Online-Backup.dk v9

Guide for Synology NAS

Ahsay Systems Corporation Limited

11 February 2022

Copyright Notice

© 2022 Ahsay Systems Corporation Limited. All rights reserved.

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

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

Trademarks

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

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

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

Dropbox is a registered trademark of Dropbox Inc.

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

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

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

MariaDB is a registered trademark of MariaDB Corporation AB.

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

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

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

OpenJDK is a registered trademark of Oracle America, Inc.

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

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

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

Ubuntu is a registered trademark of Canonical Ltd.

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

Rocky is a registered trademark of Rocky Brands.

ShadowProtect is a registered trademark of StorageCraft Technology Corporation.

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

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

Disclaimer

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

Revision History

Date	Descriptions	Version
25 January 2022	▪ Ch. 6.6 – added Deduplication ▪ Ch. 9.2 – added Migrate Data	9.1.0.0

Table of Contents

1 Overview 1

1.1 What is this software? 1

1.2 System Architecture 1

2 Requirements for AhsayOBM on Synology NAS 2

2.1 Hardware Requirements 2

2.2 Software Requirements 2

2.3 AhsayOBM Installation 2

2.4 NAS-Synology Add-on Module 2

2.5 Backup Quota Storage 3

2.6 Java Requirement 3

2.7 Memory Requirement 3

2.8 TCP Port Requirement 3

2.9 Synology NAS User Account Permission 3

2.10 Synology NAS Trust Level 4

2.11 Network Bandwidth 4

2.12 Limitations 4

2.13 Best Practices and Recommendations 5

2.14 Supported Features from AhsayCBS Web Console 6

3 Get started with AhsayOBM 7

4 Download and Install AhsayOBM 8

4.1 Download AhsayOBM 8

4.2 Install AhsayOBM using SPK online installer 9

4.3 AhsayOBM Scheduler Service Check 14

5 Start AhsayOBM 16

5.1 Add an AhsayOBM Shortcut Icon to the Desktop 16

5.2 Login to AhsayOBM 18

6 AhsayOBM Overview 22

6.1 Profile 23

6.1.1 General 23

6.1.2 Contacts 24

6.1.3 Time Zone 26

6.1.4 Encryption Recovery 27

6.1.5 Password 28

6.1.7 Security Settings 29

6.2 Online Help 30

6.3 Language 31
6.4 Information 31
6.5 Backup 32
6.6 Backup Sets 32
Backup Set Settings 32
General 33
Source 34
Backup Schedule 35
Destination 39
Deduplication 40
Others 43
6.7 Report 48
6.7.1 Backup 48
6.7.2 Restore 52
6.8 Restore 54
6.9 Settings 55
6.9.1 Scheduler 55
6.9.2 Proxy 56
6.10 Utilities 57
6.10.1 Data Integrity Check 57
Data Integrity Check Result 67
6.10.2 Delete Backup Data 69
7 Create a Backup Set 73
8 Overview on the Backup Process 7
8.1 Periodic Data Integrity Check (PDIC) Process 8
8.2 Backup Set Index Handling Process 10
8.2.1 Start Backup Job 10
8.2.2 Completed Backup Job 11
8.3 Data Validation Check Process 12
9 Run Backup Jobs 13
9.1 Login to AhsayOBM 13
9.2 Start a Manual Backup 13
10 Restore Data 17
10.1 Login to AhsayOBM 17
10.2 Restore Data 17
11 Contact Ahsay 26

11.1 Technical Assistance 26
11.2 Documentation 26
Appendix 27
Appendix A: Cloud Storage as Backup Destination 27
Appendix B: Uninstall AhsayOBM 29
Appendix C: Scheduler Scenarios 31
Appendix D: Create Free Trial Account in AhsayOBM 35

1 Overview

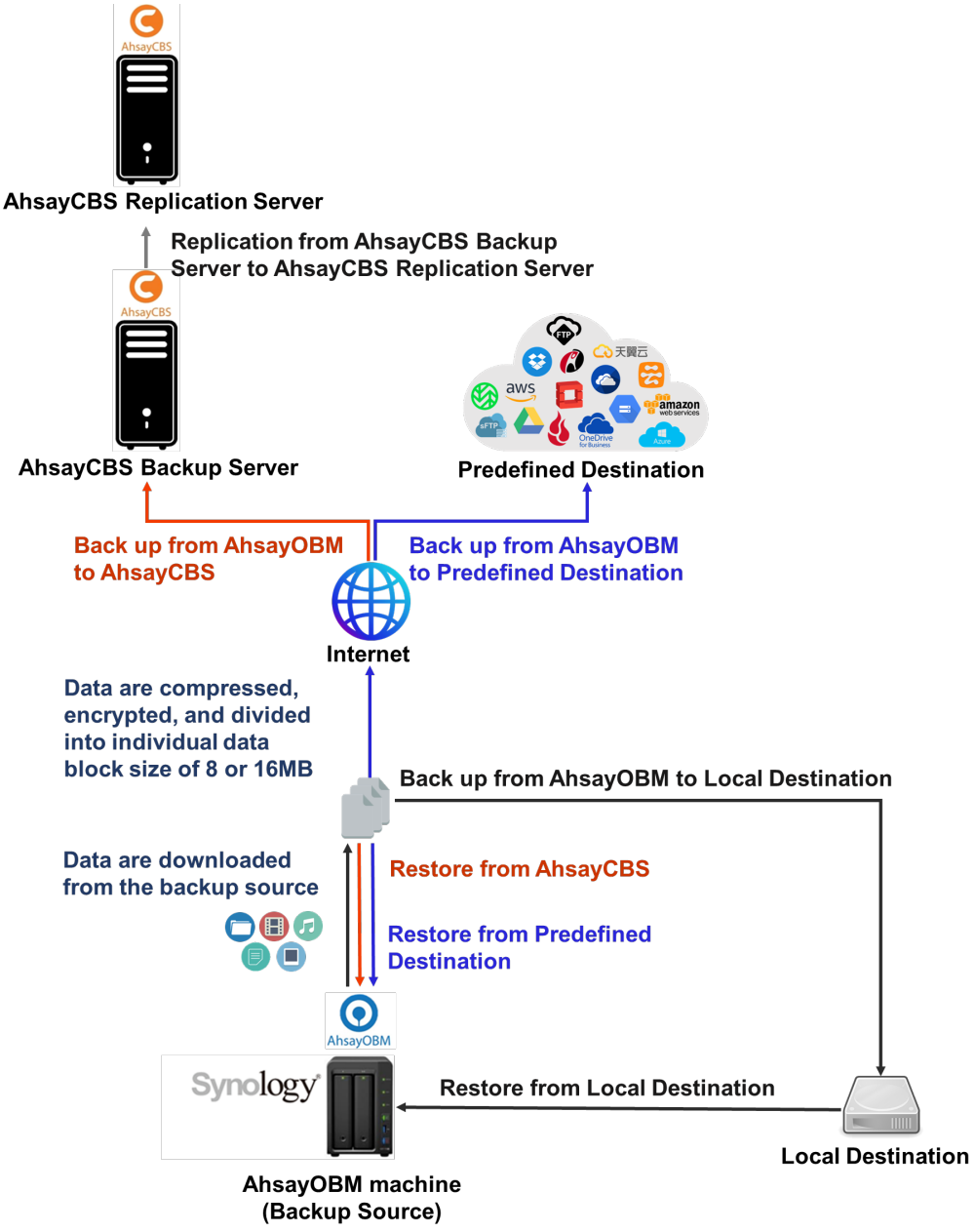
1.1 What is this software?

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.



2 Requirements for AhsayOBM on Synology NAS

2.1 Hardware Requirements

Refer to the following article for the list of supported Synology NAS models:

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

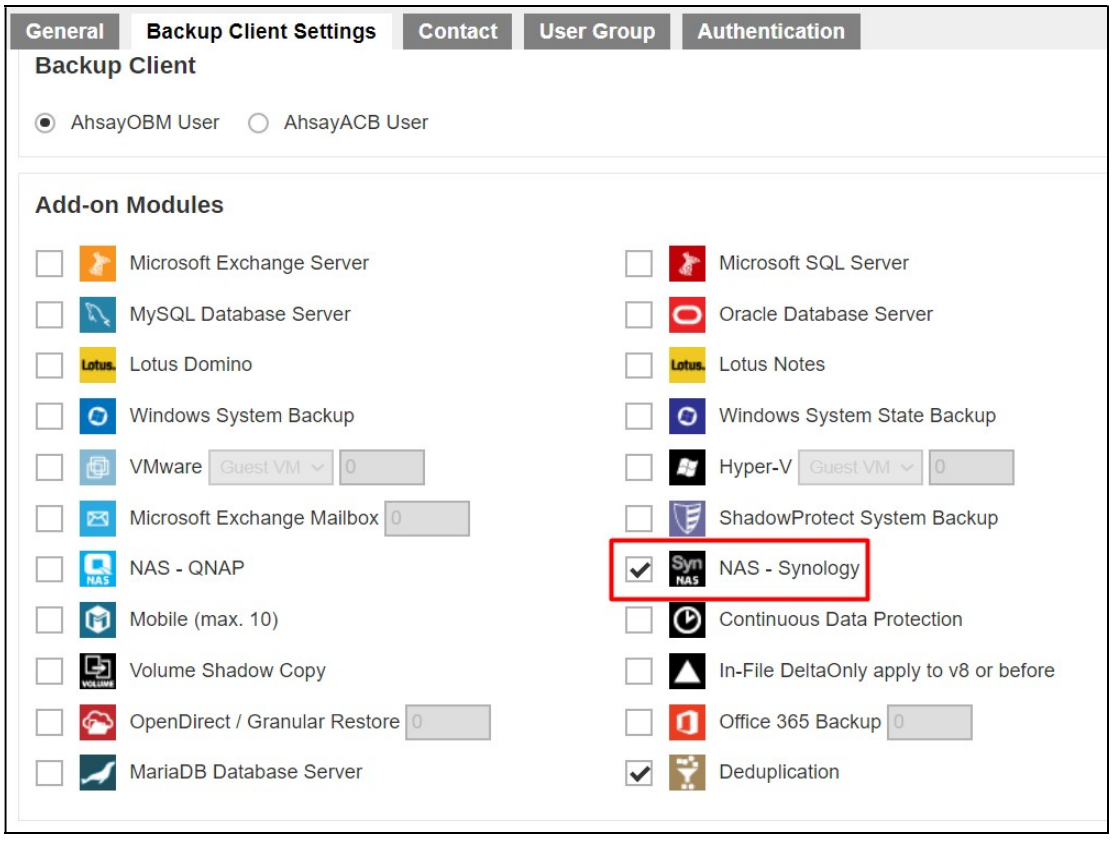
The latest version of AhsayOBM must be installed on the Synology NAS.

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.



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 v8, 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.

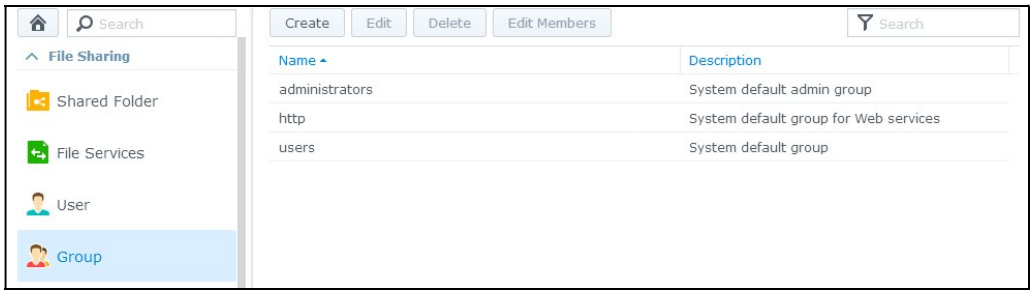
2.8 TCP Port Requirement

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.

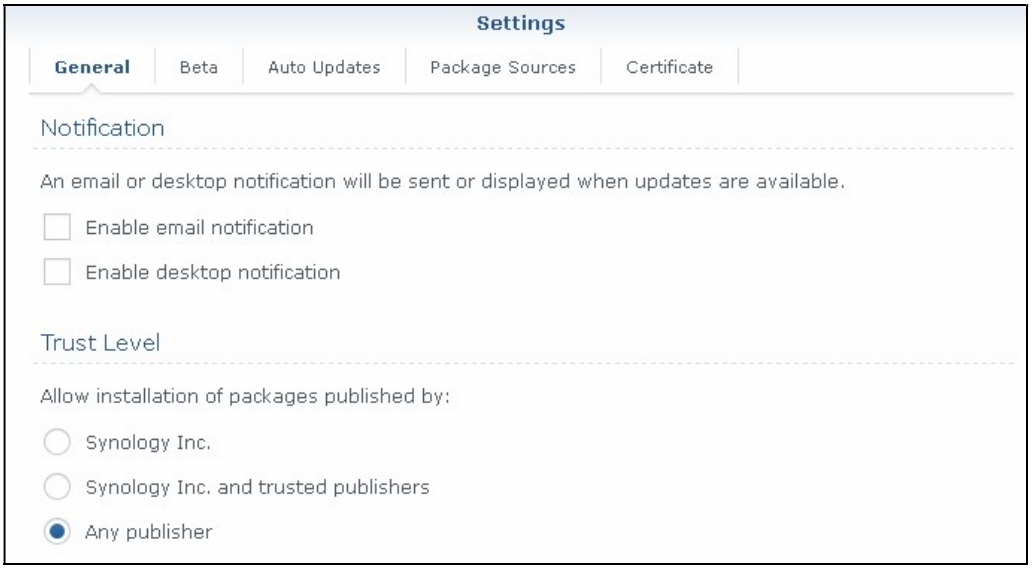
2.9 Synology NAS User Account Permission

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



2.10 Synology NAS Trust Level

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

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.

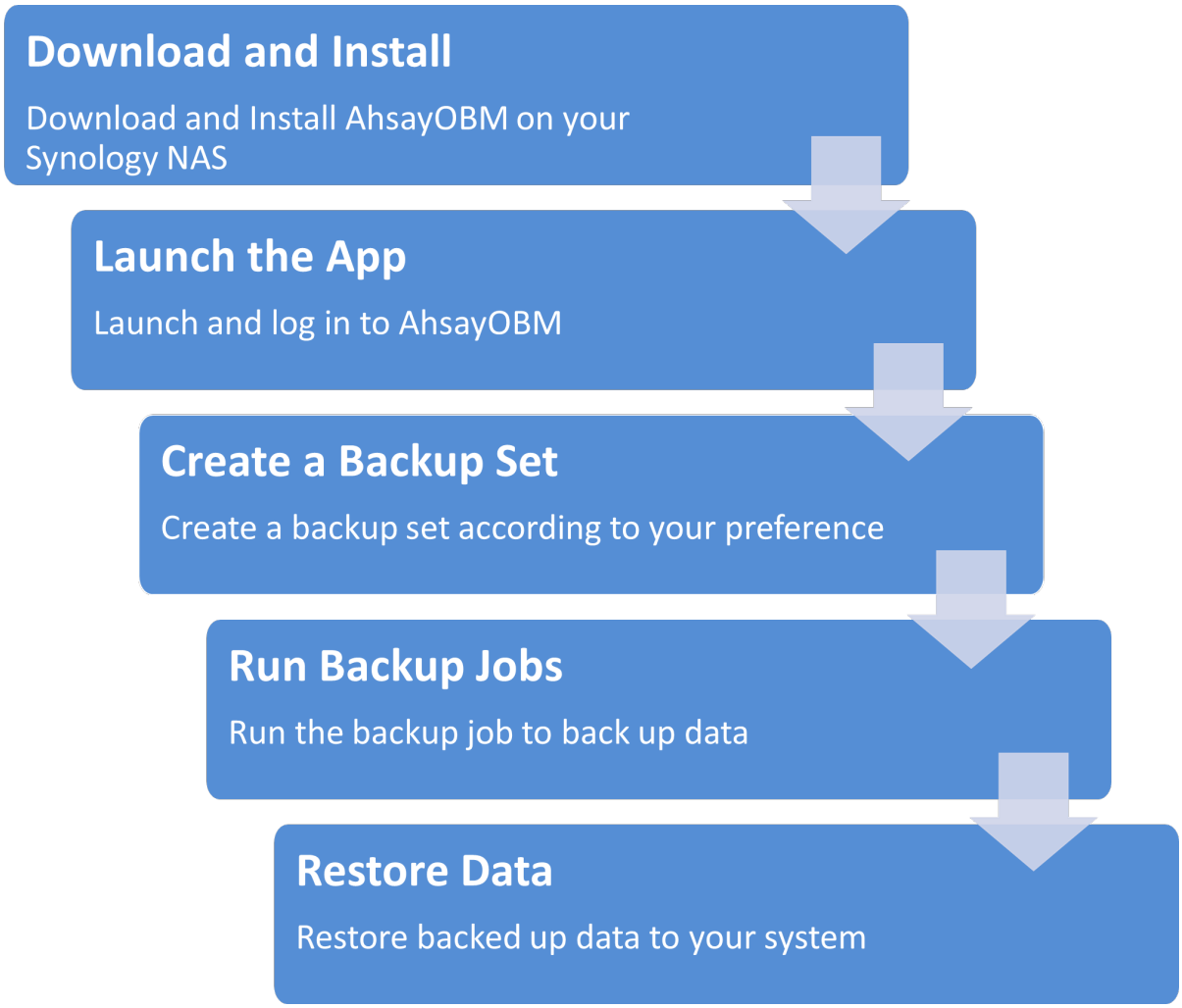
2.14 Supported Features from AhsayCBS Web Console

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.



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**.

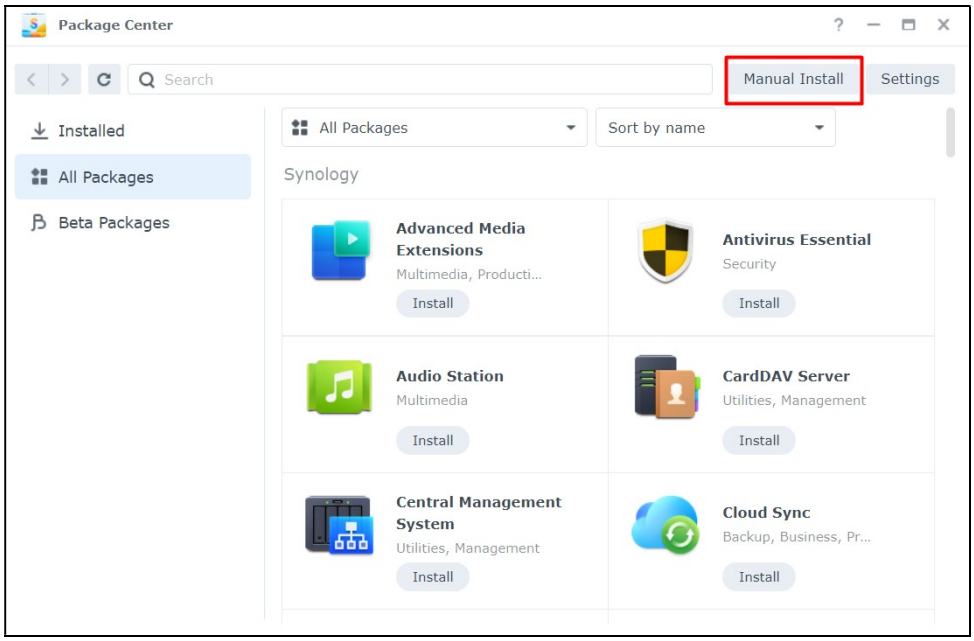
4.2 Install AhsayOBM using SPK online installer

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

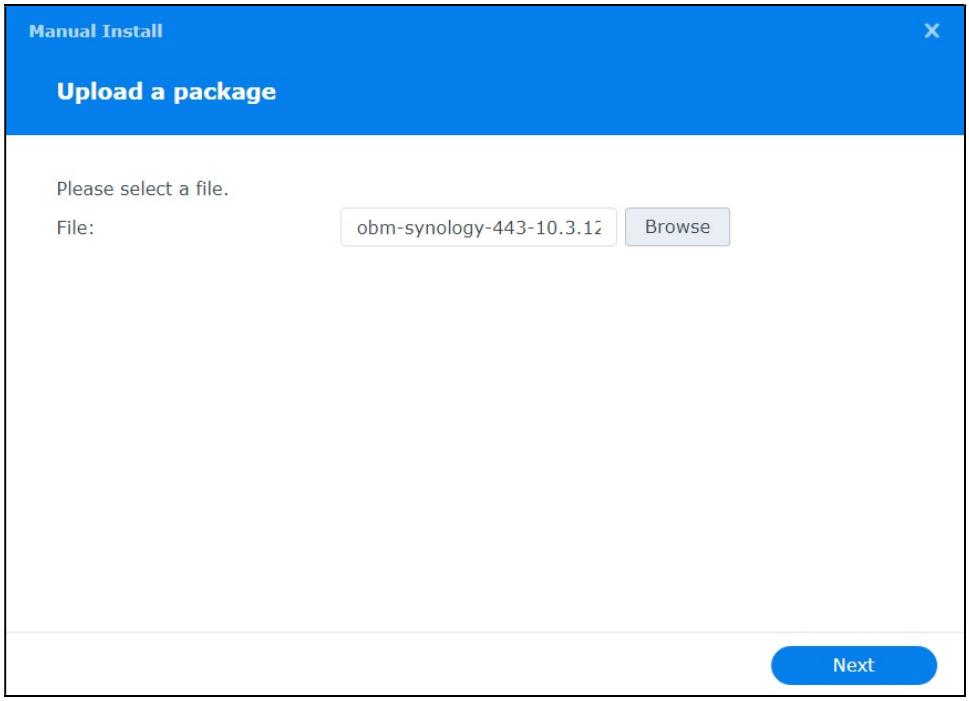
   NOTE: *Refer to the following Synology article for information on how to sign into DSM:*
   https://www.synology.com/en-us/knowledgebase/DSM/help/DSM/MainMenu/get_started

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

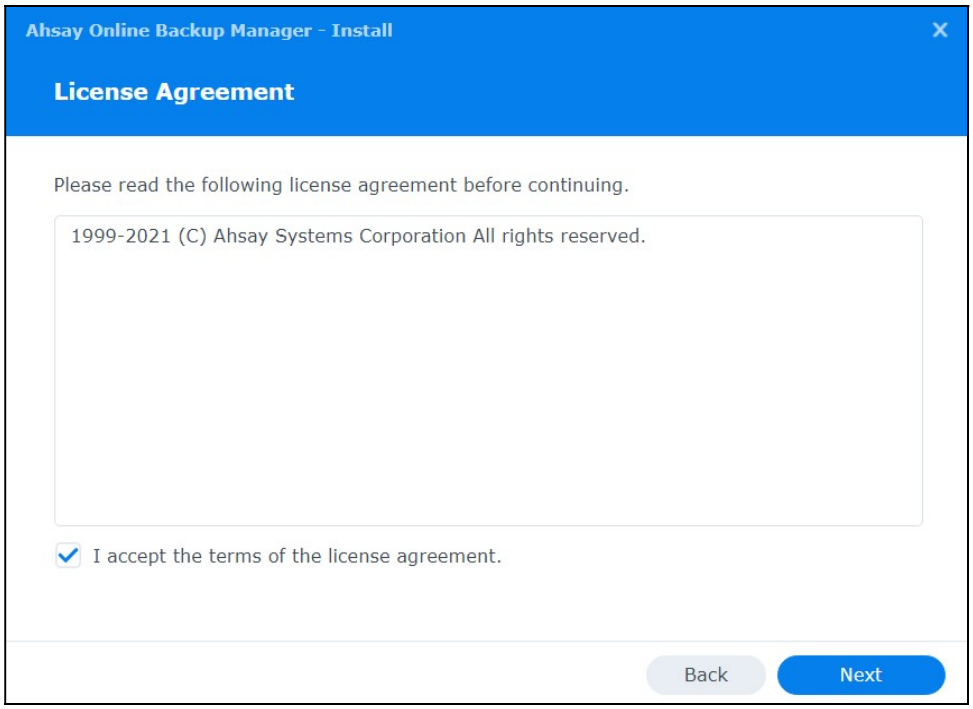
3. When the Package Center window appears, select **Manual Install**.



