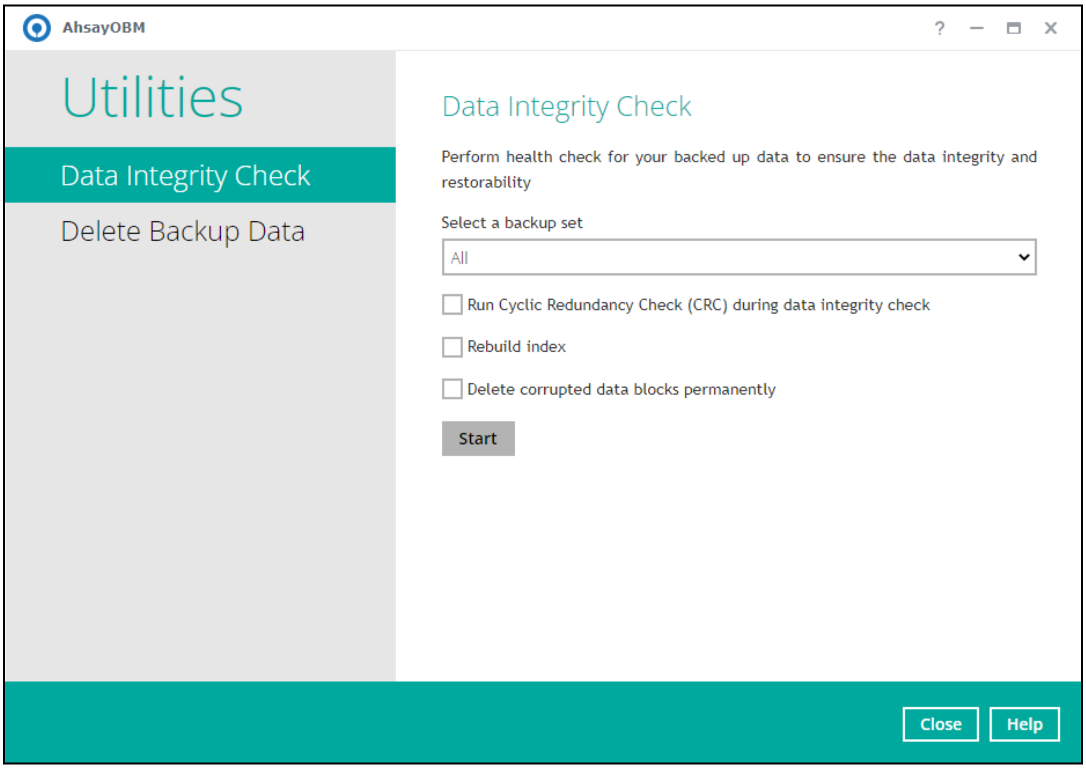
r Corrupted files will be automatically removed from the backup destination(s).

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

### Perform a Data Integrity Check

To perform a DIC, follow the instructions below:

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



AhsayOBM

Utilities

Data Integrity Check

Delete Backup Data

Data Integrity Check

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

Select a backup set

All

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

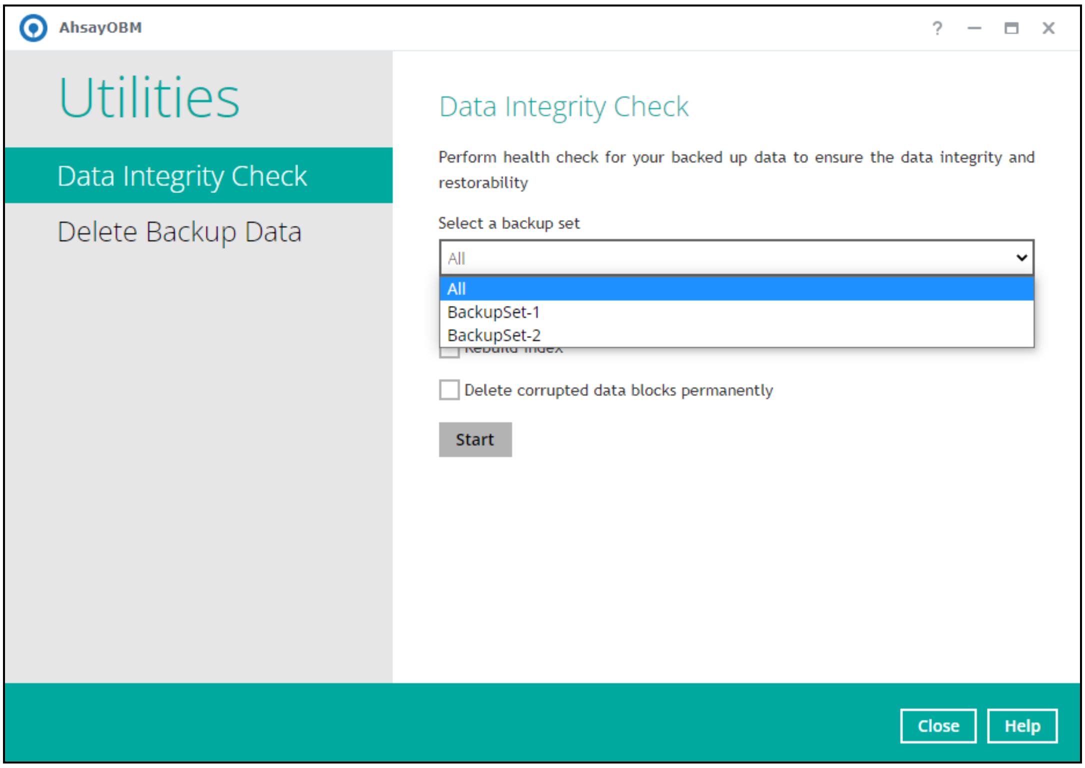
□ Rebuild index

□ Delete corrupted data blocks permanently

Start

Close Help

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



AhsayOBM

Utilities

Data Integrity Check

Delete Backup Data

Data Integrity Check

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

Select a backup set

All

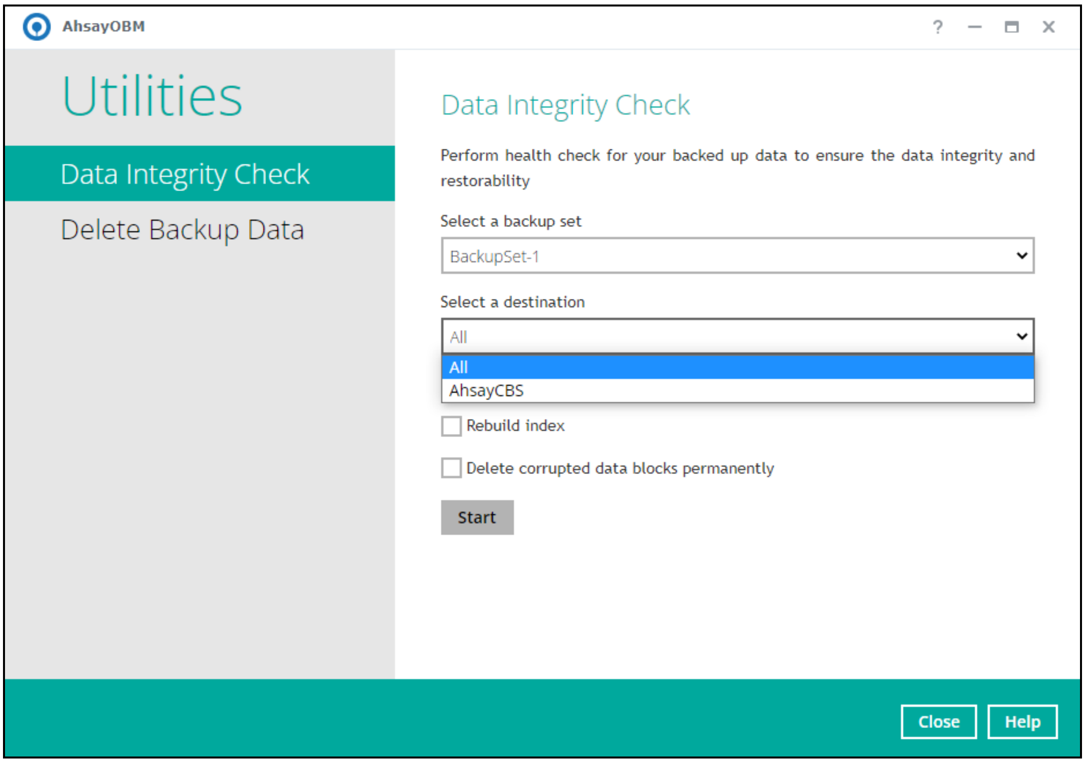
All
BackupSet-1
BackupSet-2

□ Delete corrupted data blocks permanently

Start

Close Help

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



Data Integrity Check

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

Select a backup set

BackupSet-1

Select a destination

All

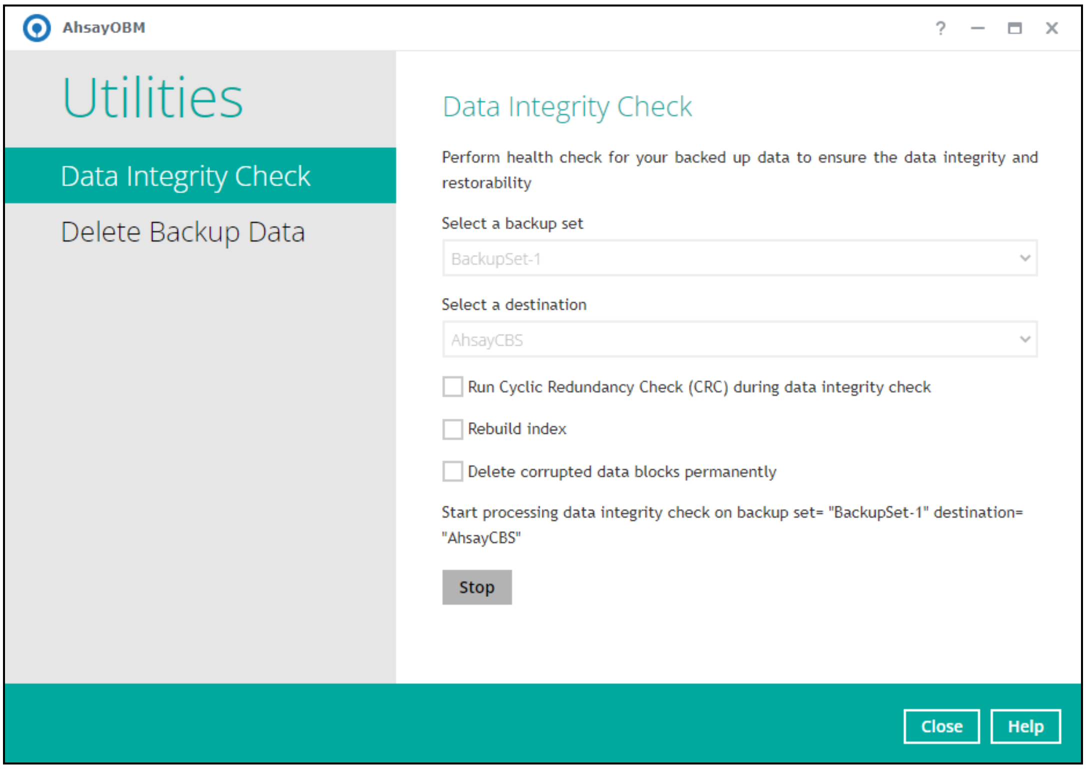
All
AhsayCBS

□ Rebuild index

□ Delete corrupted data blocks permanently

4. Click the **Start** button to begin the DIC.

5. DIC will start running on the selected backup set(s) and backup destination(s).



Data Integrity Check

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

Select a backup set

BackupSet-1

Select a destination

AhsayCBS

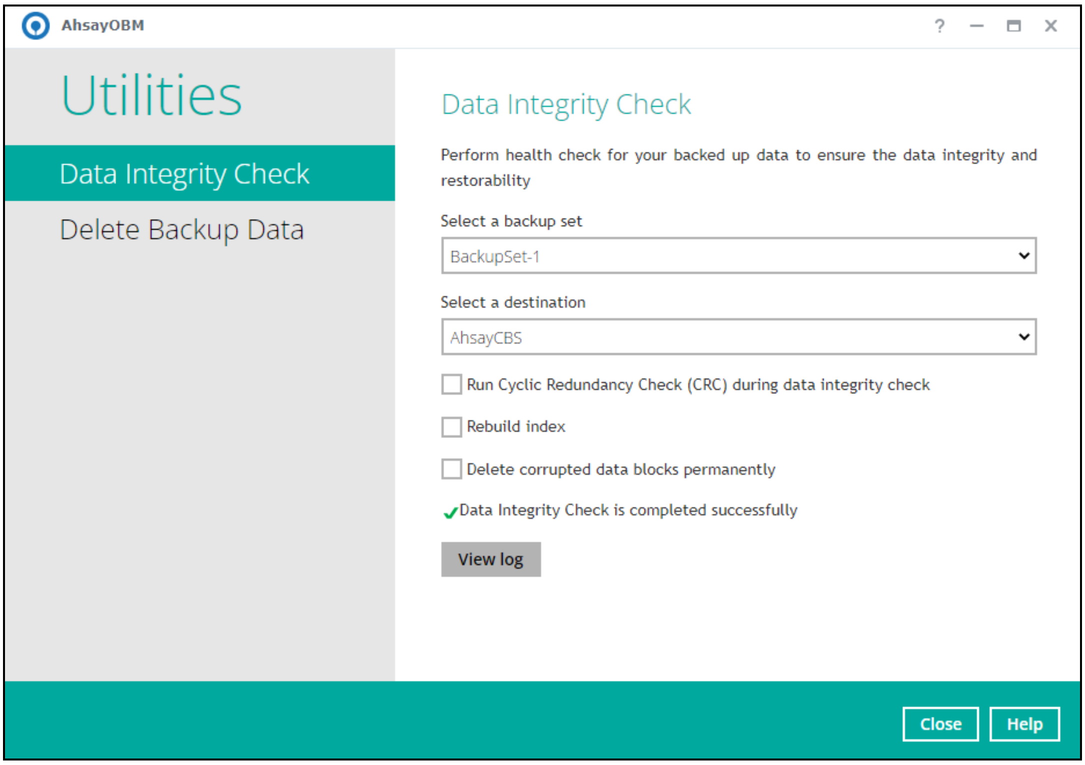
□ Run Cyclic Redundancy Check (CRC) during data integrity check

□ Rebuild index

□ Delete corrupted data blocks permanently

Start processing data integrity check on backup set= "BackupSet-1" destination= "AhsayCBS"

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



Data Integrity Check

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

Select a backup set: BackupSet-1

Select a destination: AhsayCBS

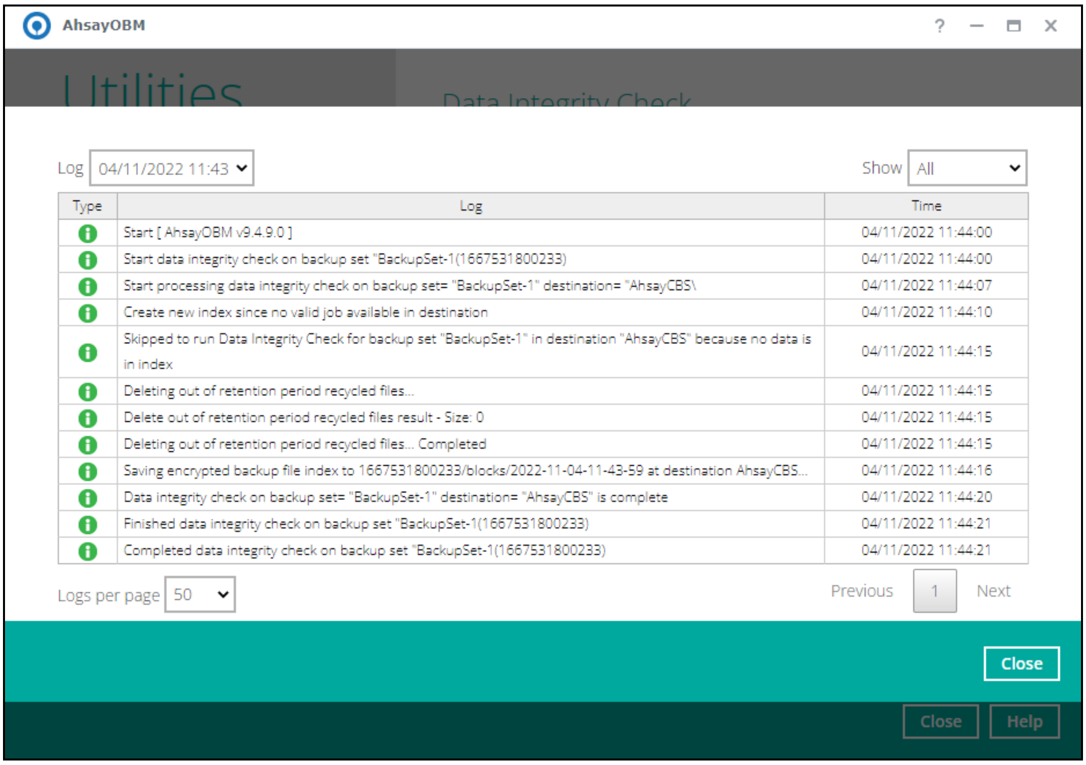
□ Run Cyclic Redundancy Check (CRC) during data integrity check

□ Rebuild index

□ Delete corrupted data blocks permanently

✓Data Integrity Check is completed successfully

7. The detailed log of DIC process will be displayed.



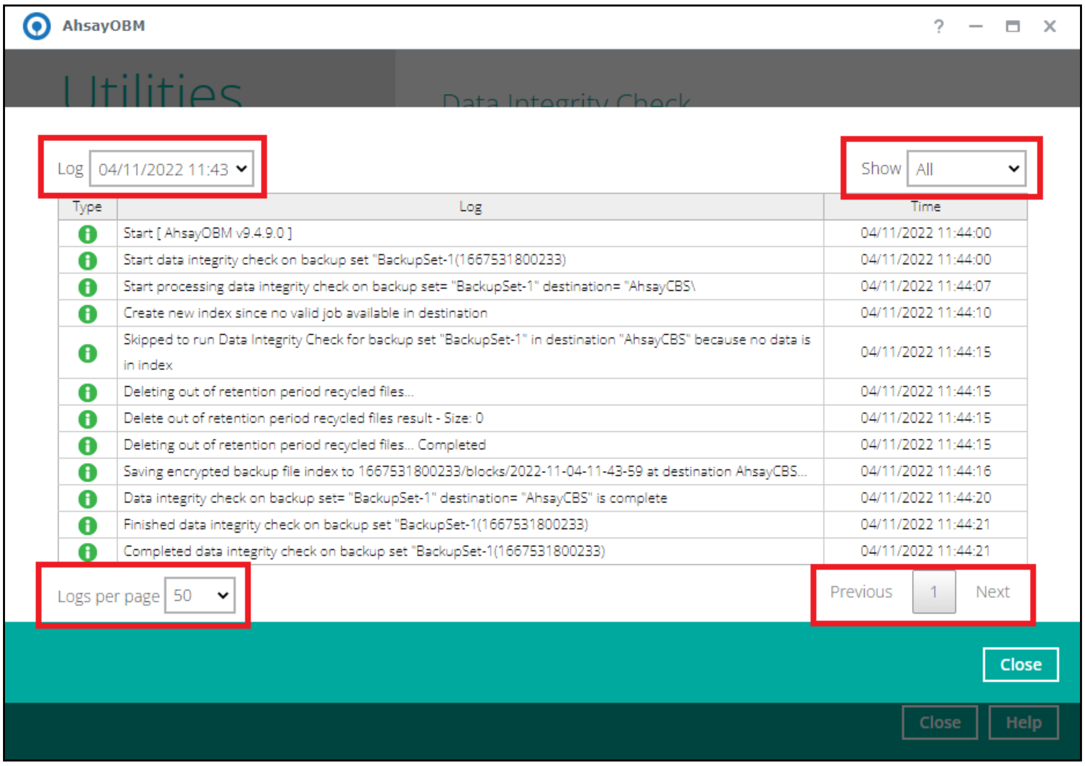
Log 04/11/2022 11:43 Show All

| Type | Log | Time |
|---|---|---|
| ⓘ | Start [ AhsayOBM v9.4.9.0 ] | 04/11/2022 11:44:00 |
| ⓘ | Start data integrity check on backup set "BackupSet-1(1667531800233) | 04/11/2022 11:44:00 |
| ⓘ | Start processing data integrity check on backup set= "BackupSet-1" destination= "AhsayCBS\ | 04/11/2022 11:44:07 |
| ⓘ | Create new index since no valid job available in destination | 04/11/2022 11:44:10 |
| ⓘ | Skipped to run Data Integrity Check for backup set "BackupSet-1" in destination "AhsayCBS" because no data is in index | 04/11/2022 11:44:15 |
| ⓘ | Deleting out of retention period recycled files... | 04/11/2022 11:44:15 |
| ⓘ | Delete out of retention period recycled files result - Size: 0 | 04/11/2022 11:44:15 |
| ⓘ | Deleting out of retention period recycled files... Completed | 04/11/2022 11:44:15 |
| ⓘ | Saving encrypted backup file index to 1667531800233/blocks/2022-11-04-11-43-59 at destination AhsayCBS... | 04/11/2022 11:44:16 |
| ⓘ | Data integrity check on backup set= "BackupSet-1" destination= "AhsayCBS" is complete | 04/11/2022 11:44:20 |
| ⓘ | Finished data integrity check on backup set "BackupSet-1(1667531800233) | 04/11/2022 11:44:21 |
| ⓘ | Completed data integrity check on backup set "BackupSet-1(1667531800233) | 04/11/2022 11:44:21 |

Logs per page 50

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

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

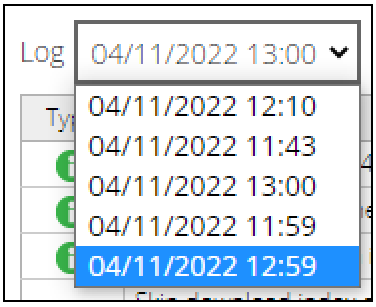
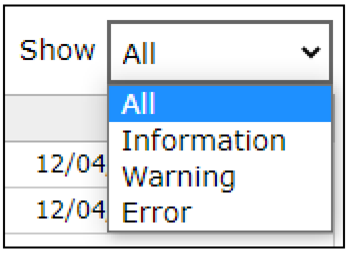
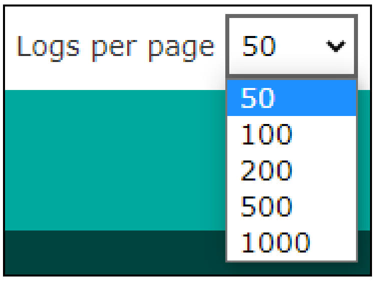
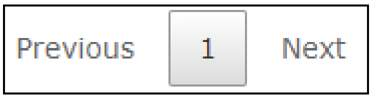


Log 04/11/2022 11:43

Show All

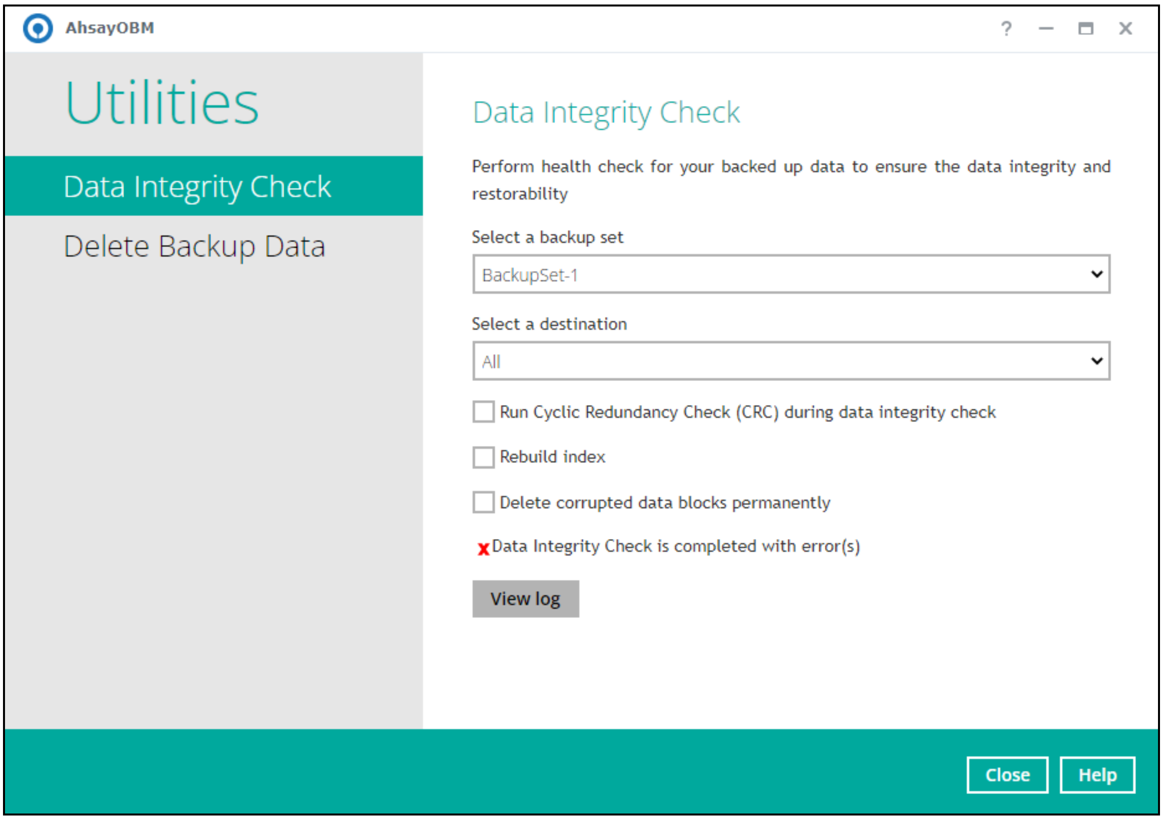
| Type | Log | Time |
|---|---|---|
| ℹ | Start [ AhsayOBM v9.4.9.0 ] | 04/11/2022 11:44:00 |
| ℹ | Start data integrity check on backup set "BackupSet-1(1667531800233) | 04/11/2022 11:44:00 |
| ℹ | Start processing data integrity check on backup set= "BackupSet-1" destination= "AhsayCBS\ | 04/11/2022 11:44:07 |
| ℹ | Create new index since no valid job available in destination | 04/11/2022 11:44:10 |
| ℹ | Skipped to run Data Integrity Check for backup set "BackupSet-1" in destination "AhsayCBS" because no data is in index | 04/11/2022 11:44:15 |
| ℹ | Deleting out of retention period recycled files... | 04/11/2022 11:44:15 |
| ℹ | Delete out of retention period recycled files result - Size: 0 | 04/11/2022 11:44:15 |
| ℹ | Deleting out of retention period recycled files... Completed | 04/11/2022 11:44:15 |
| ℹ | Saving encrypted backup file index to 1667531800233/blocks/2022-11-04-11-43-59 at destination AhsayCBS... | 04/11/2022 11:44:16 |
| ℹ | Data integrity check on backup set= "BackupSet-1" destination= "AhsayCBS" is complete | 04/11/2022 11:44:20 |
| ℹ | Finished data integrity check on backup set "BackupSet-1(1667531800233) | 04/11/2022 11:44:21 |
| ℹ | Completed data integrity check on backup set "BackupSet-1(1667531800233) | 04/11/2022 11:44:21 |

Logs per page 50

| Option | Screenshot | Function |
|---|---|---|
| **Log filter** |   Log<br>04/11/2022 13:00<br>04/11/2022 12:10<br>04/11/2022 11:43<br>04/11/2022 13:00<br>04/11/2022 11:59<br>04/11/2022 12:59 | This option can be used to display logs of the previous DIC jobs. |
| **Show filter** |  | This option can be used to sort the DIC log by its status (i.e., All, Information, Warning, and Error).<br>With this filter, it will be easier to sort the DIC logs by its status especially for longer DIC logs. |
| **Logs per page** |  | This option allows user to control the displayed number of logs per page. |
| **Page** |  | This option allows user to navigate the logs to the next page(s). |

### Data Integrity Check Completed with Errors

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



Data Integrity Check

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

Select a backup set: BackupSet-1

Select a destination: All

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

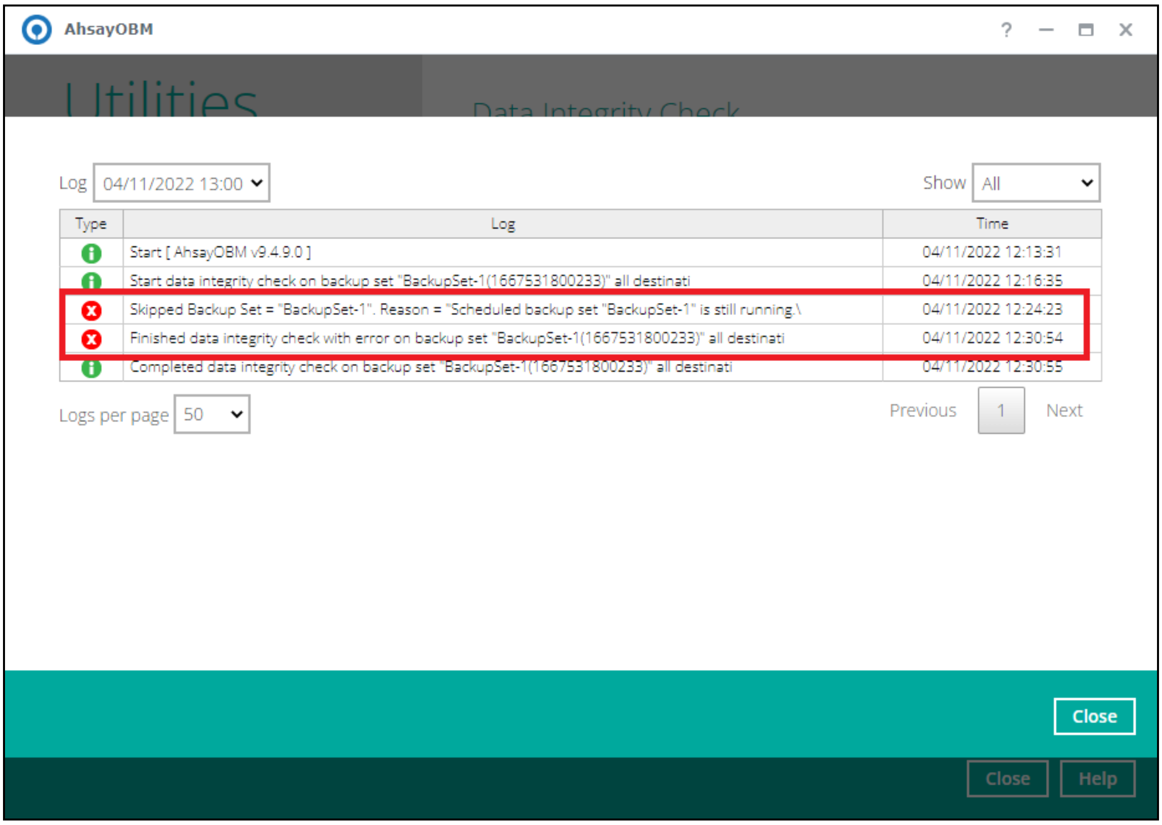
□ Rebuild index

□ Delete corrupted data blocks permanently

✗ Data Integrity Check is completed with error(s)

View log

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



Log: 04/11/2022 13:00 Show: All

| Type | Log | Time |
|---|---|---|
| ⓘ | Start [ AhsayOBM v9.4.9.0 ] | 04/11/2022 12:13:31 |
| ⓘ | Start data integrity check on backup set "BackupSet-1(1667531800233)" all destinati | 04/11/2022 12:16:35 |
| ✖ | Skipped Backup Set = "BackupSet-1". Reason = "Scheduled backup set "BackupSet-1" is still running.\ | 04/11/2022 12:24:23 |
| ✖ | Finished data integrity check with error on backup set "BackupSet-1(1667531800233)" all destinati | 04/11/2022 12:30:54 |
| ⓘ | Completed data integrity check on backup set "BackupSet-1(1667531800233)" all destinati | 04/11/2022 12:30:55 |

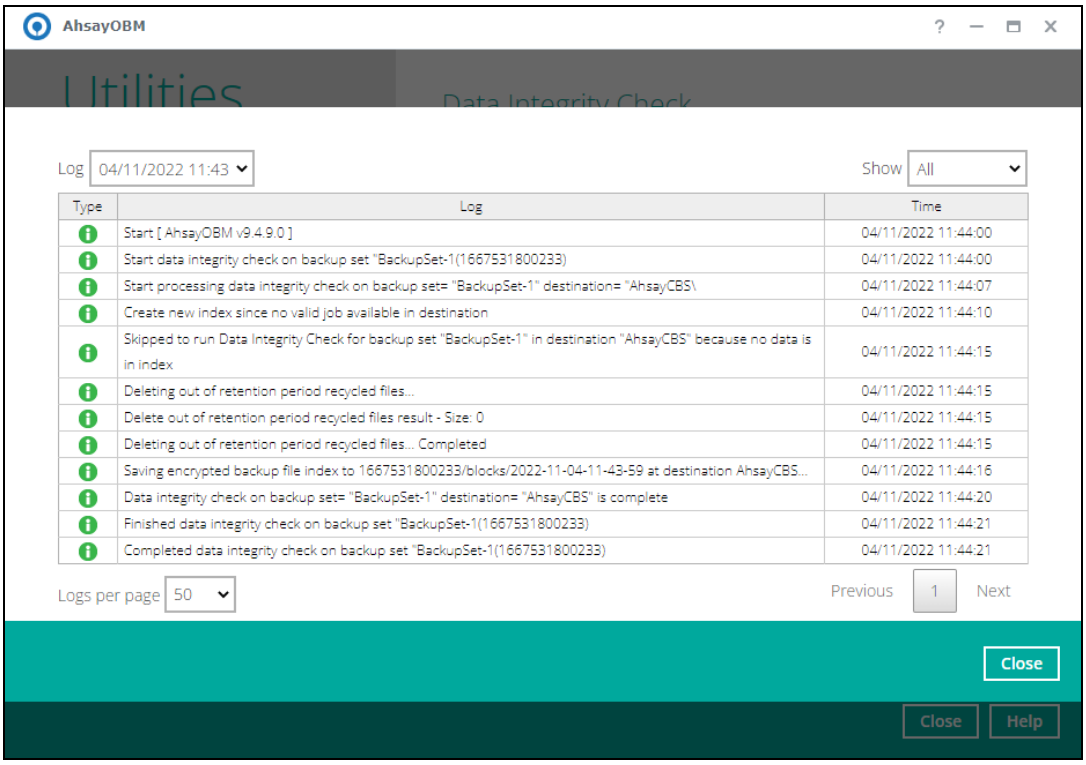
Logs per page: 50 Previous 1 Next

## Data Integrity Check Result

There are two possible outcomes after the completion of a DIC:

- DIC 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 DIC log with NO data corruption/issues detected.



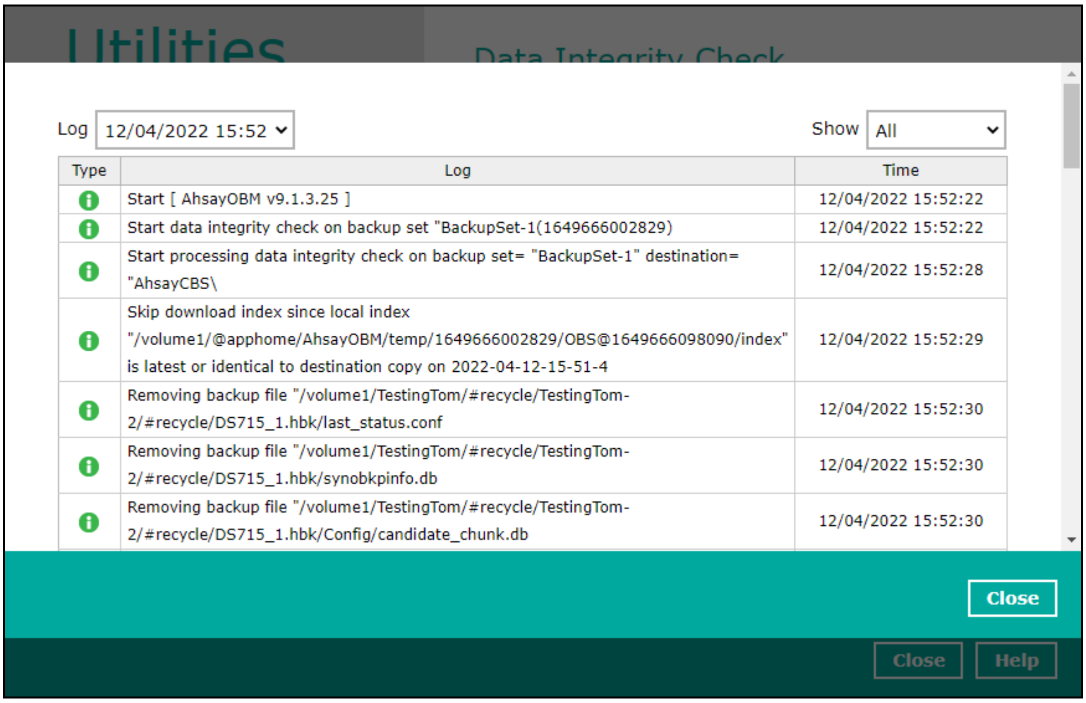
Log 04/11/2022 11:43

Show All

| Type | Log | Time |
|---|---|---|
| ℹ | Start [ AhsayOBM v9.4.9.0 ] | 04/11/2022 11:44:00 |
| ℹ | Start data integrity check on backup set "BackupSet-1(1667531800233) | 04/11/2022 11:44:00 |
| ℹ | Start processing data integrity check on backup set= "BackupSet-1" destination= "AhsayCBS\ | 04/11/2022 11:44:07 |
| ℹ | Create new index since no valid job available in destination | 04/11/2022 11:44:10 |
| ℹ | Skipped to run Data Integrity Check for backup set "BackupSet-1" in destination "AhsayCBS" because no data is in index | 04/11/2022 11:44:15 |
| ℹ | Deleting out of retention period recycled files... | 04/11/2022 11:44:15 |
| ℹ | Delete out of retention period recycled files result - Size: 0 | 04/11/2022 11:44:15 |
| ℹ | Deleting out of retention period recycled files... Completed | 04/11/2022 11:44:15 |
| ℹ | Saving encrypted backup file index to 1667531800233/blocks/2022-11-04-11-43-59 at destination AhsayCBS... | 04/11/2022 11:44:16 |
| ℹ | Data integrity check on backup set= "BackupSet-1" destination= "AhsayCBS" is complete | 04/11/2022 11:44:20 |
| ℹ | Finished data integrity check on backup set "BackupSet-1(1667531800233) | 04/11/2022 11:44:21 |
| ℹ | Completed data integrity check on backup set "BackupSet-1(1667531800233) | 04/11/2022 11:44:21 |

Logs per page 50

The screenshot below shows an example of a Data Integrity Check log when corrupted data has been detected. If any corrupted data is found, these corrupted files are automatically removed from the backup destination(s).



Log 12/04/2022 15:52

Show All

| Type | Log | Time |
|---|---|---|
| ℹ | Start [ AhsayOBM v9.1.3.25 ] | 12/04/2022 15:52:22 |
| ℹ | Start data integrity check on backup set "BackupSet-1(1649666002829) | 12/04/2022 15:52:22 |
| ℹ | Start processing data integrity check on backup set= "BackupSet-1" destination= "AhsayCBS\ | 12/04/2022 15:52:28 |
| ℹ | Skip download index since local index "/volume1/@apphome/AhsayOBM/temp/1649666002829/OBS@1649666098090/index" is latest or identical to destination copy on 2022-04-12-15-51-4 | 12/04/2022 15:52:29 |
| ℹ | Removing backup file "/volume1/TestingTom/#recycle/TestingTom-2/#recycle/DS715_1.hbk/last_status.conf | 12/04/2022 15:52:30 |
| ℹ | Removing backup file "/volume1/TestingTom/#recycle/TestingTom-2/#recycle/DS715_1.hbk/synobkpinfo.db | 12/04/2022 15:52:30 |
| ℹ | Removing backup file "/volume1/TestingTom/#recycle/TestingTom-2/#recycle/DS715_1.hbk/Config/candidate_chunk.db | 12/04/2022 15:52:30 |

**Test Mode confirmation**

The (TEST MODE) confirmation screen is not supported on Synology NAS.

When running a data integrity check on other platforms such as Windows, Mac, or Linux (GUI), a (TEST MODE) confirmation screen will prompt if either of the **criteria** below matches the backup data during the data integrity check process:

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

However, on Synology NAS, during the data integrity check job, corrective actions will be taken automatically if the DIC has detected the following:

- Index-related issues
- Broken data blocks
- Discrepancy against checksum file (when the Cyclic Redundancy Check is enabled)

This means that the DIC will automatically remove any corrupted file(s) from the backup destination(s), and will update storage statistics without requiring user confirmation.

Aside from viewing the DIC logs directly on the AhsayOBM client, they can be viewed on the file system of the AhsayOBM client machine. For AhsayOBM on Synology NAS, the DIC logs are located in the following directory:

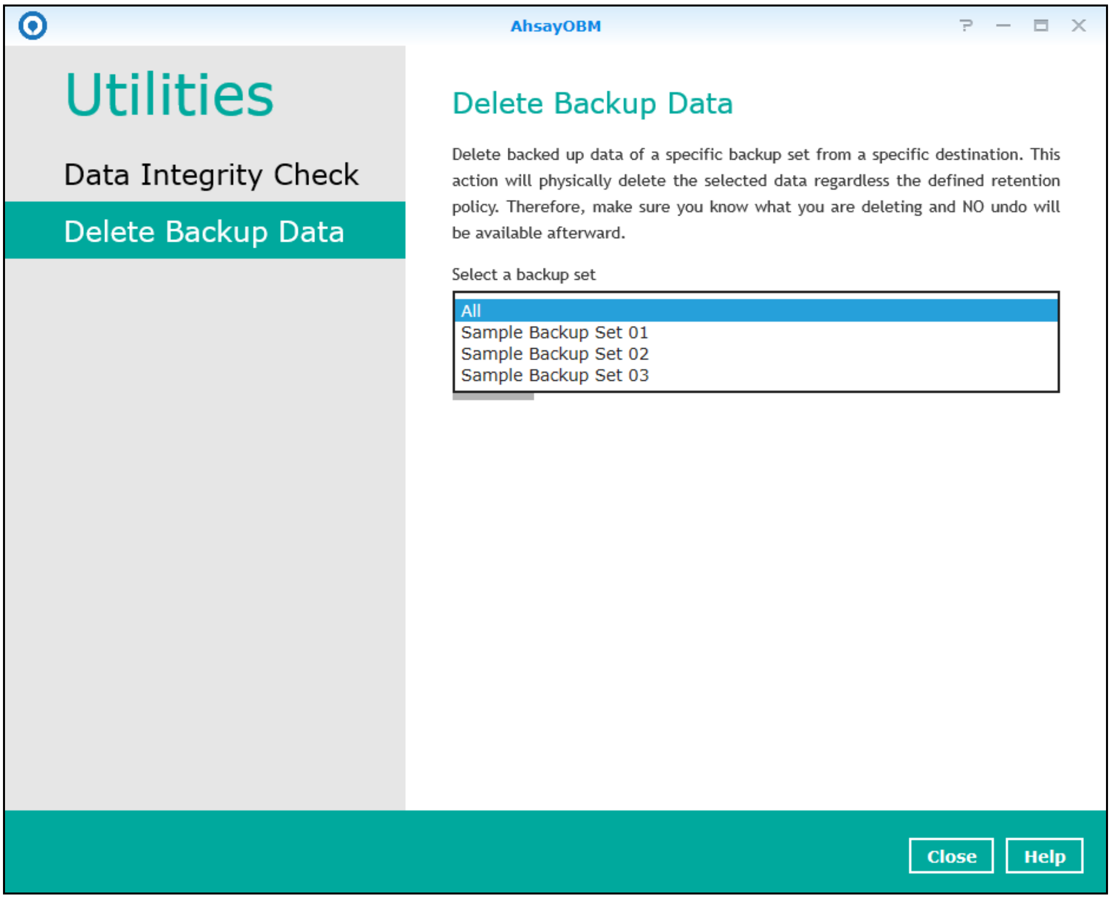
***/volume_id/@appstore/product_name/.obm/system/IntegrityCheck***

### 8.10.2 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.



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.

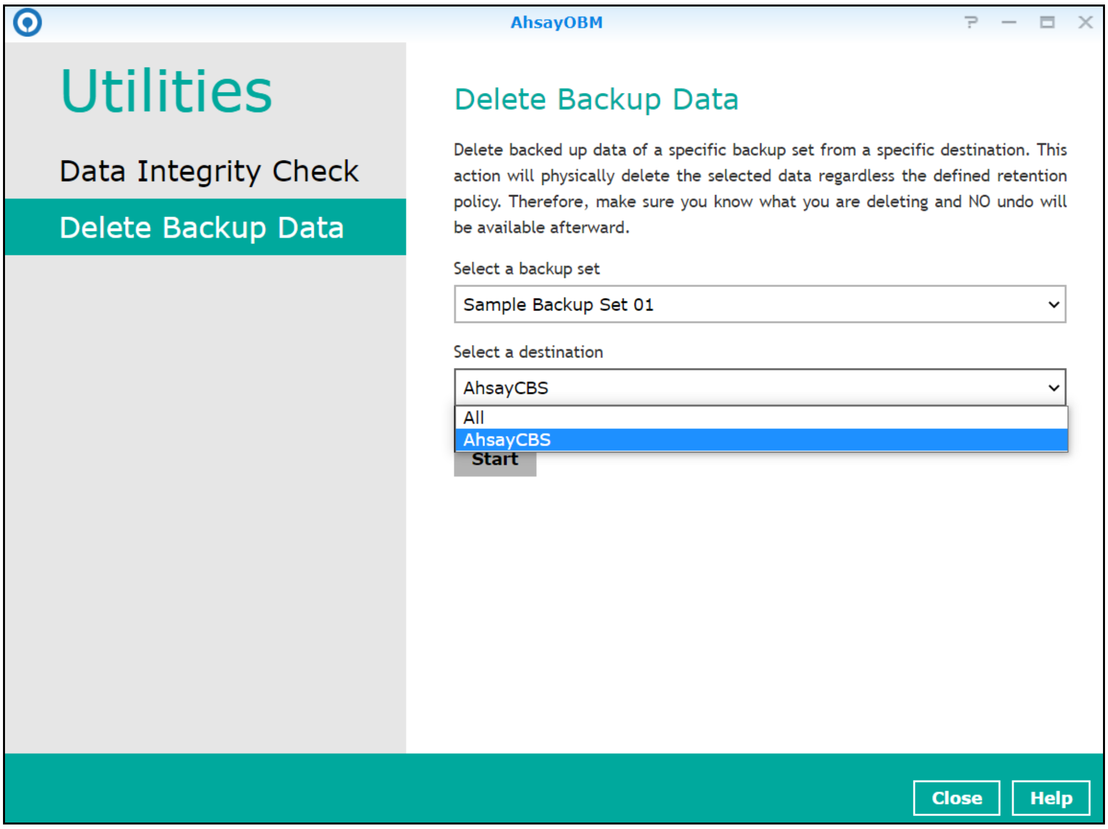
Select a backup set

- All
- Sample Backup Set 01
- Sample Backup Set 02
- Sample Backup Set 03

**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.



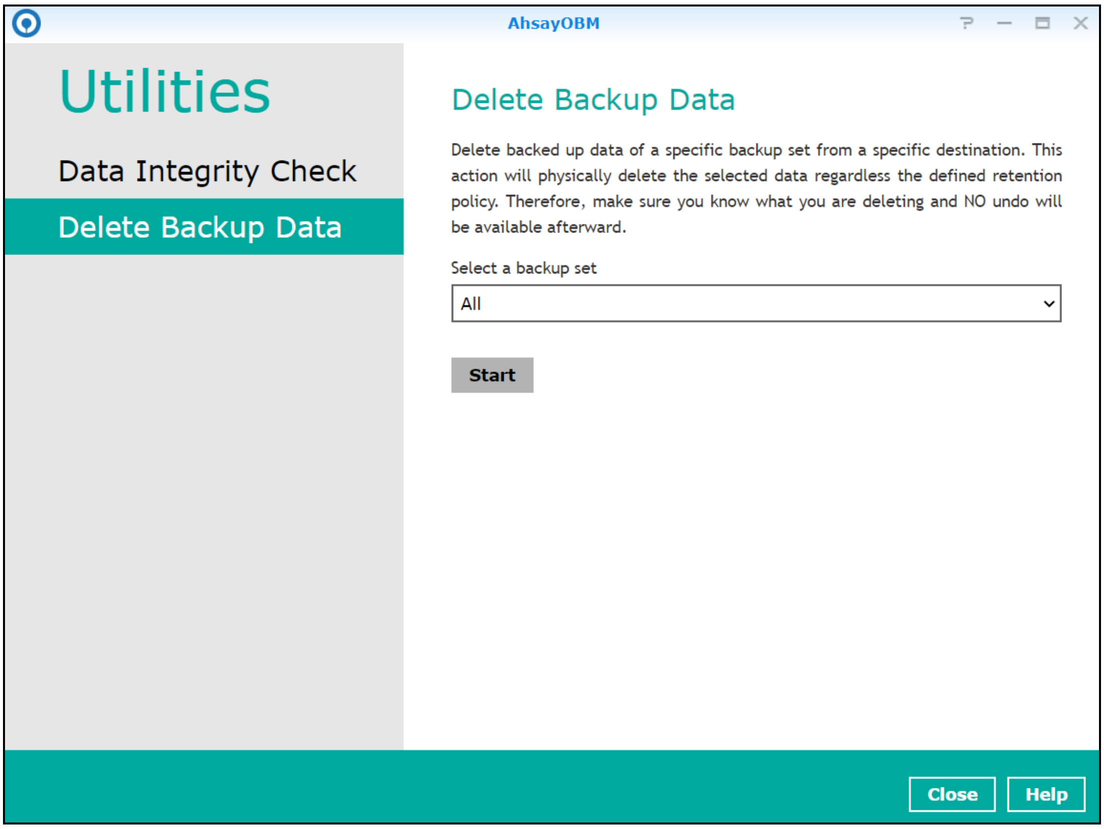
Delete Backup Data

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: AhsayCBS

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

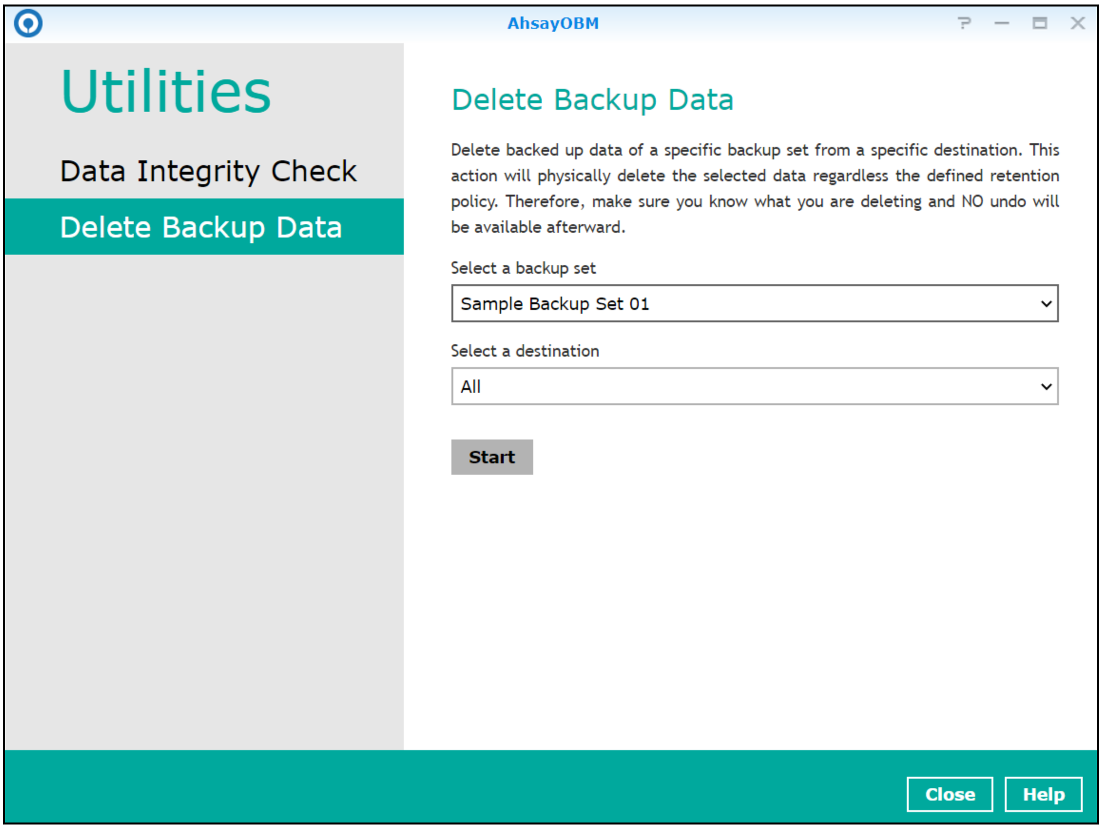


Delete Backup Data

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

2. Click the **Start** button, then click **Yes** to proceed. This process will delete backed up data on the selected backup set(s) and destination(s).