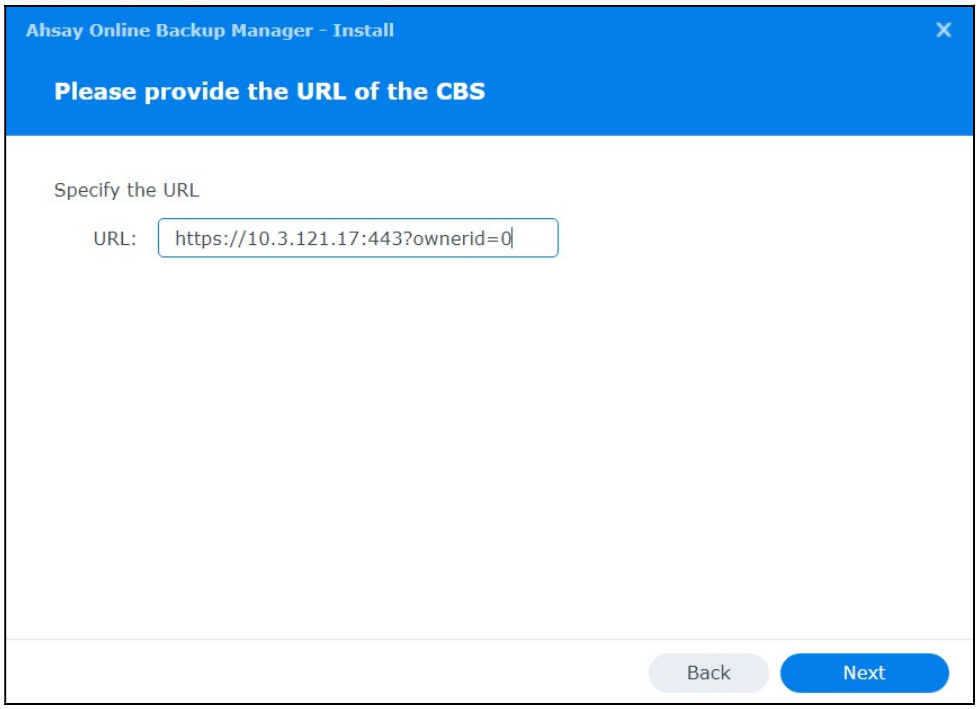
4. When the Manual Install window appears, click **Browse** to select the AhsayOBM SPK file which you have downloaded (e.g., obm-synology-443-10.3.121.17-https-0O.spk). Then, click **Next** to proceed.



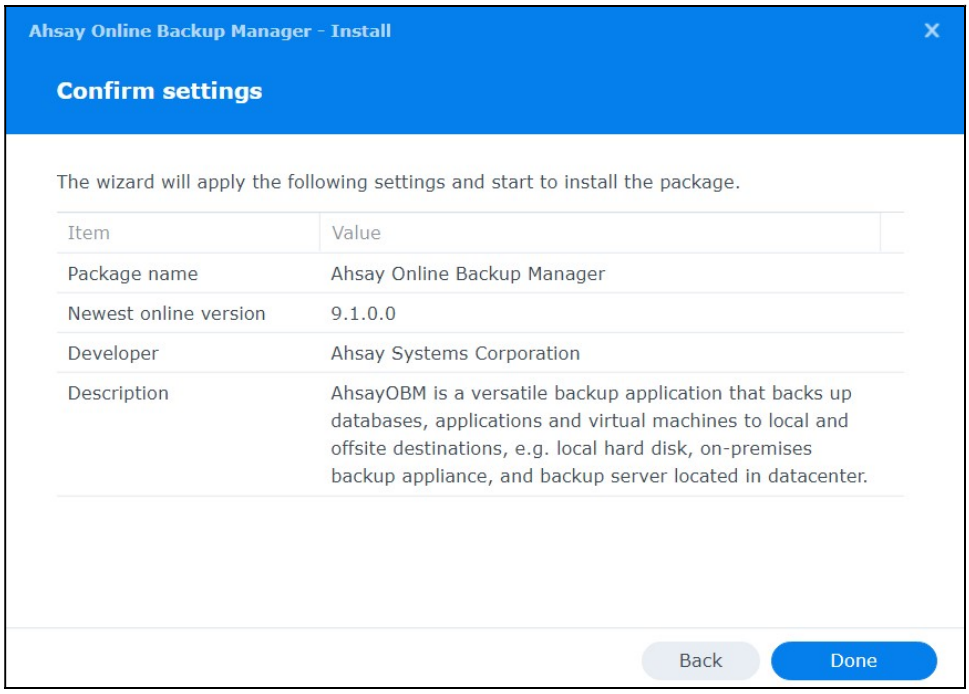
5. After reading the License Agreement carefully, tick the checkbox next to **I accept the terms of the license agreement**. Then, click **Next** to proceed.

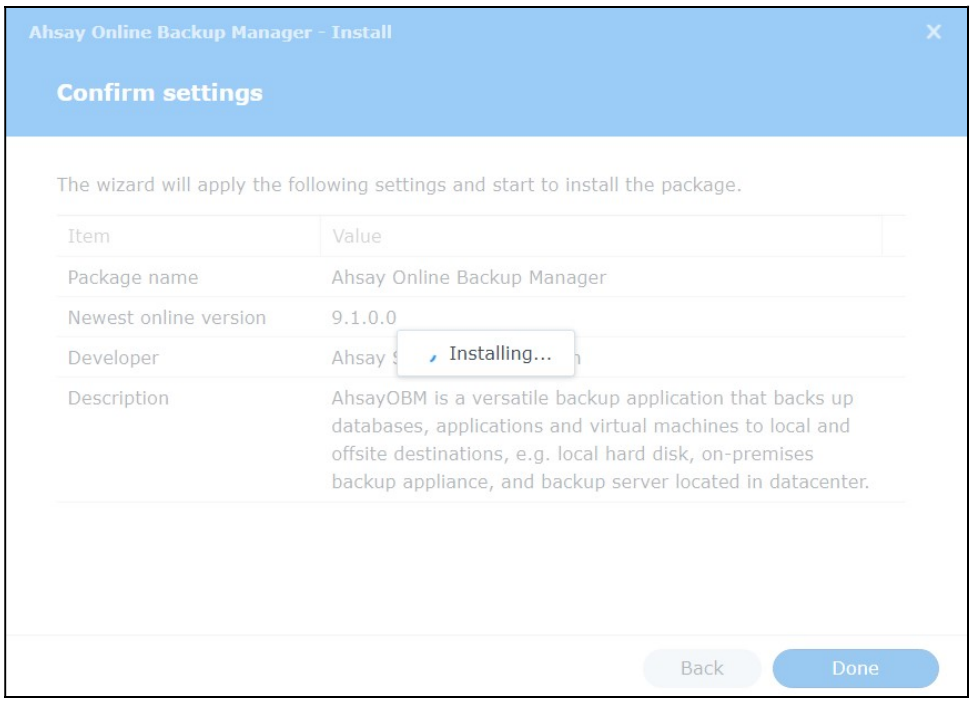


6. From the download page of your backup service provider's website, copy and paste the URL on the Ahsay Online Backup Manager – Install window, then click **Next** to proceed.

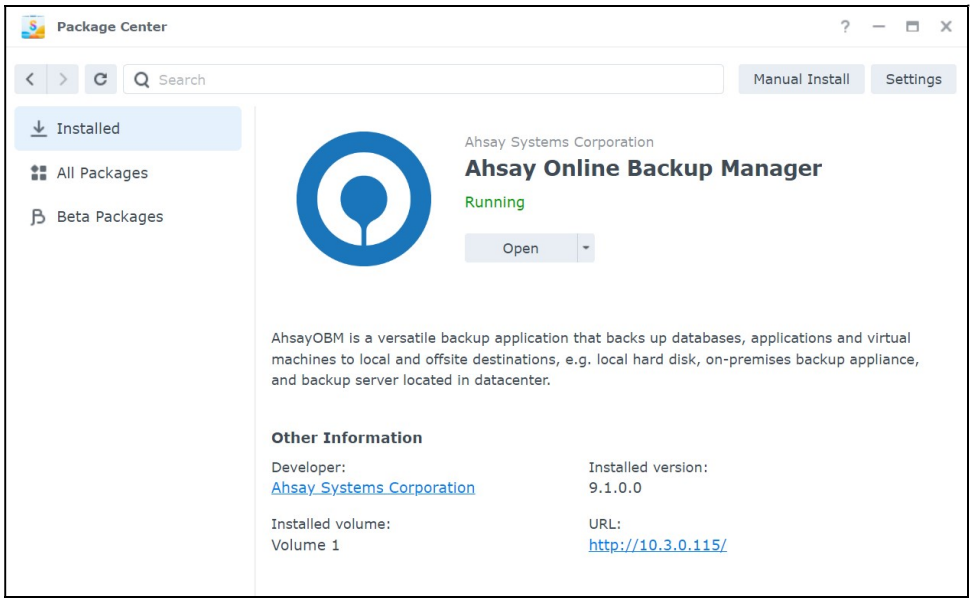


7. Review the following information on the screen, then click **Done** to start the installation of AhsayOBM.





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



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

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

11. 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.