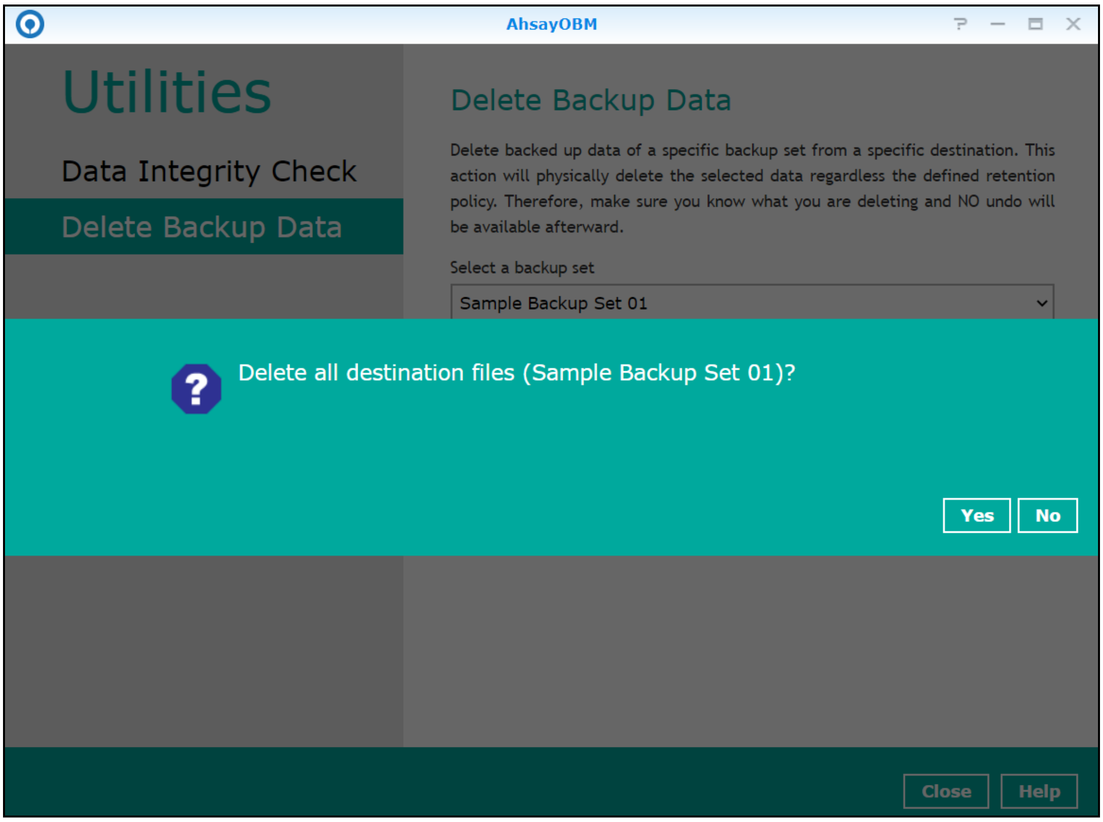


Delete Backup Data

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



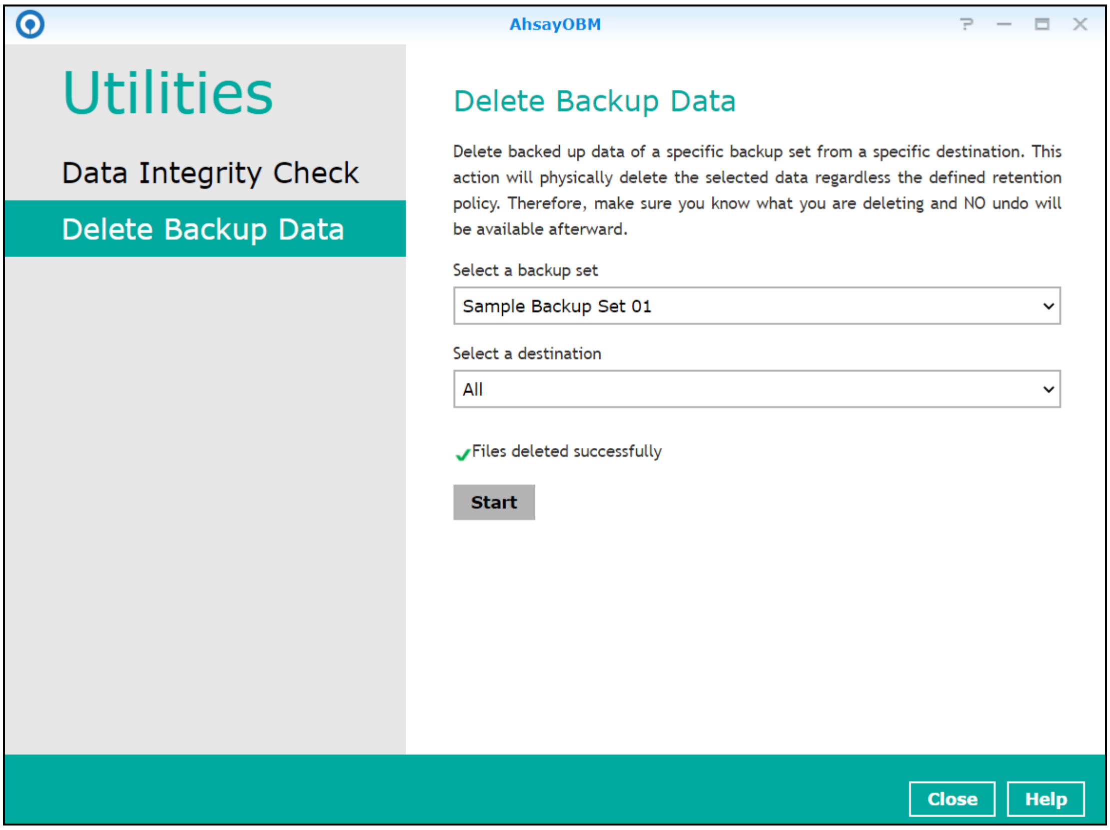
Delete Backup Data

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

Delete all destination files (Sample Backup Set 01)?

3. Files are successfully deleted.



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.

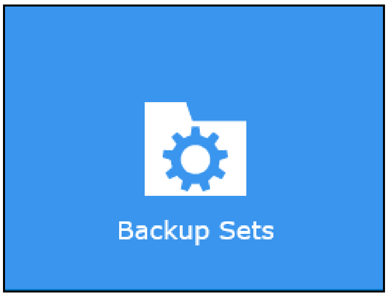
Select a backup set: Sample Backup Set 01

Select a destination: All

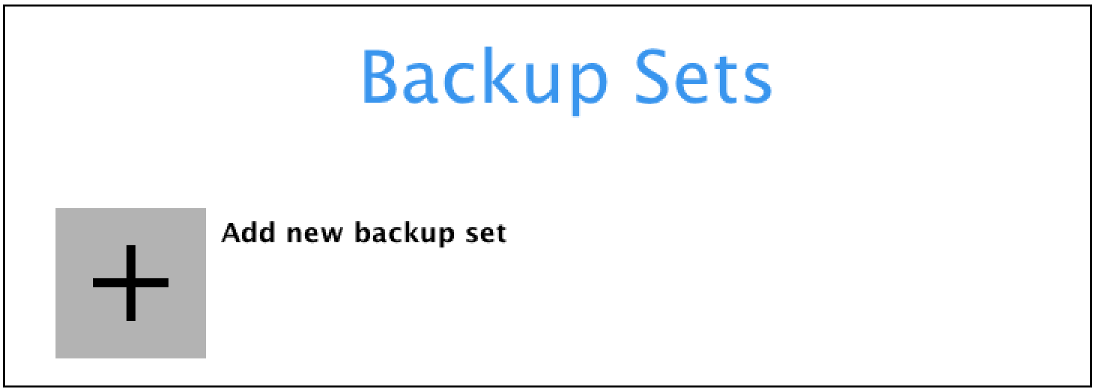
✓Files deleted successfully

# 9 Create a Backup Set

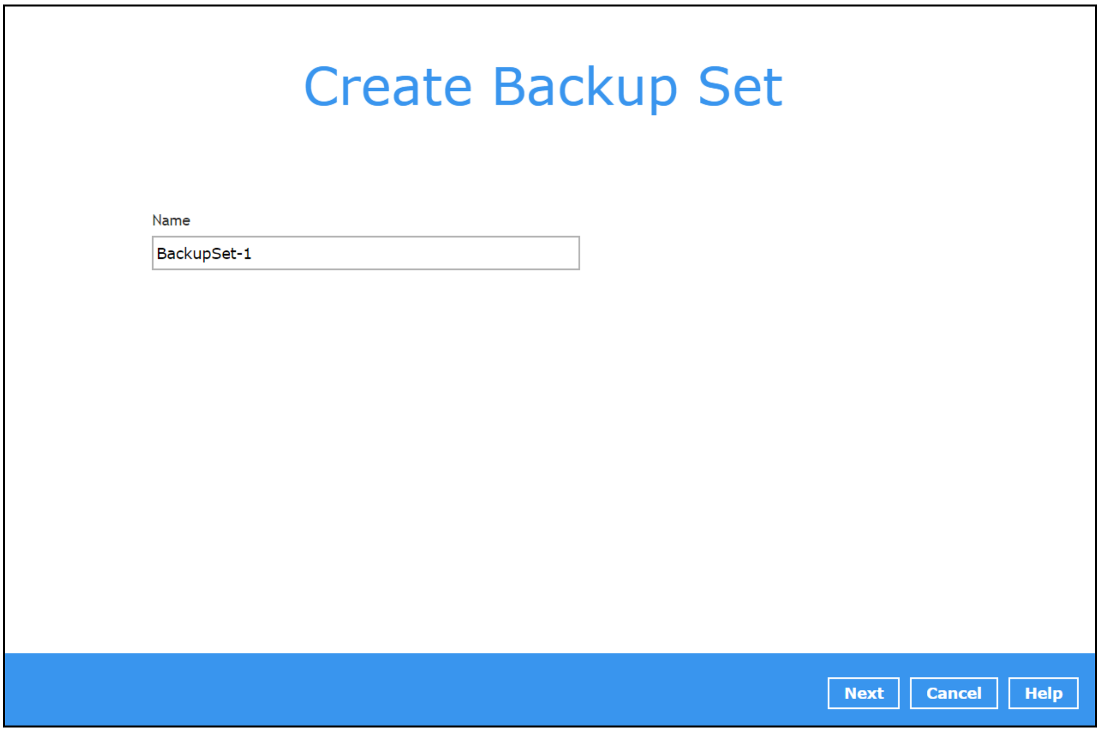
1. Click the **Backup Sets** icon on the main interface of AhsayOBM.



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



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

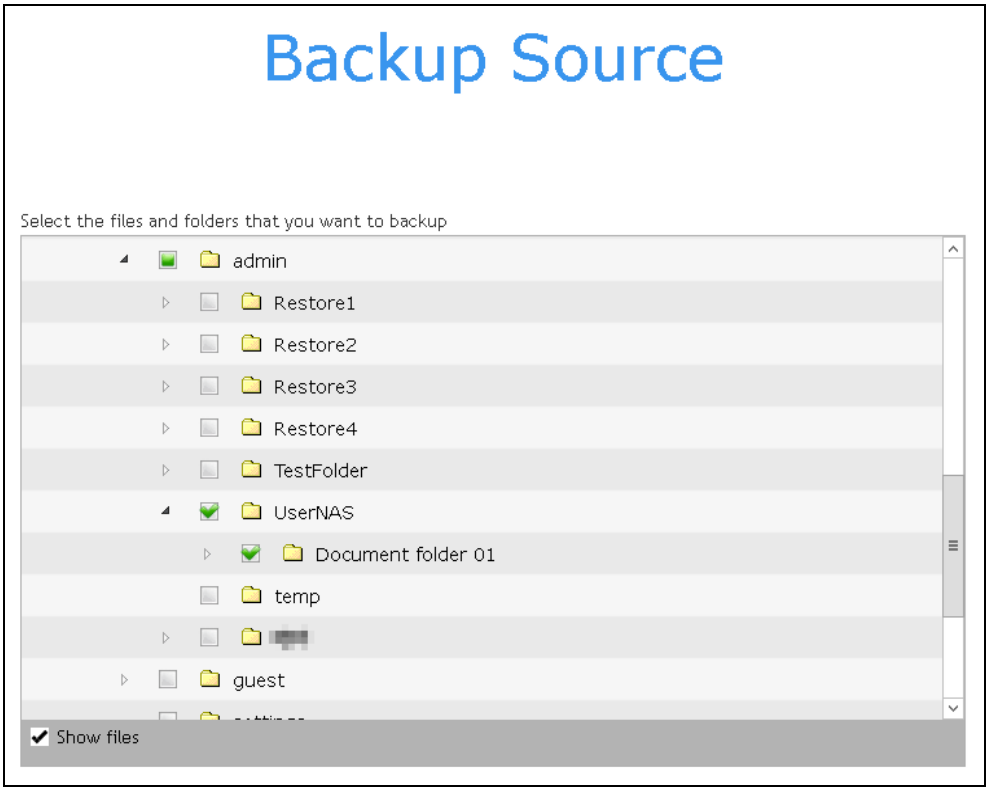


Create Backup Set

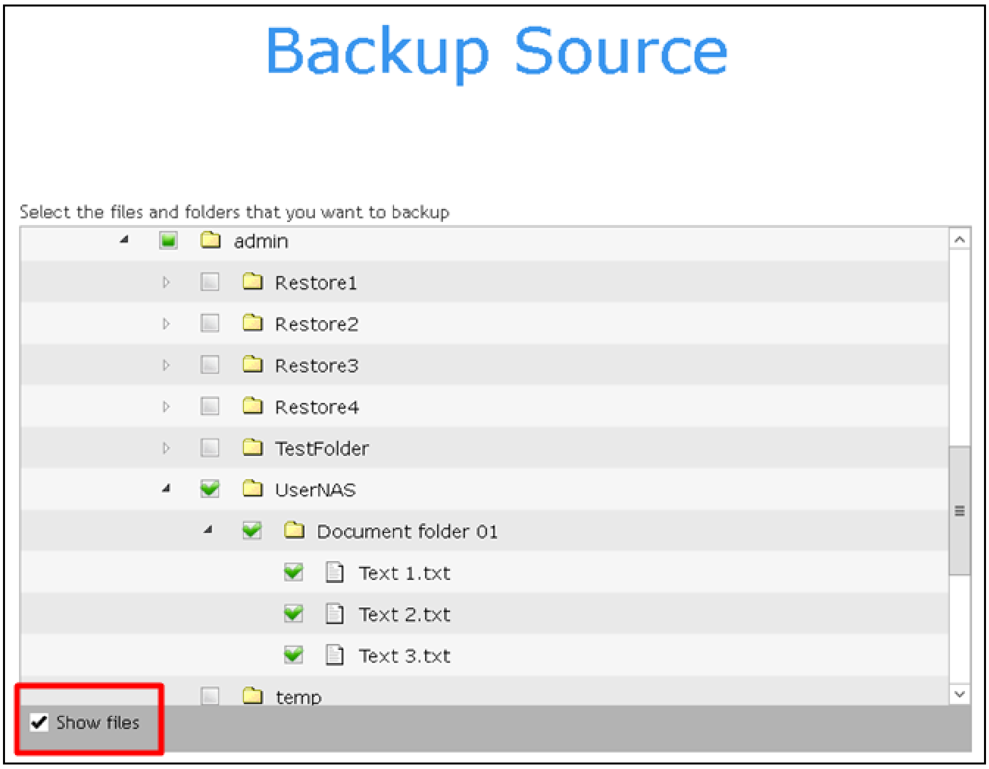
Name

BackupSet-1

4. In the Backup Source window, you can select the source files and/or folders for backup.



5. Click the **Show files** checkbox if you want to select individual file(s) for backup.



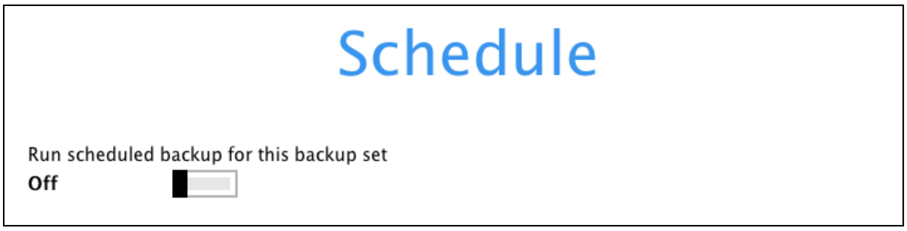
**NOTE**

AhsayOBM can only back up files or folders displayed under the File Station on the DiskStation Manager.

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

7. When the Schedule window appears, you can configure a backup schedule to automatically run a backup job at your specified time interval.

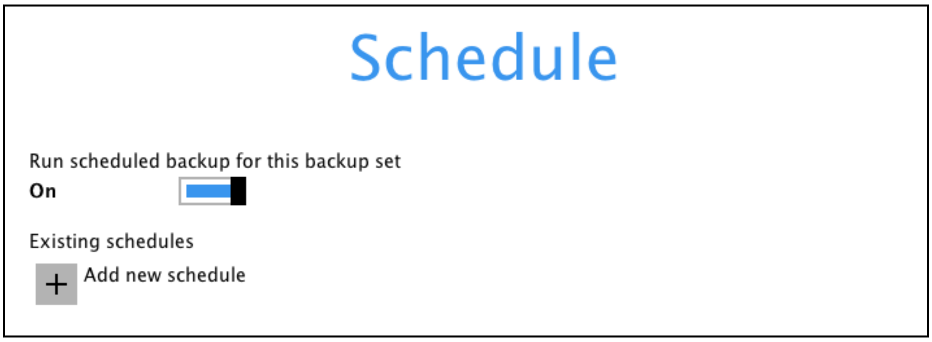
   - In the Schedule window, the Run scheduled backup for this backup set is **Off** by default. You can leave it as is if you want to add a schedule later.



Schedule

Run scheduled backup for this backup set
Off

If you want to add a schedule now, switch on **Run scheduled backup for this backup set**. Then, click "**+**" next to Add New schedule.

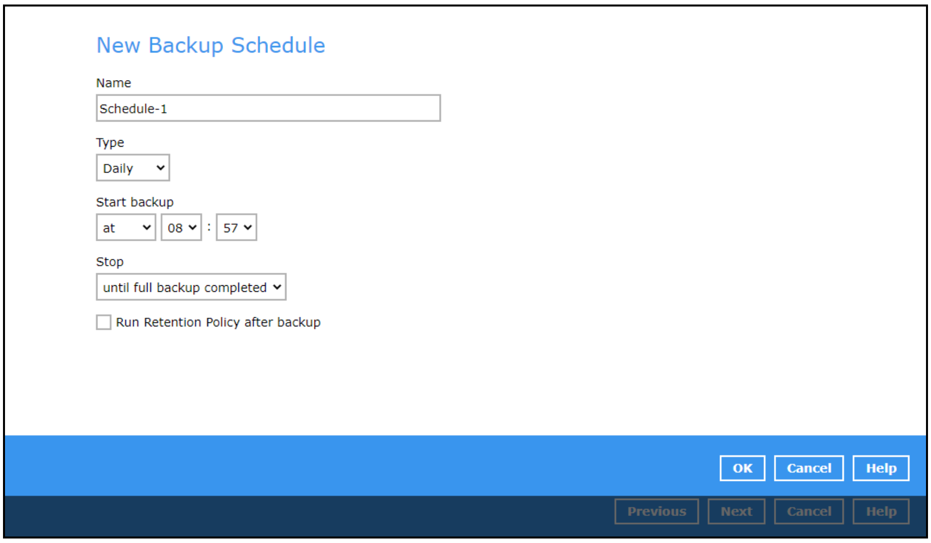


Schedule

Run scheduled backup for this backup set
On

Existing schedules

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



New Backup Schedule

Name: Schedule-1

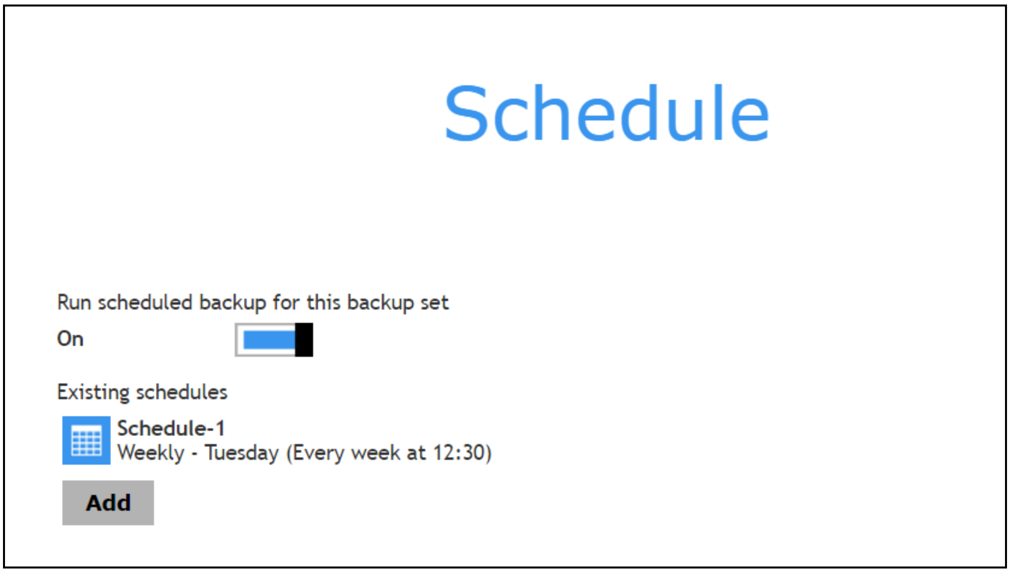
Type: Daily

Start backup: at 08 : 57

Stop: until full backup completed

□ Run Retention Policy after backup

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



Schedule

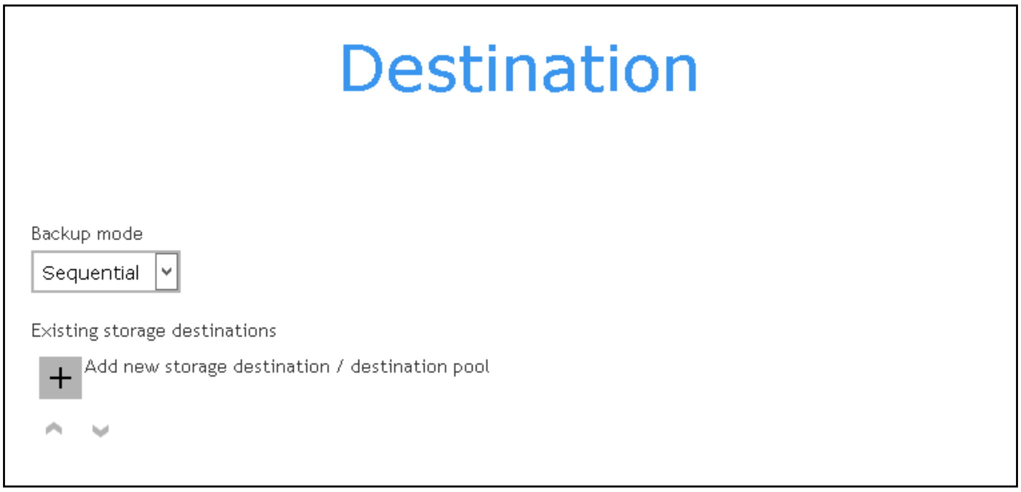
Run scheduled backup for this backup set

On

Existing schedules

Schedule-1
Weekly - Tuesday (Every week at 12:30)

9. Configure the backup destination.



Destination

Backup mode

Sequential

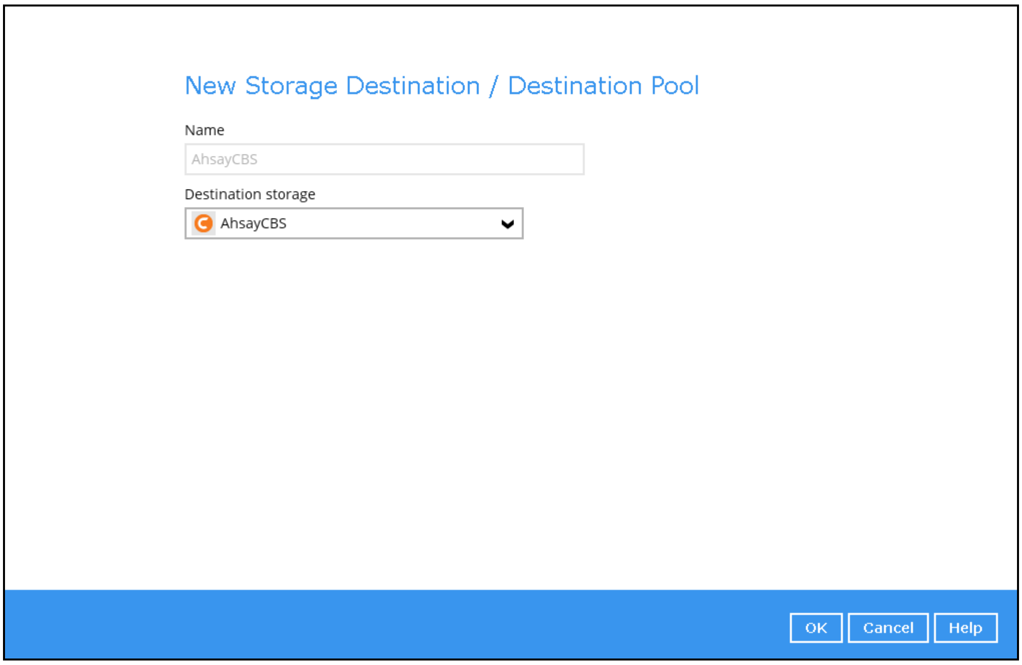
Existing storage destinations

Select the appropriate option from the **Backup mode** drop down menu.

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

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

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



New Storage Destination / Destination Pool

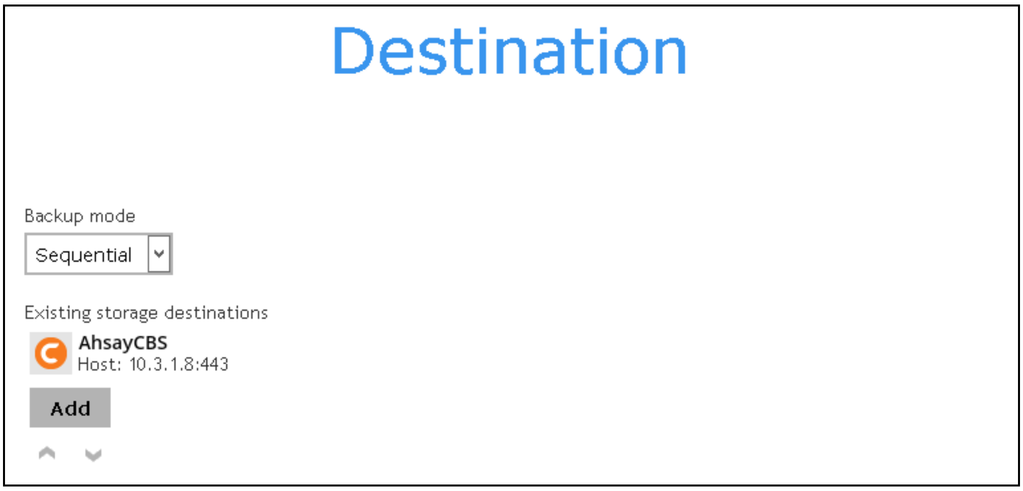
Name: AhsayCBS

Destination storage: AhsayCBS

**NOTE**

For more details on configuration of cloud storage as backup destination, refer to Appendix A: Cloud Storage as Backup Destination.

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



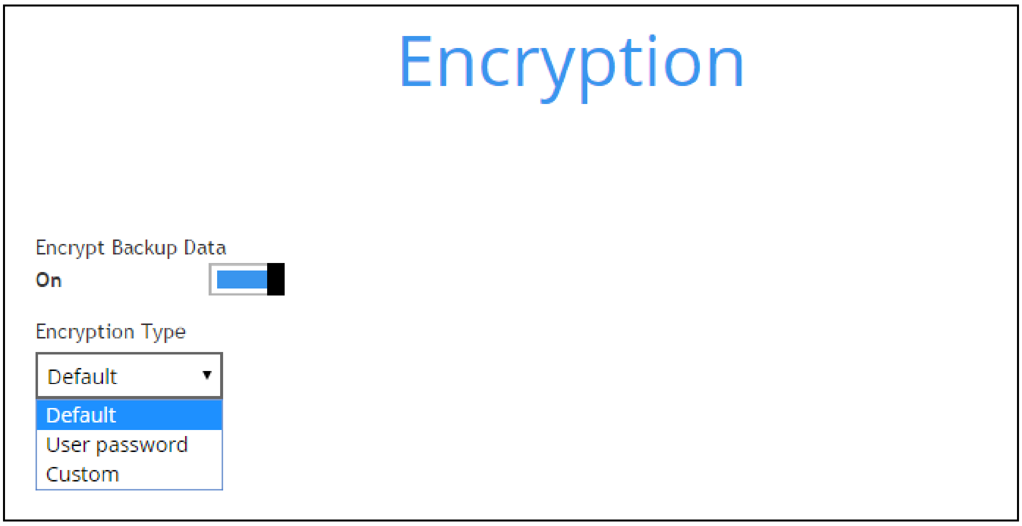
Destination

Backup mode: Sequential

Existing storage destinations

AhsayCBS
Host: 10.3.1.8:443

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



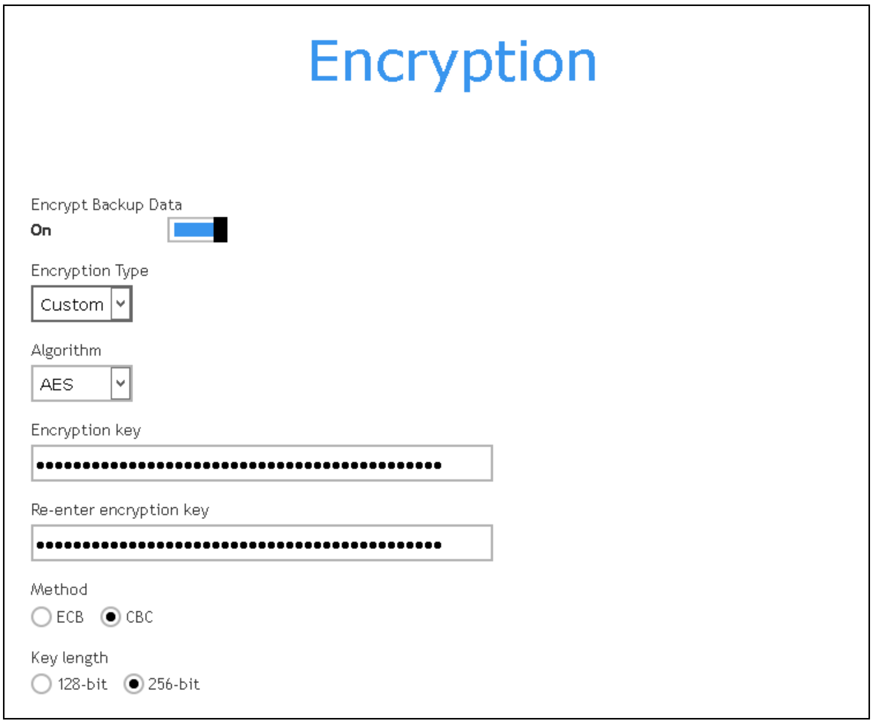
Encryption

Encrypt Backup Data
On

Encryption Type
Default

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

- **Default** – an encryption key with 44 alphanumeric characters will be randomly generated by the system.
- **User password** – the encryption key will be the same as the login password of your AhsayOBM at the time when this backup 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
••••••••••••••••••••••••••••••••••••••••••••

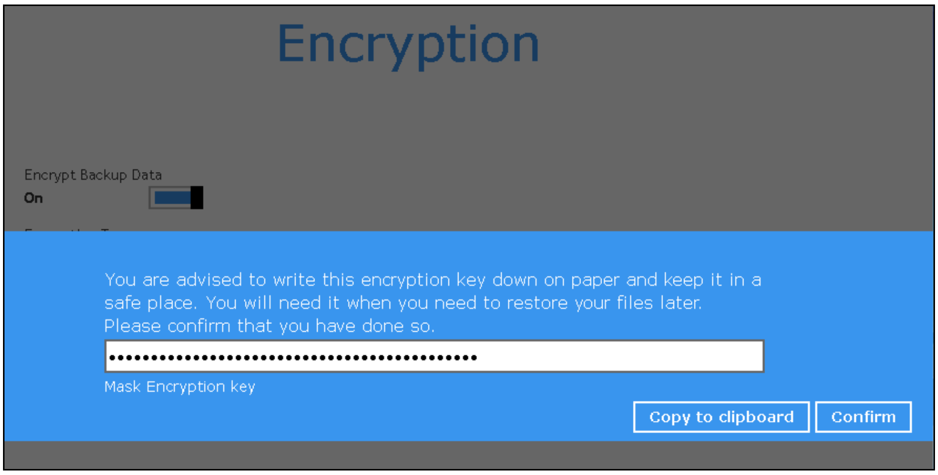
Method
○ ECB ● CBC

Key length
○ 128-bit ● 256-bit

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

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

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



Encryption

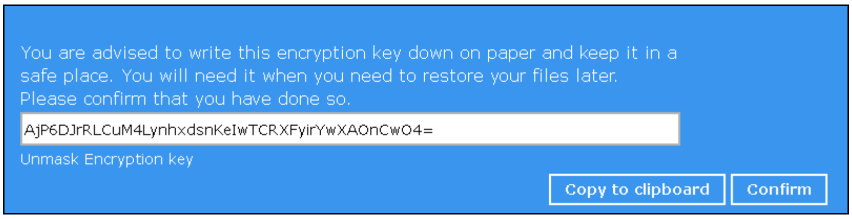
Encrypt Backup Data
On

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.

••••••••••••••••••••••••••••••••••••••••••••

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.



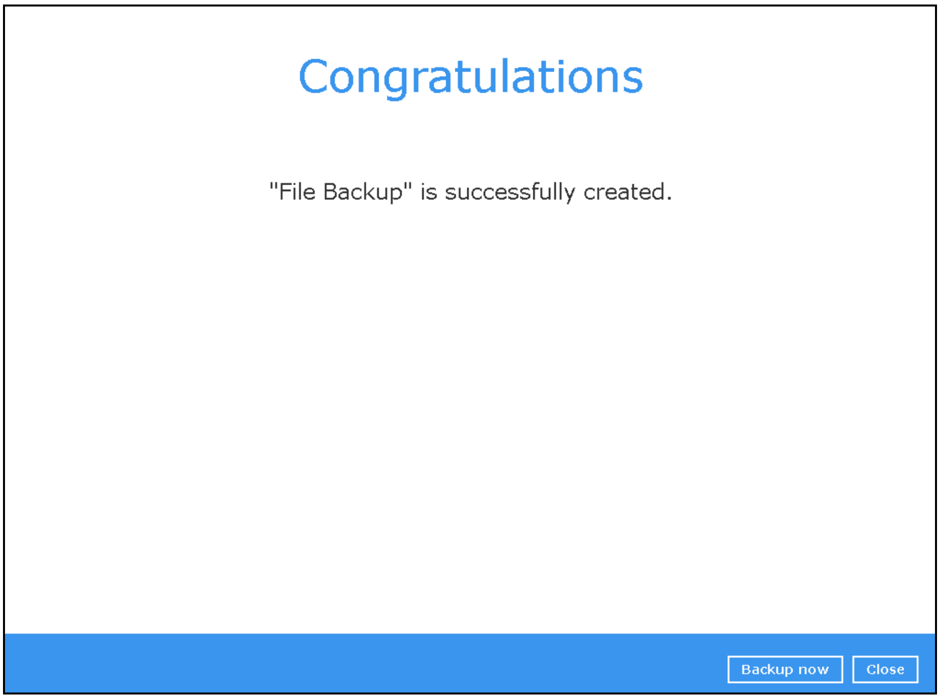
You are advised to write this encryption key down on paper and keep it in a safe place. You will need it when you need to restore your files later.
Please confirm that you have done so.

AjP6DJrRLCuM4LynhxdsnKeIwTCRXFyirYwXAOnCwO4=

- **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.

14. Upon successful creation of the backup set, the following screen will appear. You can click **Backup now** to back up your data or click **Close** to exit.

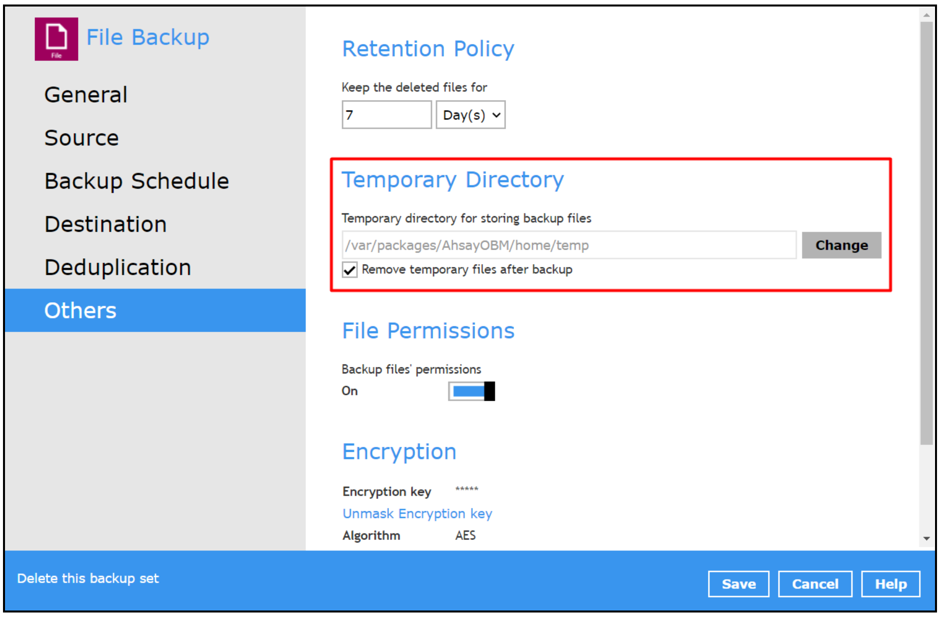


Congratulations

"File Backup" is successfully created.

15. 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.



Retention Policy

Keep the deleted files for 7 Day(s)

Temporary Directory

Temporary directory for storing backup files /var/packages/AhsayOBM/home/temp Change

☑ Remove temporary files after backup

File Permissions

Backup files' permissions On

Encryption

Encryption key *****

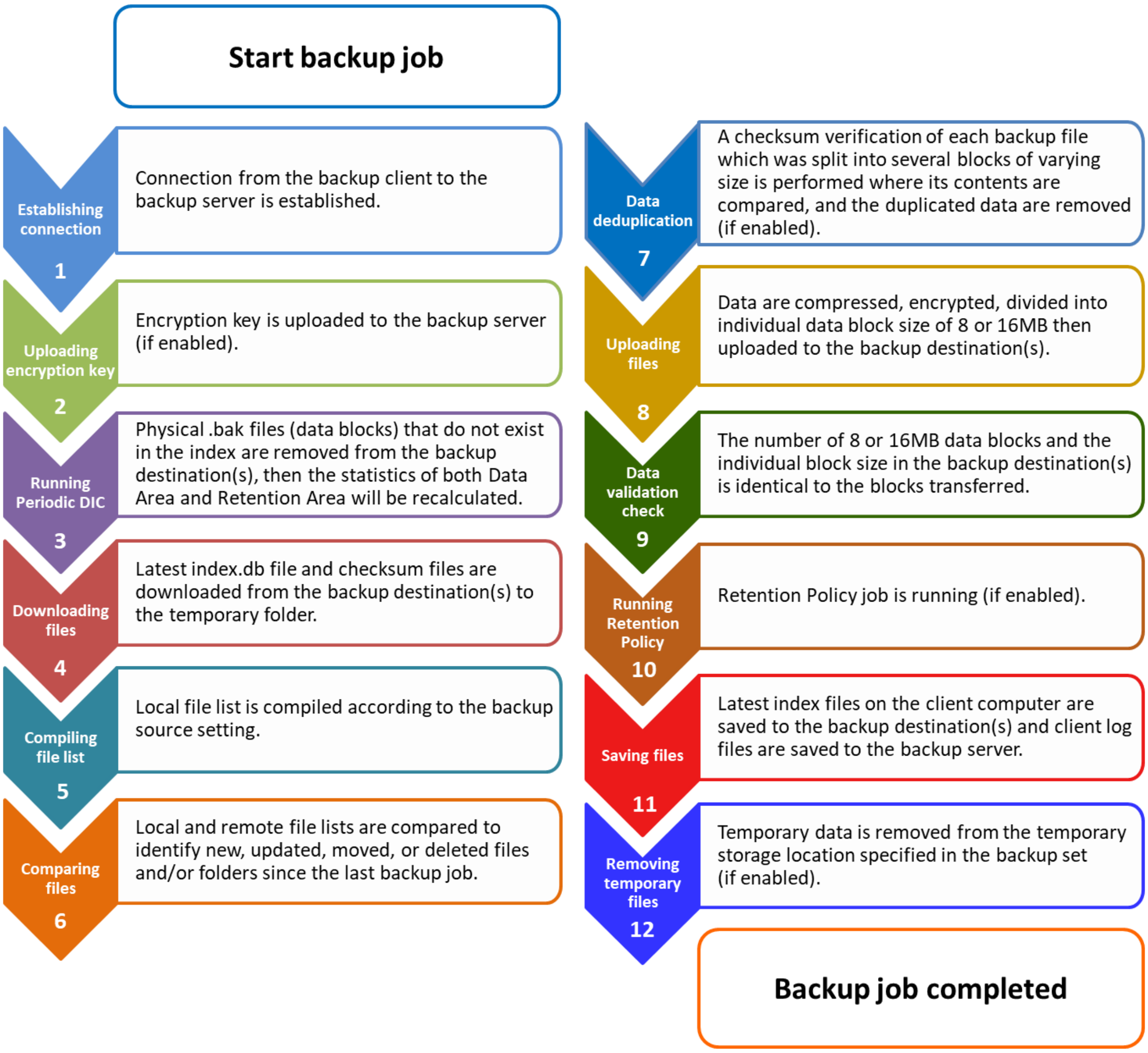
Unmask Encryption key

Algorithm AES

# 10 Overview on the Backup Process

The following steps are performed during a backup job. For an overview of the detailed process for Steps **3**, **4**, **9** and **11**, please refer to the following chapters.

- Periodic Data Integrity Check (PDIC) Process **(Step 3)**
- Backup Set Index Handling Process
  - Start Backup Job **(Step 4)**
  - Completed Backup Job **(Step 11)**
- Data Validation Check Process **(Step 9)**



Start backup job

1 Establishing connection: Connection from the backup client to the backup server is established.

2 Uploading encryption key: Encryption key is uploaded to the backup server (if enabled).

3 Running Periodic DIC: Physical .bak files (data blocks) that do not exist in the index are removed from the backup destination(s), then the statistics of both Data Area and Retention Area will be recalculated.

4 Downloading files: Latest index.db file and checksum files are downloaded from the backup destination(s) to the temporary folder.

5 Compiling file list: Local file list is compiled according to the backup source setting.

6 Comparing files: Local and remote file lists are compared to identify new, updated, moved, or deleted files and/or folders since the last backup job.

7 Data deduplication: A checksum verification of each backup file which was split into several blocks of varying size is performed where its contents are compared, and the duplicated data are removed (if enabled).

8 Uploading files: Data are compressed, encrypted, divided into individual data block size of 8 or 16MB then uploaded to the backup destination(s).

9 Data validation check: The number of 8 or 16MB data blocks and the individual block size in the backup destination(s) is identical to the blocks transferred.

10 Running Retention Policy: Retention Policy job is running (if enabled).

11 Saving files: Latest index files on the client computer are saved to the backup destination(s) and client log files are saved to the backup server.

12 Removing temporary files: Temporary data is removed from the temporary storage location specified in the backup set (if enabled).

Backup job completed

## 10.1 Periodic Data Integrity Check (PDIC) Process

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

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

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

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

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

**NOTE: The PDIC schedule cannot be changed.**

**Example:**

Backup set ID: 1594627447932

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

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

In this example:

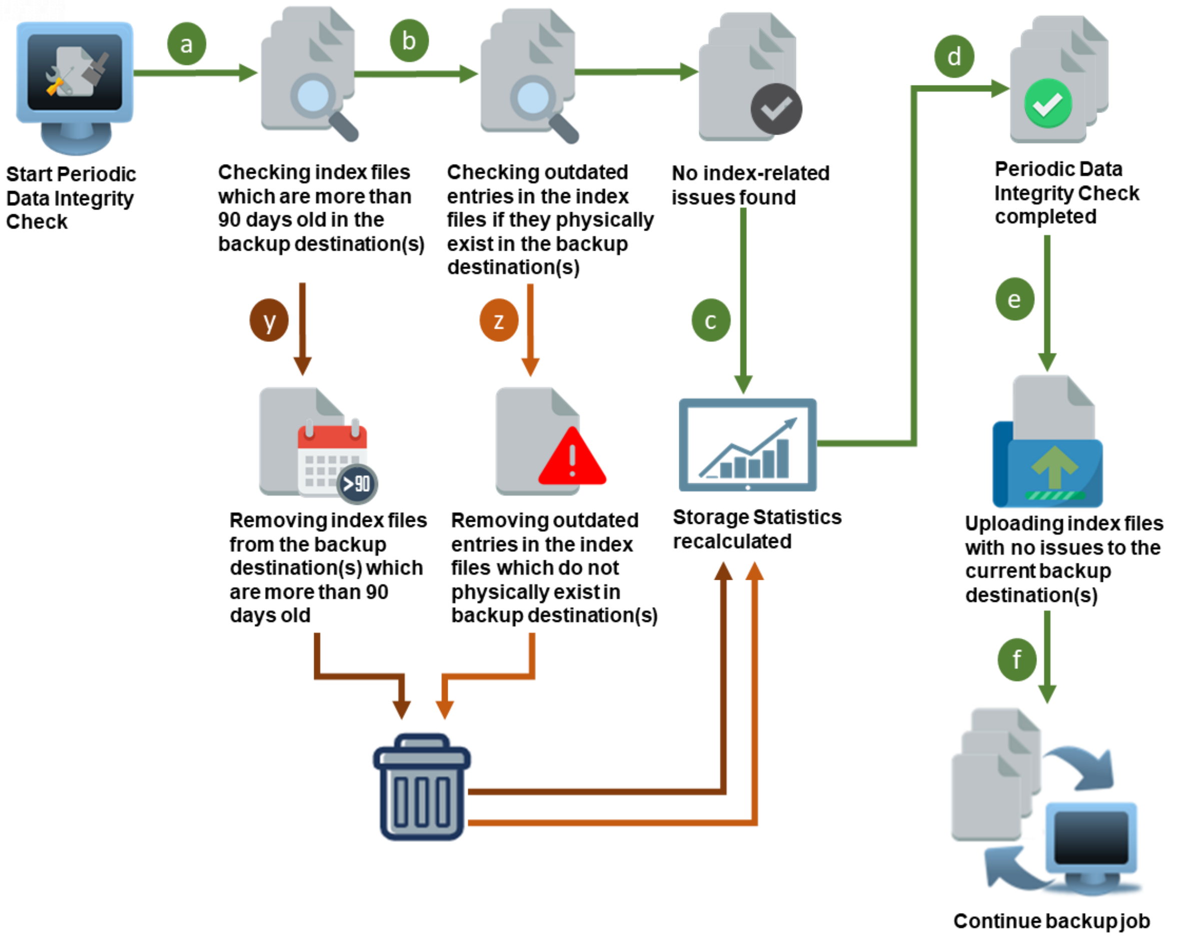
- the PDIC will run on the first backup job that falls on Wednesday; or
- if there is no active backup job(s) running from Monday to Friday, then the PDIC will run on the next available backup job.

**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.


Start Periodic Data Integrity Check
a
Checking index files which are more than 90 days old in the backup destination(s)
b
Checking outdated entries in the index files if they physically exist in the backup destination(s)
No index-related issues found
d
Periodic Data Integrity Check completed
y
z
c
e
Removing index files from the backup destination(s) which are more than 90 days old
Removing outdated entries in the index files which do not physically exist in backup destination(s)
Storage Statistics recalculated
Uploading index files with no issues to the current backup destination(s)
f
Continue backup job

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

➔ If **YES**, proceed to y

➔ If **NO**, proceed to b

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

➔ If **YES**, proceed to c

➔ If **NO**, proceed to z

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

d Periodic Data Integrity check is completed.

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

f The backup job process will continue.

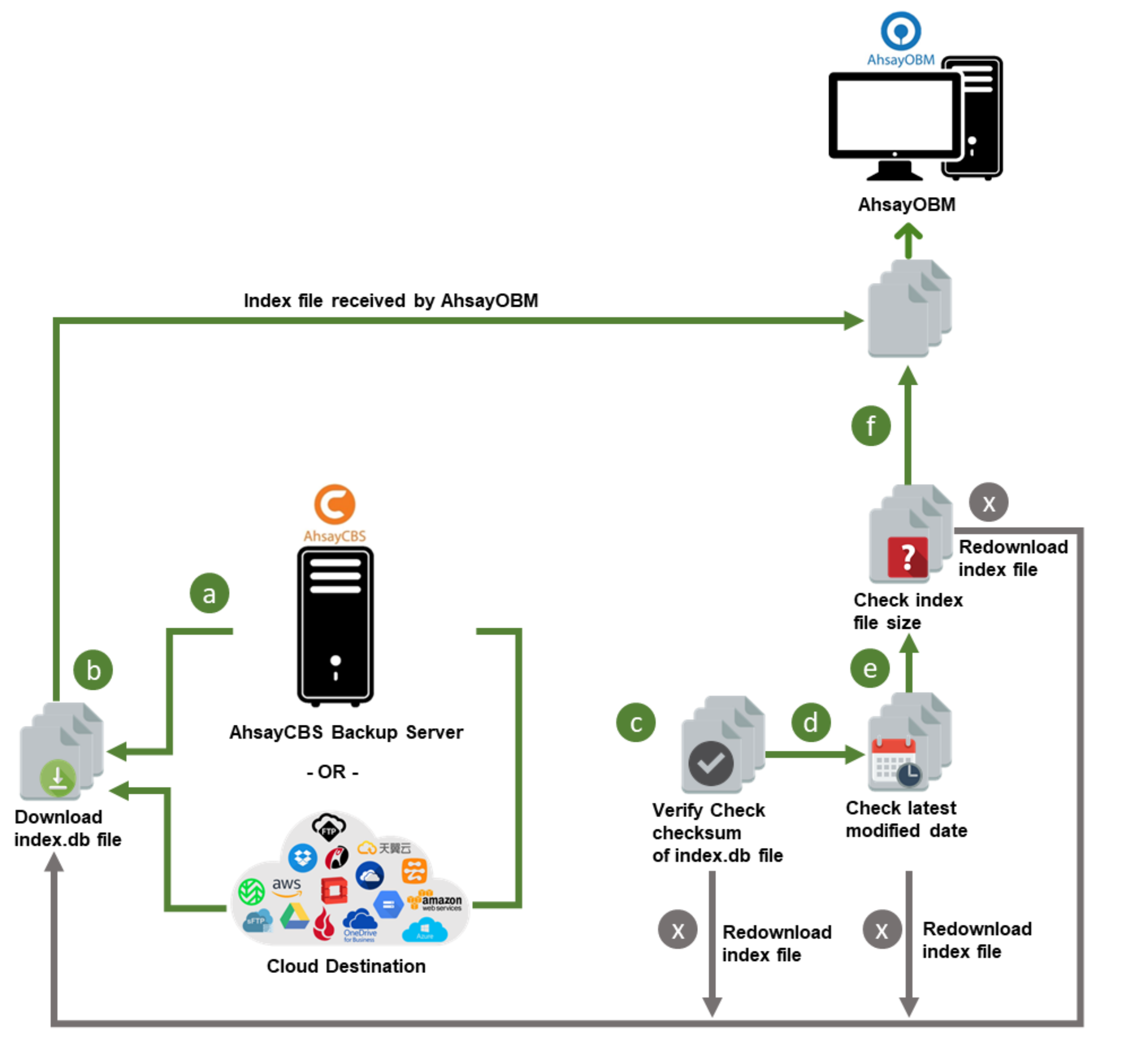
y Index files which are more than 90 days old will be removed from the backup destination(s).

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

## 10.2 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.

### 10.2.1 Start Backup Job



a Index file is retrieved from the current directory (i.e., AhsayCBS, Cloud Destination, FTP or SFTP).

b Index file will be downloaded.

c Verify Check checksum of index.db file.

- ➔ If checksum is correct, proceed to d
- ➔ If **NOT**, proceed to x

d Check modified date.

- ➔ If latest modified date is correct, proceed to e
- ➔ If **NOT**, proceed to x

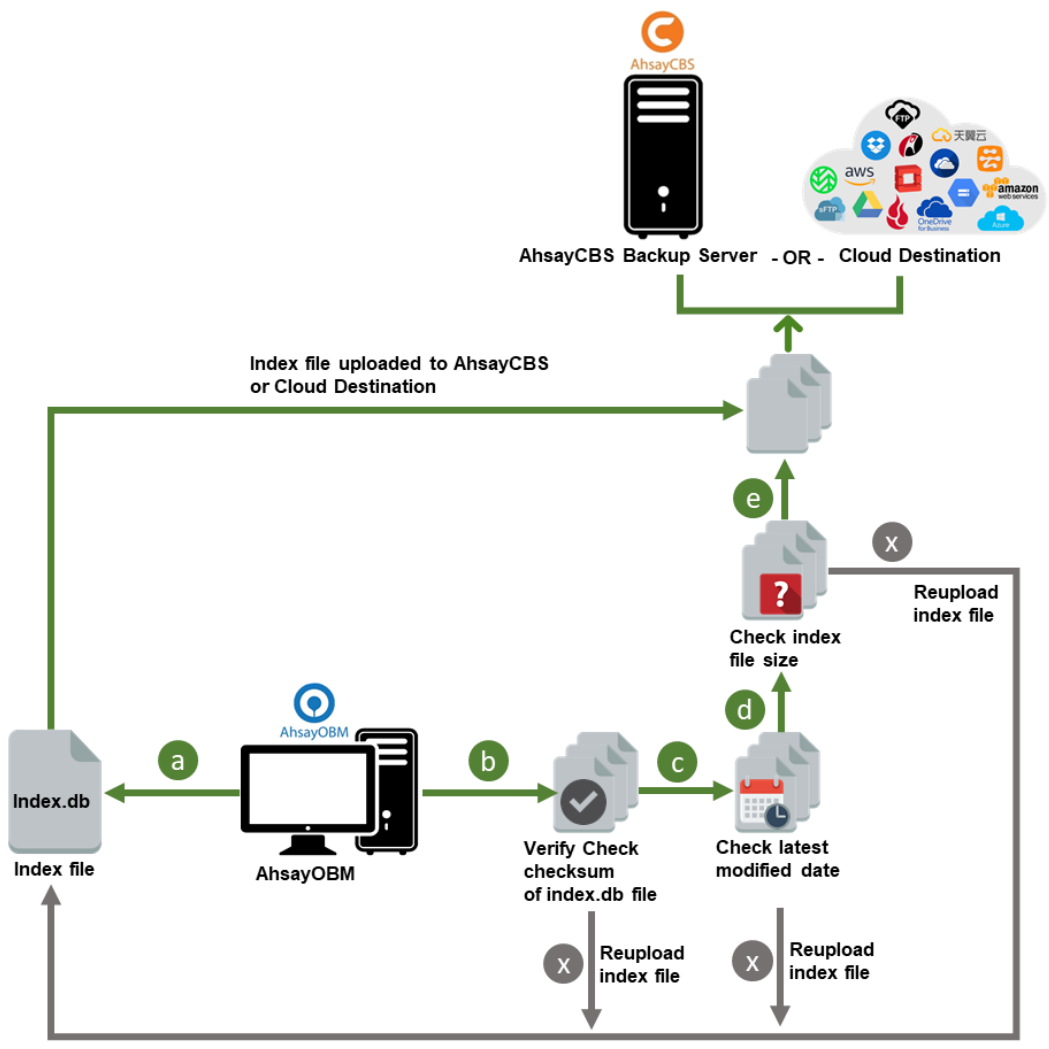
e Check index file size.