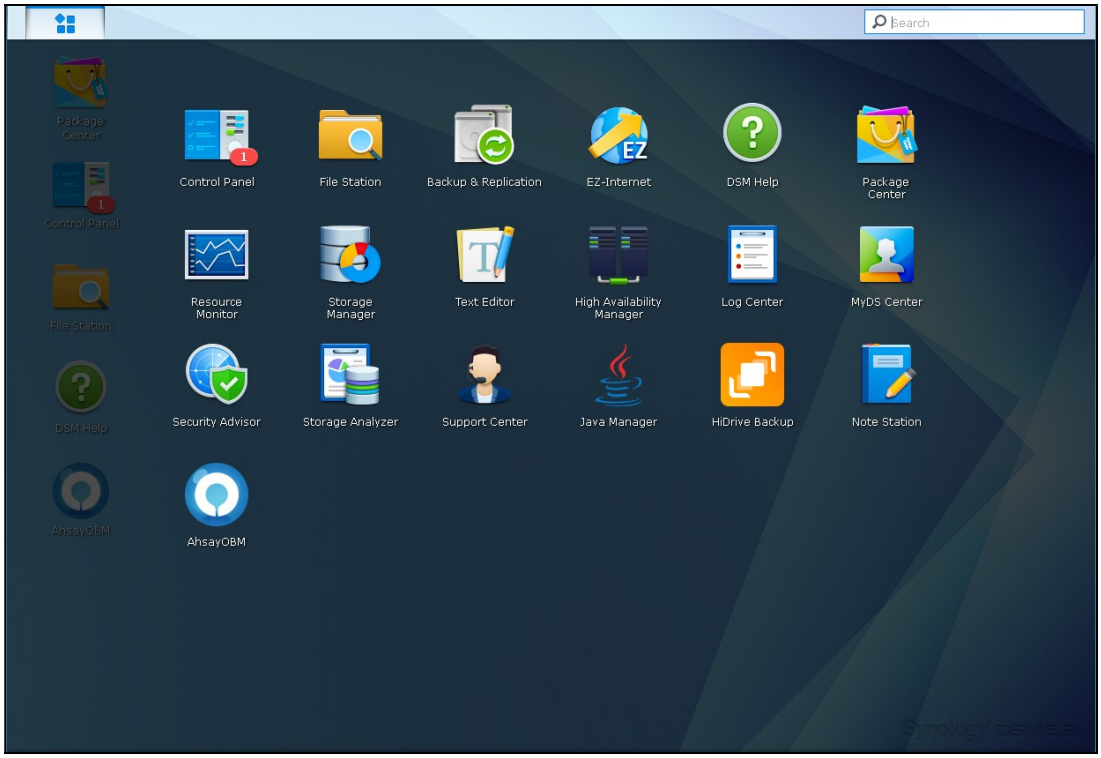
```
admin@dev-ds215j:/volume1/@appstore/AhsayOBM/obm/bin$
/volume1/@appstore/AhsayOBM/obm/bin/Scheduler.sh

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 Start AhsayOBM

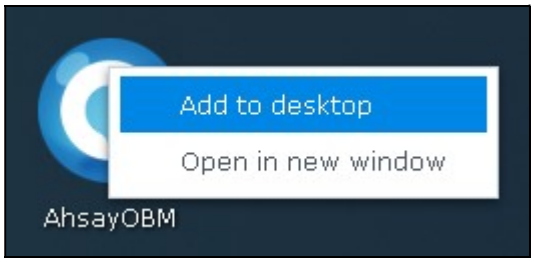
5.1 Add an AhsayOBM Shortcut Icon to the Desktop

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

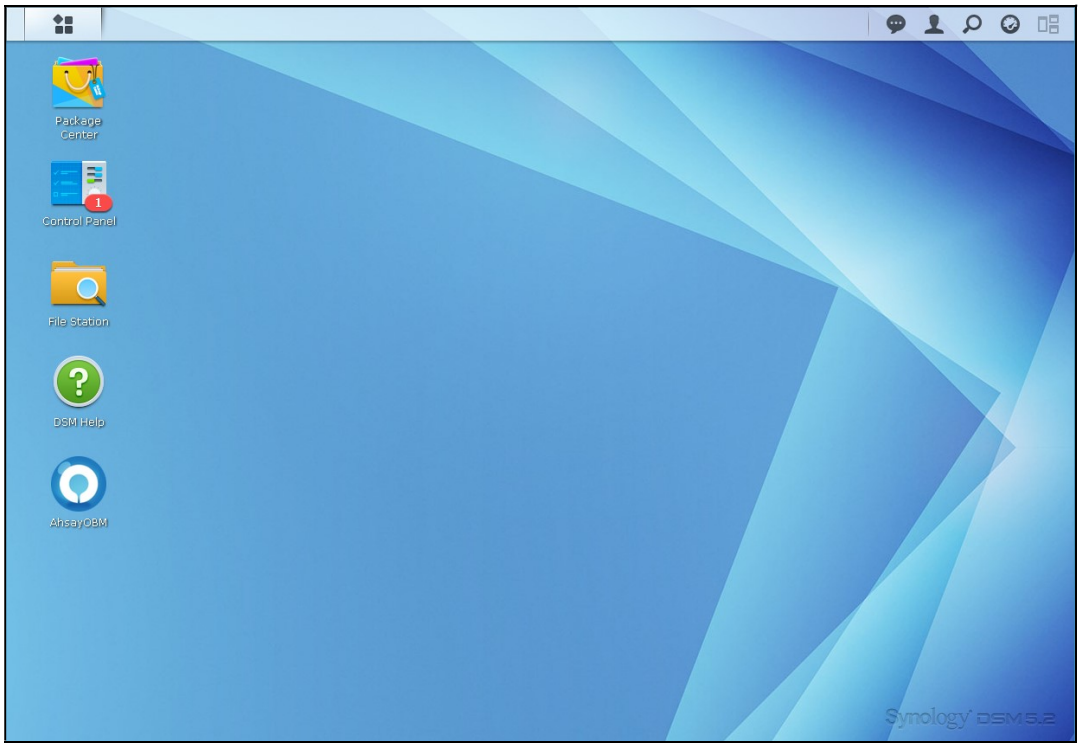
2. All application icons will be shown. Look for the **AhsayOBM** icon.



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

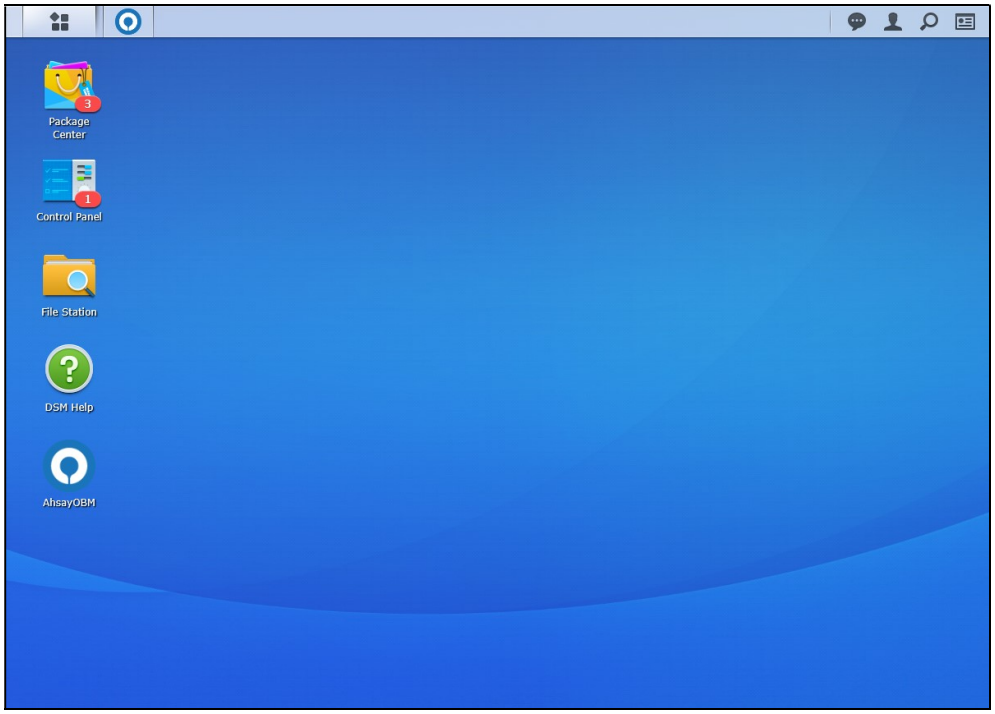


4. The AhsayOBM shortcut icon will be added to the desktop.

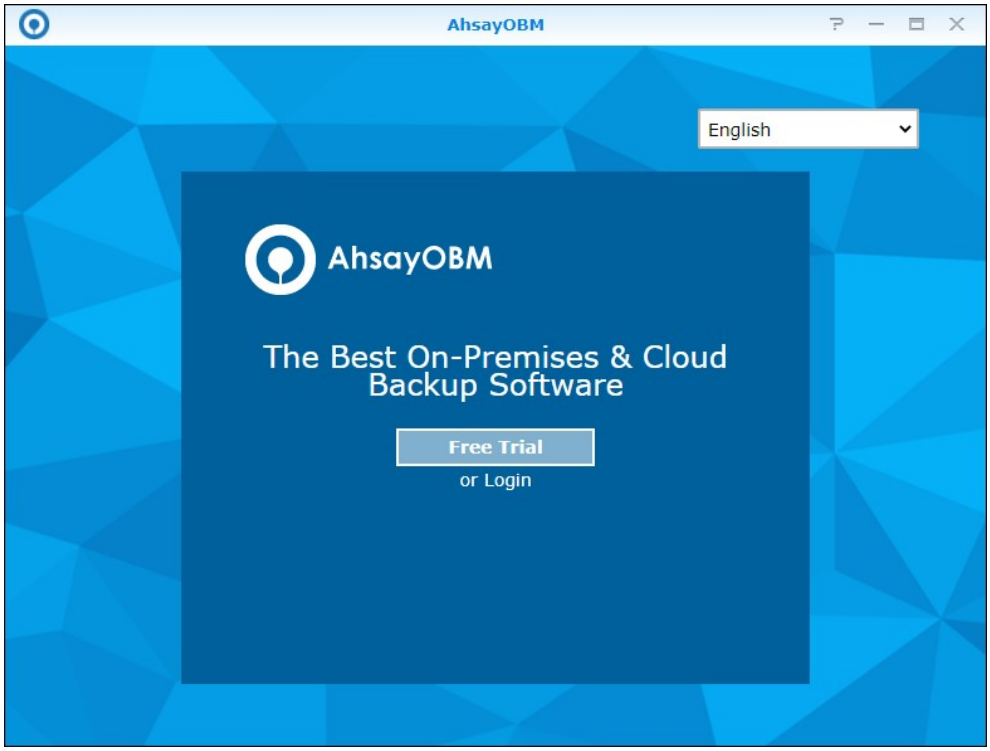


5.2 Login to AhsayOBM

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



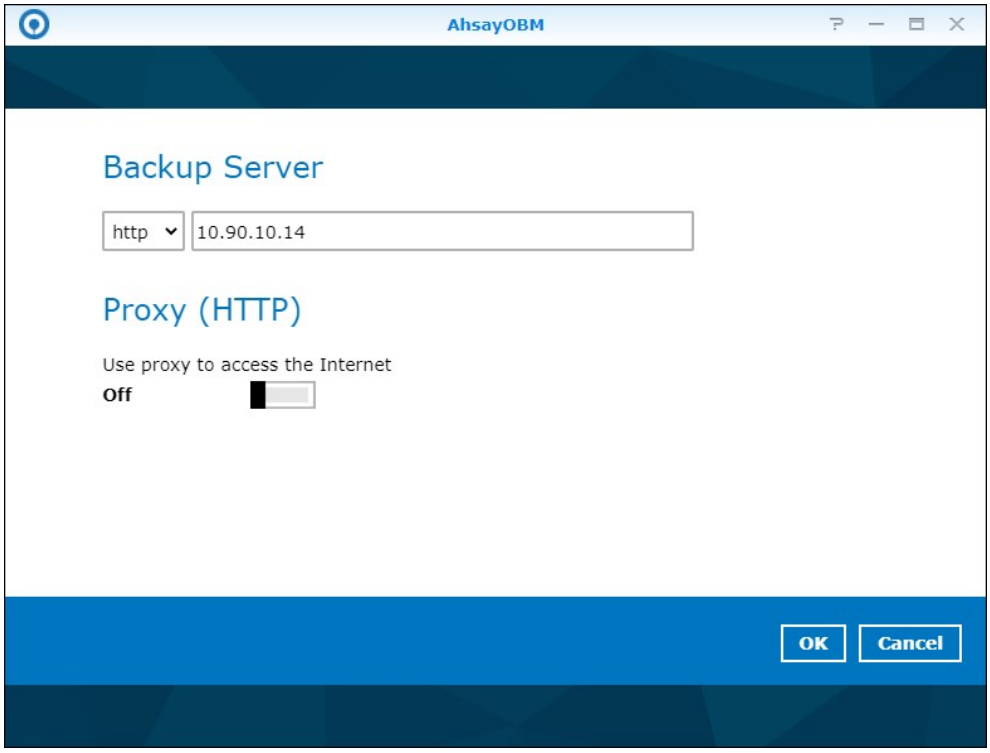
2. The Free Trial registration menu may be displayed when you login for the first time. Click **Login** if you already have an AhsayOBM account or click **Free Trial** to register for a trial backup account. For more details, refer to Appendix D: Create Free Trial Account in AhsayOBM.



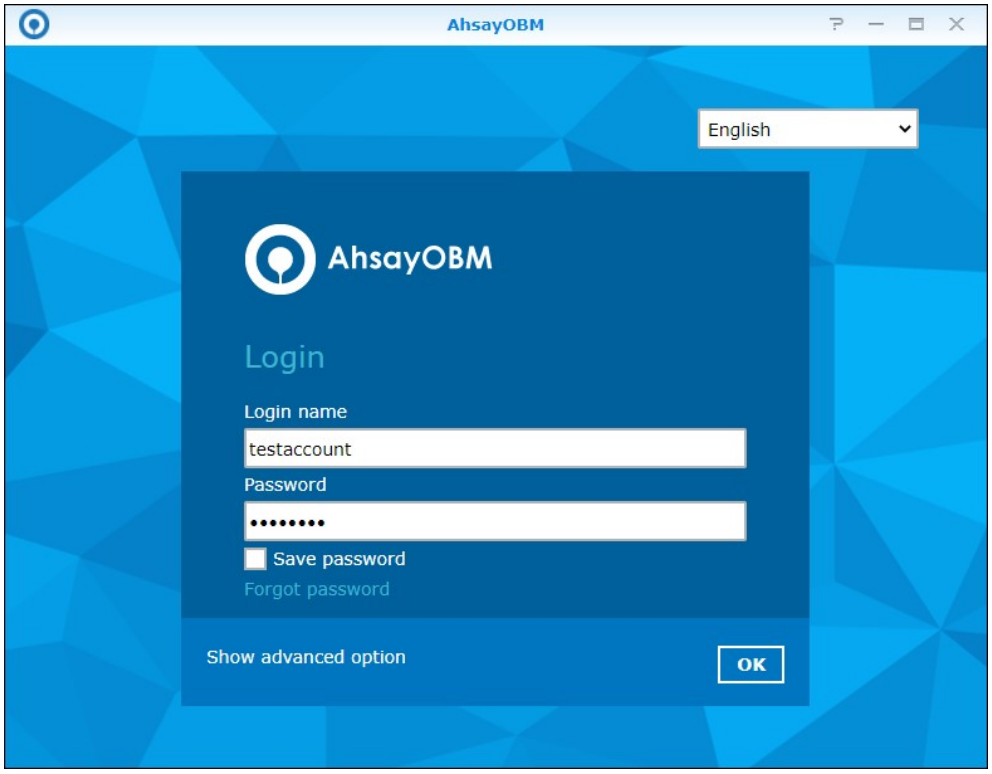
NOTE

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**.



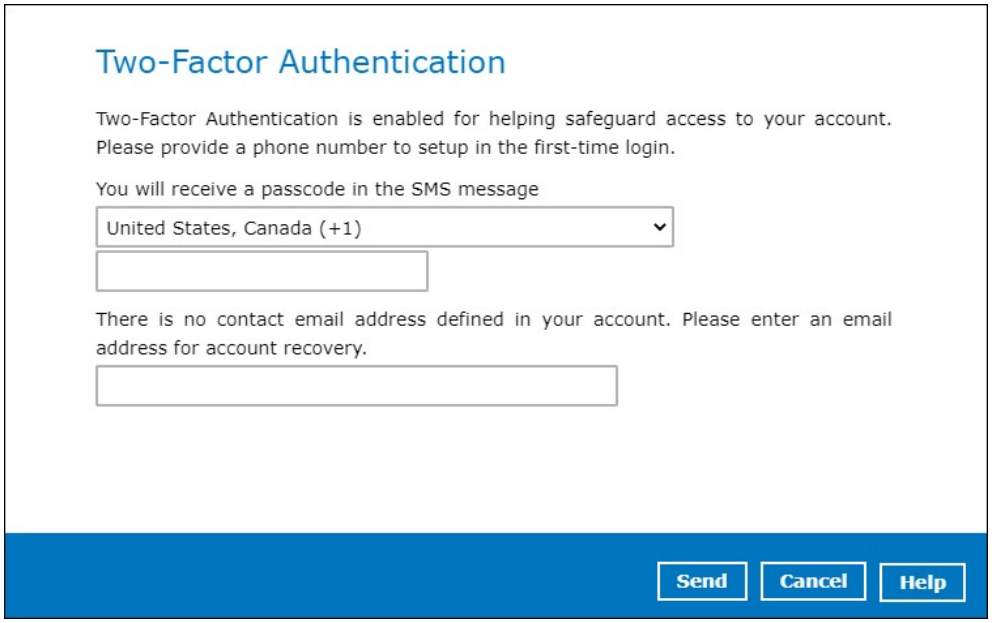
4. Enter the Login Name and Password of your AhsayOBM account provided by your backup service provider. Then, click **OK** to login.



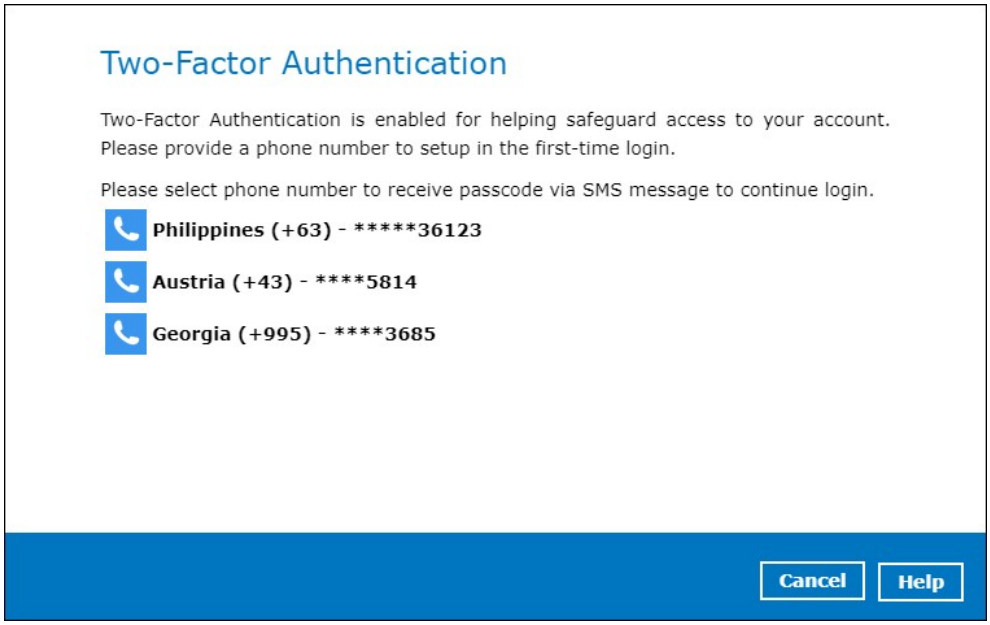
NOTE

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 details.

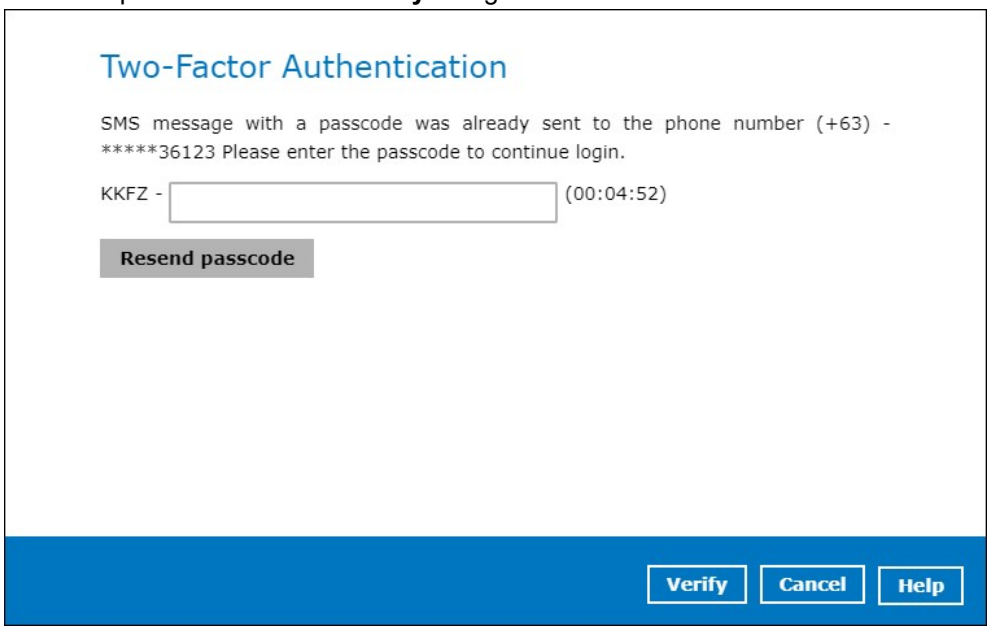
5. If Two-Factor Authentication is enabled, the following screen will appear. If not, skip to Step 7. For first time log in, this will be the screen displayed. Select your country code and enter your phone number. Also enter your email address. Click **Send** to receive the passcode.



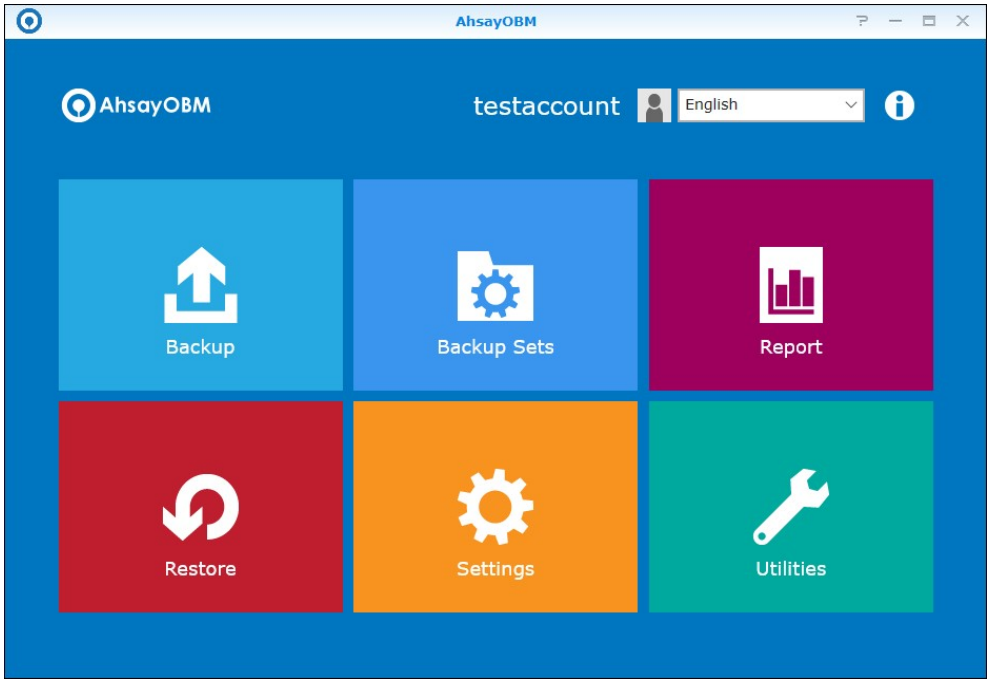
For succeeding login this will be the screen displayed. Select your phone number.



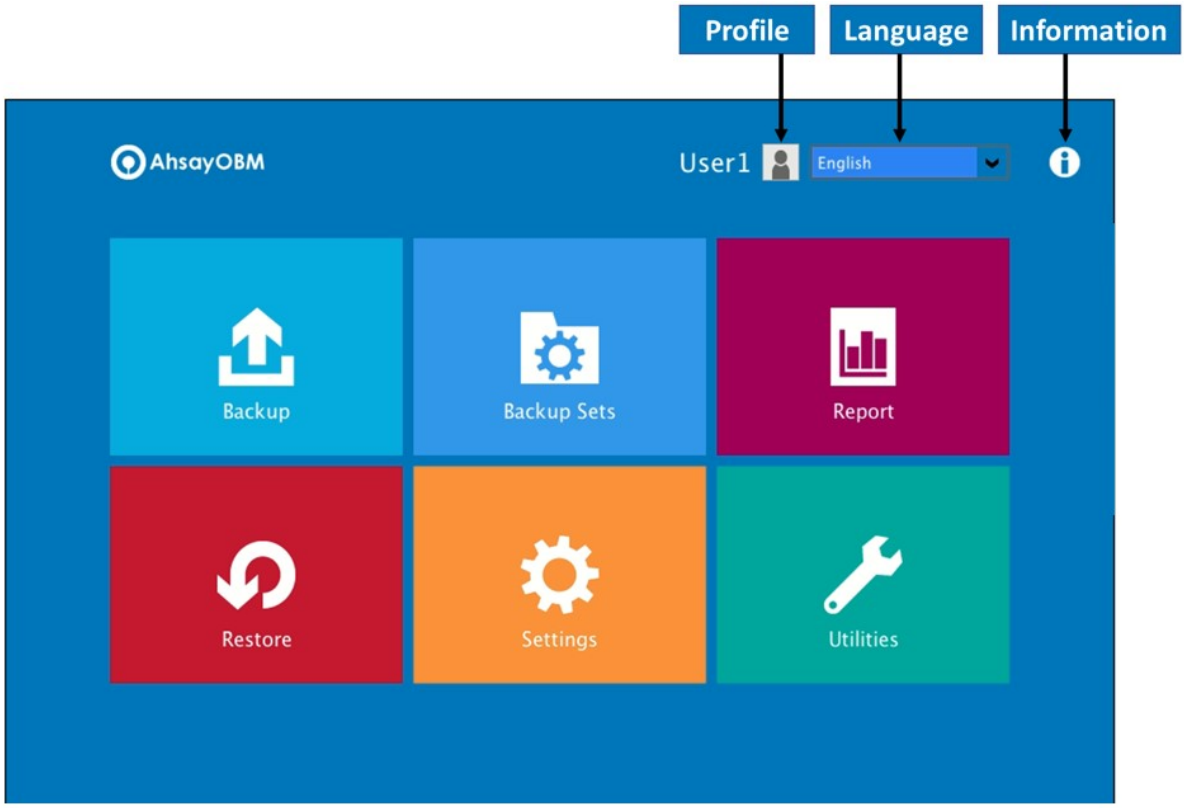
6. Enter the passcode and click **Verify** to login.



7. Upon successful login, the following screen will be displayed.



6 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**

6.1 Profile

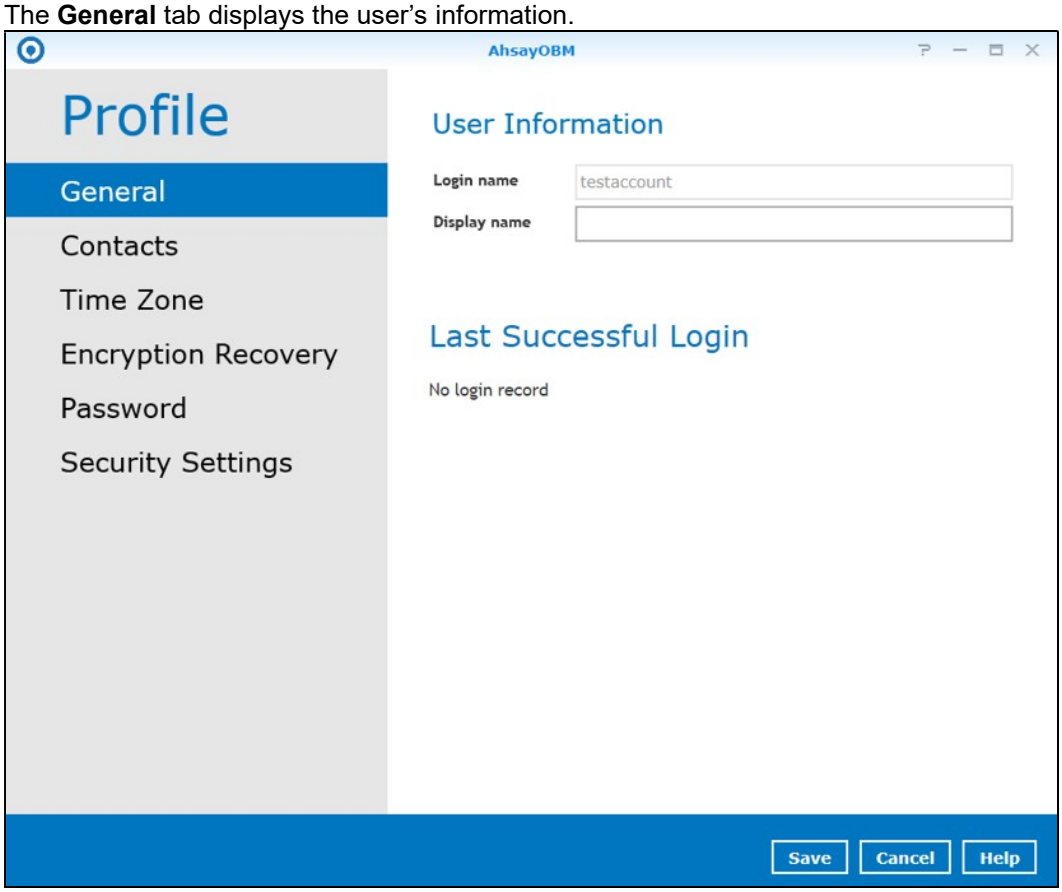
The **Profile** icon shows the profile settings that can be modified by the user.

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.)

6.1.1 General

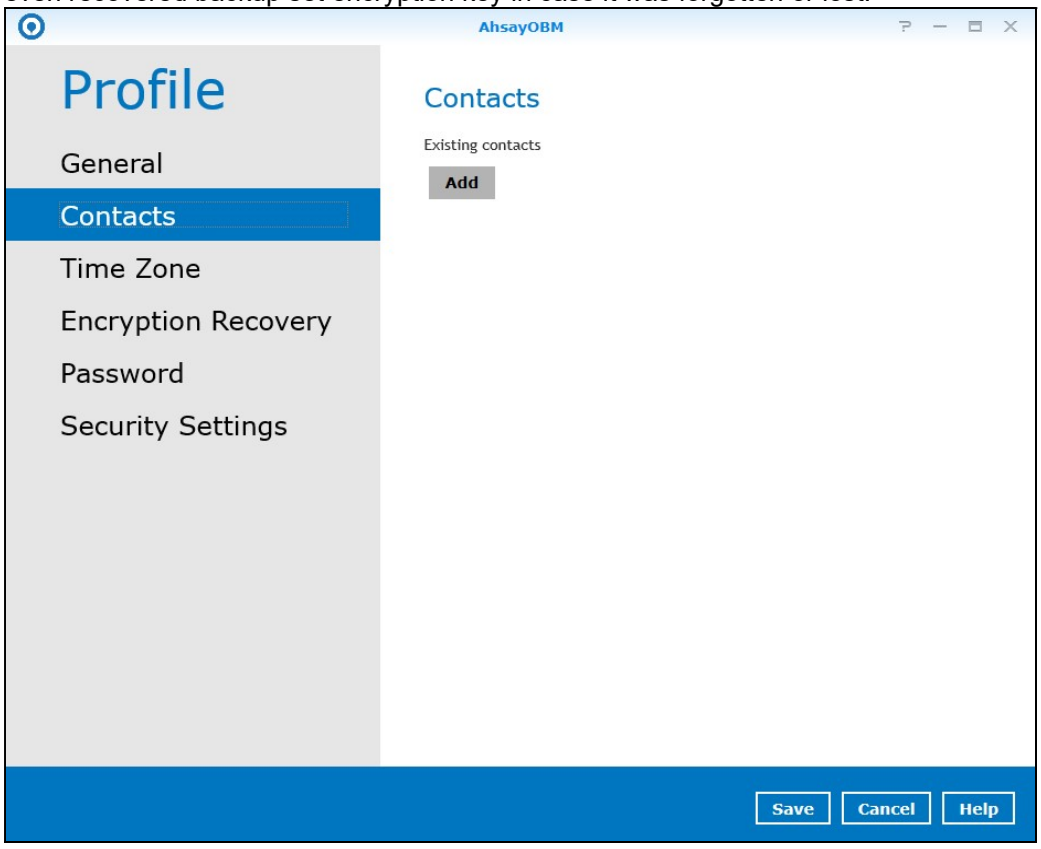
The **General** tab displays the user's information.



- 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.

6.1.2 Contacts

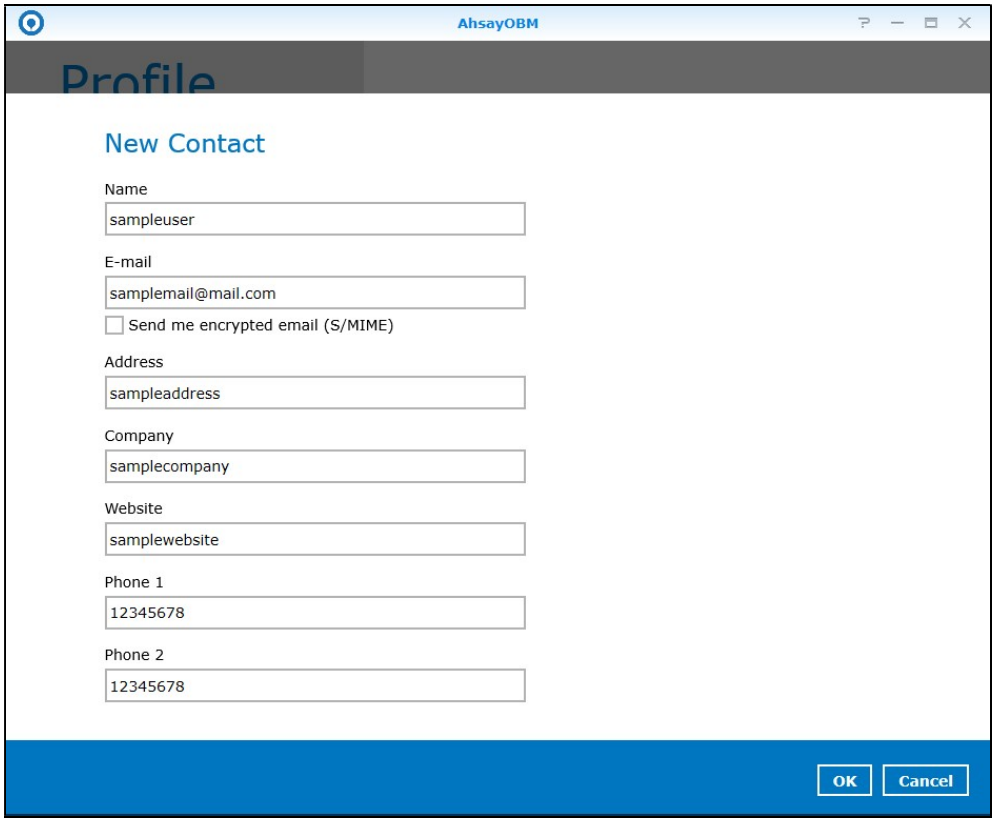