- ➔ If index file size is correct, proceed to f
- ➔ If **NOT**, proceed to x

f If index is valid, use the index.db file to compile file list for backup.

x Index file will be redownloaded. Proceed to b

### 10.2.2 Completed Backup Job



a Index file from AhsayOBM is uploaded to AhsayCBS, Cloud Destination, FTP or SFTP.

b Verify Check checksum of index.db file.

- ➔ If checksum is correct, proceed to c
- ➔ If **NOT**, proceed to x

c Check modified date.

- ➔ If latest modified date is correct, proceed to d
- ➔ If **NOT**, proceed to x

d Check index file size.

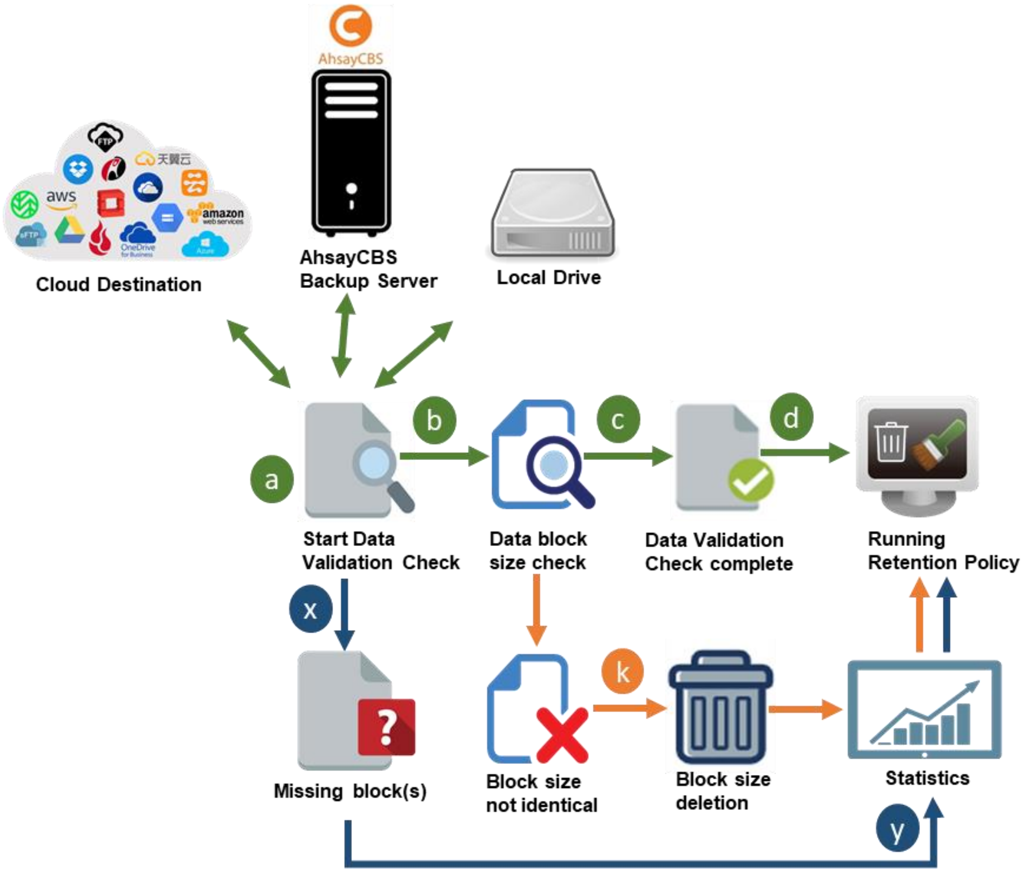
- ➔ If index file size is correct, proceed to e
- ➔ If **NOT**, proceed to x

e Index file is uploaded correctly to AhsayCBS or Cloud Destination.

x Index file will be reuploaded. Proceed to a

## 10.3 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 8 or 16MB data block files and the size of each block file are checked again after the files are transferred.



a Check the number of 8 or 16MB data blocks in the backup destination(s) is identical to the number of blocks transferred.

- → If YES, proceed to b
- → If NO, proceed to x

b Check the individual sizes of each data block in the backup destination(s) is identical to the sizes of each block transferred.

- → If YES, proceed to c
- → If NO, proceed to k

c Data validation check is complete.

d Retention Policy will run (if enabled).

x Files in the missing block(s) will be removed from the index.db file.

y Statistics will be updated according to the files removed.

Proceed to d

k Block size that are not identical will be removed from the backup destination(s).

Proceed to y then

Proceed to d

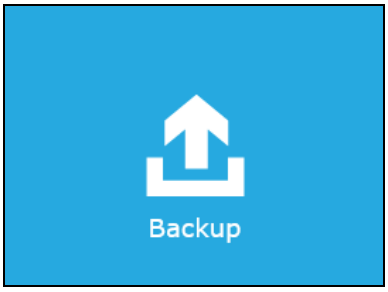
# 11 Run Backup Jobs

## 11.1 Login to AhsayOBM

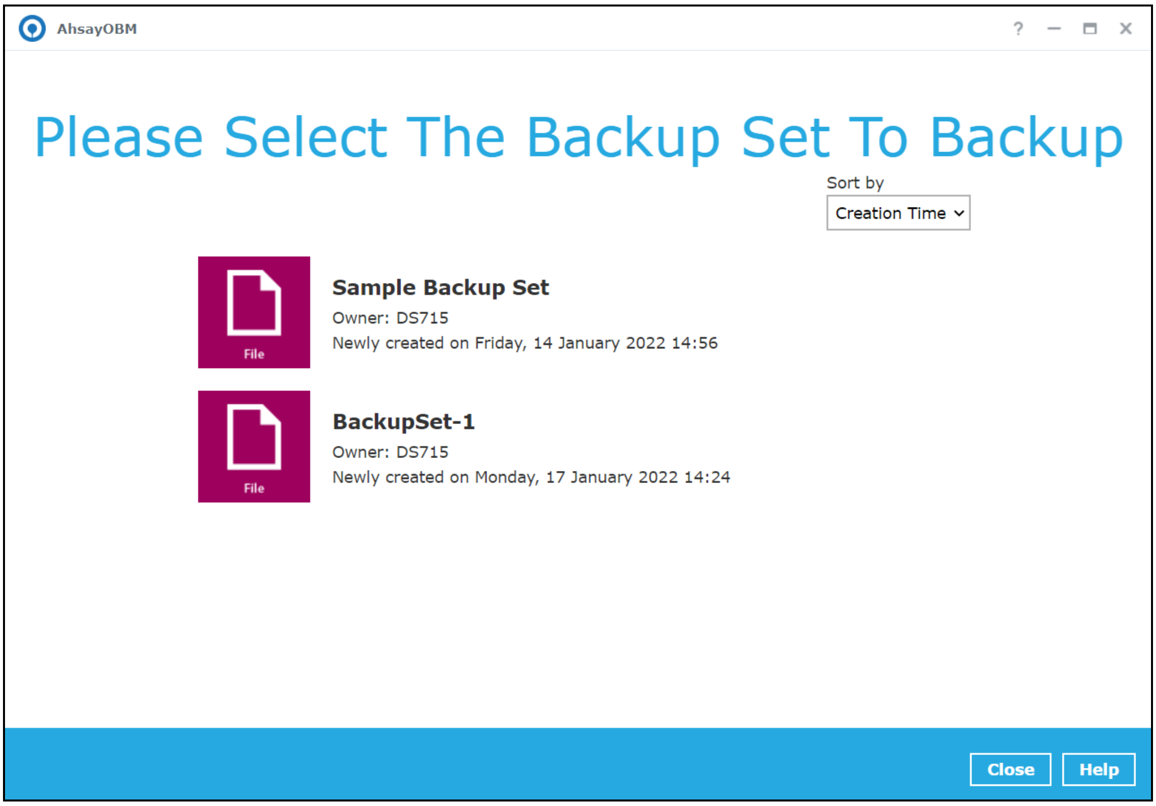
Login to the AhsayOBM application according to the instructions provided in Chapter 6.2 Login to AhsayOBM.

## 11.2 Start a Manual Backup

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



2. Select the backup set that you would like to start a backup job with.



AhsayOBM

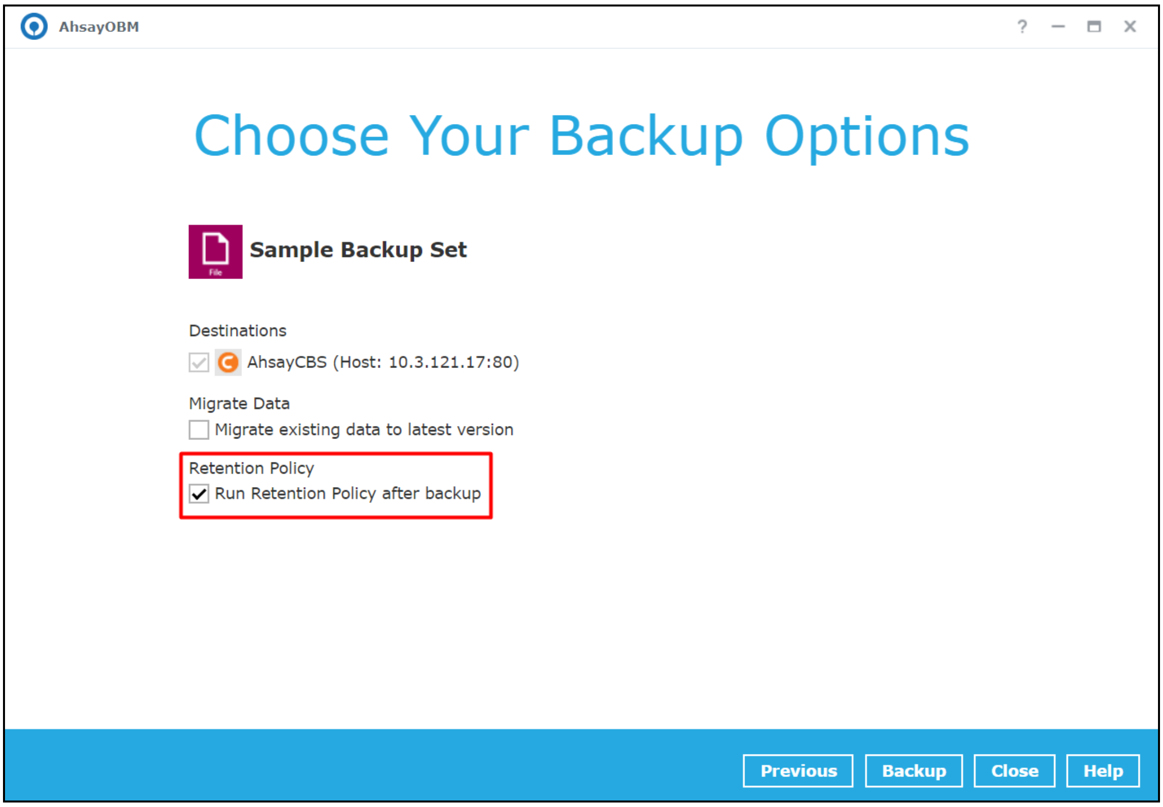
Please Select The Backup Set To Backup

Sort by: Creation Time

**Sample Backup Set**
Owner: DS715
Newly created on Friday, 14 January 2022 14:56

**BackupSet-1**
Owner: DS715
Newly created on Monday, 17 January 2022 14:24

3. When the following screen is displayed, it is recommended to enable the **Run Retention Policy after backup**. This will help you save hard disk quota in the long run.

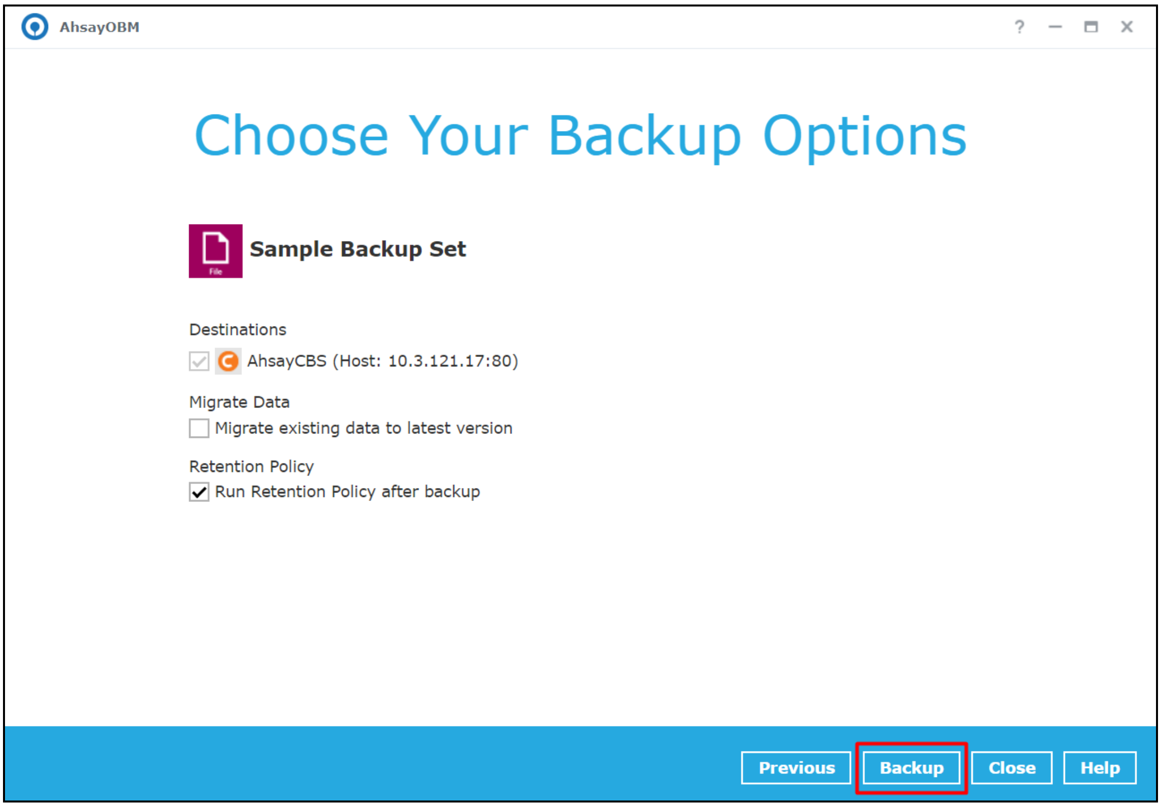


AhsayOBM
Choose Your Backup Options
Sample Backup Set
Destinations
☑ AhsayCBS (Host: 10.3.121.17:80)
Migrate Data
□ Migrate existing data to latest version
Retention Policy
☑ Run Retention Policy after backup
Previous
Backup
Close
Help

**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.

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



Choose Your Backup Options

Sample Backup Set

Destinations

☑ AhsayCBS (Host: 10.3.121.17:80)

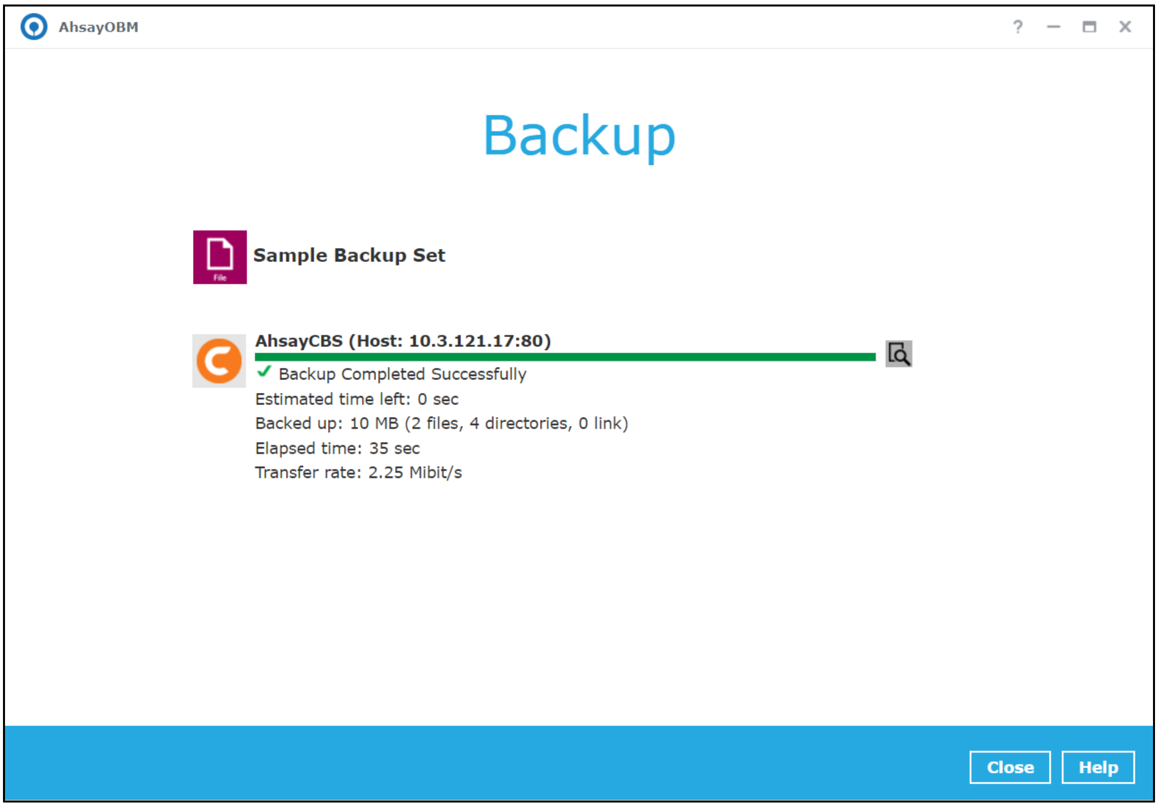
Migrate Data

□ Migrate existing data to latest version

Retention Policy

☑ Run Retention Policy after backup

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



Backup

Sample Backup Set

AhsayCBS (Host: 10.3.121.17:80)

✓ Backup Completed Successfully

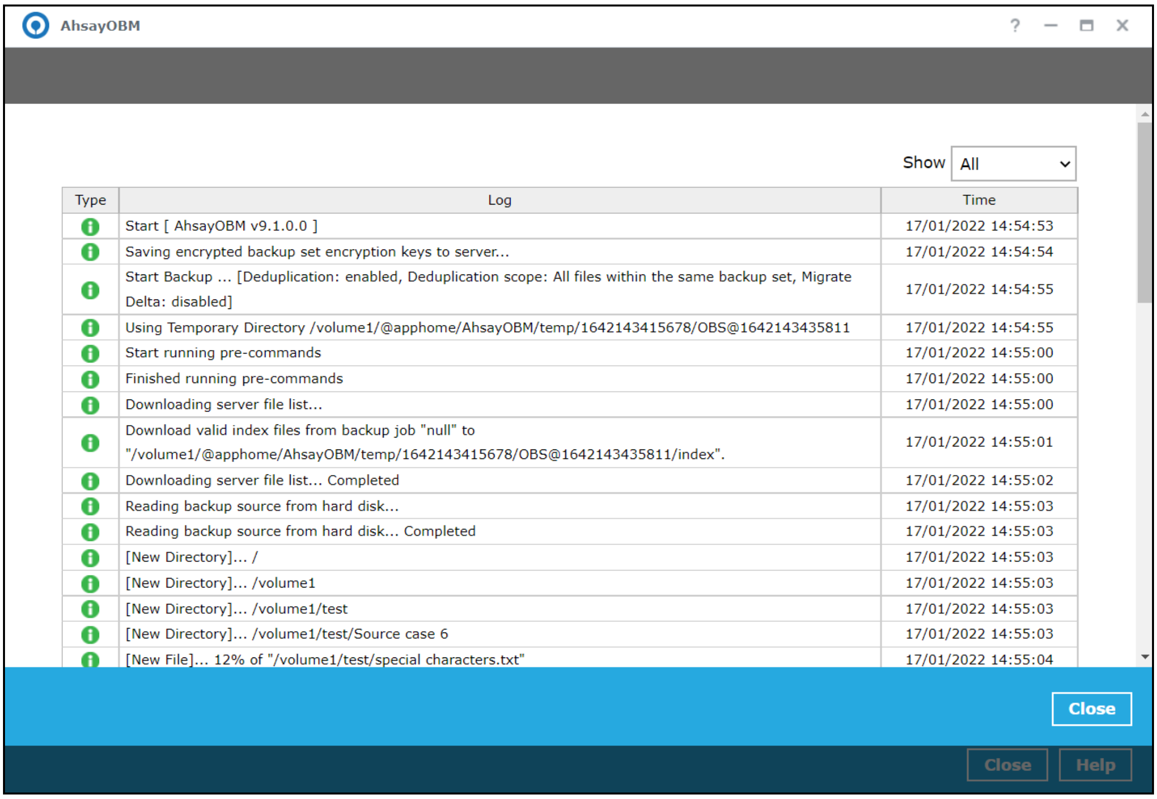
Estimated time left: 0 sec

Backed up: 10 MB (2 files, 4 directories, 0 link)

Elapsed time: 35 sec

Transfer rate: 2.25 Mibit/s

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



Show All

| Type | Log | Time |
|---|---|---|
| ℹ | Start [ AhsayOBM v9.1.0.0 ] | 17/01/2022 14:54:53 |
| ℹ | Saving encrypted backup set encryption keys to server... | 17/01/2022 14:54:54 |
| ℹ | Start Backup ... [Deduplication: enabled, Deduplication scope: All files within the same backup set, Migrate Delta: disabled] | 17/01/2022 14:54:55 |
| ℹ | Using Temporary Directory /volume1/@apphome/AhsayOBM/temp/1642143415678/OBS@1642143435811 | 17/01/2022 14:54:55 |
| ℹ | Start running pre-commands | 17/01/2022 14:55:00 |
| ℹ | Finished running pre-commands | 17/01/2022 14:55:00 |
| ℹ | Downloading server file list... | 17/01/2022 14:55:00 |
| ℹ | Download valid index files from backup job "null" to "/volume1/@apphome/AhsayOBM/temp/1642143415678/OBS@1642143435811/index". | 17/01/2022 14:55:01 |
| ℹ | Downloading server file list... Completed | 17/01/2022 14:55:02 |
| ℹ | Reading backup source from hard disk... | 17/01/2022 14:55:03 |
| ℹ | Reading backup source from hard disk... Completed | 17/01/2022 14:55:03 |
| ℹ | [New Directory]... / | 17/01/2022 14:55:03 |
| ℹ | [New Directory]... /volume1 | 17/01/2022 14:55:03 |
| ℹ | [New Directory]... /volume1/test | 17/01/2022 14:55:03 |
| ℹ | [New Directory]... /volume1/test/Source case 6 | 17/01/2022 14:55:03 |
| ℹ | [New File]... 12% of "/volume1/test/special characters.txt" | 17/01/2022 14:55:04 |

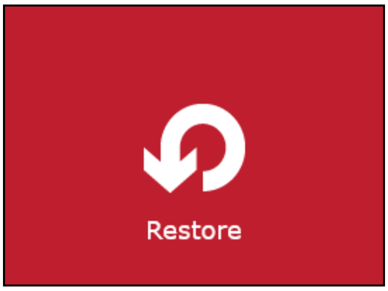
# 12 Restore Data

## 12.1 Login to AhsayOBM

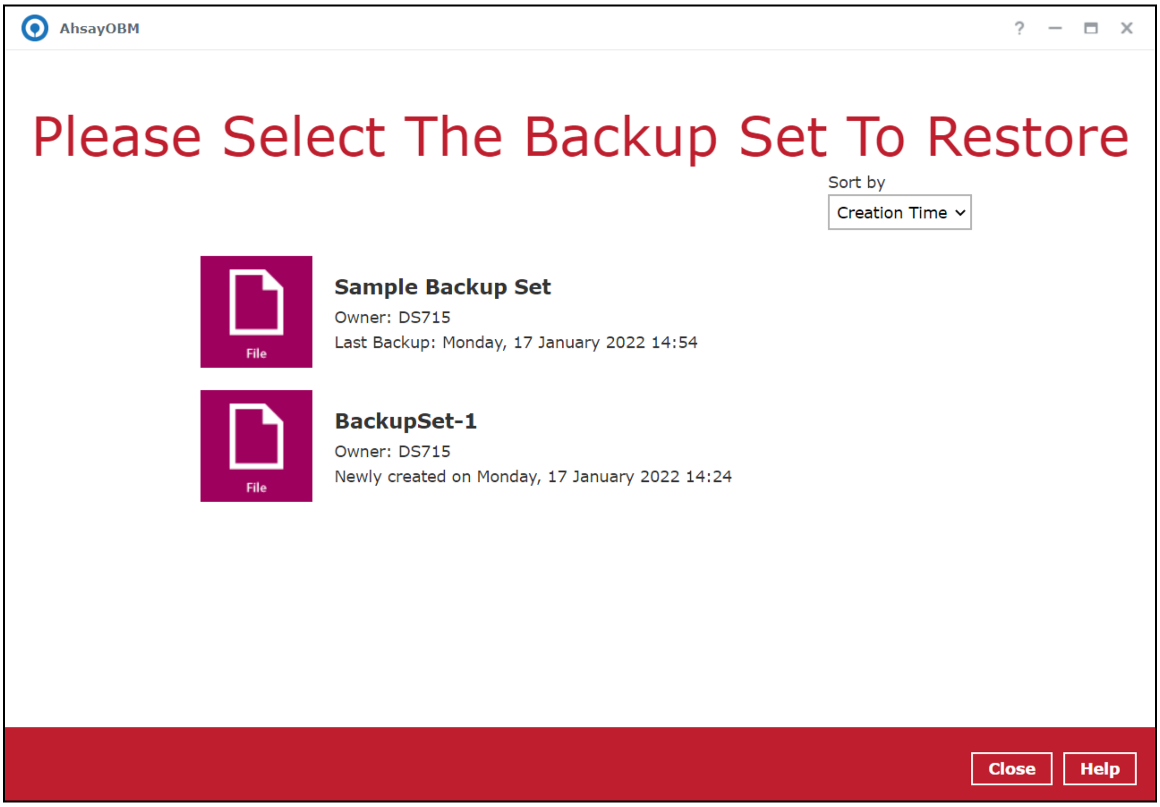
Login to the AhsayOBM application according to the instructions provided in Chapter 6.2 Login to AhsayOBM.

## 12.2 Restore Data

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



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



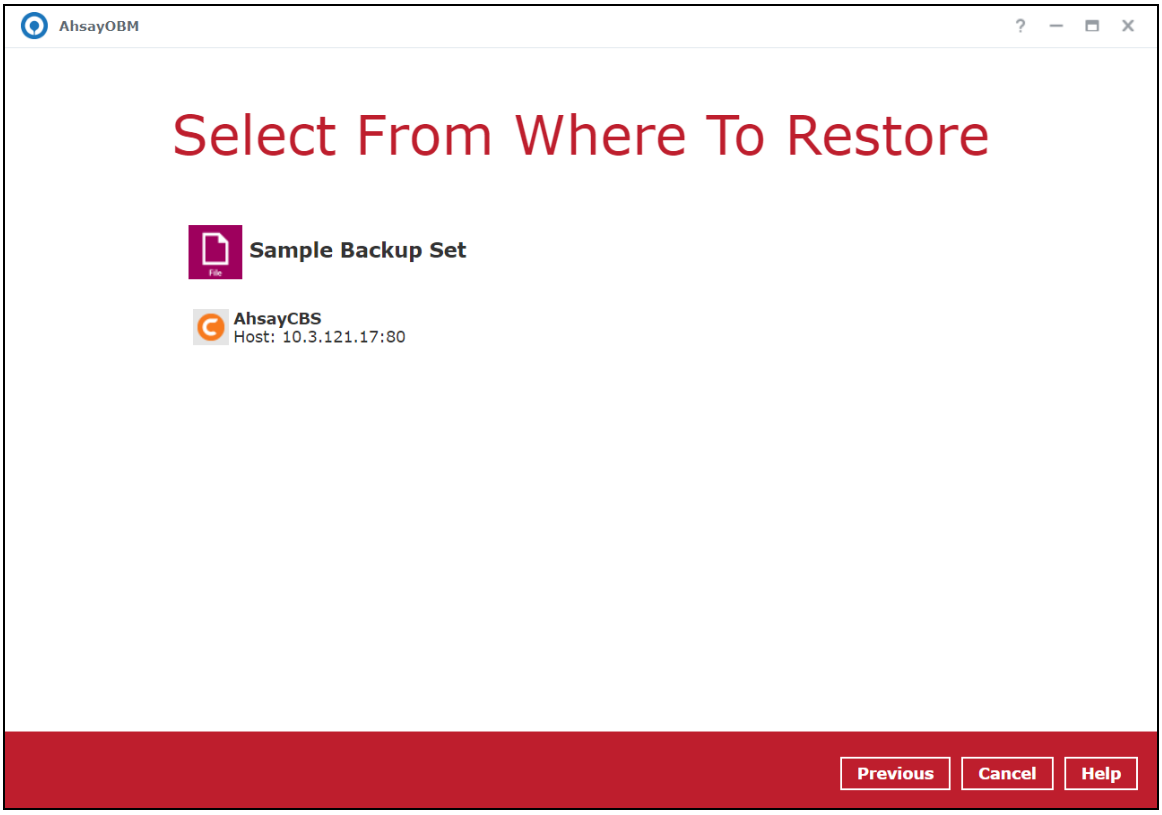
Please Select The Backup Set To Restore

Sort by: Creation Time

**Sample Backup Set**
Owner: DS715
Last Backup: Monday, 17 January 2022 14:54

**BackupSet-1**
Owner: DS715
Newly created on Monday, 17 January 2022 14:24

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



Select From Where To Restore

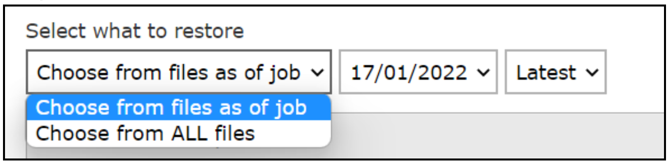
Sample Backup Set

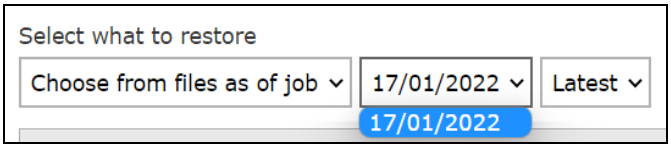
AhsayCBS
Host: 10.3.121.17:80

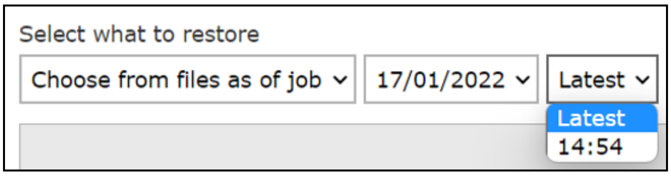
4. Select to restore files from a specific backup job, or from ALL files available. Then, select the files or folders that you would like to restore.

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

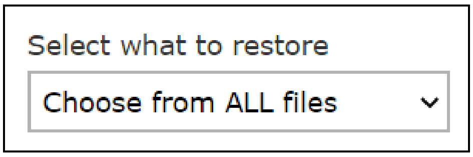
   - **Choose from files as of job** – This option allows you to select a backup version from a specific date and time to restore.





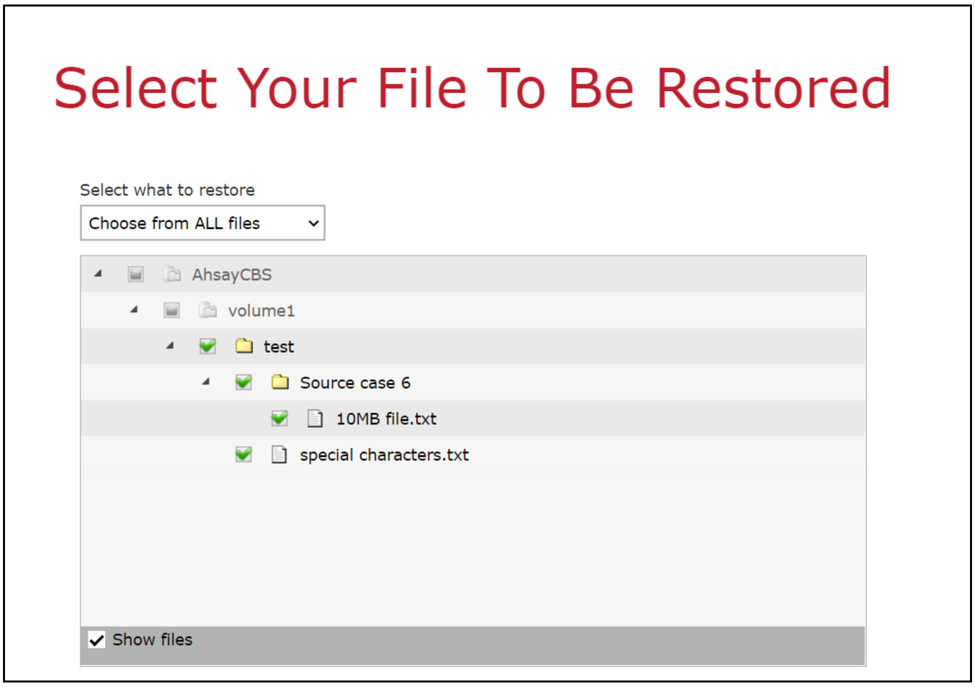


- **Choose from ALL files** – This option allows you to restore all the available backup versions for this backup set. Among all the available backup versions, you can also select only some of the backup versions of a file to restore.



Select what to restore

Choose from ALL files ⌄



Select Your File To Be Restored

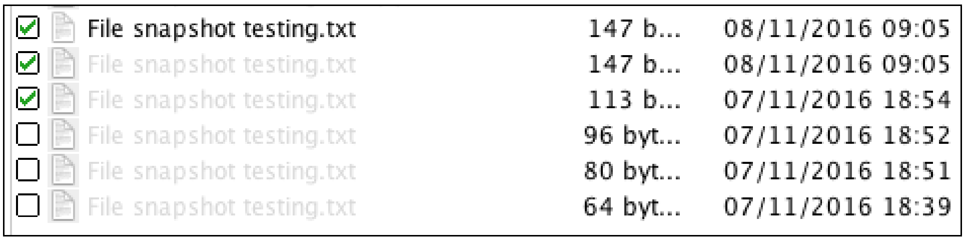
Select what to restore

Choose from ALL files ⌄

```
◢ ▣ AhsayCBS
   ◢ ▣ volume1
      ◢ ☑ test
         ◢ ☑ Source case 6
              ☑ 10MB file.txt
           ☑ special characters.txt
```

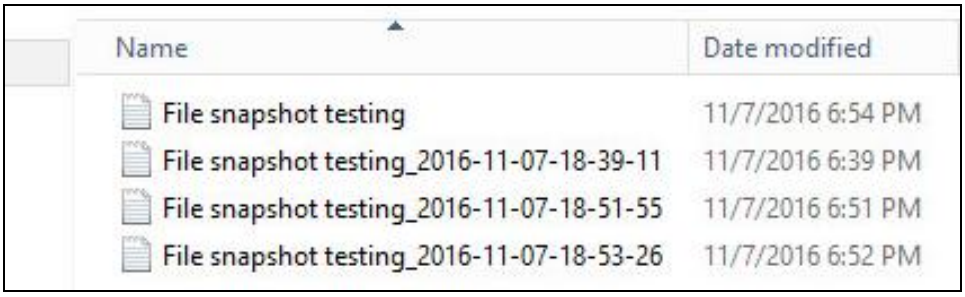
☑ Show files

Below is an example showing all the available backup versions of the file **File snapshot testing.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.



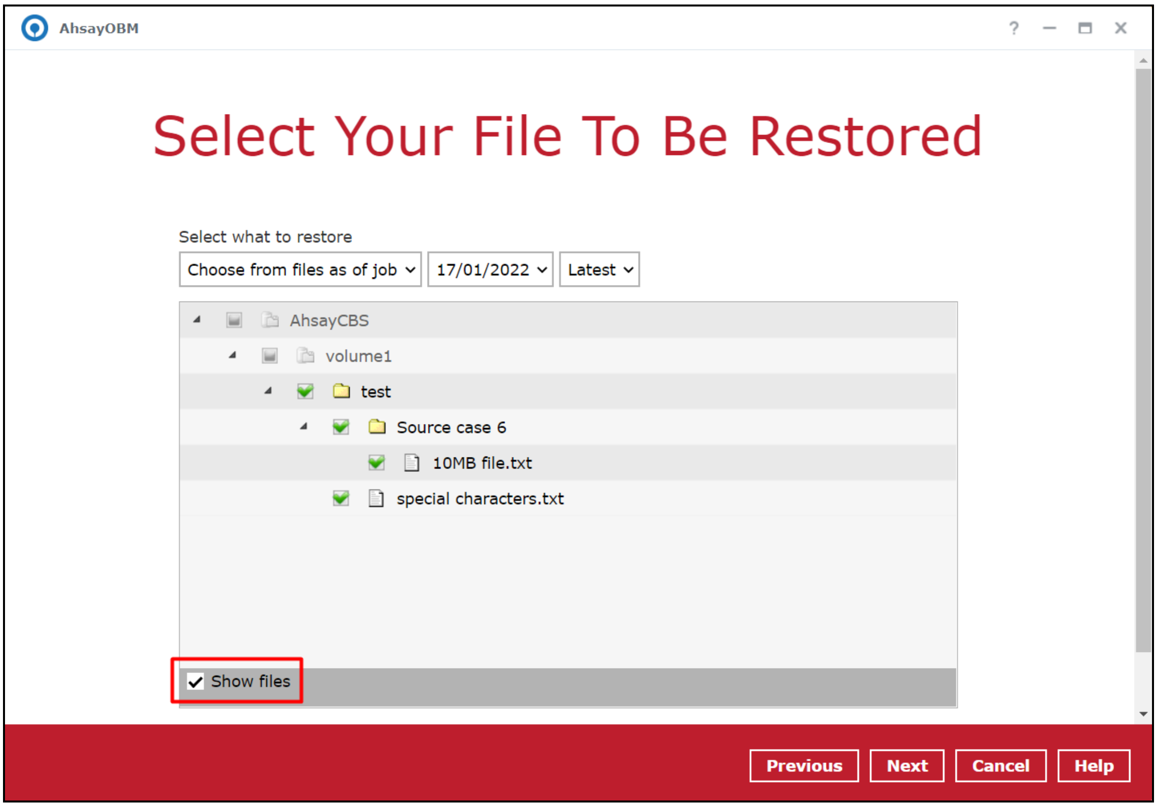
| | | | |
|---|---|---|---|
| ☑ | File snapshot testing.txt | 147 b... | 08/11/2016 09:05 |
| ☑ | File snapshot testing.txt | 147 b... | 08/11/2016 09:05 |
| ☑ | File snapshot testing.txt | 113 b... | 07/11/2016 18:54 |
| ☐ | File snapshot testing.txt | 96 byt... | 07/11/2016 18:52 |
| ☐ | File snapshot testing.txt | 80 byt... | 07/11/2016 18:51 |
| ☐ | File snapshot testing.txt | 64 byt... | 07/11/2016 18:39 |

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



| Name | Date modified |
|---|---|
| File snapshot testing | 11/7/2016 6:54 PM |
| File snapshot testing_2016-11-07-18-39-11 | 11/7/2016 6:39 PM |
| File snapshot testing_2016-11-07-18-51-55 | 11/7/2016 6:51 PM |
| File snapshot testing_2016-11-07-18-53-26 | 11/7/2016 6:52 PM |

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



Select Your File To Be Restored

Select what to restore

Choose from files as of job | 17/01/2022 | Latest

- AhsayCBS
  - volume1
    - ☑ test
      - ☑ Source case 6
        - ☑ 10MB file.txt
      - ☑ special characters.txt

☑ Show files

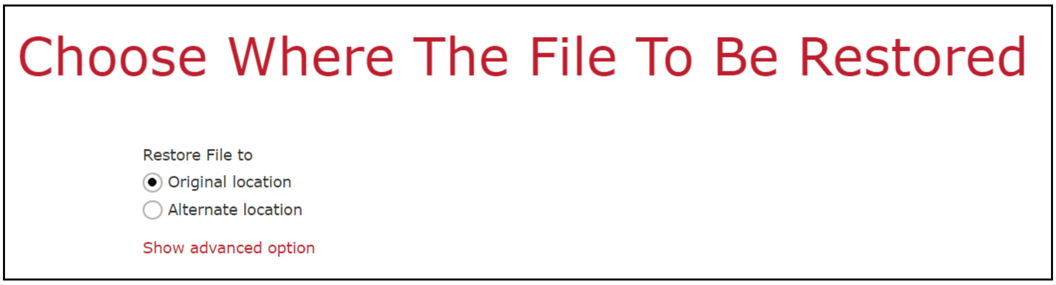
6. Select to restore the files to their **Original location**, or to an **Alternate location**. Then click **Next** to proceed.

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

  For example, if the backup source files are stored under the path

  **Users/[User's Name]/Downloads**,

  then the data will also be restored to **Users/[User's Name]/Downloads** on the computer running AhsayOBM.



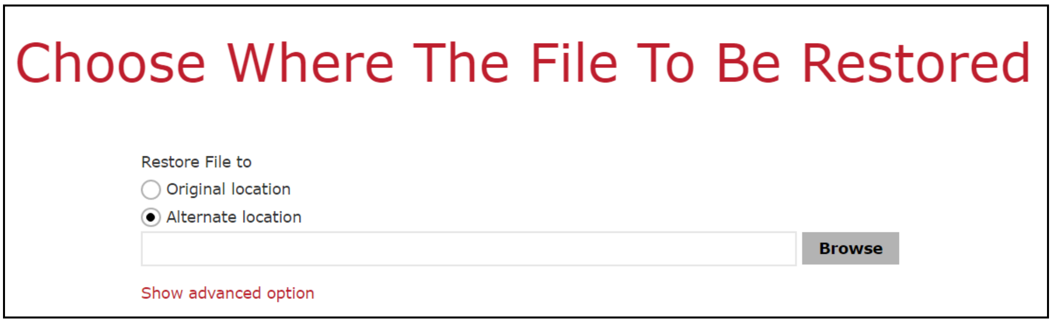
Choose Where The File To Be Restored

Restore File to

● Original location

○ Alternate location

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

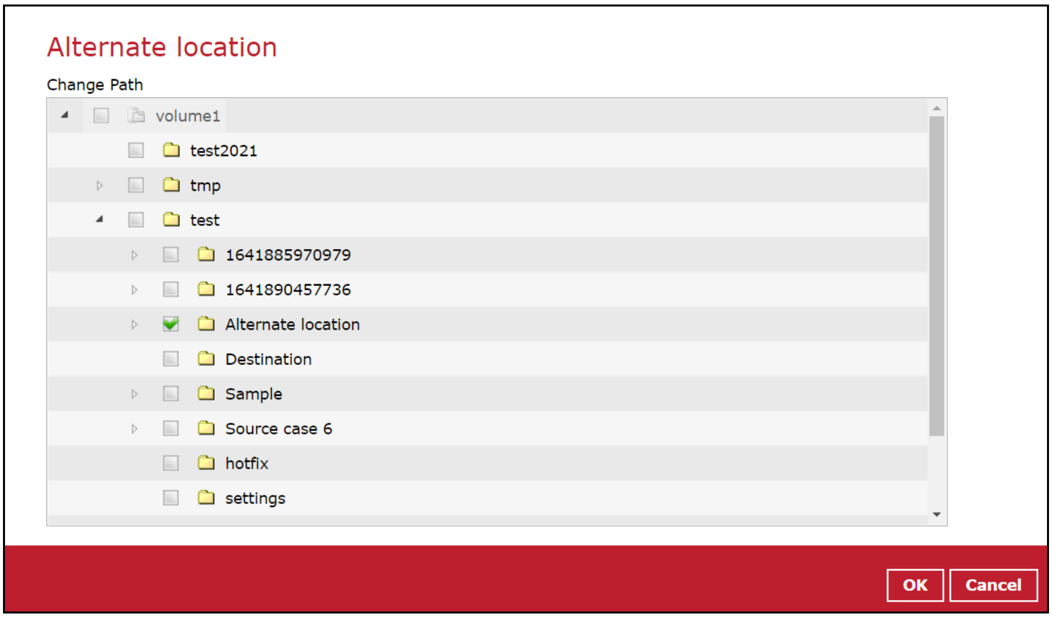


Choose Where The File To Be Restored

Restore File to

○ Original location

● Alternate location

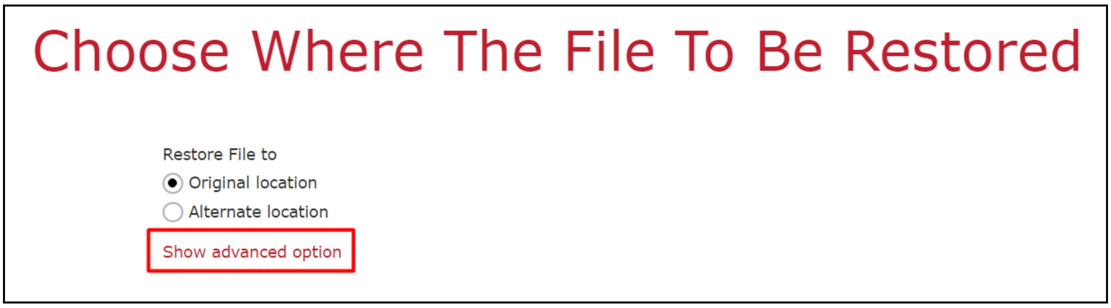


Alternate location

Change Path

- volume1
  - test2021
  - tmp
  - test
    - 1641885970979
    - 1641890457736
    - ☑ Alternate location
    - Destination
    - Sample
    - Source case 6
    - hotfix
    - settings

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

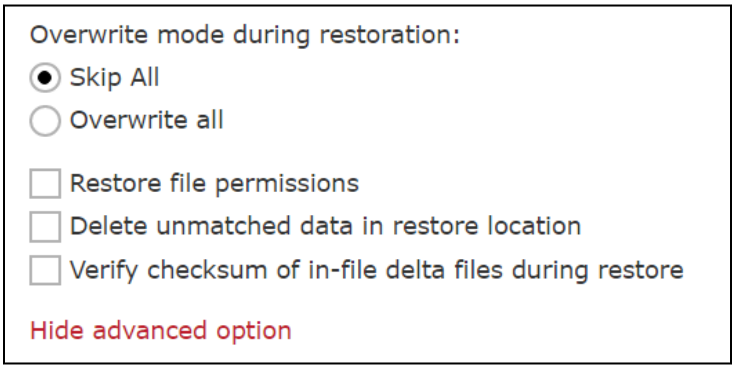


Choose Where The File To Be Restored

Restore File to

● Original location

○ Alternate location



Overwrite mode during restoration:

● Skip All

○ Overwrite all

□ Restore file permissions

□ Delete unmatched data in restore location

□ Verify checksum of in-file delta files during restore

- **Overwrite mode during restoration**

  When there are file name conflicts during restoration, you can choose to skip them all by selecting **Skip All** or overwrite all existing files in the restore destination by selecting **Overwrite all**.

- **Restore file permissions**

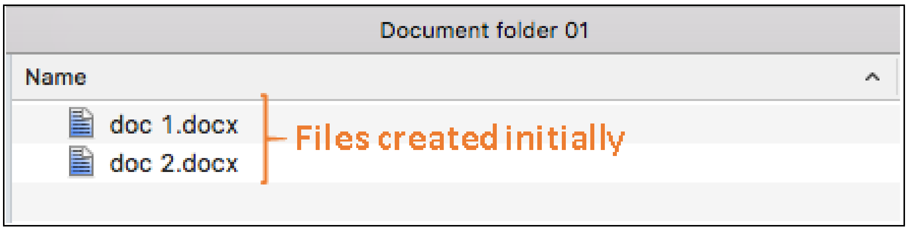
  Restore file permissions is disabled by default. When you perform a file restore on a shared computer, it is recommended that you enable Restore file permissions by ticking the checkbox so that the files restored will not be fully accessible to everyone using the shared computer.

- **Delete unmatched data in restore location**

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

  **Example:**

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



Document folder 01

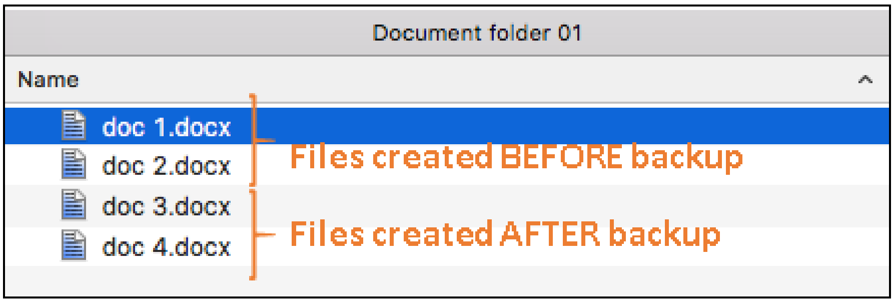
Name

doc 1.docx
doc 2.docx

Files created initially

  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
doc 2.docx

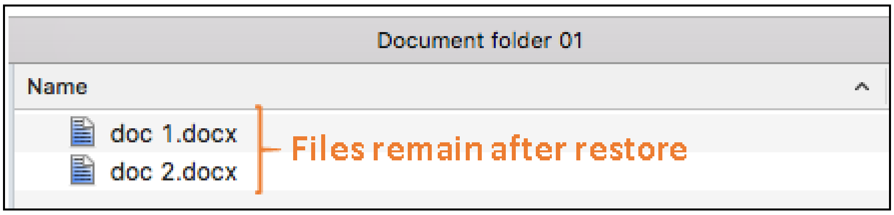
Files created BEFORE backup

doc 3.docx
doc 4.docx

Files created AFTER backup

  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
doc 2.docx

Files remain after restore

**WARNING**

Please exercise extra caution when enabling this feature. Consider what data in the restore source has not been backed up and what impact it would cause if those data were deleted. Prior to the data restore and synchronization, a warning message shows as the one shown below. Only clicking **Yes** will the “unmatched data” be deleted. You can click **Apply to all** to confirm deleting all the “unmatched data” at a time.

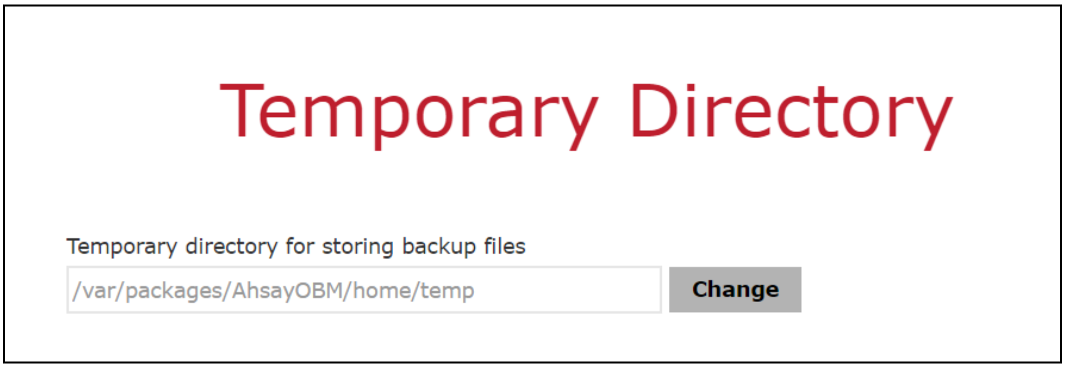
- **Verify checksum of in-file delta files during restore**

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

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

9. Select the temporary directory for storing temporary restore files.

   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.