This refers to the contact information of the user. You can also add multiple contacts or modify existing contact information. Having this filled in will help us in sending backup and daily reports and even recovered backup set encryption key in case it was forgotten or lost.



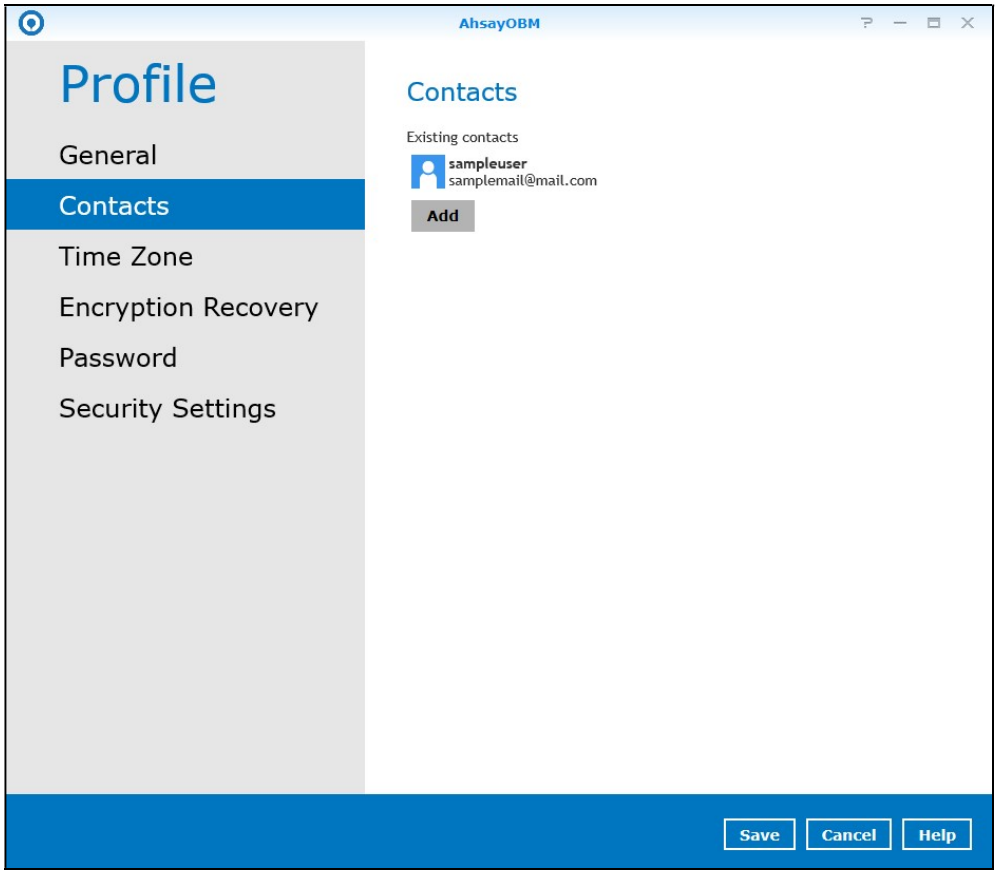
To add a new contact, follow the instructions below:

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



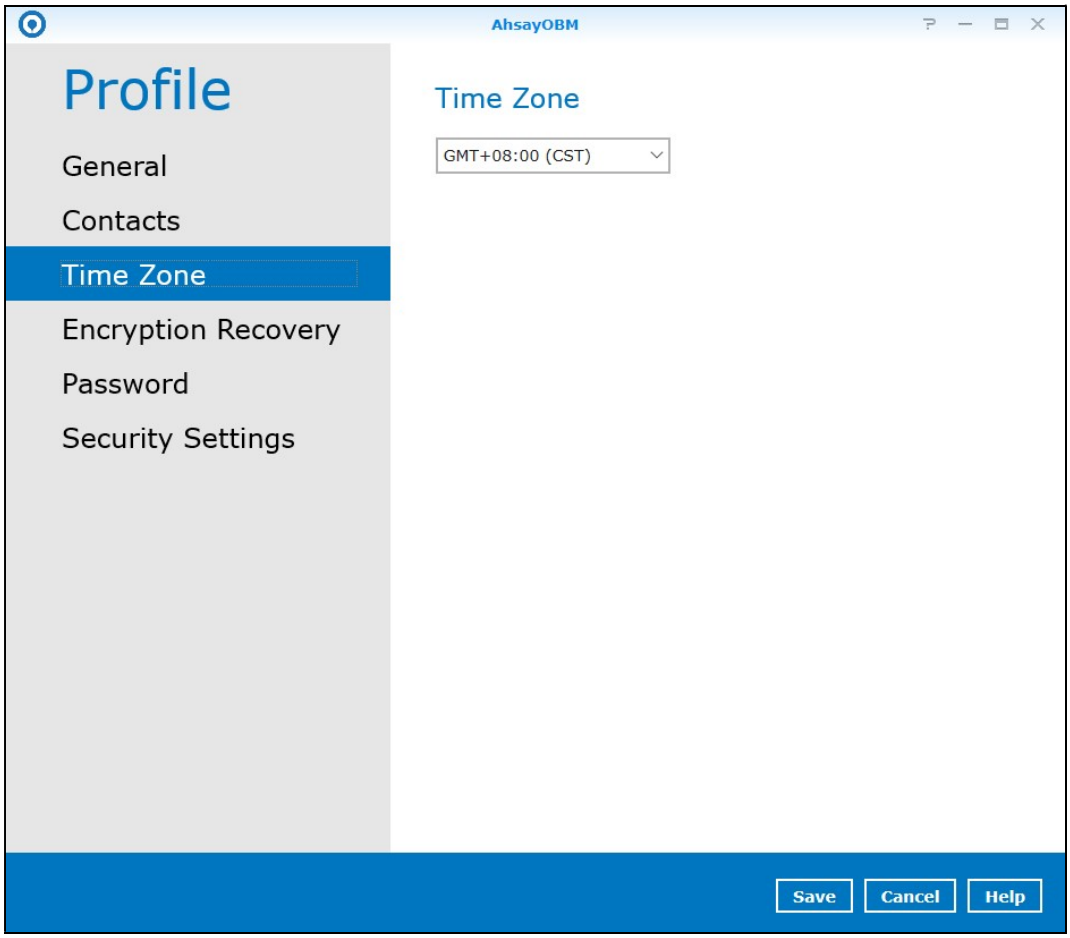
3. Click the **Save** button to store the contact information.



NOTE: You can add multiple contacts here

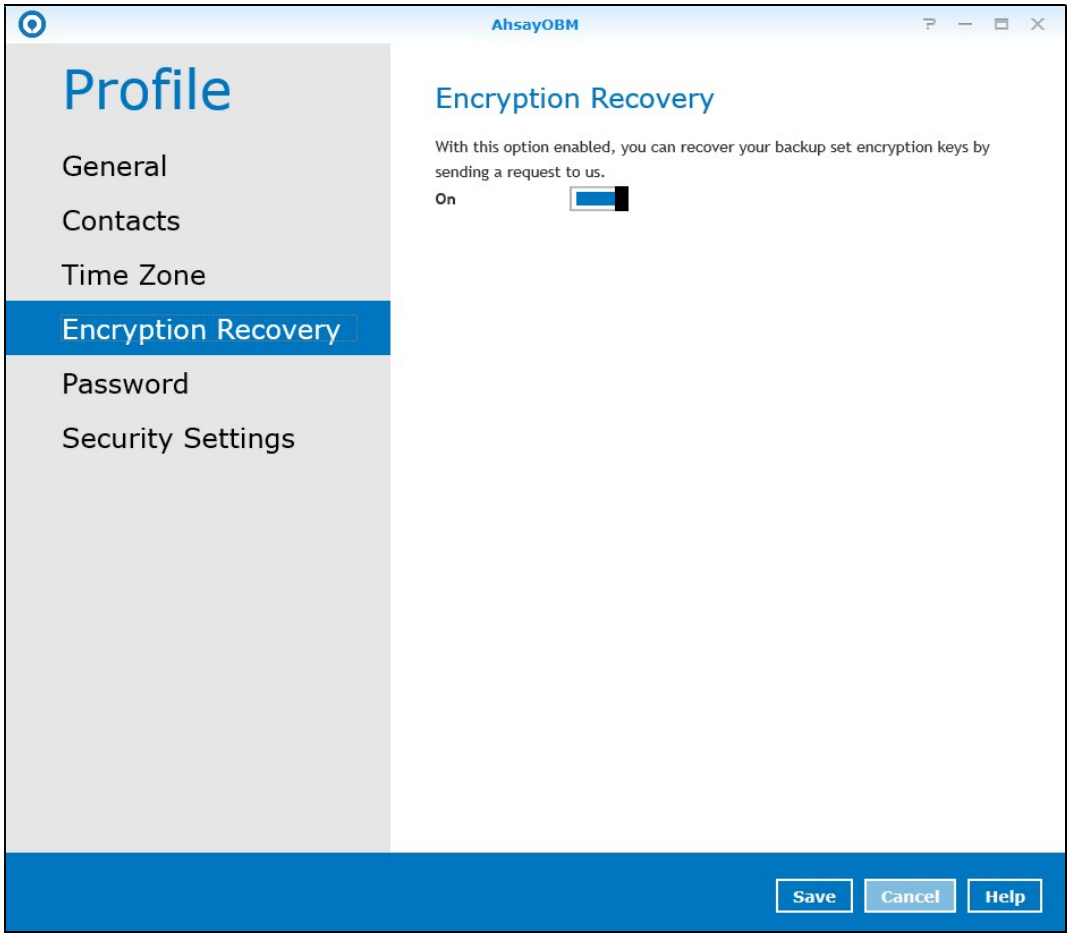
6.1.3 Time Zone

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.



6.1.4 Encryption Recovery

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

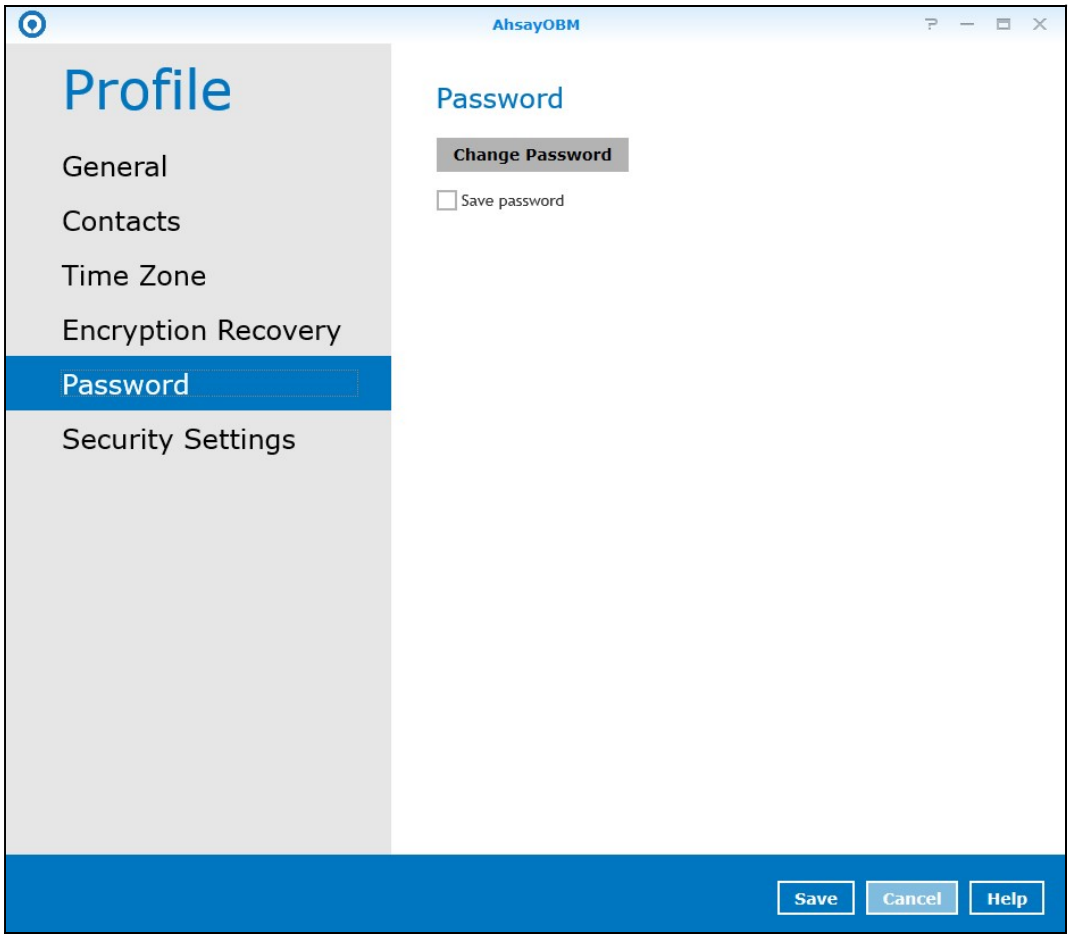


NOTE

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

6.1.5 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.

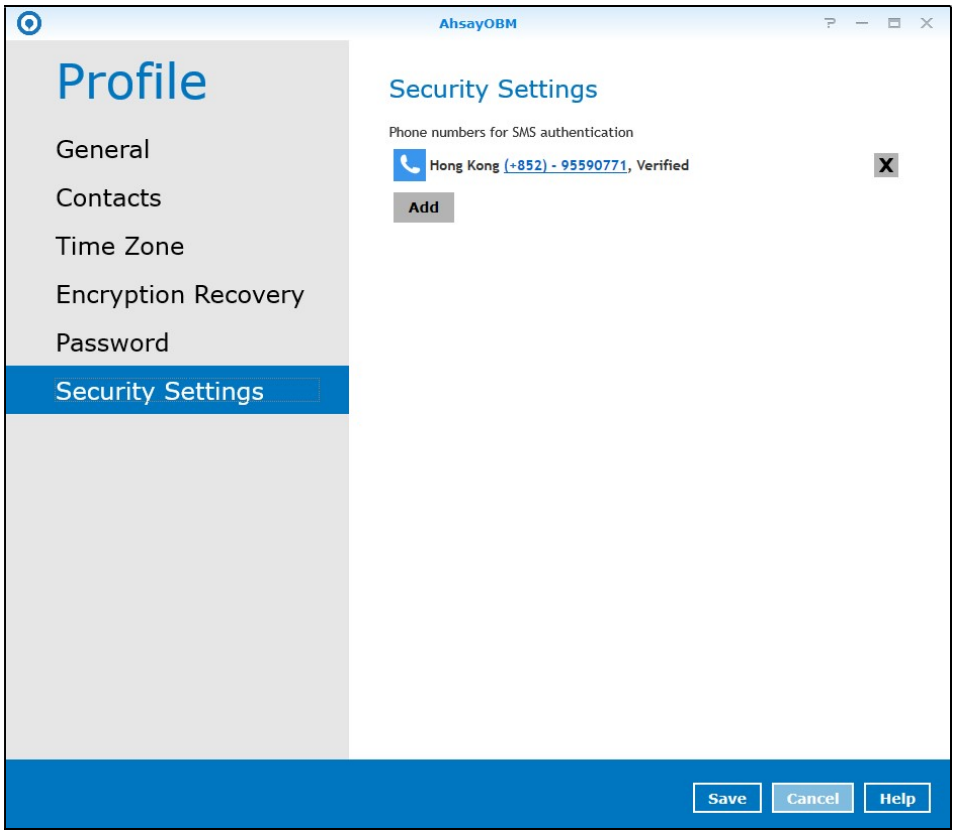


NOTE

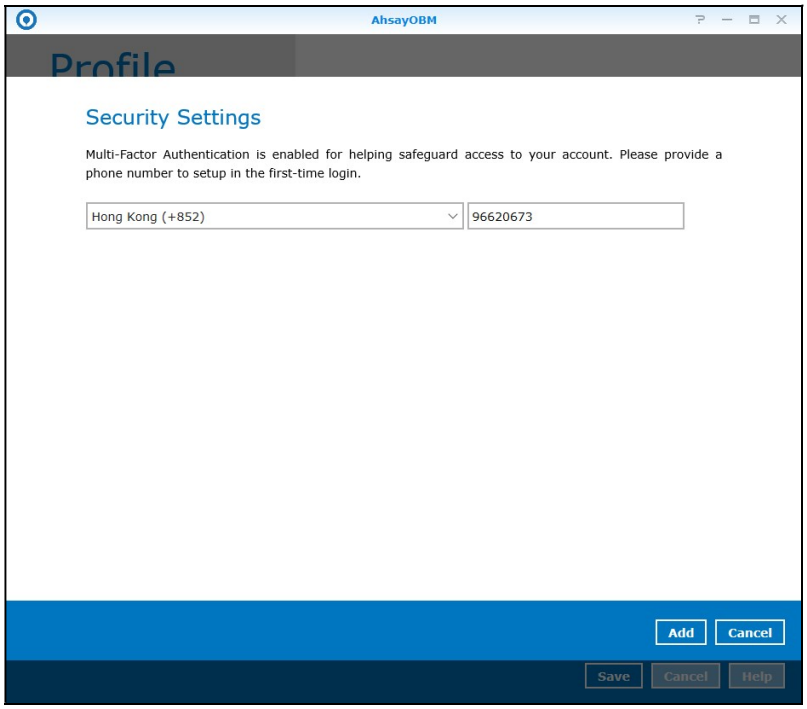
The **Save password** option may not be available. This depends on the settings of your backup service provider. Please contact your backup service provider for more details.

6.1.7 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.

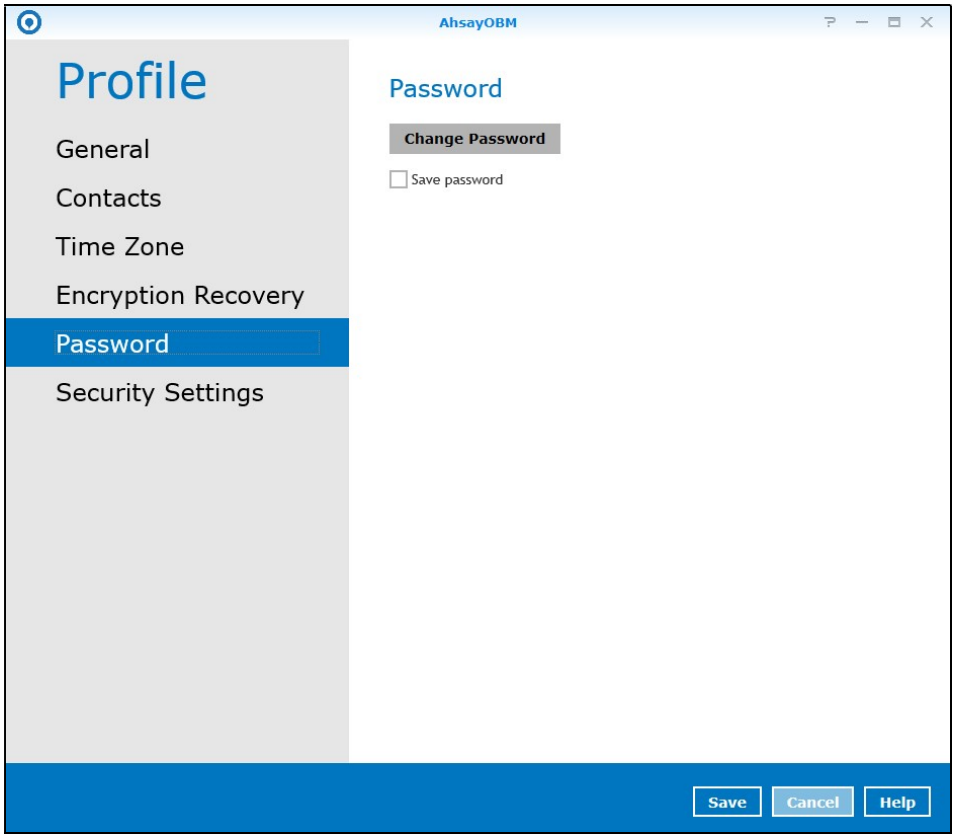


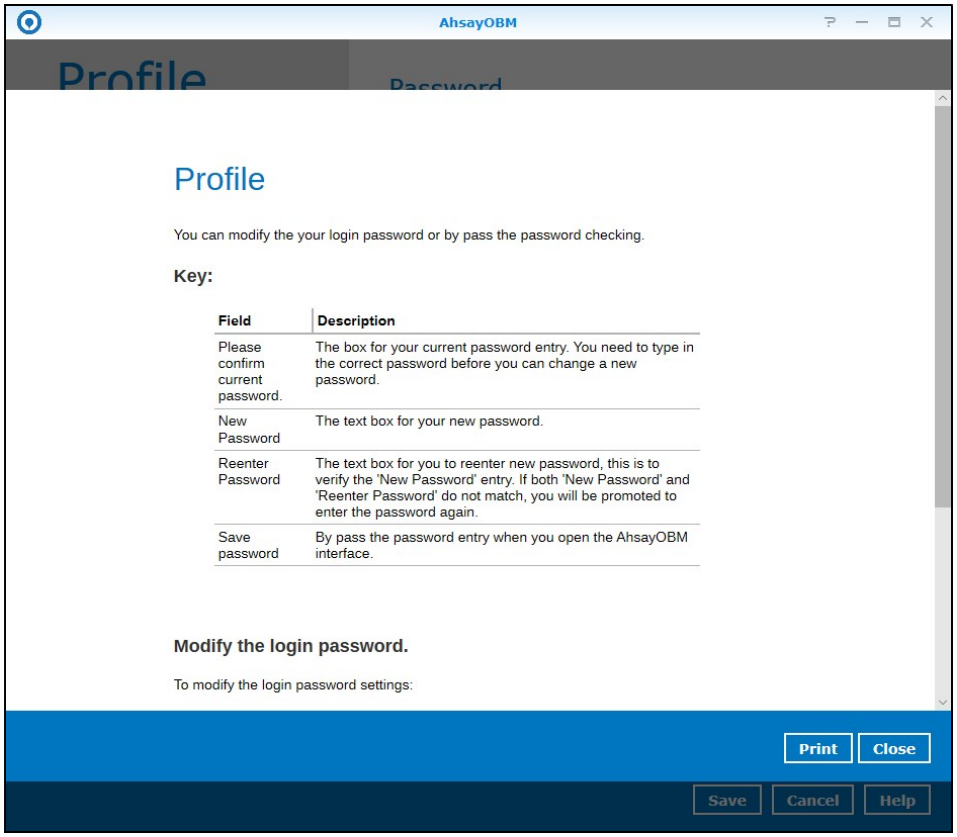
1. Click the **Add** button.
2. Select the country and enter the phone number, then click **Add**.



6.2 Online Help

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





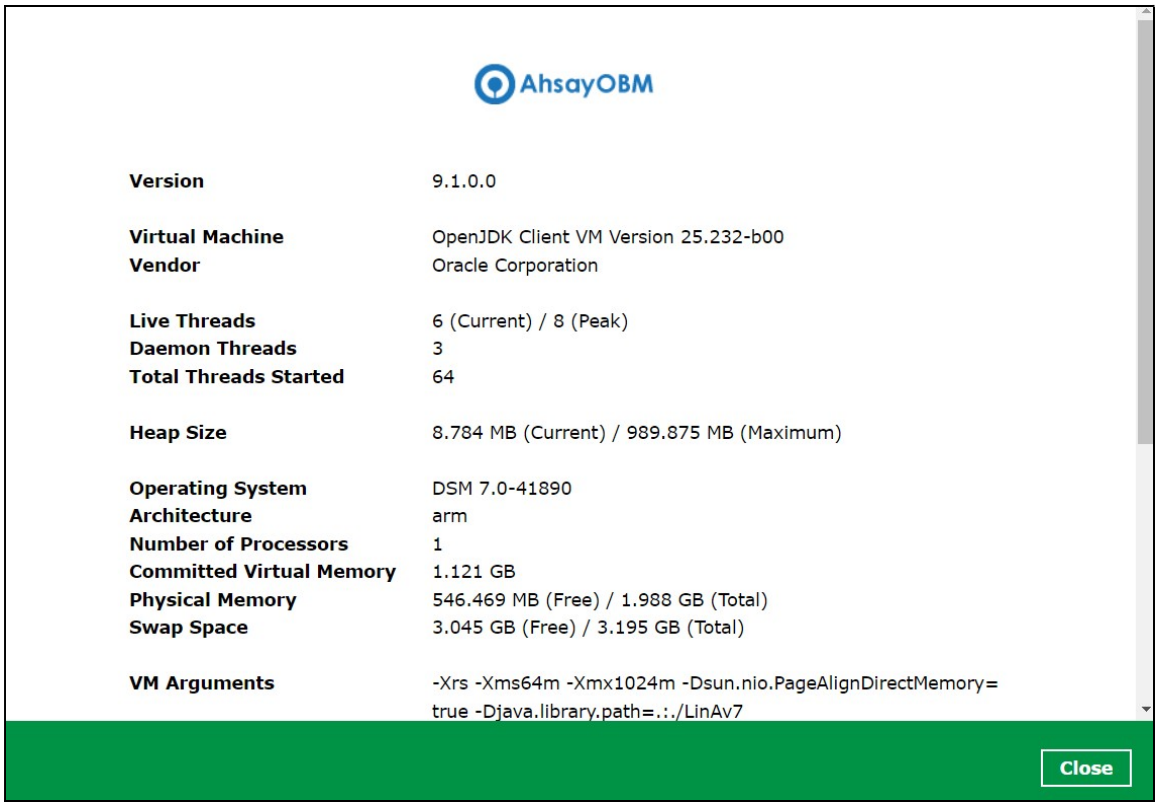
6.3 Language

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.

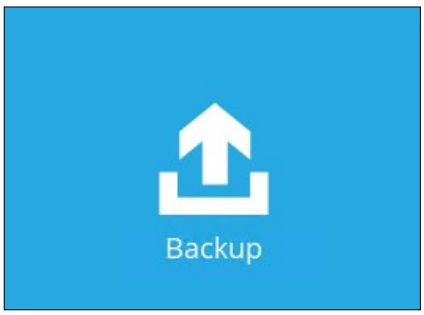
6.4 Information

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



6.5 Backup

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



For instructions on how to start a backup, refer to Chapter 9.2 Start a Manual Backup.

6.6 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.

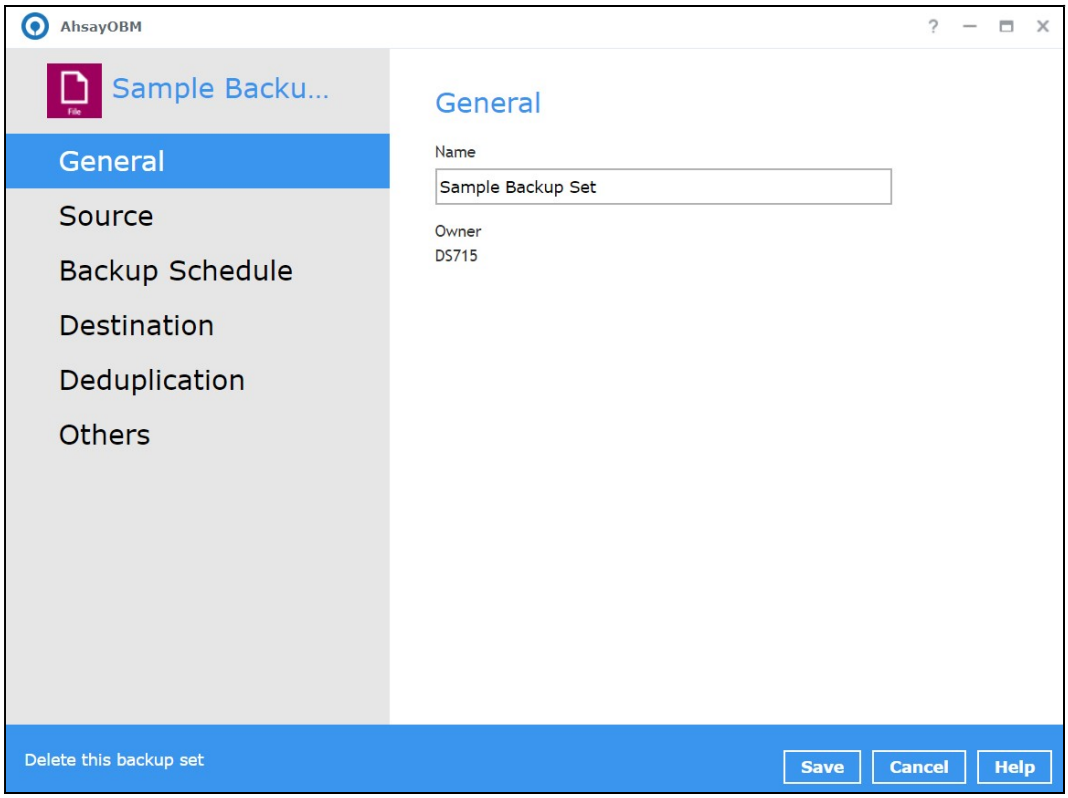
Backup Set Settings

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.

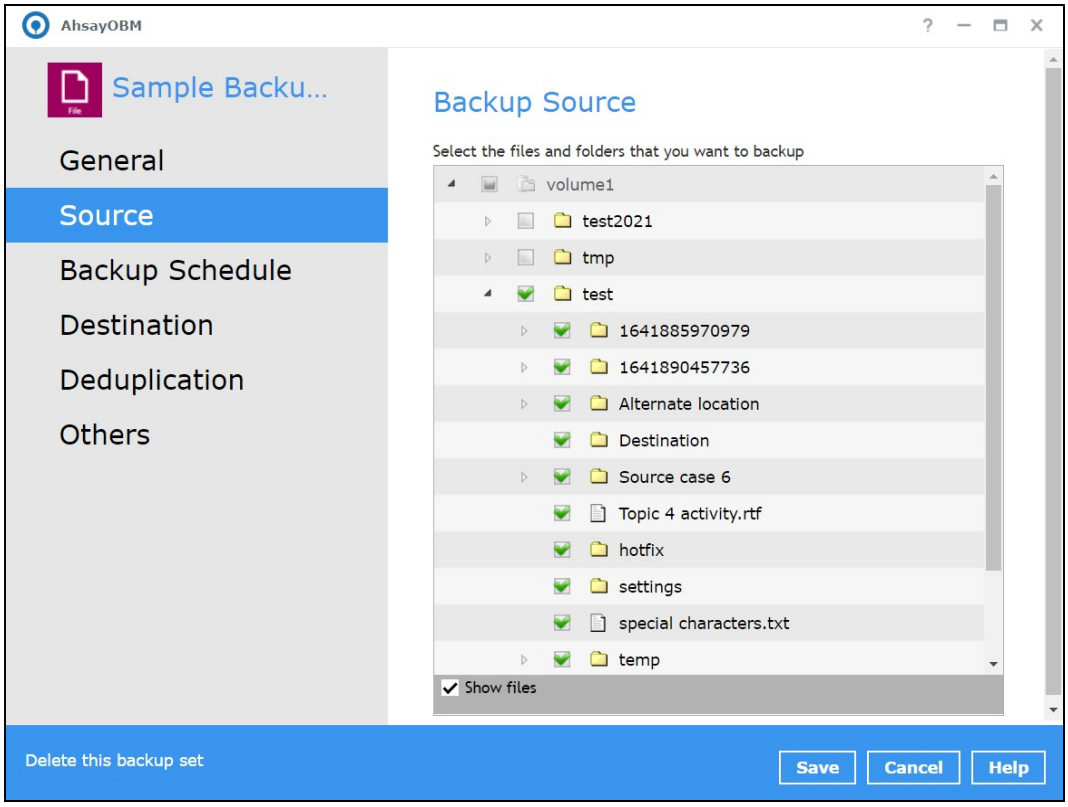


To modify the backup set name, follow the instructions below:

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.

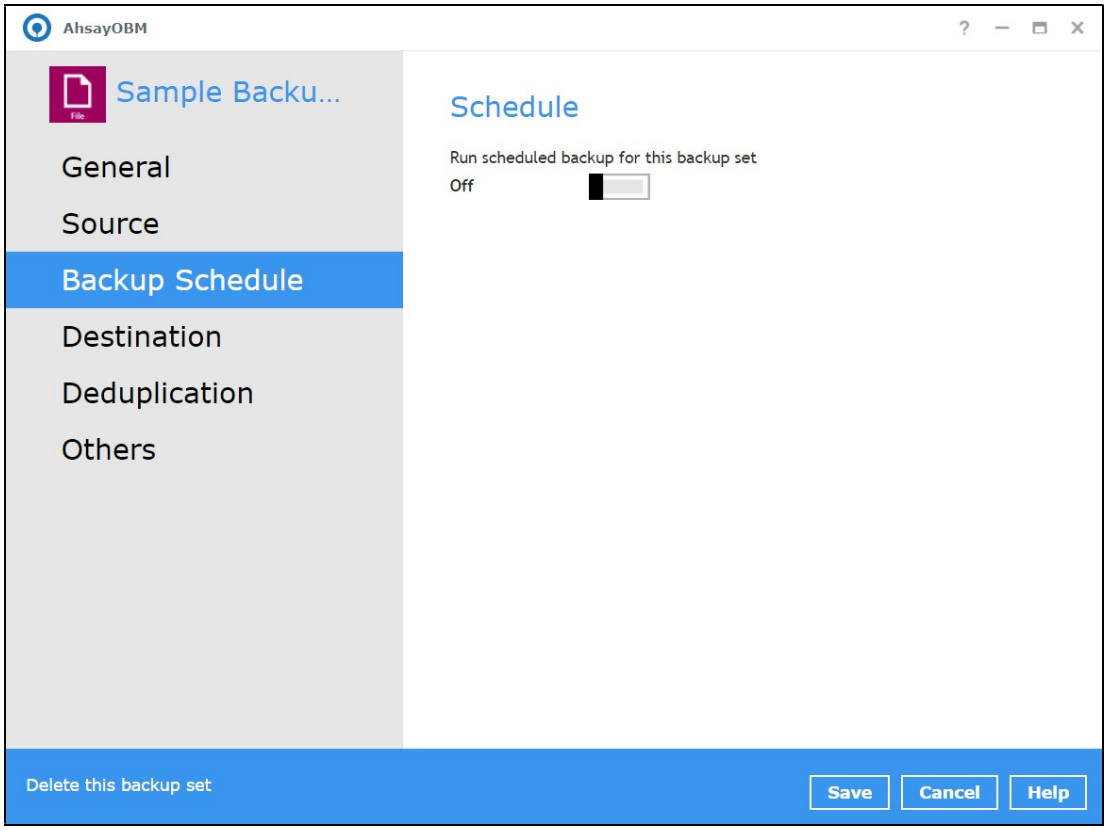


To add backup source, follow the instructions below:

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.

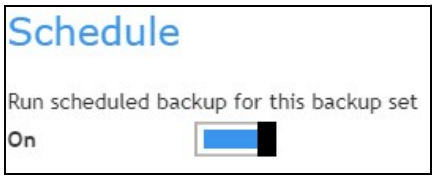
Backup Schedule

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

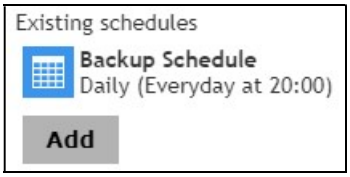


To configure a backup schedule, follow the steps below:

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