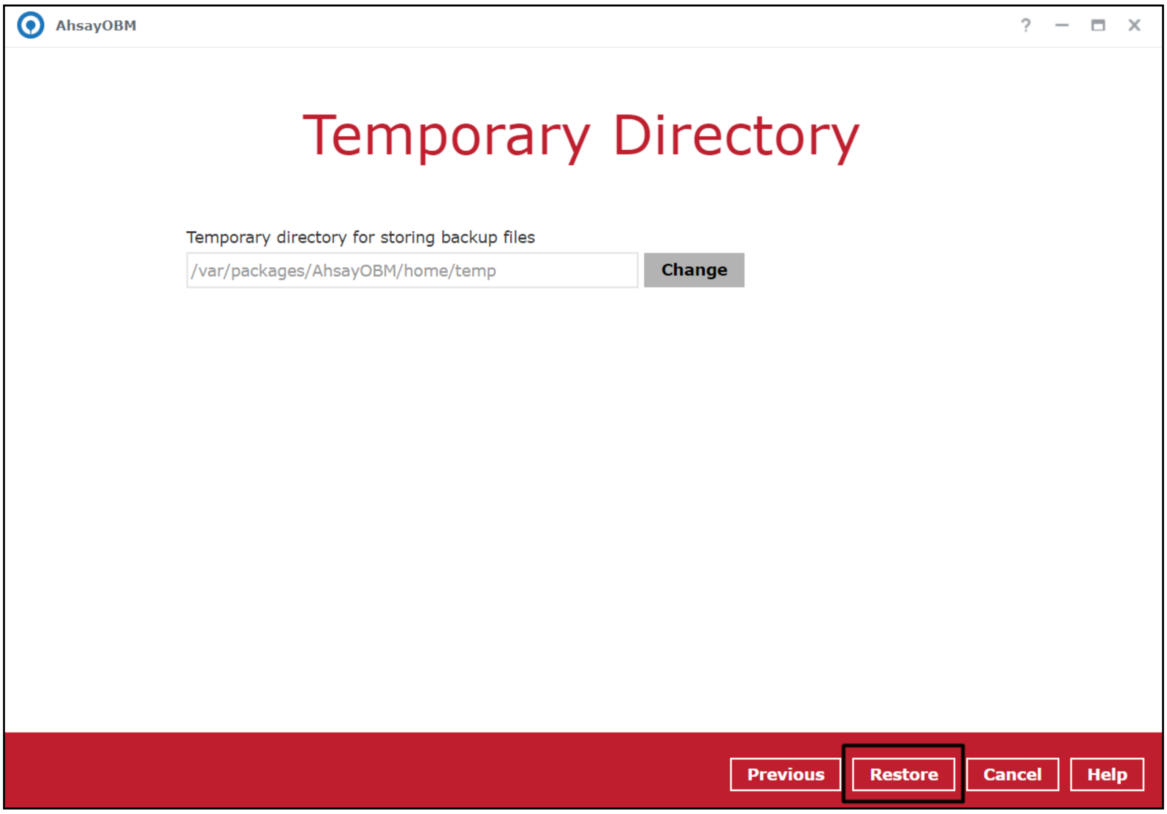


Temporary Directory

Temporary directory for storing backup files

/var/packages/AhsayOBM/home/temp

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

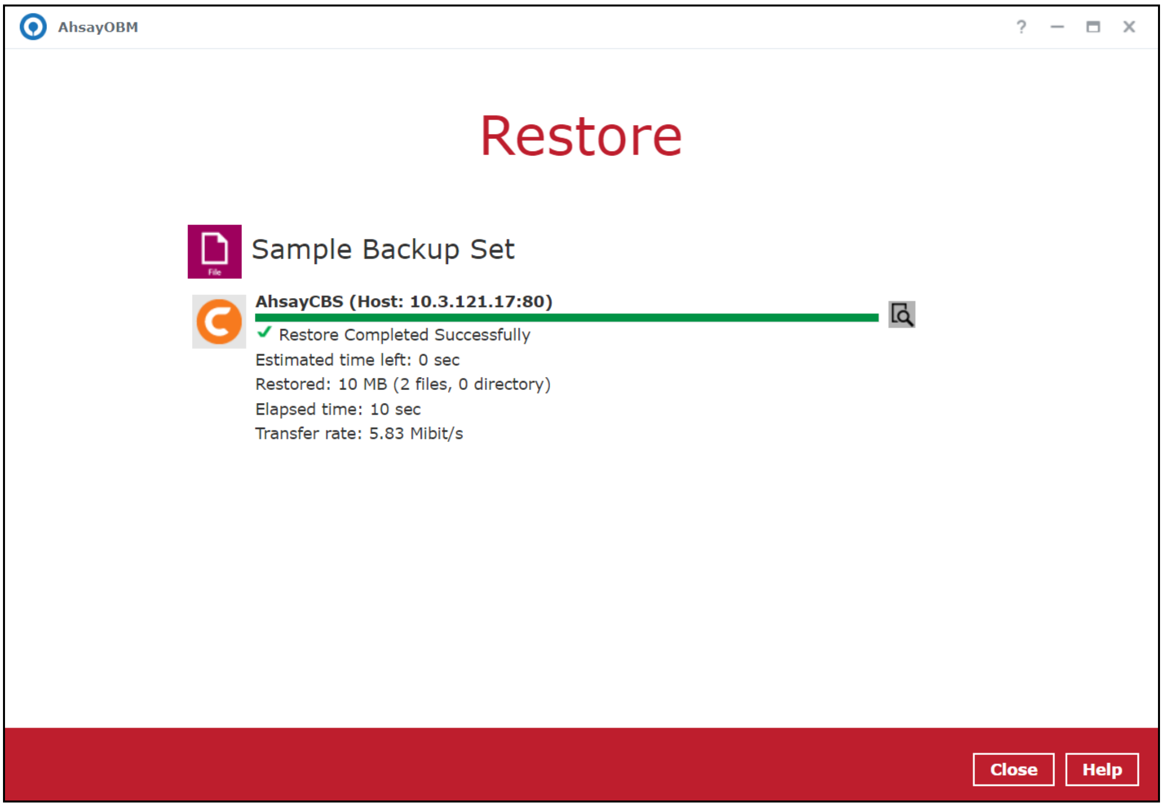


Temporary Directory

Temporary directory for storing backup files

/var/packages/AhsayOBM/home/temp

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



Restore

Sample Backup Set

AhsayCBS (Host: 10.3.121.17:80)

✓ Restore Completed Successfully

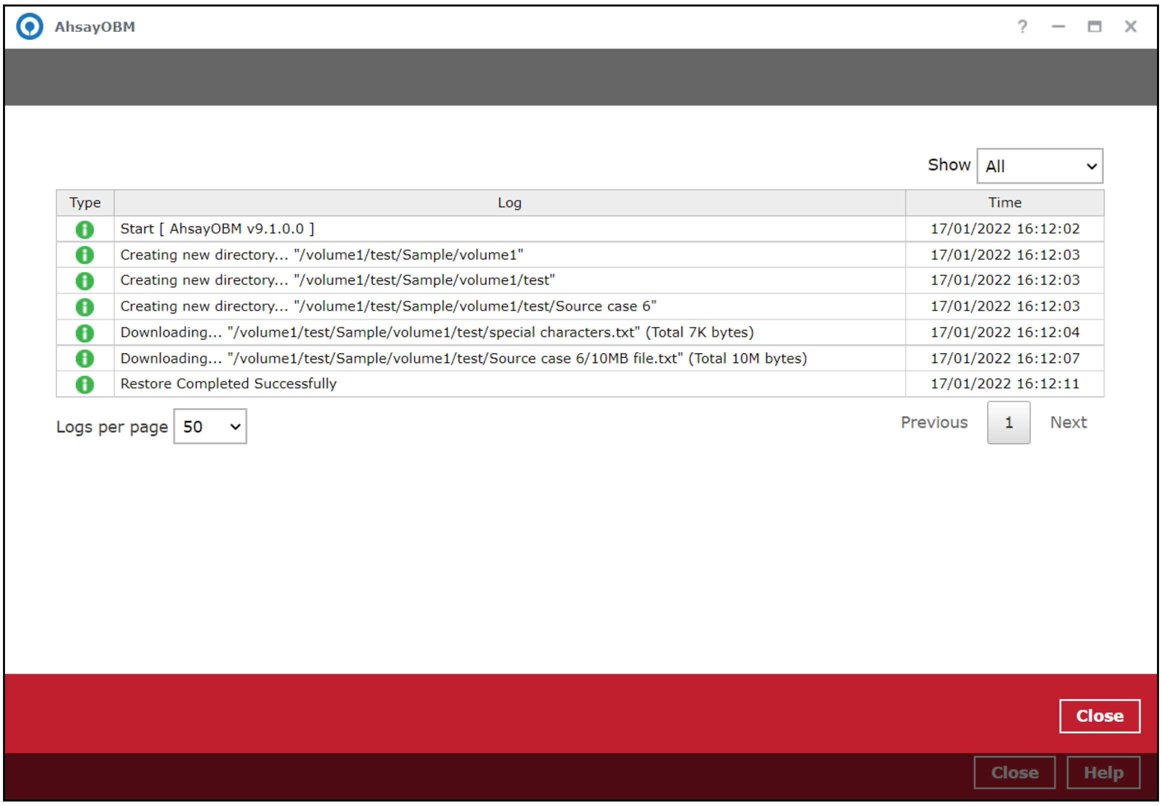
Estimated time left: 0 sec

Restored: 10 MB (2 files, 0 directory)

Elapsed time: 10 sec

Transfer rate: 5.83 Mibit/s

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



| Type | Log | Time |
|---|---|---|
| ● | Start [ AhsayOBM v9.1.0.0 ] | 17/01/2022 16:12:02 |
| ● | Creating new directory... "/volume1/test/Sample/volume1" | 17/01/2022 16:12:03 |
| ● | Creating new directory... "/volume1/test/Sample/volume1/test" | 17/01/2022 16:12:03 |
| ● | Creating new directory... "/volume1/test/Sample/volume1/test/Source case 6" | 17/01/2022 16:12:03 |
| ● | Downloading... "/volume1/test/Sample/volume1/test/special characters.txt" (Total 7K bytes) | 17/01/2022 16:12:04 |
| ● | Downloading... "/volume1/test/Sample/volume1/test/Source case 6/10MB file.txt" (Total 10M bytes) | 17/01/2022 16:12:07 |
| ● | Restore Completed Successfully | 17/01/2022 16:12:11 |

# 13 Contact Ahsay

## 13.1 Technical Assistance

To contact Ahsay support representatives for technical assistance, visit the Partner Portal:
https://www.ahsay.com/partners/

Also use the Ahsay Wikipedia for resource such as Hardware Compatibility List, Software Compatibility List, and other product information:
http://wiki.ahsay.com/

## 13.2 Documentation

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

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

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

# Appendix

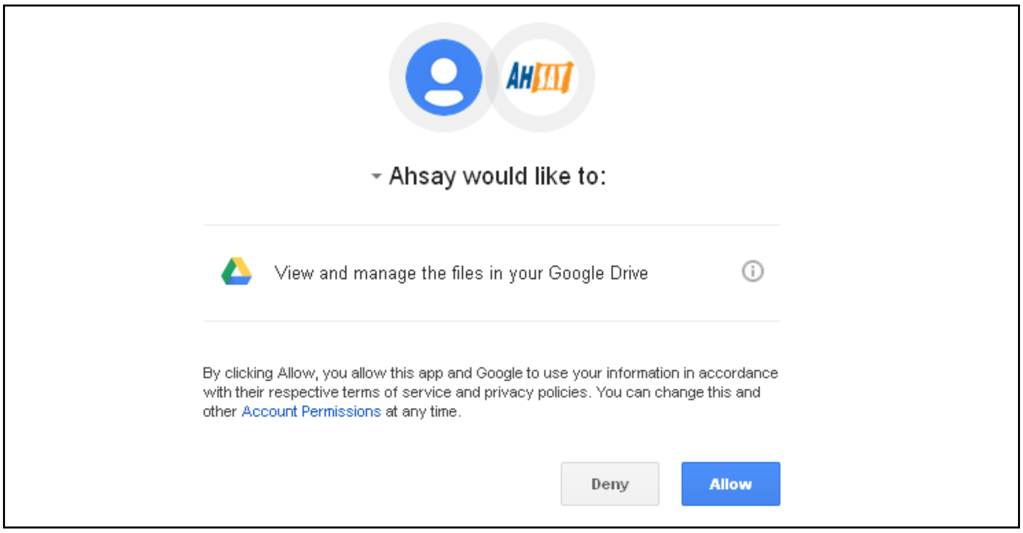
## Appendix A: Cloud Storage as Backup Destination

For most cloud storage providers (e.g. Dropbox, Google Drive, etc.), you need to enable access of AhsayOBM on your cloud destination. To do this, click **OK**/**Test**. You will be prompted to login to the corresponding cloud service.

**IMPORTANT**

The authentication request will be opened in a new tab / window on the browser. Ensure that the pop-up tab / window is not blocked.

1. Click **Allow** to permit AhsayOBM to access the cloud storage.

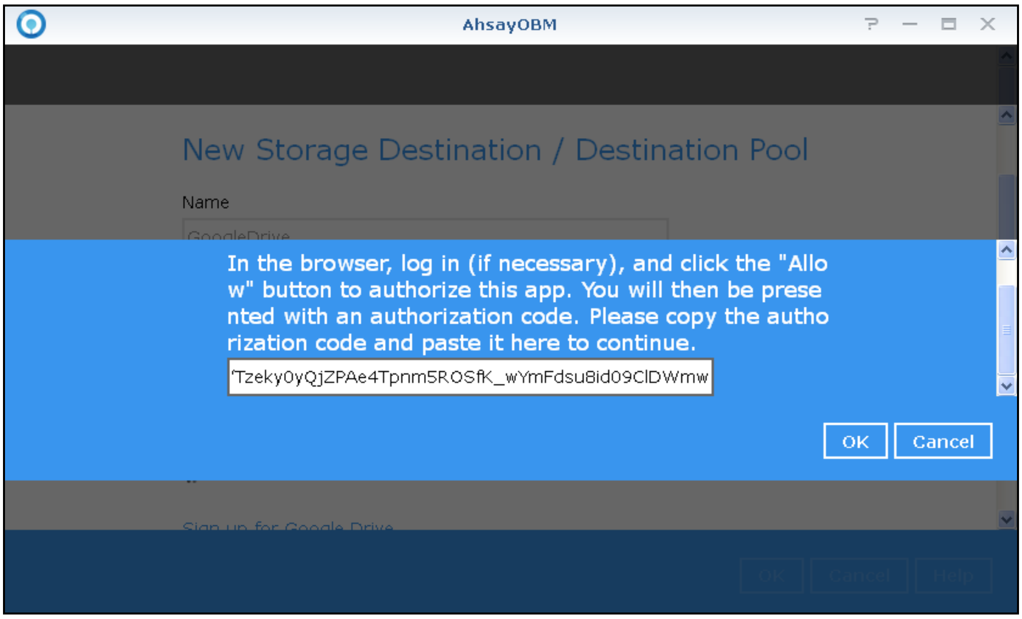


Ahsay would like to:

View and manage the files in your Google Drive

By clicking Allow, you allow this app and Google to use your information in accordance with their respective terms of service and privacy policies. You can change this and other Account Permissions at any time.

2. Enter the authentication code returned in AhsayOBM to complete the destination setup.



New Storage Destination / Destination Pool

Name

GoogleDrive

In the browser, log in (if necessary), and click the "Allow" button to authorize this app. You will then be presented with an authorization code. Please copy the authorization code and paste it here to continue.

'Tzeky0yQjZPAe4Tpnm5ROSfK_wYmFdsu8id09ClDWmw

**NOTE**

A backup destination can be set to a supported cloud storage, backup server, FTP / SFTP server, network storage, or local / removable drive on your computer.

Multiple backup destinations can be configured for a single backup set. In fact, it is recommended for you to set up at least 2 backup destinations for your backup set.

For more details on backup destination, for example which cloud service providers are supported, destination type, or limitation, you can refer to the following wiki article:

FAQ: Frequently Asked Questions on Backup Destination

# Appendix B: Uninstall AhsayOBM

Refer to the following steps to uninstall AhsayOBM.

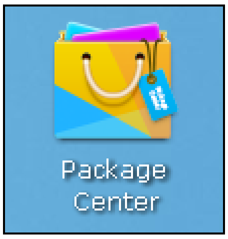
1. Sign into DiskStation Manager (DSM) with the admin account. In a web browser, enter the Synology NAS device IP address, followed by 5000

   https://nas_hostname:5000

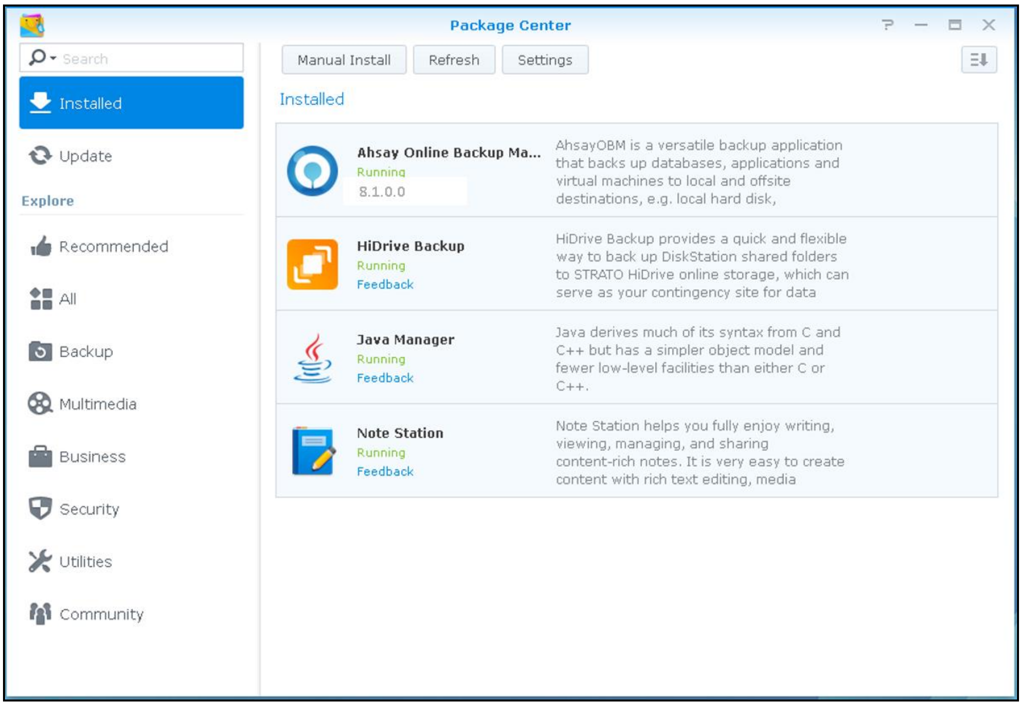
   **NOTE**

   Refer to the following Synology wiki article for information on how to sign into DSM:
   https://www.synology.com/en-us/knowledgebase/DSM/help/DSM/MainMenu/get_started

2. Double-click the Package Center icon on the desktop.



3. When the Package Center window appears, select **Ahsay Online Backup Manager** from the listed installed packages.



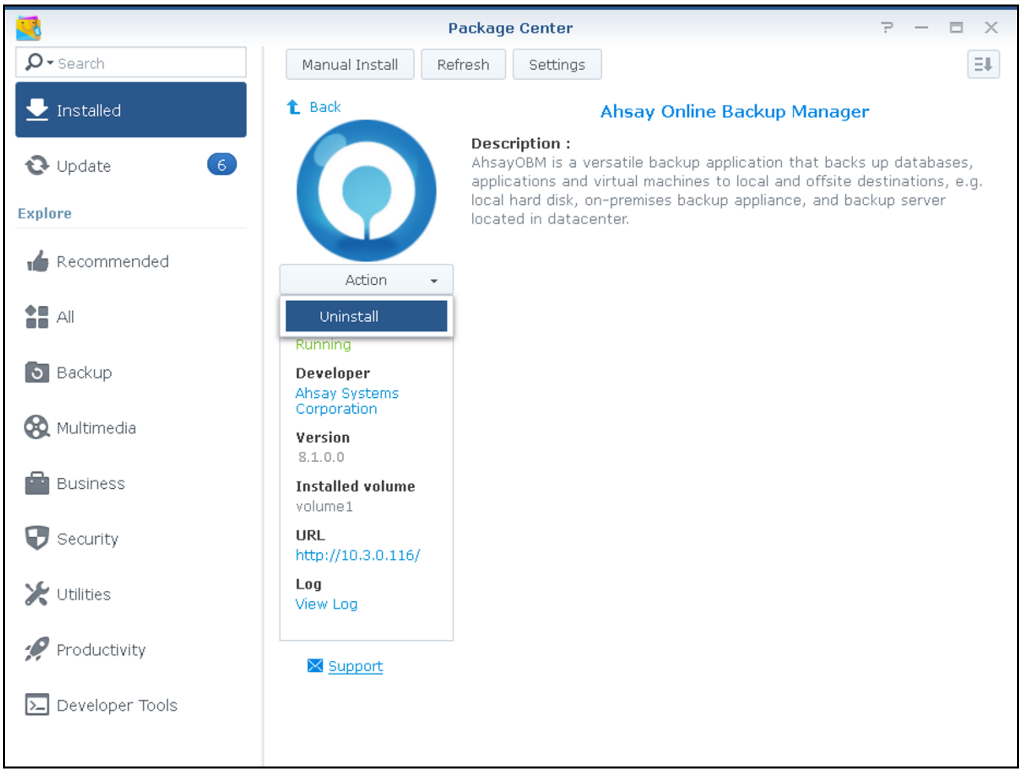
Ahsay Online Backup Ma...
Running
8.1.0.0
AhsayOBM is a versatile backup application that backs up databases, applications and virtual machines to local and offsite destinations, e.g. local hard disk,

HiDrive Backup
Running
Feedback
HiDrive Backup provides a quick and flexible way to back up DiskStation shared folders to STRATO HiDrive online storage, which can serve as your contingency site for data

Java Manager
Running
Feedback
Java derives much of its syntax from C and C++ but has a simpler object model and fewer low-level facilities than either C or C++.

Note Station
Running
Feedback
Note Station helps you fully enjoy writing, viewing, managing, and sharing content-rich notes. It is very easy to create content with rich text editing, media

4. When the Ahsay Online Backup Manager properties appears, select **Action** > **Uninstall**.



**Description :**
AhsayOBM is a versatile backup application that backs up databases, applications and virtual machines to local and offsite destinations, e.g. local hard disk, on-premises backup appliance, and backup server located in datacenter.

**Developer**
Ahsay Systems Corporation

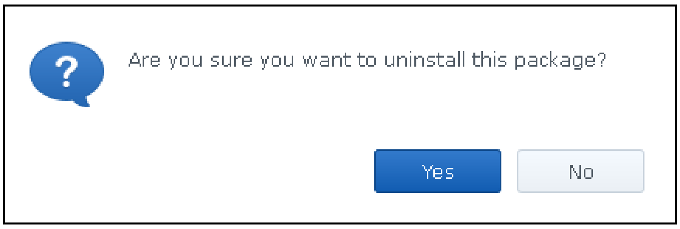
**Version**
8.1.0.0

**Installed volume**
volume1

**URL**
http://10.3.0.116/

**Log**
View Log

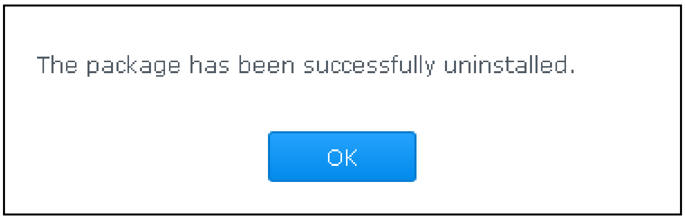
5. Click **Yes** to uninstall AhsayOBM.



Are you sure you want to uninstall this package?

| NOTE |
|---|
| If you select **Yes**, both AhsayOBM program files and user settings will be removed from the NAS drive. |

6. When the uninstallation is completed, the following message will appear.



The package has been successfully uninstalled.

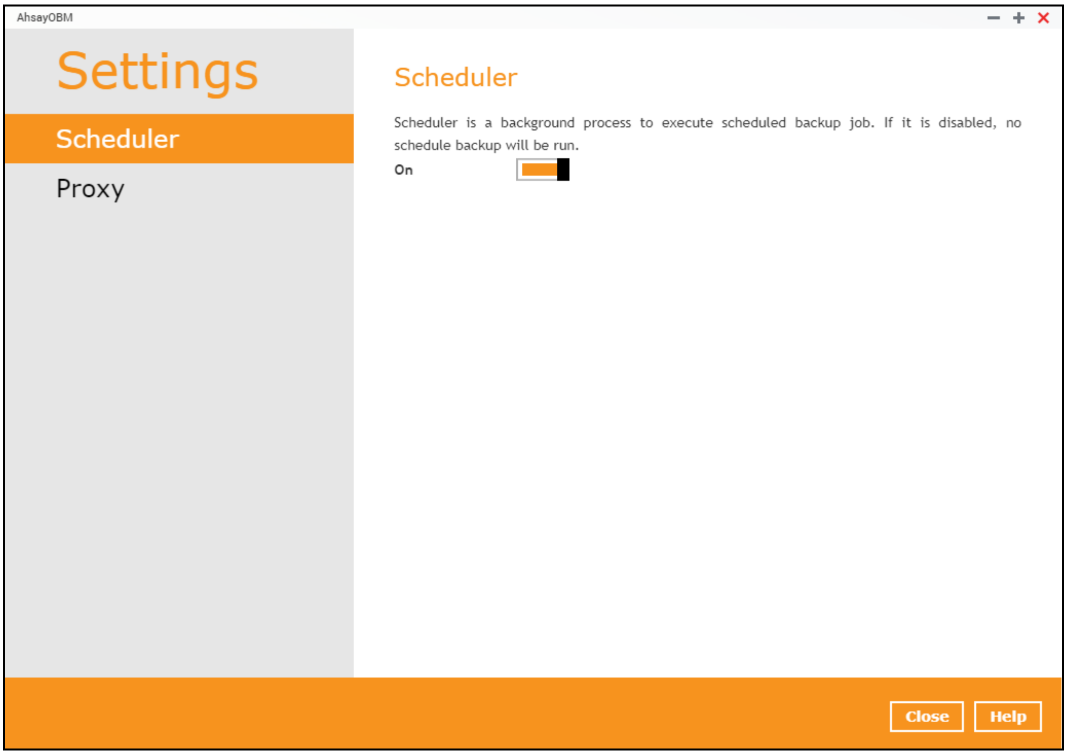
| NOTE |
|---|
| Ahsay Online Backup Manager will no longer appear in the list of Installed packages. The uninstaller will also remove the .obm folder and all binary files from the following paths respectively:<br>**/volume1/@appstore/AhsayOBM/.obm**<br>**/volume1/@appstore/AhsayOBM/** |

# Appendix C: Scheduler Scenarios (pre-v9.3.2.0)

Starting with v9.3.2.0, Scheduler under Settings has been removed since the scheduler will be running together with AhsayOBM service once AhsayOBM is started in the Package Center.

Applicable for pre-v9.3.2.0 AhsayOBM, NAS Synology has two (2) levels of Scheduler settings for scheduled backup jobs.

Level 1: Scheduler under Settings

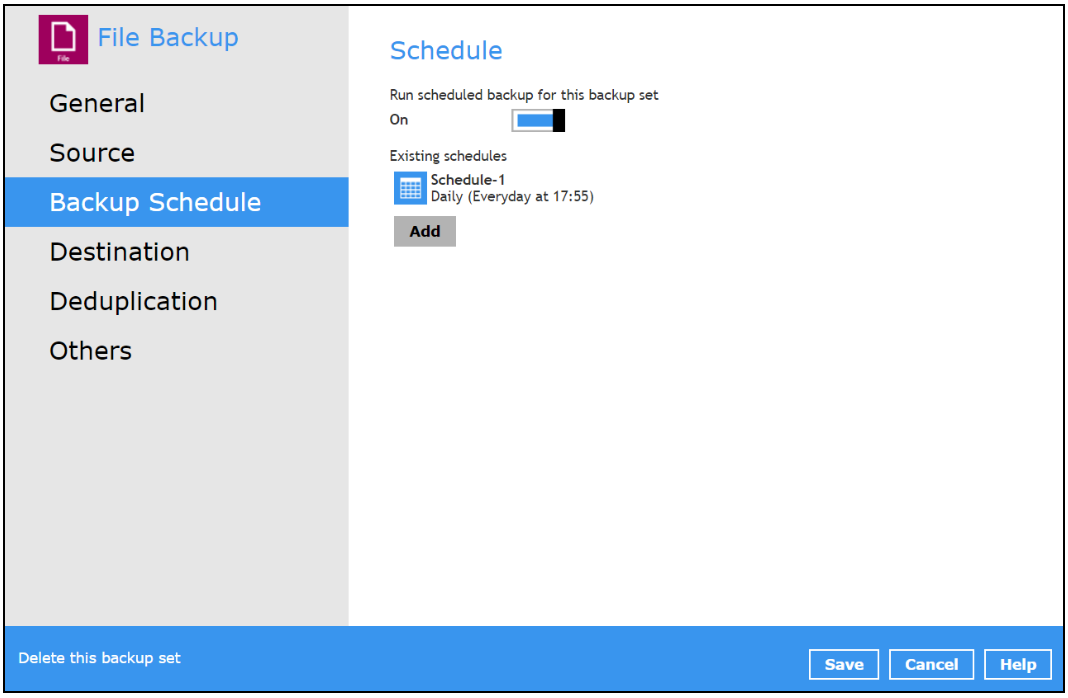


Scheduler

Scheduler is a background process to execute scheduled backup job. If it is disabled, no schedule backup will be run.

On

Level 2: Scheduler under Backup Set Settings



Schedule

Run scheduled backup for this backup set

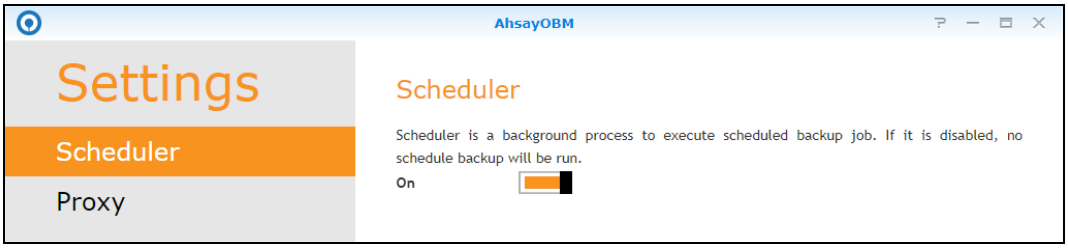
On

Existing schedules

Schedule-1
Daily (Everyday at 17:55)

Scenario no. 1: Scheduler under Settings is ON, and Scheduler under Backup Set Settings is OFF

Scheduler under Settings

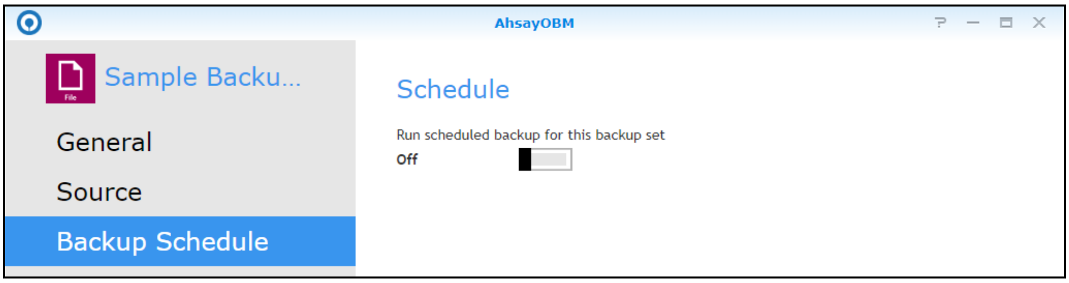


Scheduler

Scheduler is a background process to execute scheduled backup job. If it is disabled, no schedule backup will be run.

On

Scheduler under Backup Set Settings



Schedule

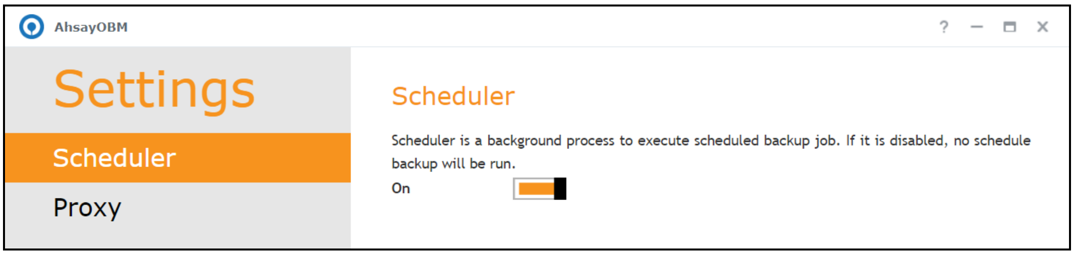
Run scheduled backup for this backup set

Off

Result: There is no scheduled backup job that will be run for the backup set.

Scenario no. 2: Scheduler under Settings is ON, and Scheduler under Backup Set Settings is ON

Scheduler under Settings

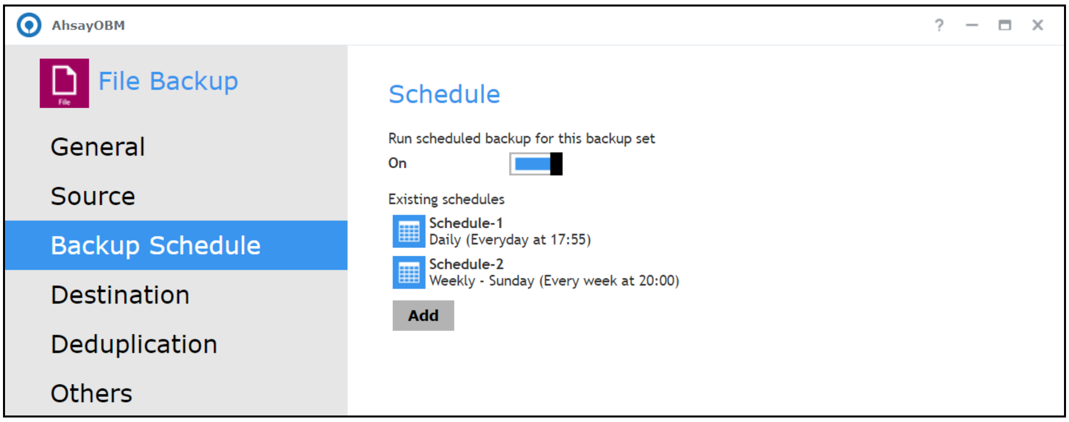


Scheduler

Scheduler is a background process to execute scheduled backup job. If it is disabled, no schedule backup will be run.

On

Scheduler under Backup Set Settings



Schedule

Run scheduled backup for this backup set

On

Existing schedules

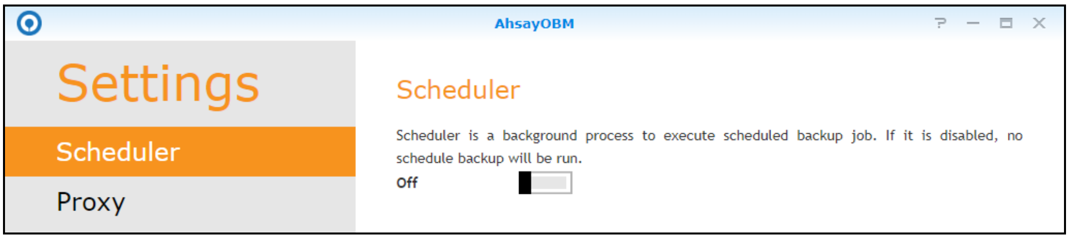
Schedule-1
Daily (Everyday at 17:55)

Schedule-2
Weekly - Sunday (Every week at 20:00)

Result: Scheduled backup jobs which are Schedule-1 and Schedule 2 for the backup set will run.

Scenario no. 3: Scheduler under settings is OFF, and Scheduler under Backup Set Settings is OFF.

Scheduler under Settings

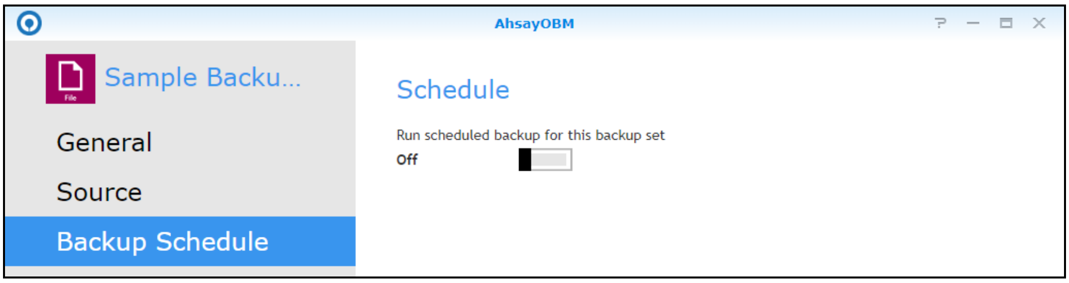


Scheduler

Scheduler is a background process to execute scheduled backup job. If it is disabled, no schedule backup will be run.

Off

Scheduler under Backup Set Settings



Schedule

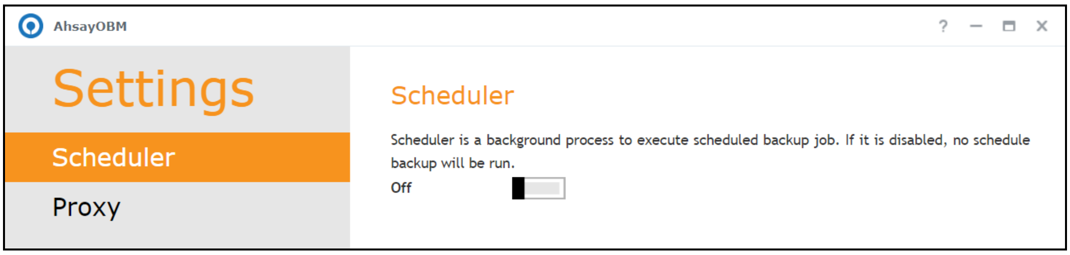
Run scheduled backup for this backup set

Off

Result: No scheduled backup job will be run for the backup set.

Scenario no. 4: Scheduler under Settings is OFF, and Scheduler under Backup Set Settings is ON.

Scheduler under Settings

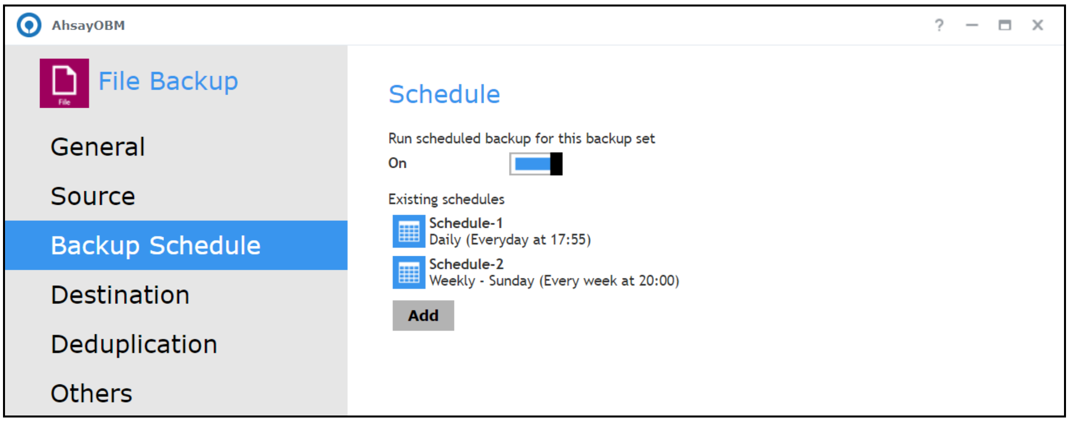


Scheduler

Scheduler is a background process to execute scheduled backup job. If it is disabled, no schedule backup will be run.

Off

Scheduler under Backup Set Settings



Schedule

Run scheduled backup for this backup set

On

Existing schedules

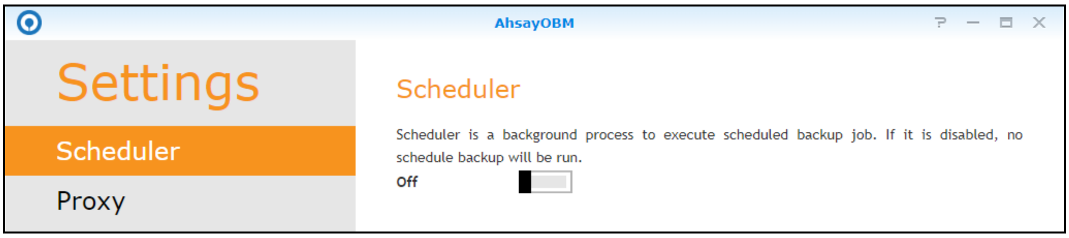
Schedule-1
Daily (Everyday at 17:55)

Schedule-2
Weekly - Sunday (Every week at 20:00)

Result: No scheduled backup job will be run for the backup set.

Scenario no. 5: Scheduler under Settings is OFF and turning ON Scheduler under Backup Set Settings.

Scheduler under Settings

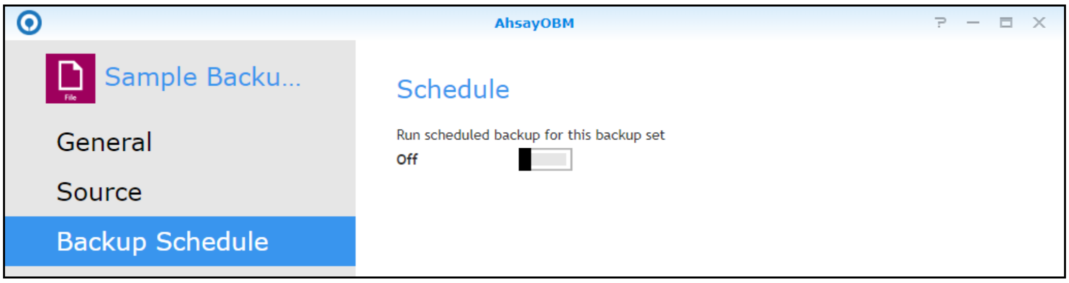


Scheduler

Scheduler is a background process to execute scheduled backup job. If it is disabled, no schedule backup will be run.

Off

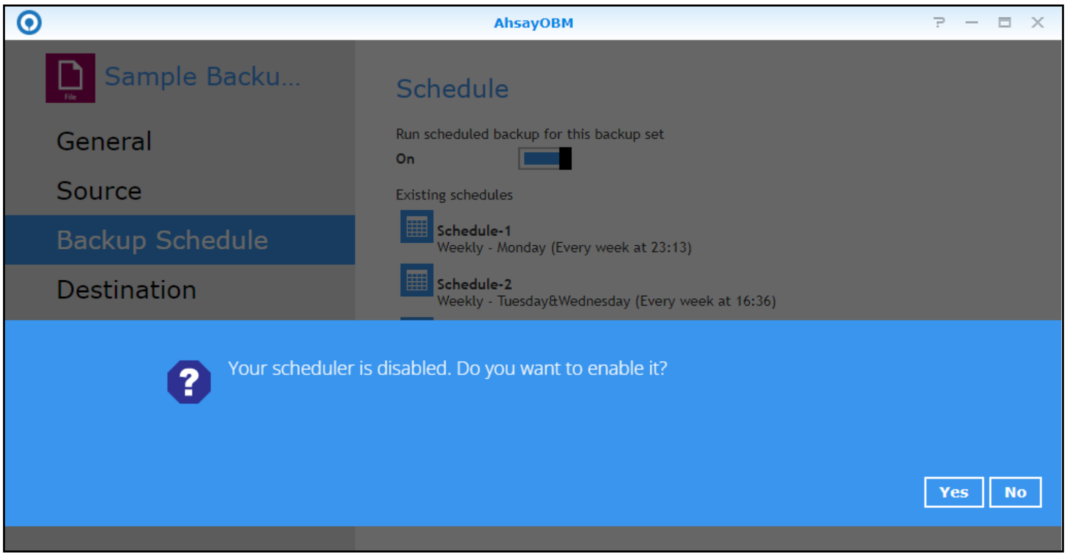
Scheduler under Backup Set Settings



Schedule

Run scheduled backup for this backup set

Off



Schedule

Run scheduled backup for this backup set

On

Existing schedules

Schedule-1
Weekly - Monday (Every week at 23:13)

Schedule-2
Weekly - Tuesday&Wednesday (Every week at 16:36)

Your scheduler is disabled. Do you want to enable it?

Result: There is an alert message that will be displayed confirming to set the Scheduler under Settings from OFF to ON.

If Yes is selected then the Scheduler under Settings will be turned ON. If No is selected, then the Scheduler under Settings will remail turned OFF.

# Appendix D: Create Free Trial Account in AhsayOBM

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

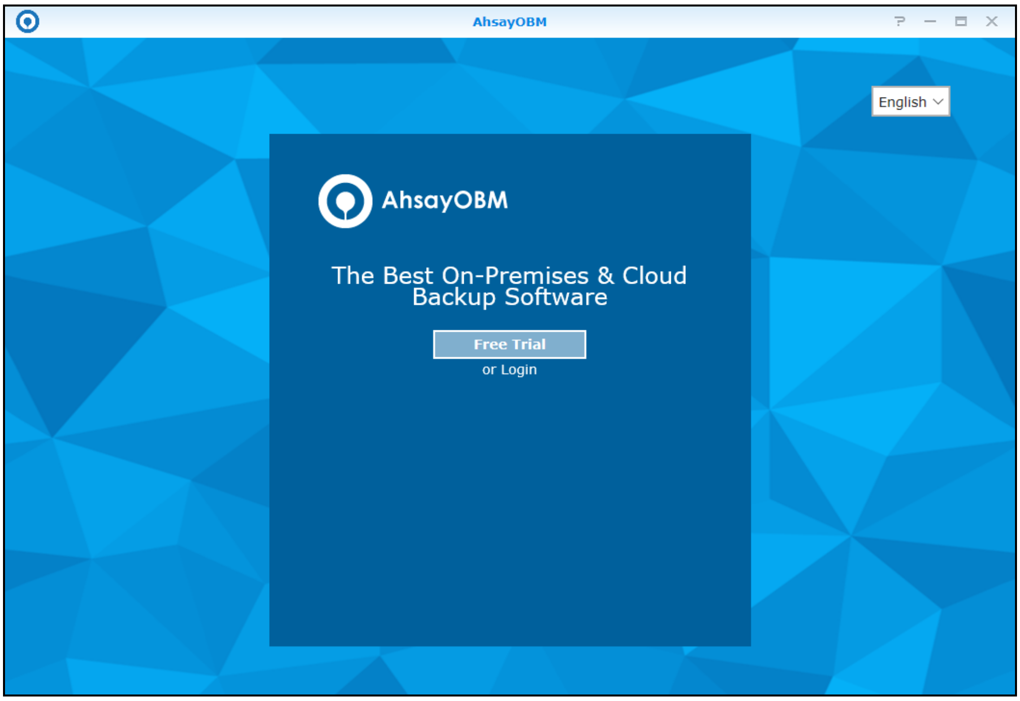
- A valid email address which will be used for receiving notices. A welcome message will also be sent upon creation of the account which specifies the User Setting and Quota set for backup in AhsayCBS.

While here are the limitations of a trial account:

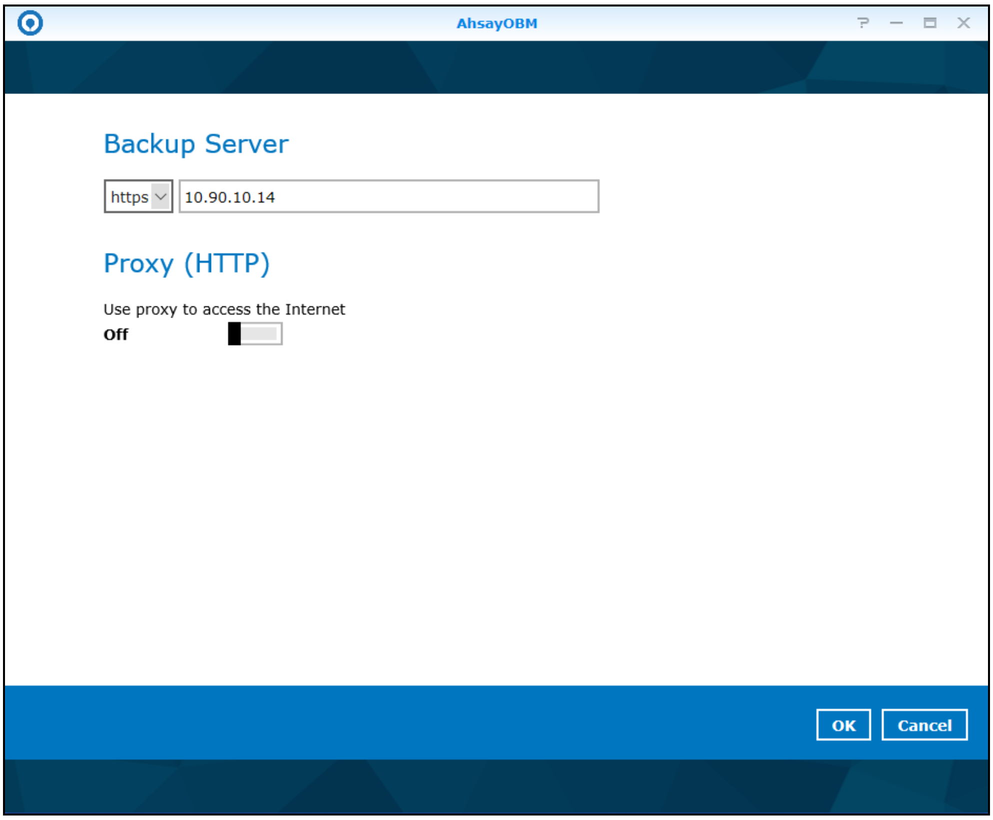
- The Free Trial button will only be displayed once when the user login for the first time. If you cannot create a free trial account kindly contact your backup service provider.
- Only alphanumeric characters and selected special characters, A to Z, 0 to 9, @, - and _, are allowed to be used for the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

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

1. Click on **Free Trial**.



2. Configure your Backup Server settings.



Backup Server

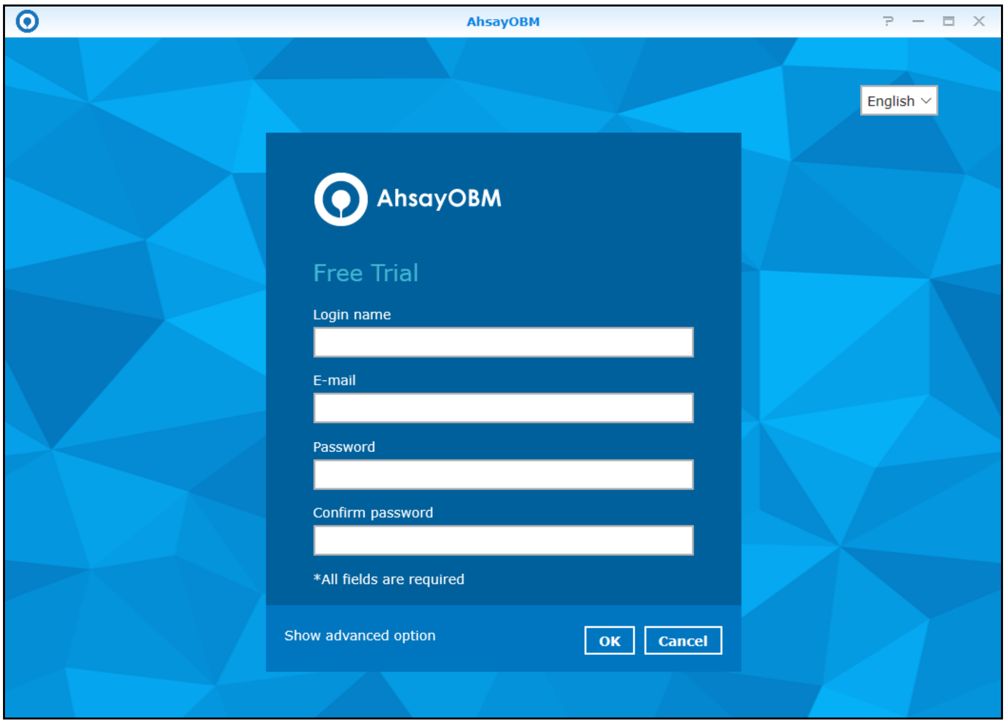
https 10.90.10.14

Proxy (HTTP)

Use proxy to access the Internet

Off

3. Enter a Login name, then provide your email address and password. Confirm your password and click **OK** to create your trial account.



Free Trial

Login name

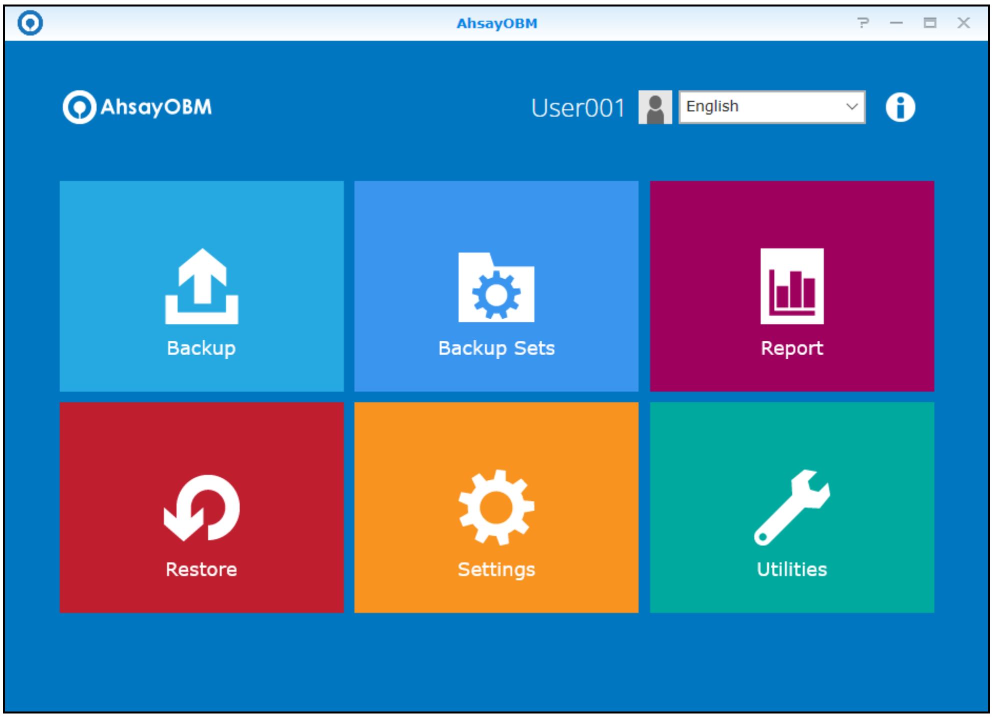
E-mail

Password

Confirm password

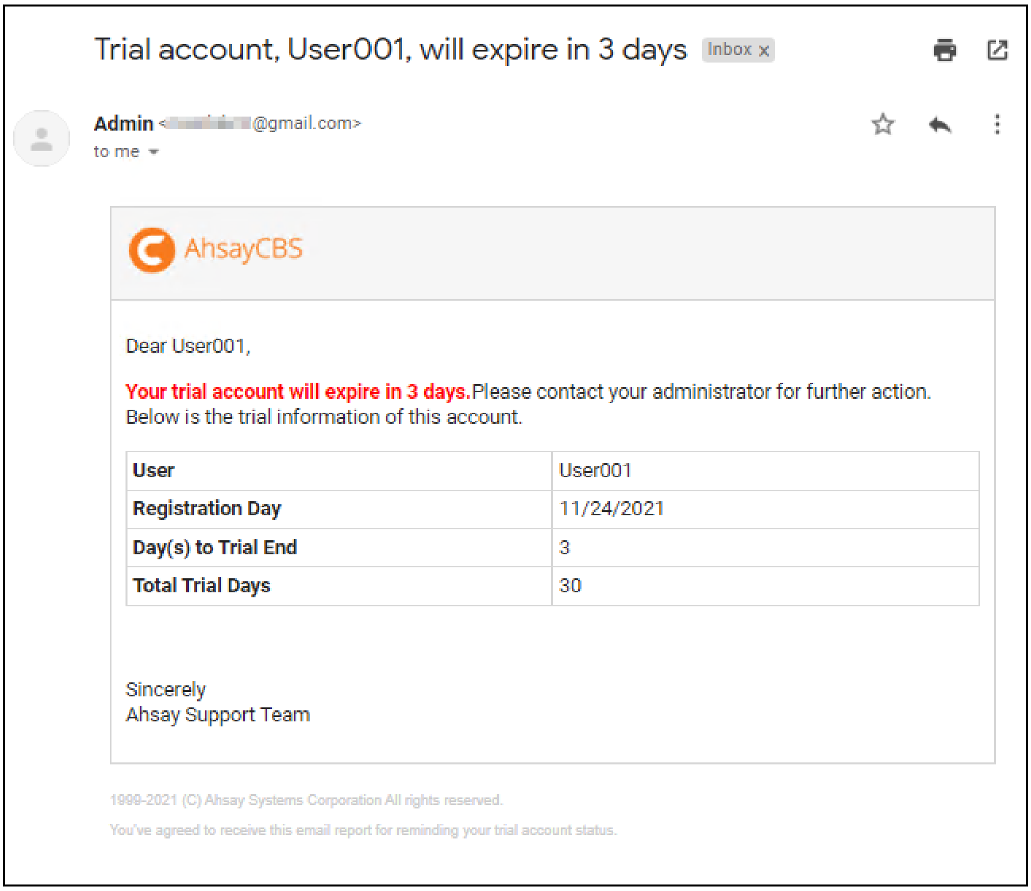
*All fields are required

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



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

   Below is an example of the trial expiration email.



Trial account, User001, will expire in 3 days

**Admin** <[redacted]@gmail.com>
to me

AhsayCBS

Dear User001,

**Your trial account will expire in 3 days.**Please contact your administrator for further action.
Below is the trial information of this account.

| | |
|---|---|
| **User** | User001 |
| **Registration Day** | 11/24/2021 |
| **Day(s) to Trial End** | 3 |
| **Total Trial Days** | 30 |

Sincerely
Ahsay Support Team

1999-2021 (C) Ahsay Systems Corporation All rights reserved.

You've agreed to receive this email report for reminding your trial account status.