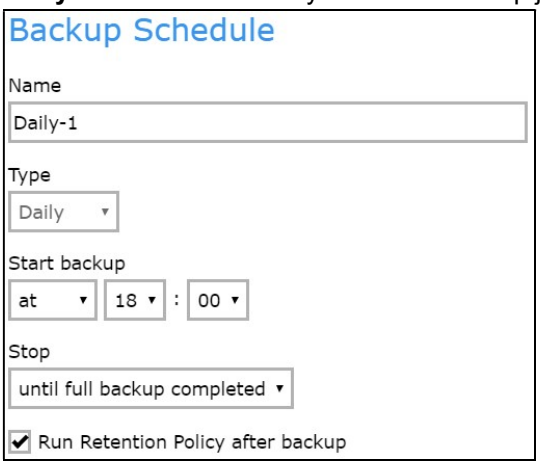


2. Select an existing backup schedule to modify or click the **Add** button to create a new one.

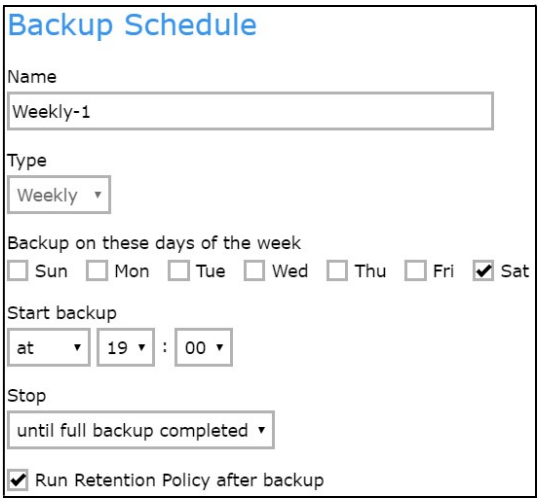


3. In the New Backup Schedule window, configure the following backup schedule settings.
   - **Name** – the name of the backup schedule.
   - **Type** – the type of the backup schedule. There are four (4) different types of backup schedule: Daily, Weekly, Monthly and Custom.

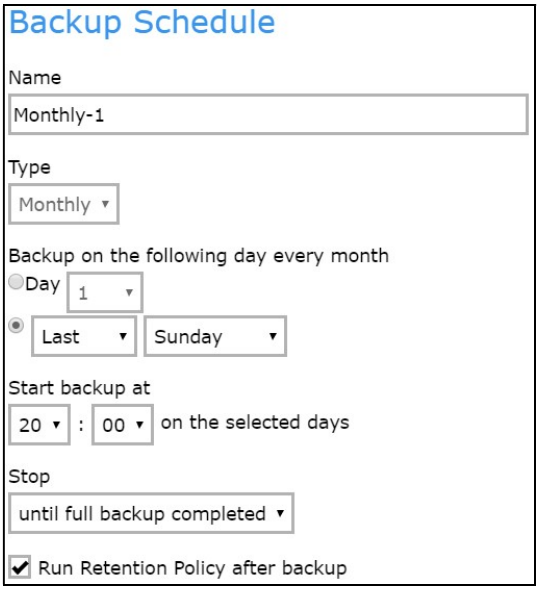
- **Daily** – the time of the day when the backup job will run.



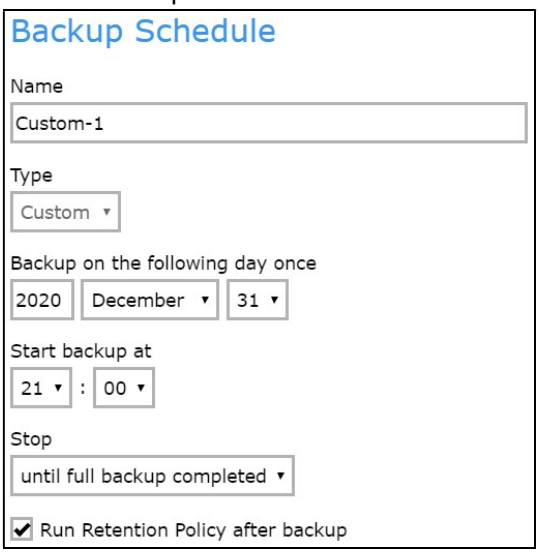
- **Weekly** – the day of the week and the time of the day when the backup job will run.



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



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



- **Start backup** – the start time of the backup job.
  - **at** – this option will start a backup job at a specific time.
- **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.

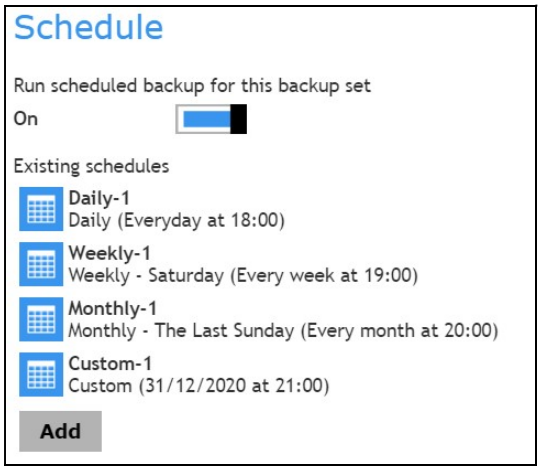
    The partially backed up data will have to be removed by running the Data Integrity Check.

    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.

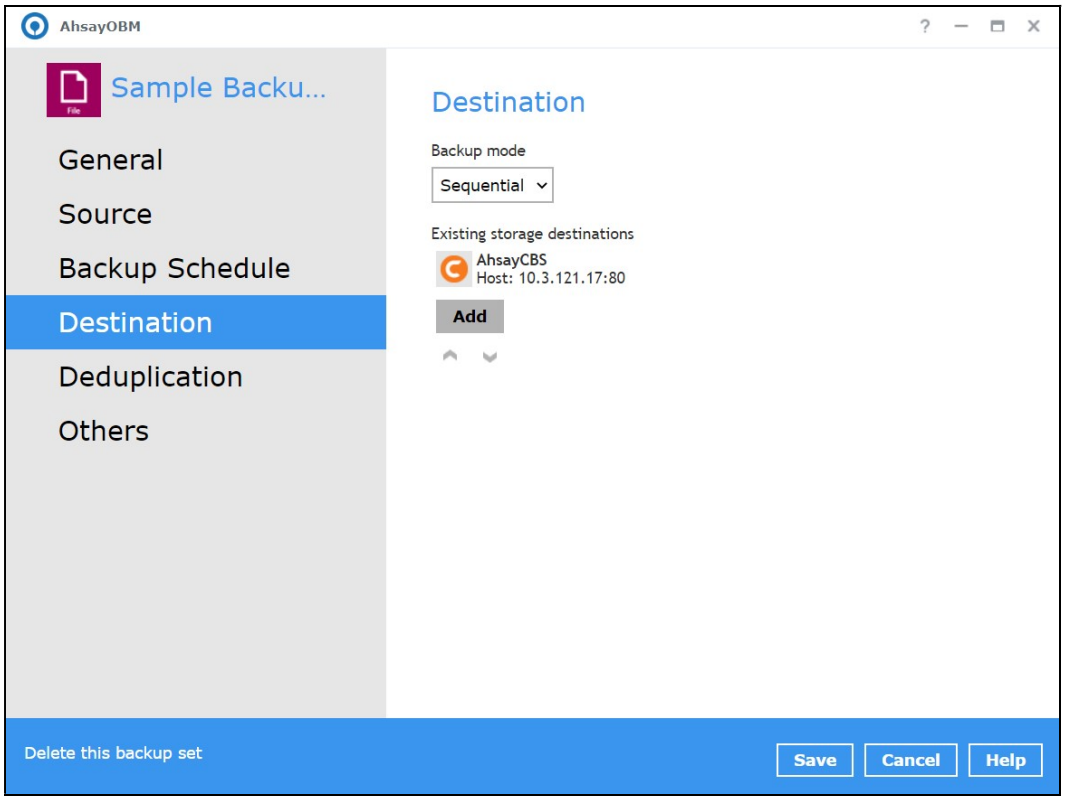


NOTE

For more details on the scenario for Backup Schedule under Backup Set Settings, refer to Appendix C: Scheduler Scenarios.

Destination

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



To add a destination, follow the instructions below:

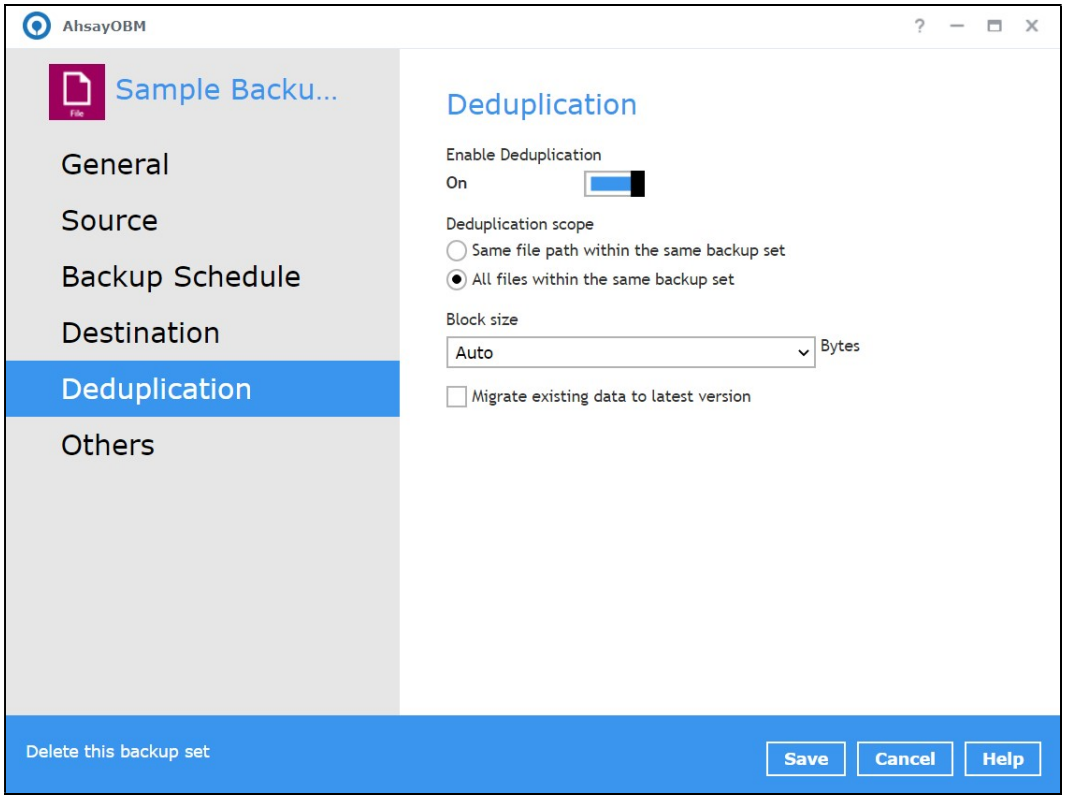
1. Select the **Destination** tab.
2. Click the **Add** button
3. Complete the following fields:
    - Name
    - Destination storage
4. Click the **OK** button to add the new destination.
5. Click the **Save** button to save the destination.

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.



There are two (2) types of Deduplication scope:

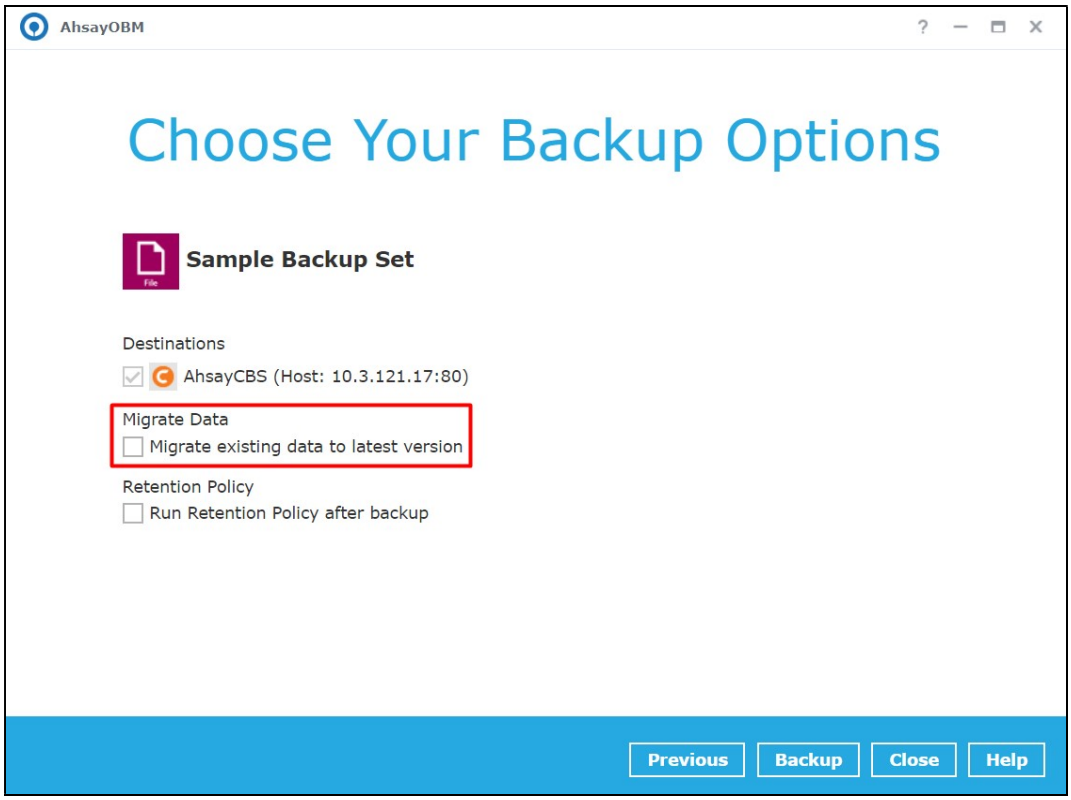
Deduplication scope	Description
Same file path within the same backup set	Deduplication will be applied to the duplicated contents within a file during the current backup job.
All files within the same backup set	Deduplication will be applied across different files in the backup set.

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.



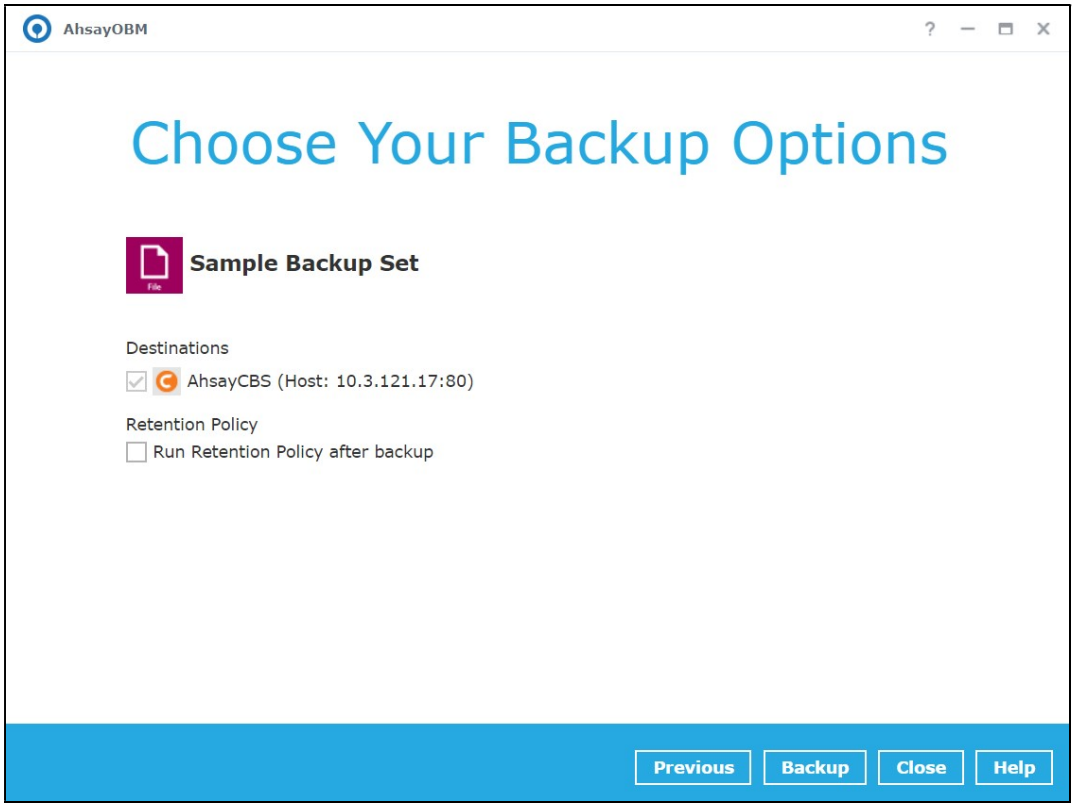
Migrate Data

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

NOTE

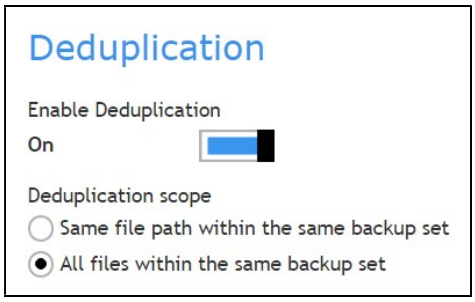
In case the Deduplication setting is **Off (disabled)** for the backup set, the Migrate Data option will not be displayed.

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

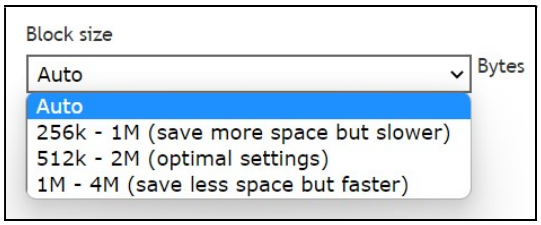


To configure the Deduplication settings, follow the steps below:

1. Select a type of Deduplication scope.



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



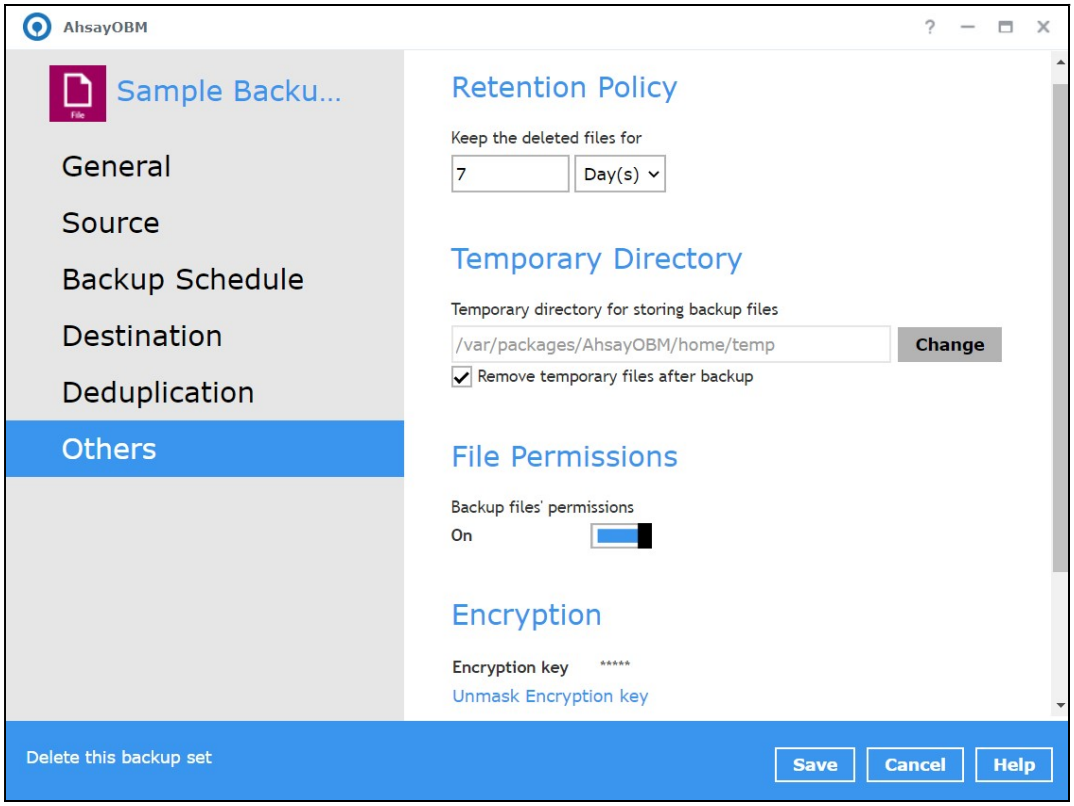
3. Tick the checkbox if you want the existing data to be migrated to the latest version during a backup job.

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

Others

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

- Retention Policy
- Temporary Directory
- File Permissions
- Encryption



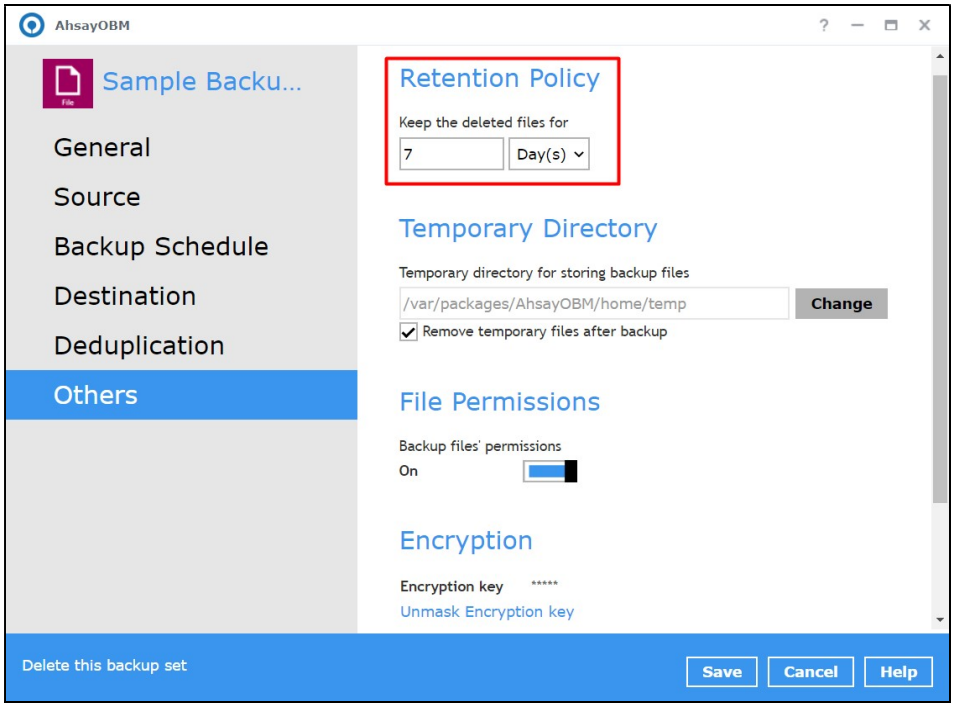
Retention Policy

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.

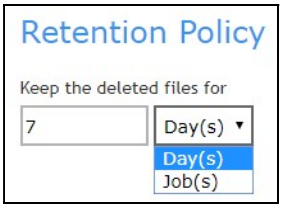


NOTE

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).

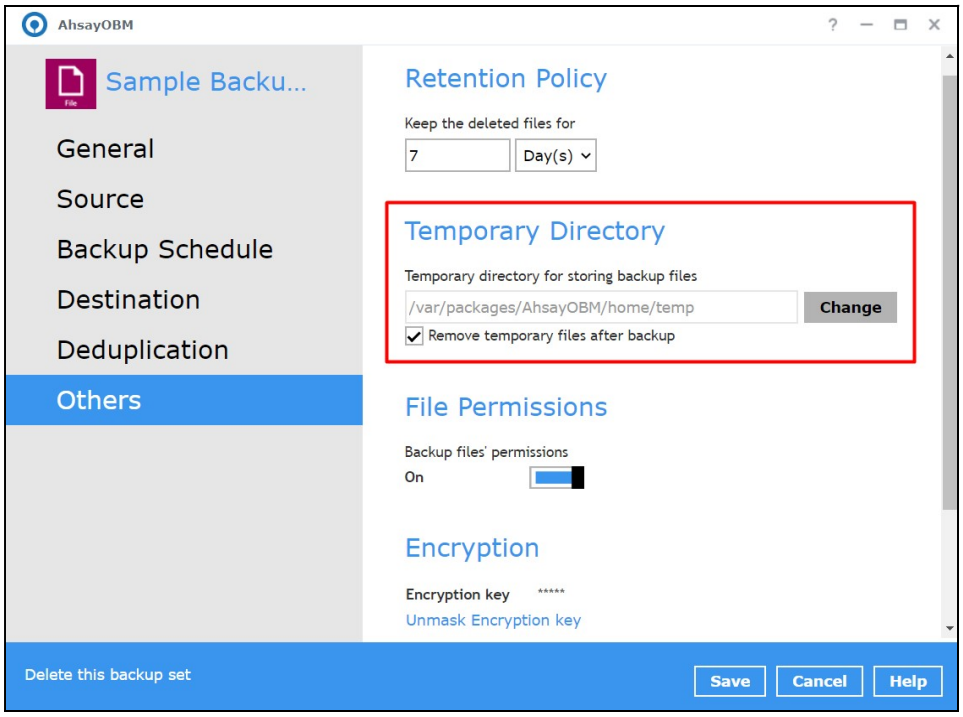


3. Input a valid number of Day(s) or Job(s), then click the **Save** button to save the Retention Policy settings.

Temporary Directory

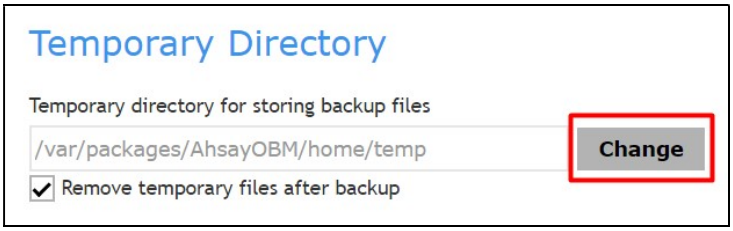
For a **backup job**, it is used to temporarily store backup set index files. An updated set of index files is generated after each backup job. The index files are synchronized to each individual backup destination at the end of each backup job.

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

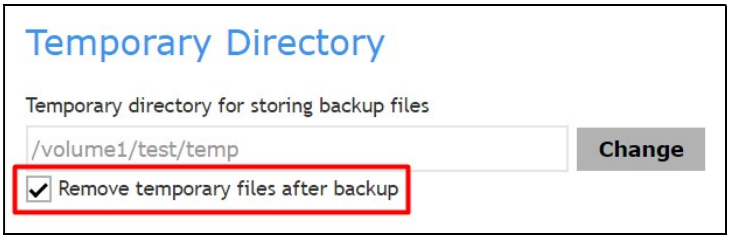


To configure the temporary directory, follow the instructions below:

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



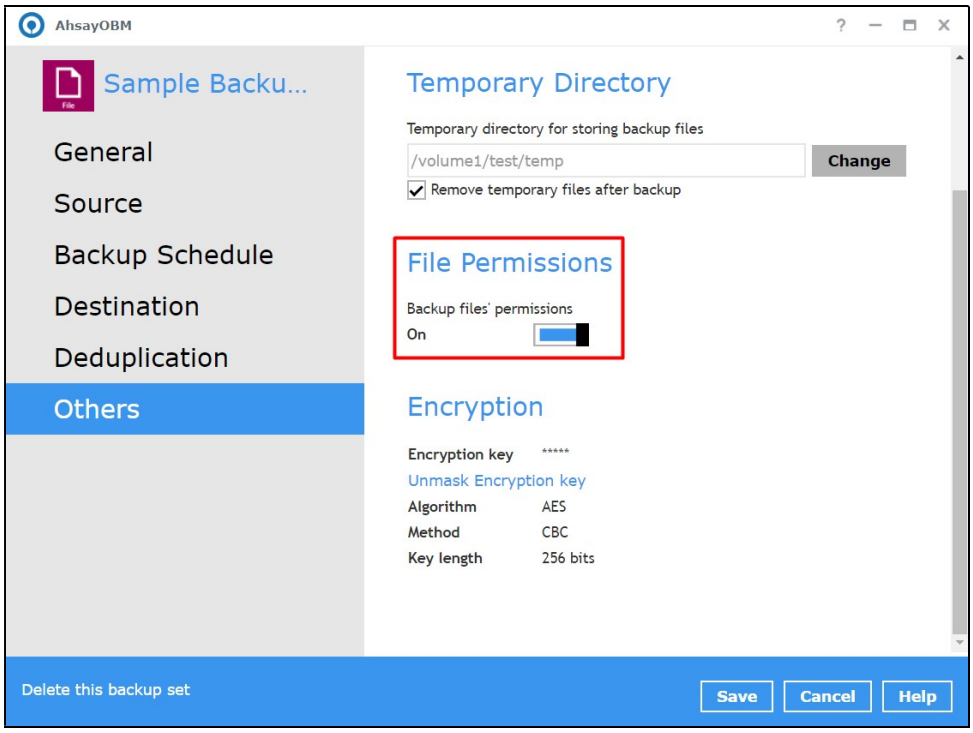
2. Locate the directory that you would like to use, then click **OK** to select the folder.
3. You also have an option to check or uncheck the **Remove temporary files after backup** checkbox.



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

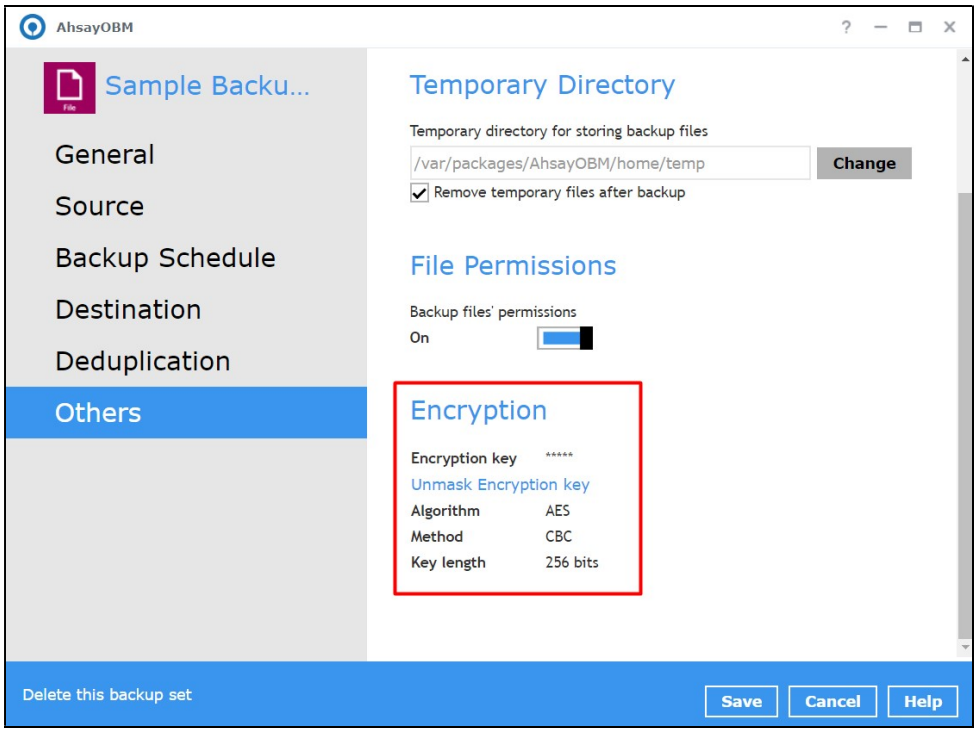
File Permissions

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.



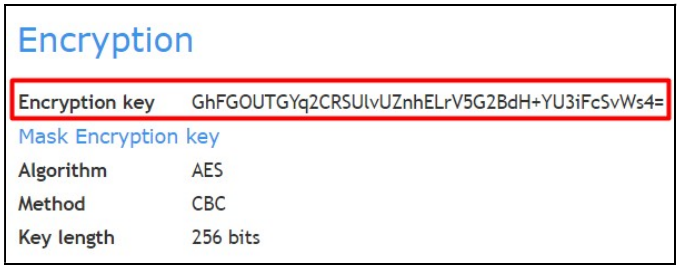
Encryption

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



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

1. 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.



NOTE

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

6.7 Report

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

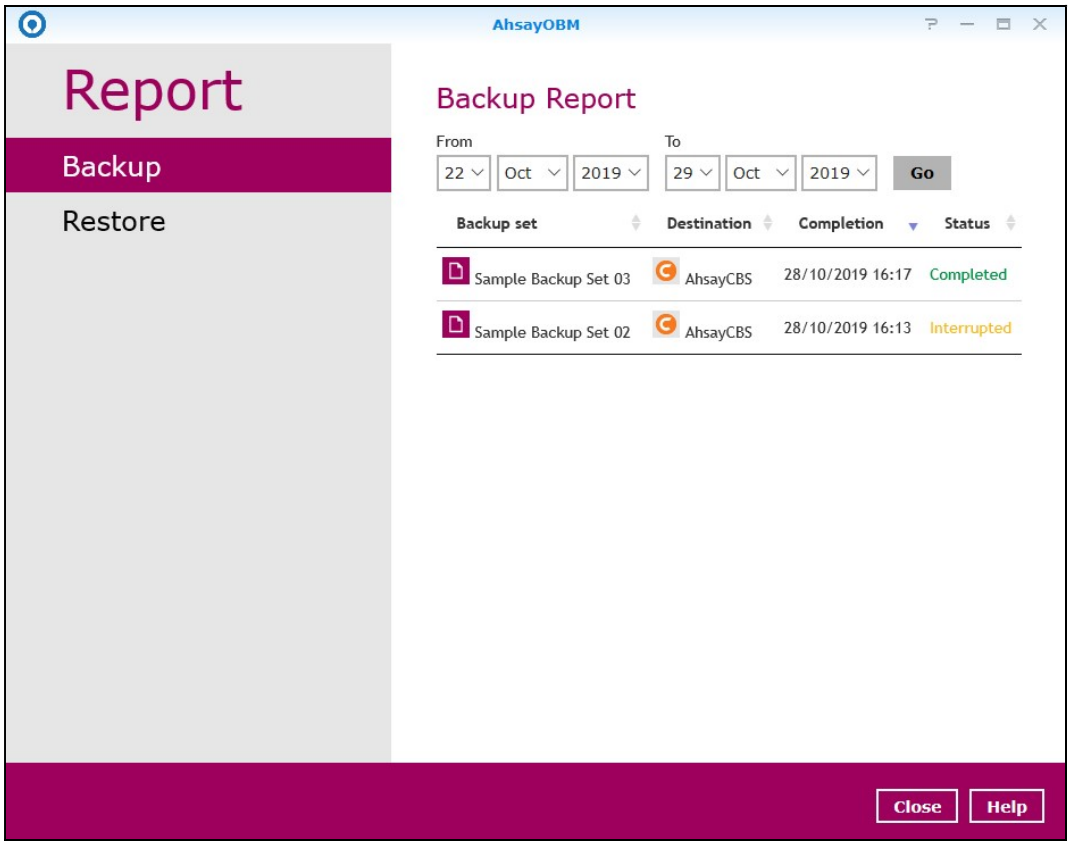
There are two (2) option available for this feature:

- Backup
- Restore

6.7.1 Backup

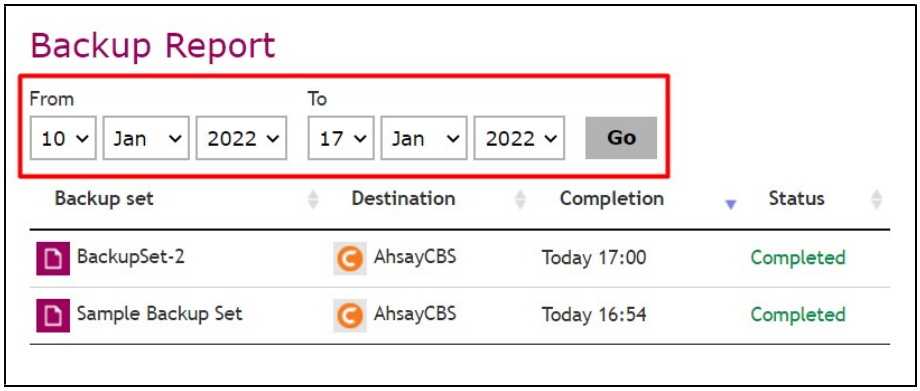
This feature displays the backup report logs for each backup set. There are four (4) filters that can be applied on this feature:

- Date
- Backup set
- Destination
- Status



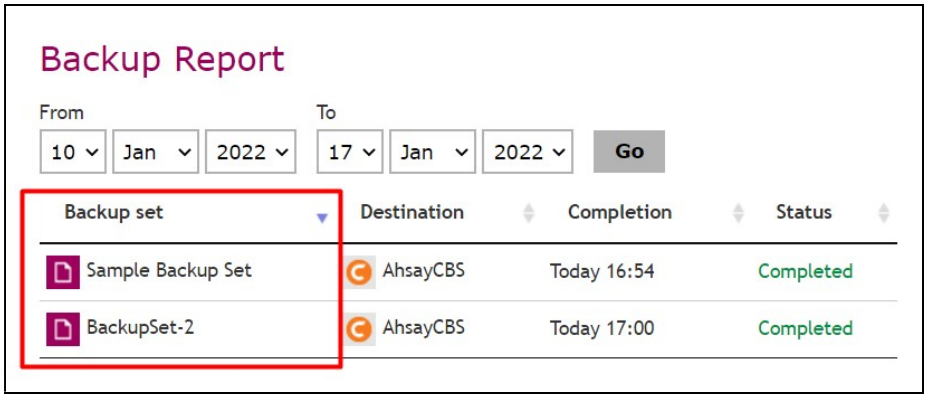
Date

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



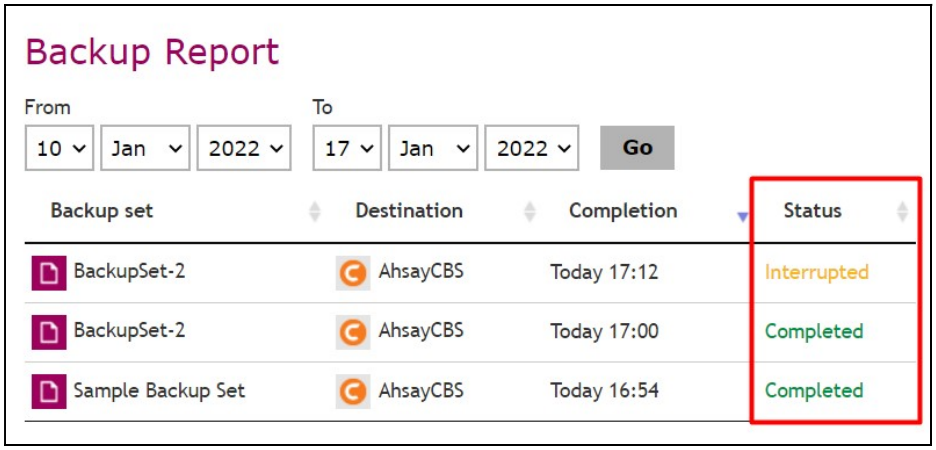
Backup set

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.



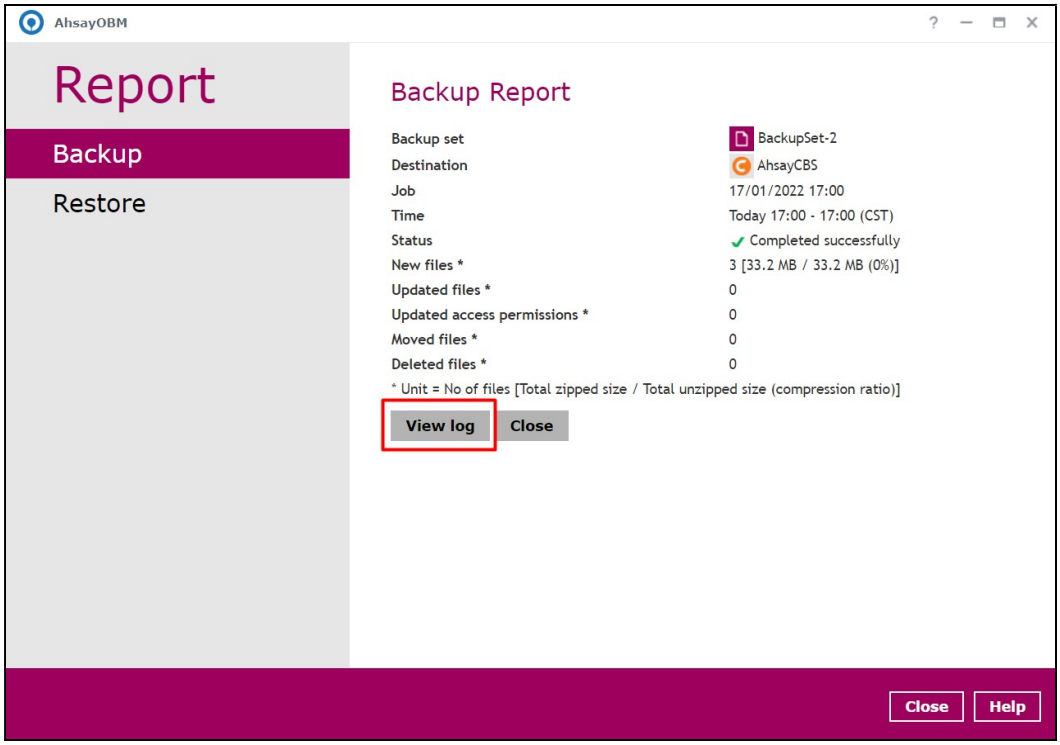
Status

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).

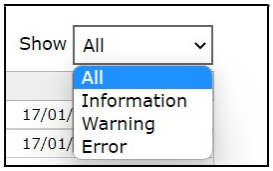


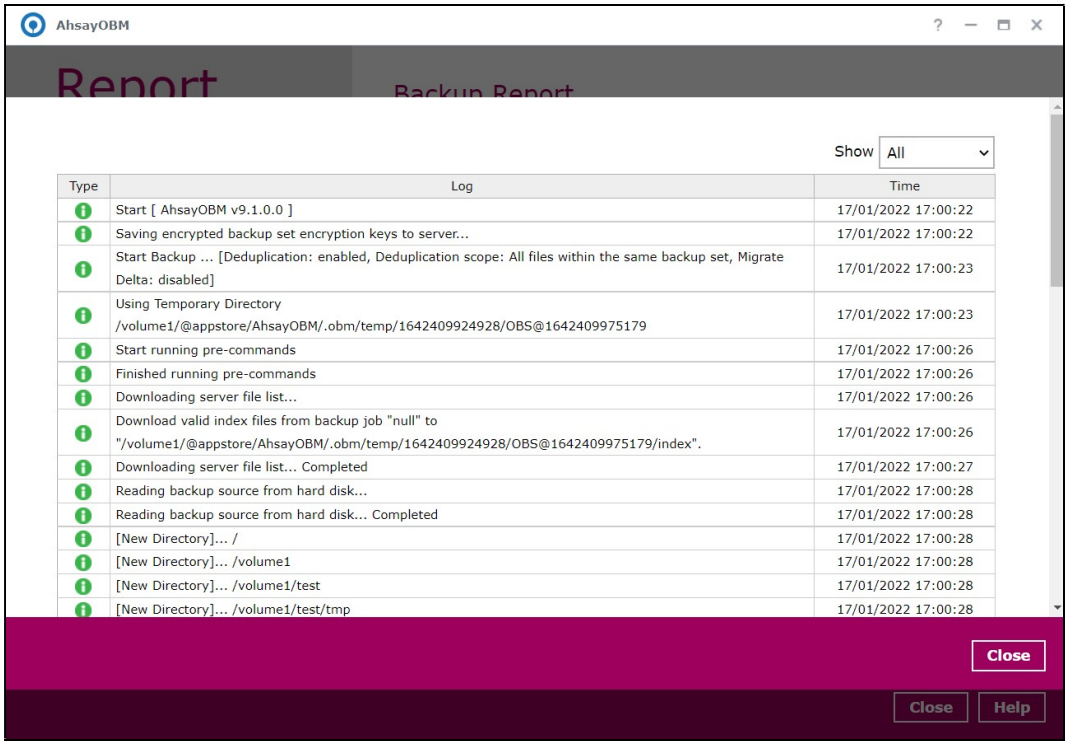
To view the backup log, follow the instructions below:

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

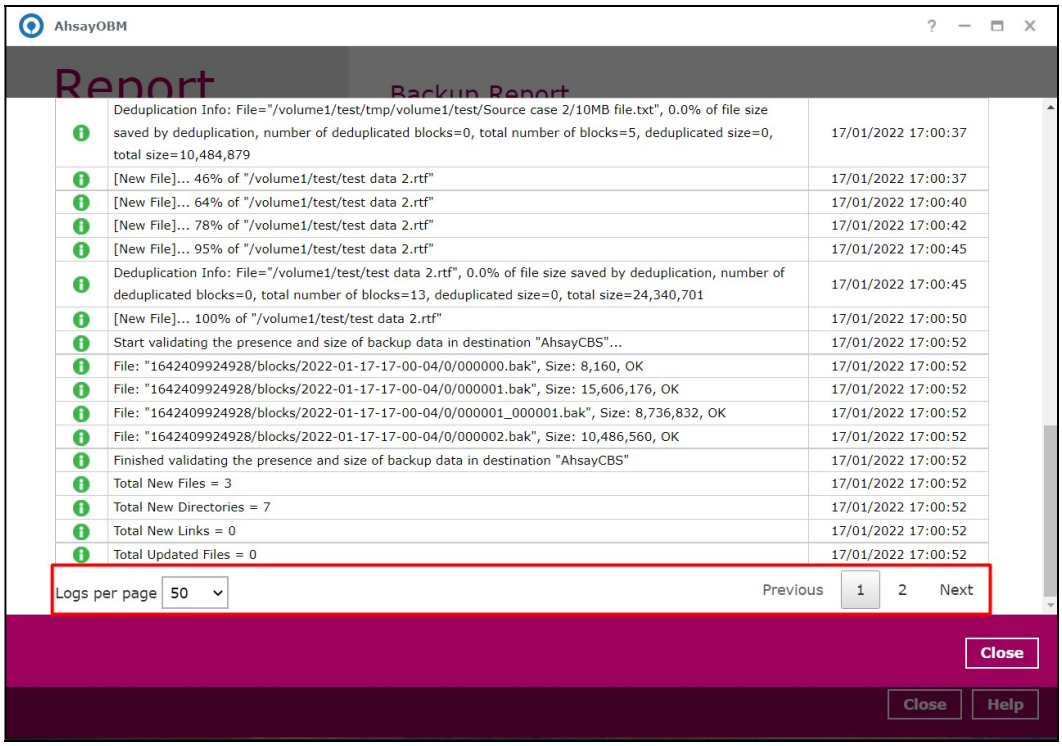


2. The status can be filtered when viewing the backup report.





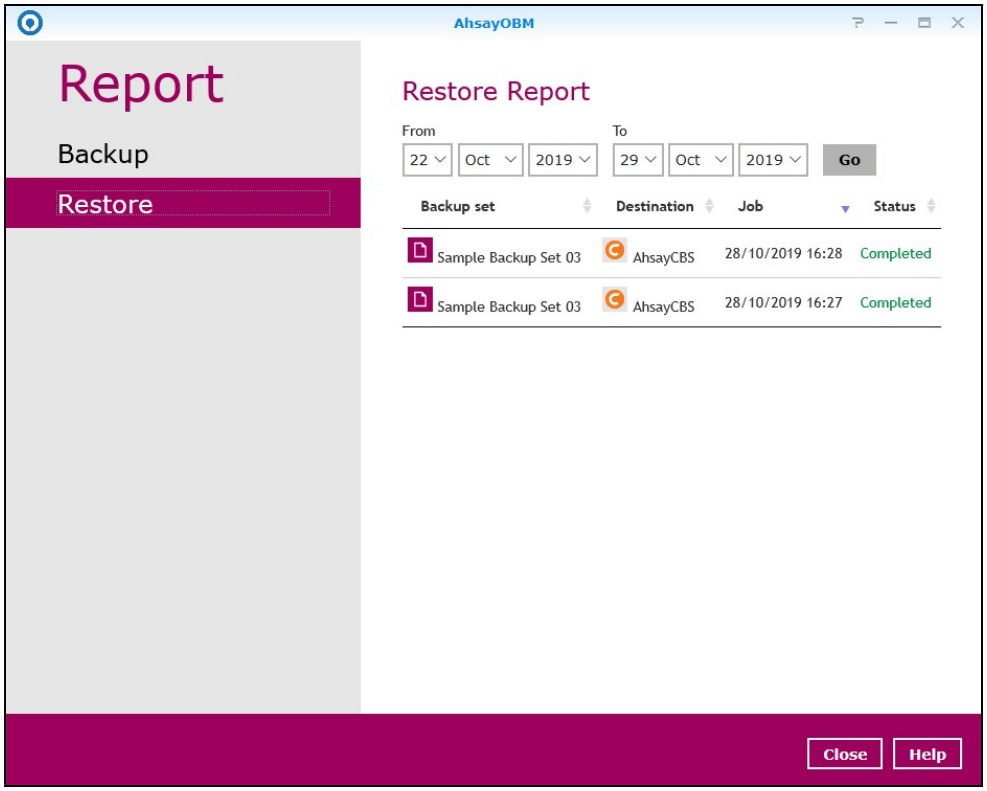
3. You can also select the number of logs per page or navigate through the backup report by clicking the next page.



6.7.2 Restore

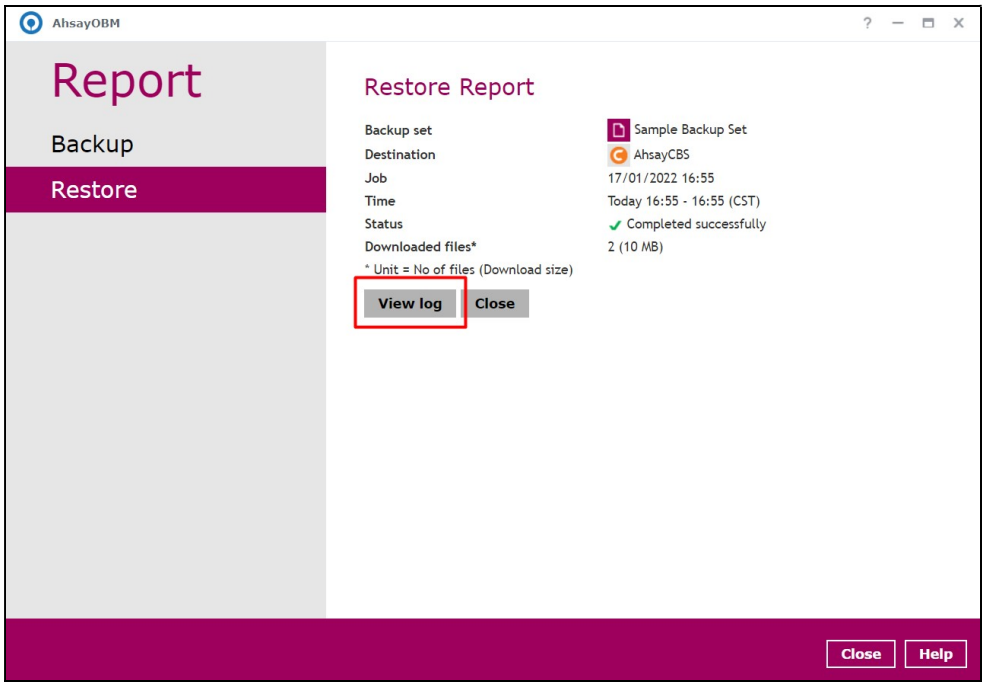
This feature displays the restore report logs for each backup set. Similar to the **Backup** tab, this feature also consists of the following filters:

- Date
- Backup set
- Destination
- Status

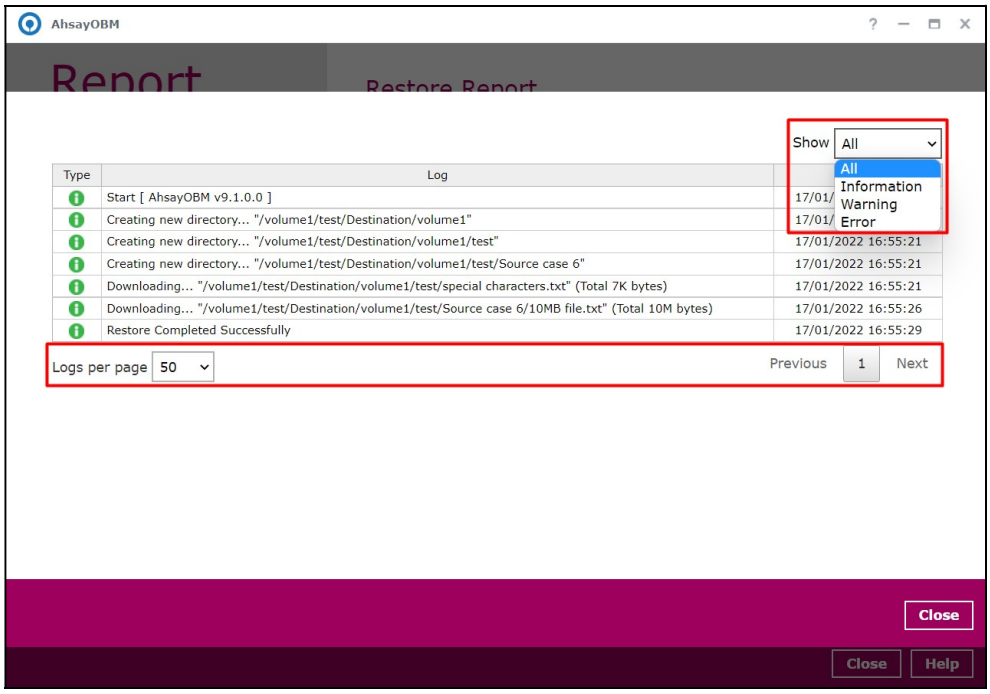


To view the restore log, follow the instructions below:

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



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.



6.8 Restore

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

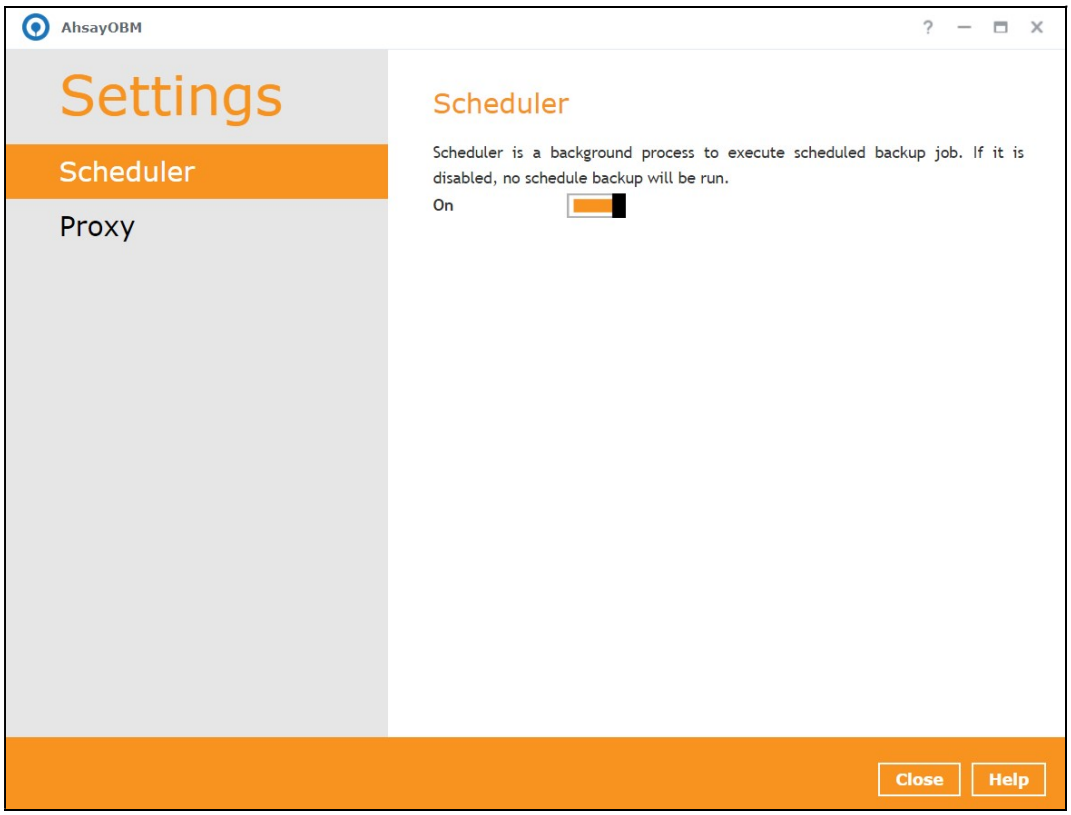
To restore backed up files, follow the instructions on Chapter 10 Restore Data.

6.9 Settings

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

6.9.1 Scheduler

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

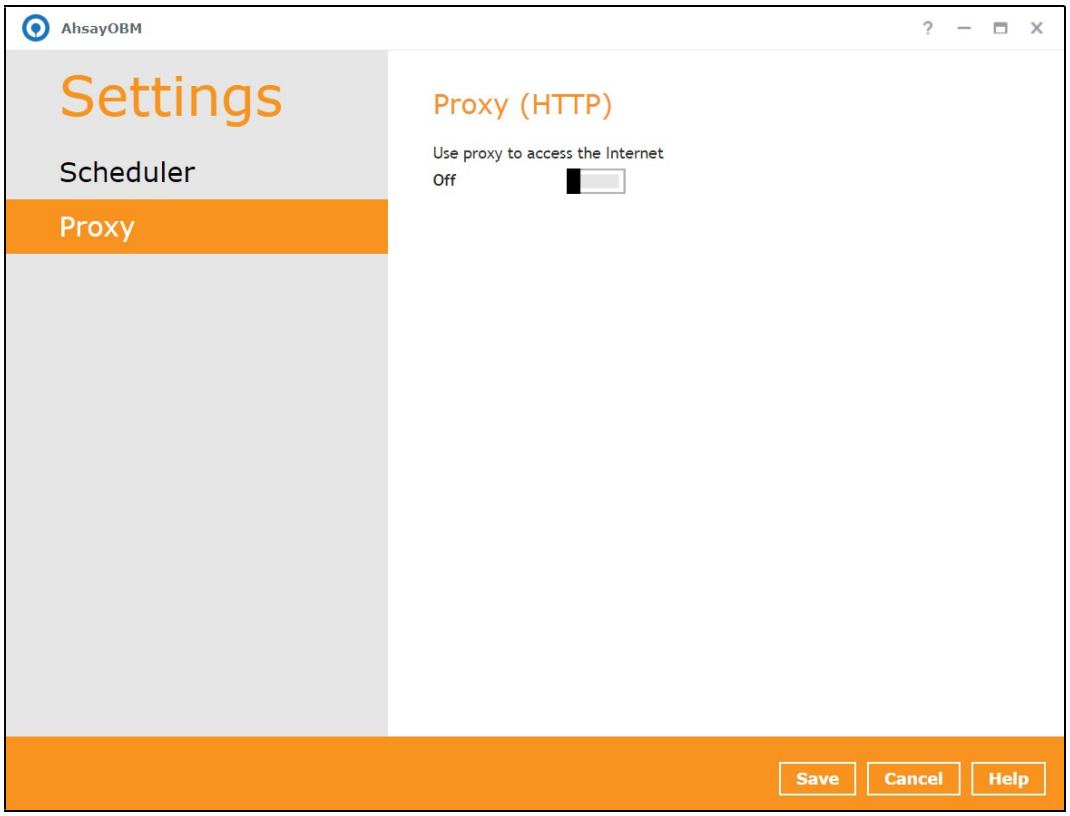


NOTE

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

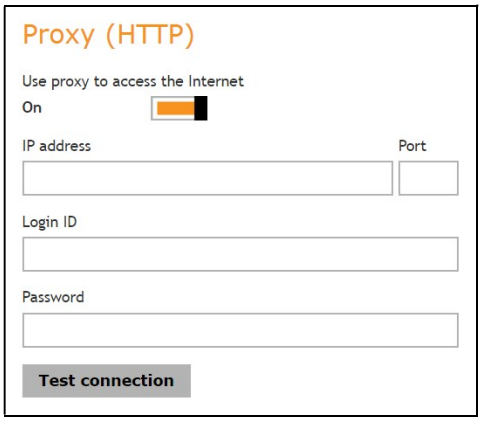
6.9.2 Proxy

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



To enable the Proxy Settings, follow the instructions below:

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



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

6.10 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

6.10.1 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 Data Integrity Check job will perform check for the backup destination(s) to remove old index files that are more than ninety (90) days old in the backup job folder(s).

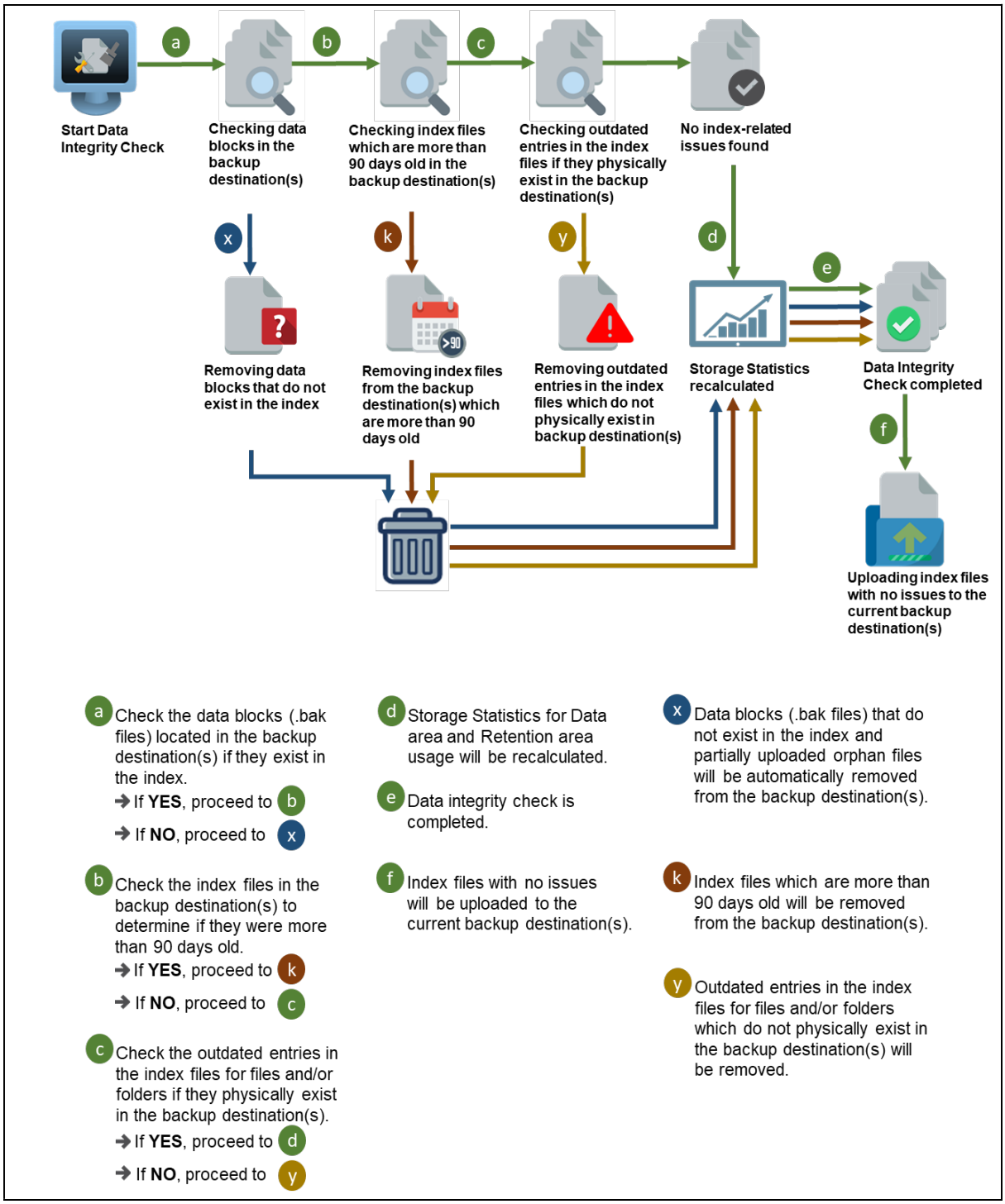
There are two (2) options in performing the Data Integrity Check:

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

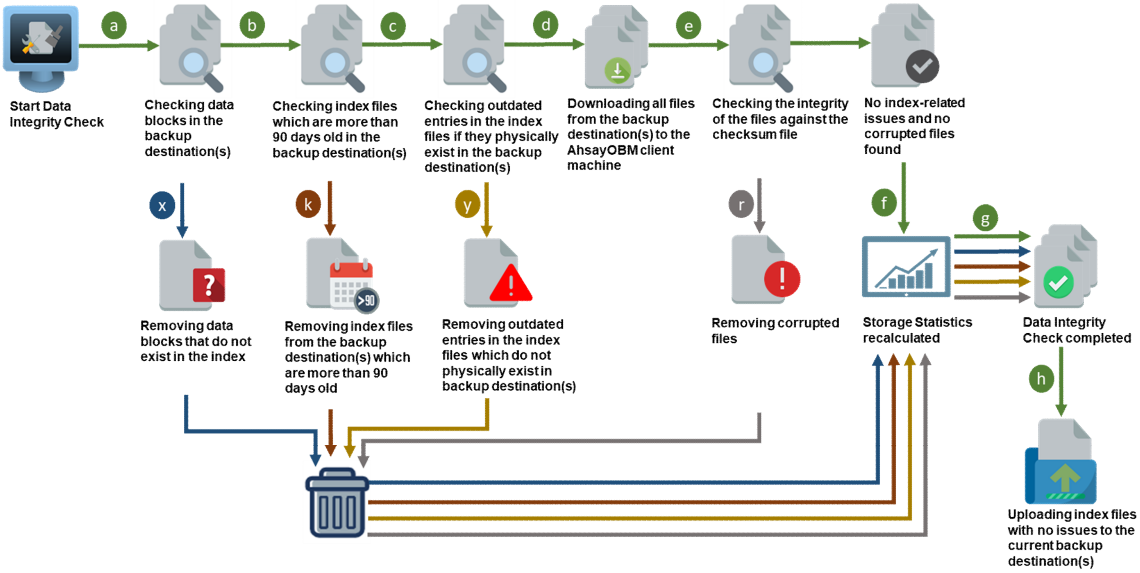
The following diagrams show the detailed process of the Data Integrity Check (DIC) in two (2) modes:

- **Option 1**
  Disabled Run Cyclic Redundancy Check (CRC) - **(Default mode)**
- **Option 2**
  Enabled Run Cyclic Redundancy Check (CRC)

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



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



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

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

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

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

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

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

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

g Data integrity check is completed.

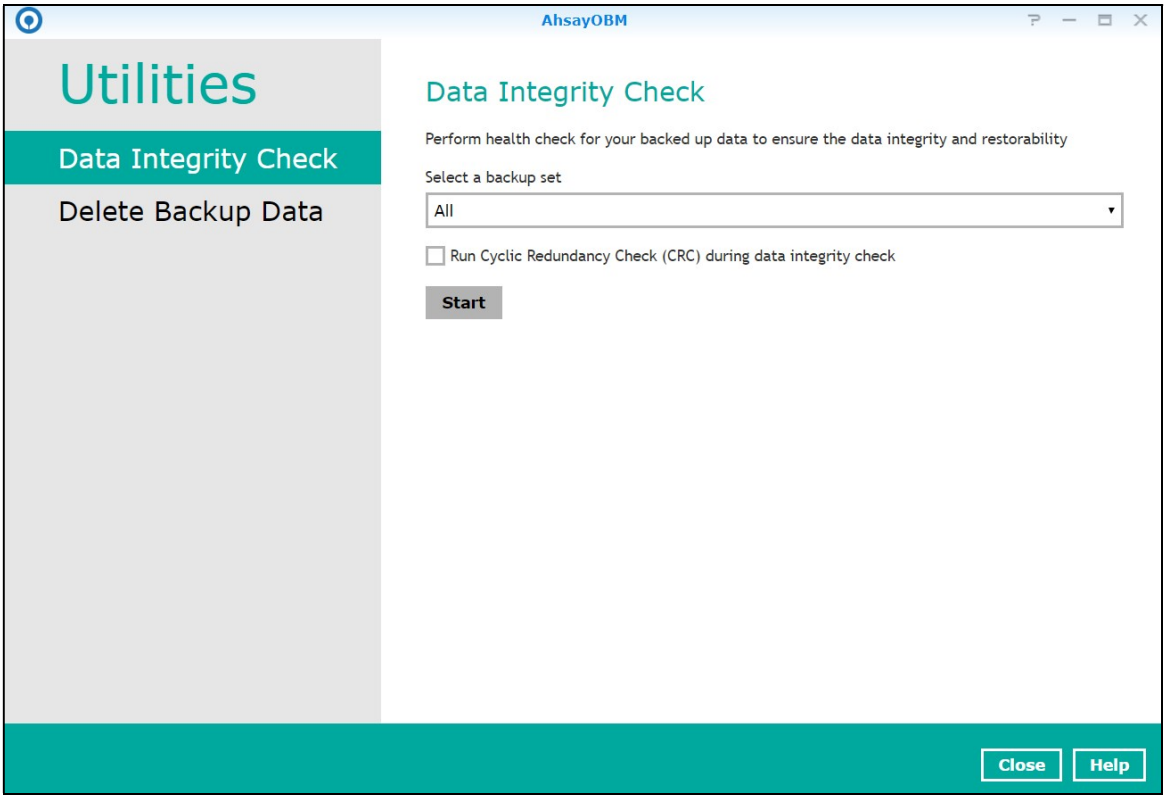
h Index files with no issues will be uploaded to the current backup destination(s).

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.

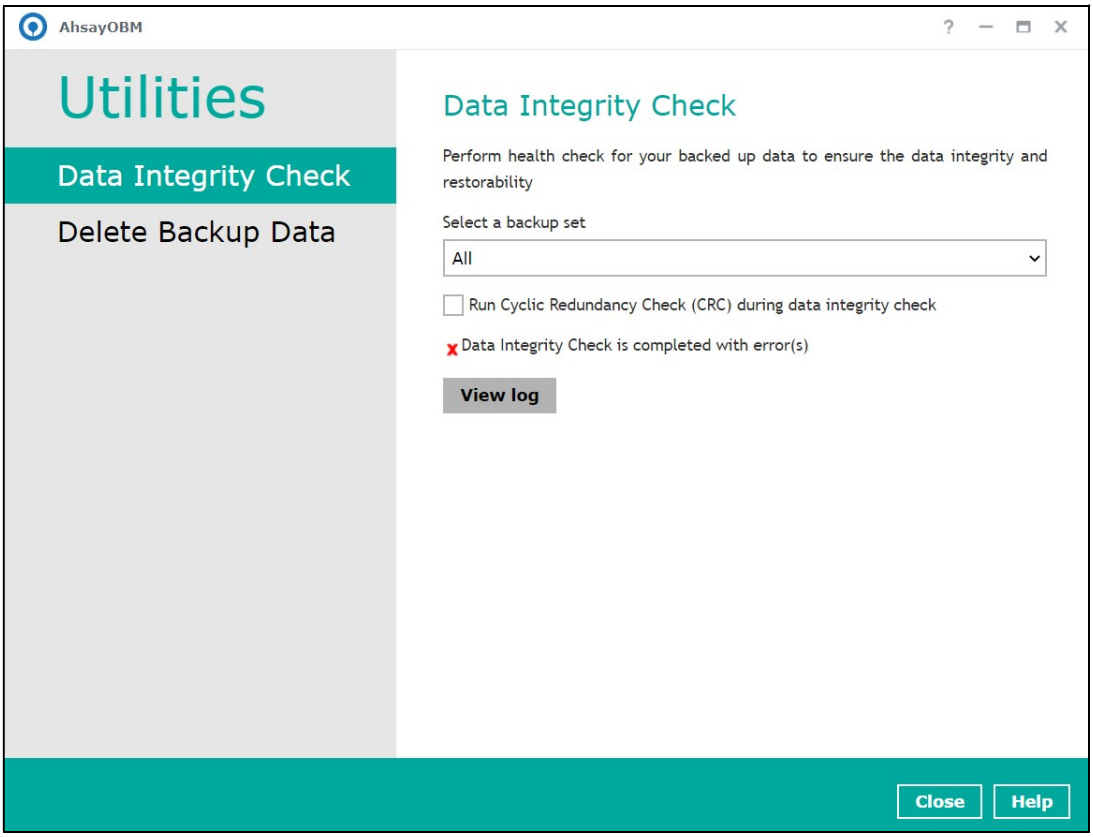
r Corrupted files will be automatically removed from the backup destination(s).

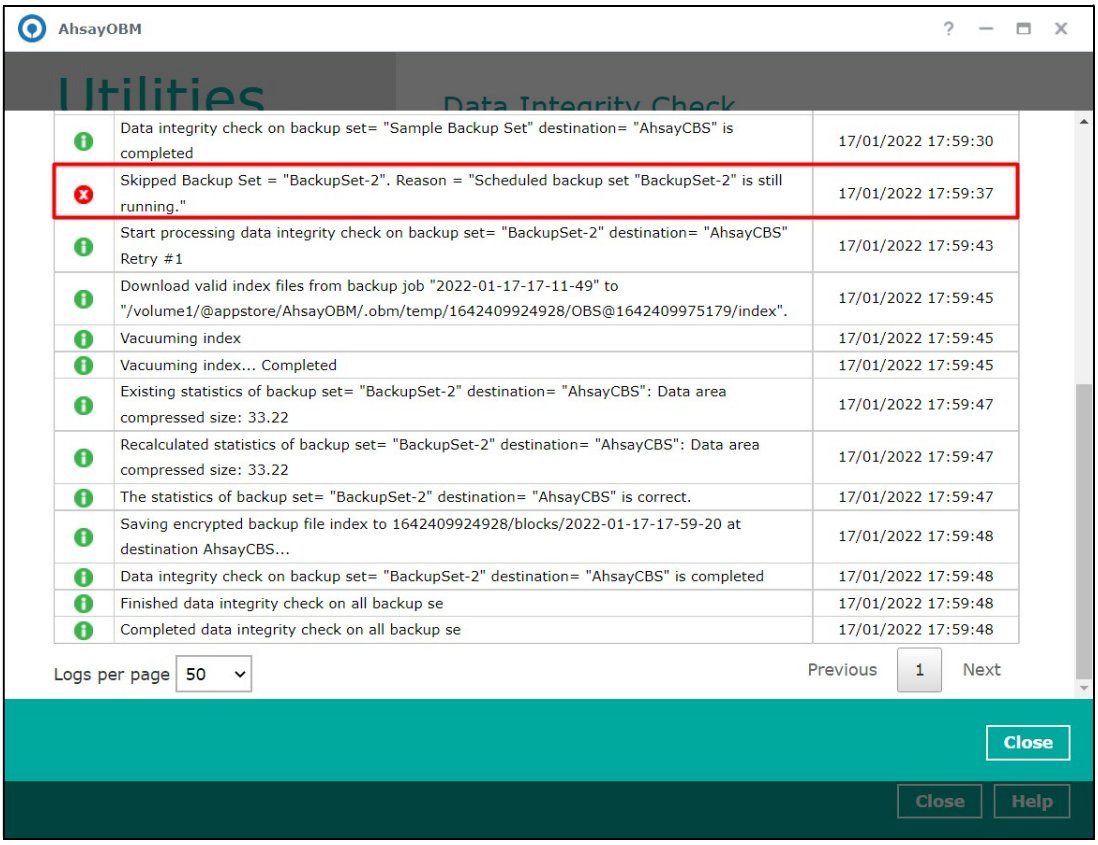


NOTES

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

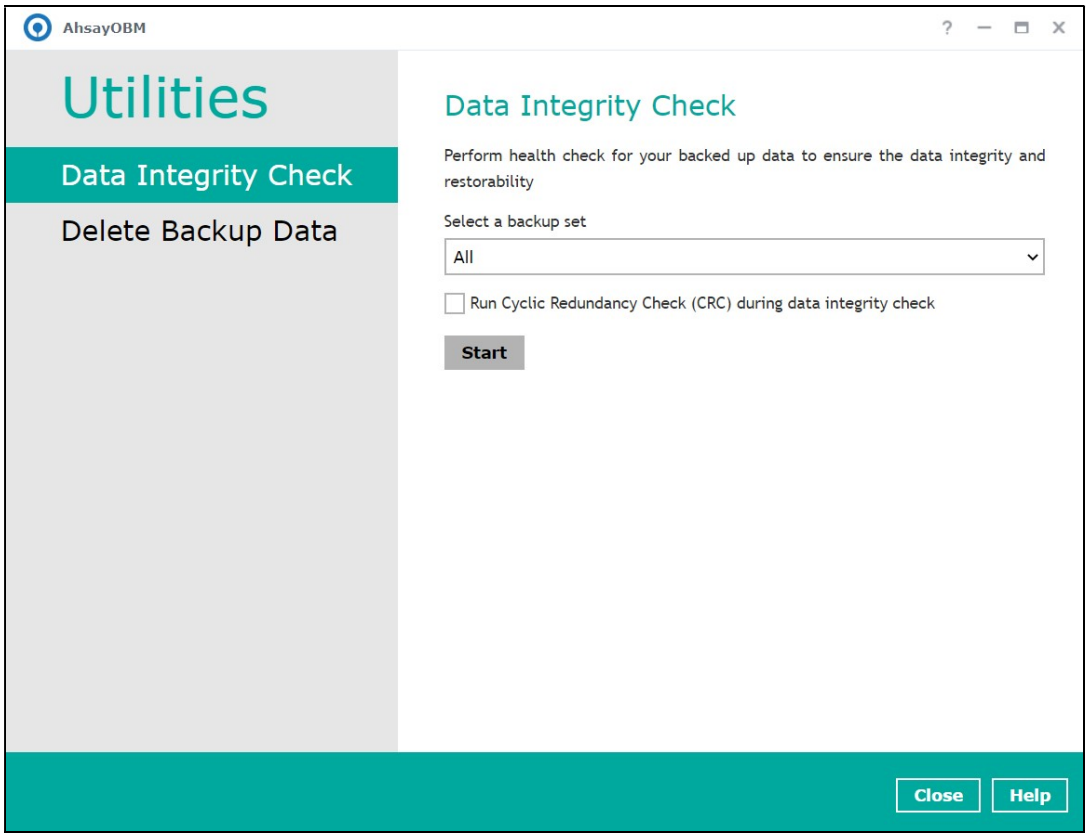
The following screenshot is an example of a Data Integrity Check completed with error(s). A Data Integrity Check is run on a backup set with an active backup job running which resulted the Data Integrity Check to stop with error(s). Clicking the **View log** button will display the details of the Data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



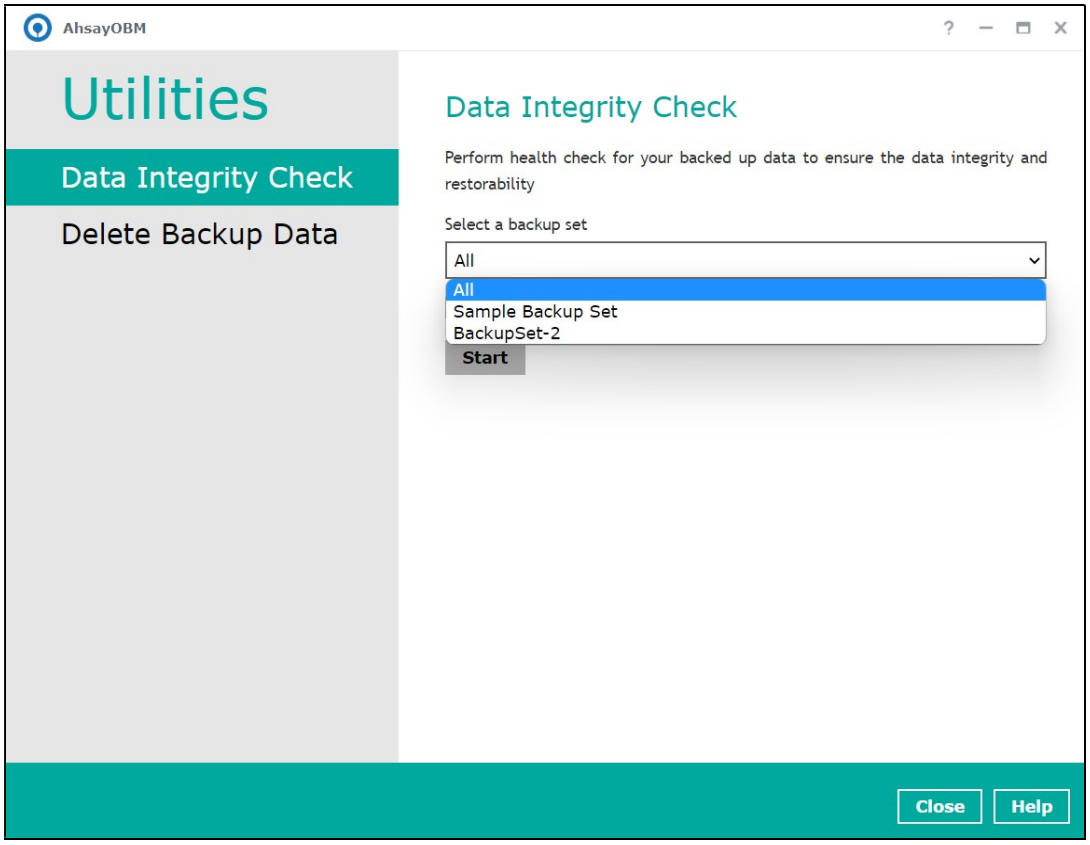


To perform a Data Integrity Check, follow the instructions below:

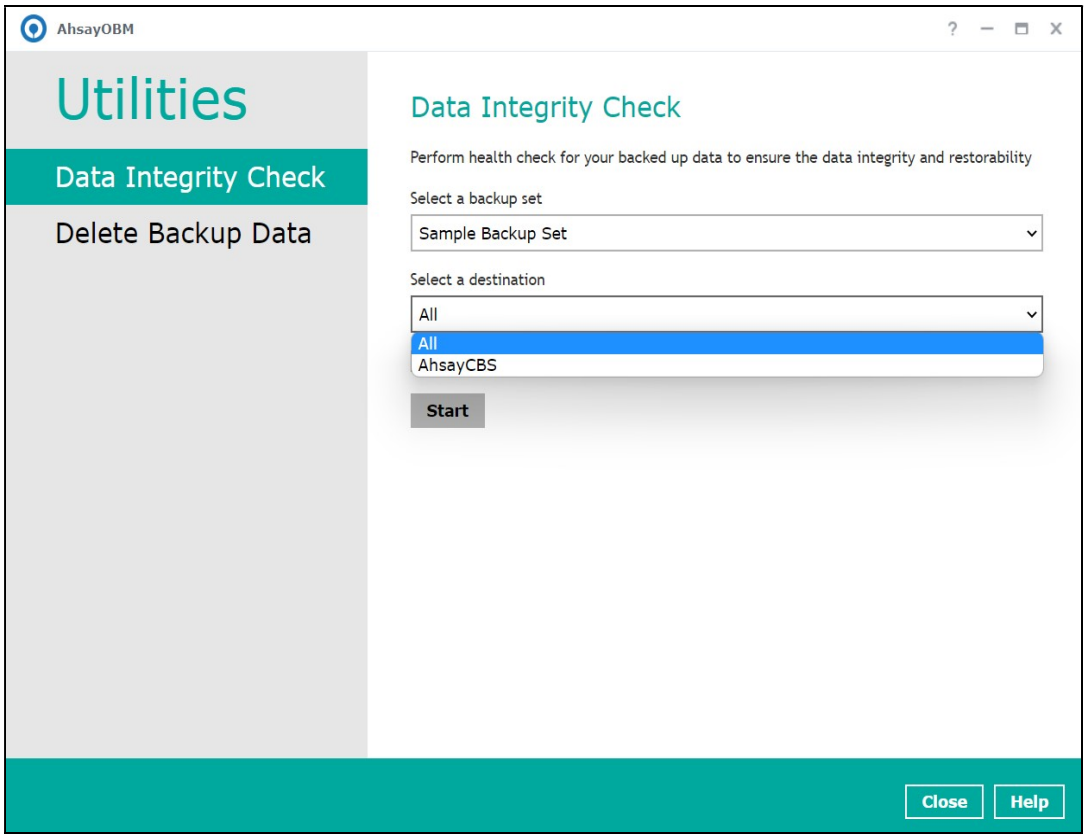
1. Go to the Data Integrity Check tab in the **Utilities** menu.



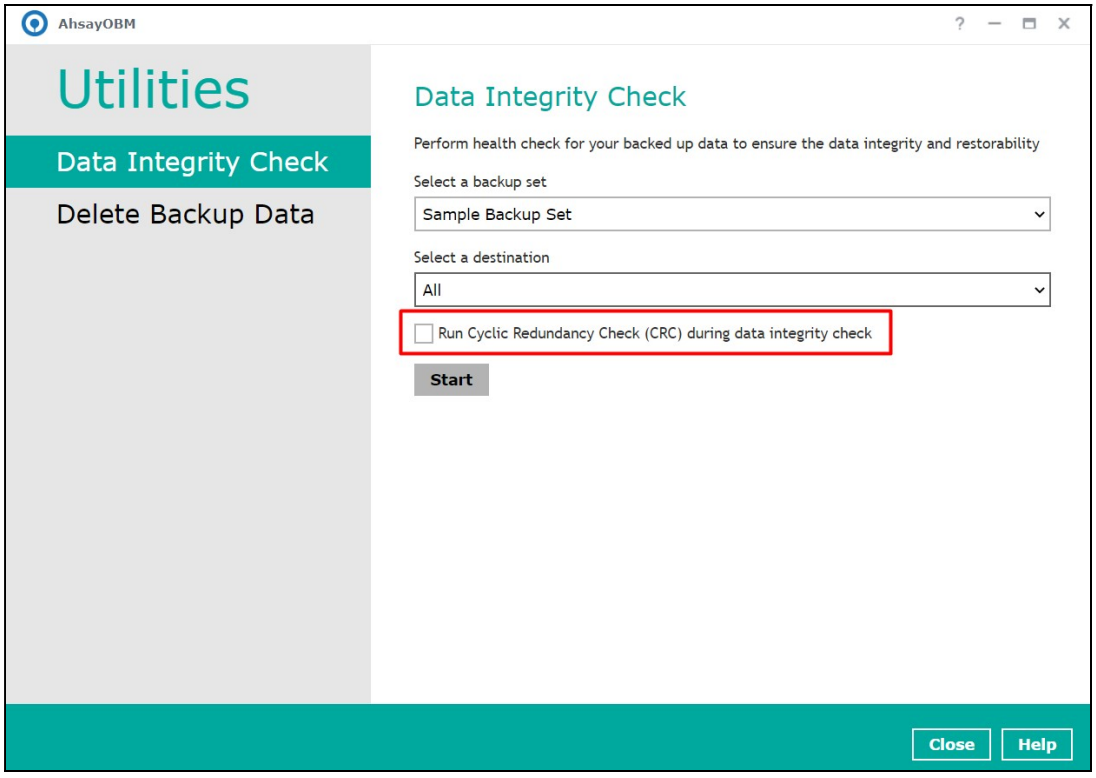
2. Click the drop-down button to select a backup set.



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



Unchecked Run Cyclic Redundancy Check (CRC) option is the default setting of Data Integrity Check.



Run Cyclic Redundancy Check (CRC)

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

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

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

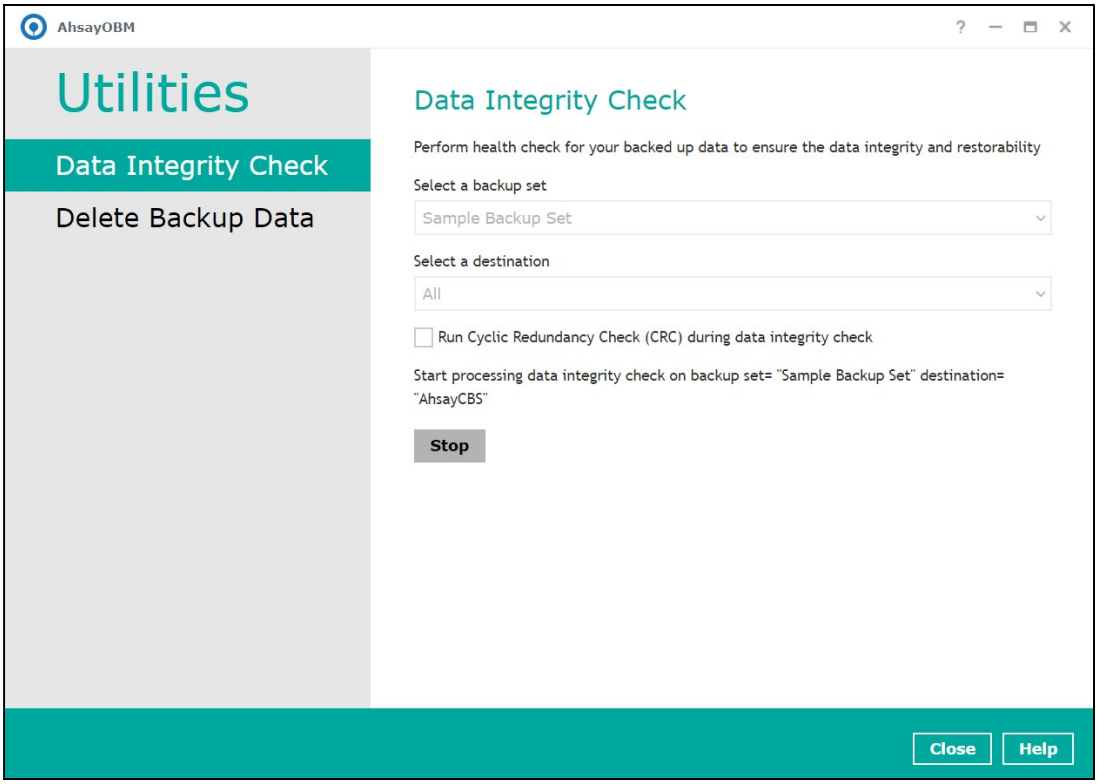
The time required to complete a Data Integrity Check depends on the number of factors such as:

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

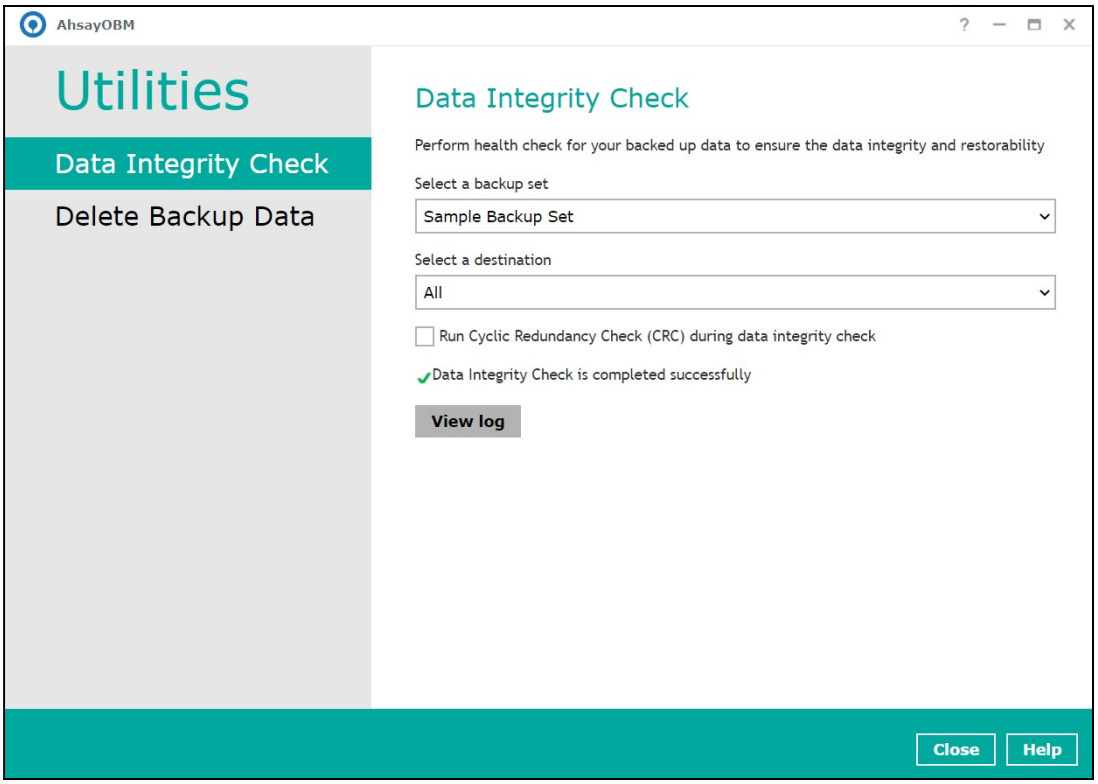
NOTE

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.

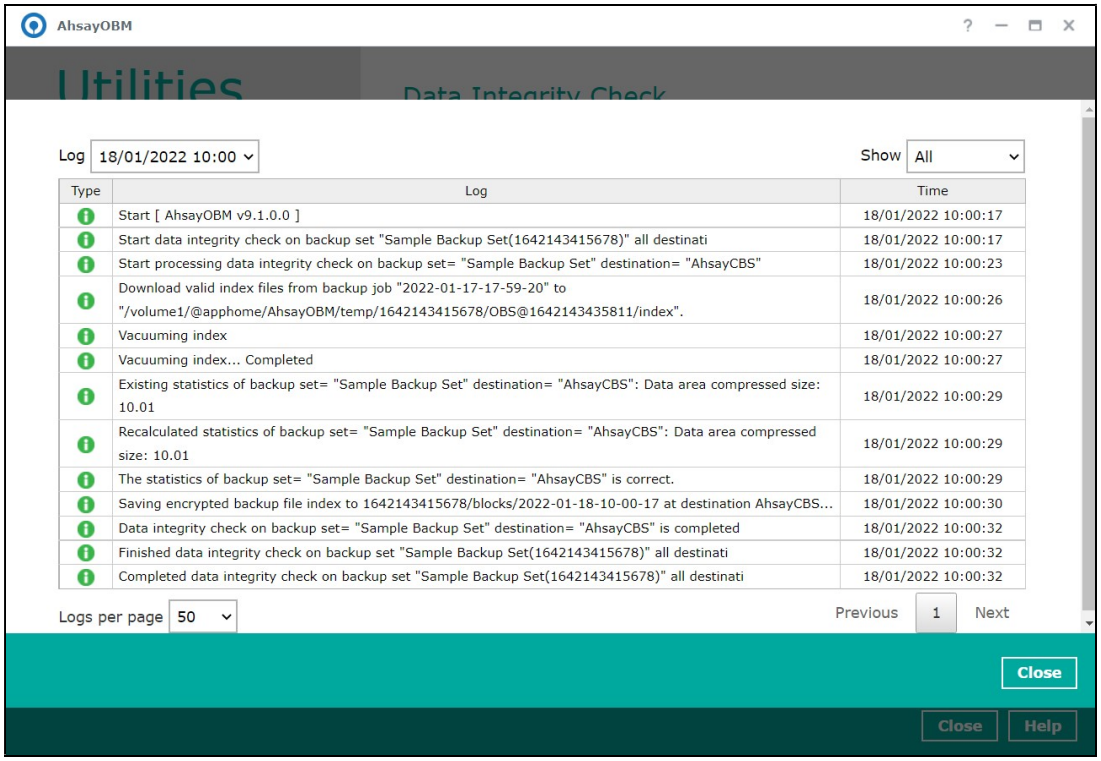
4. Click the **Start** button to begin the Data Integrity Check.
5. Data Integrity Check will start running on the selected backup set(s) and backup destination(s).



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

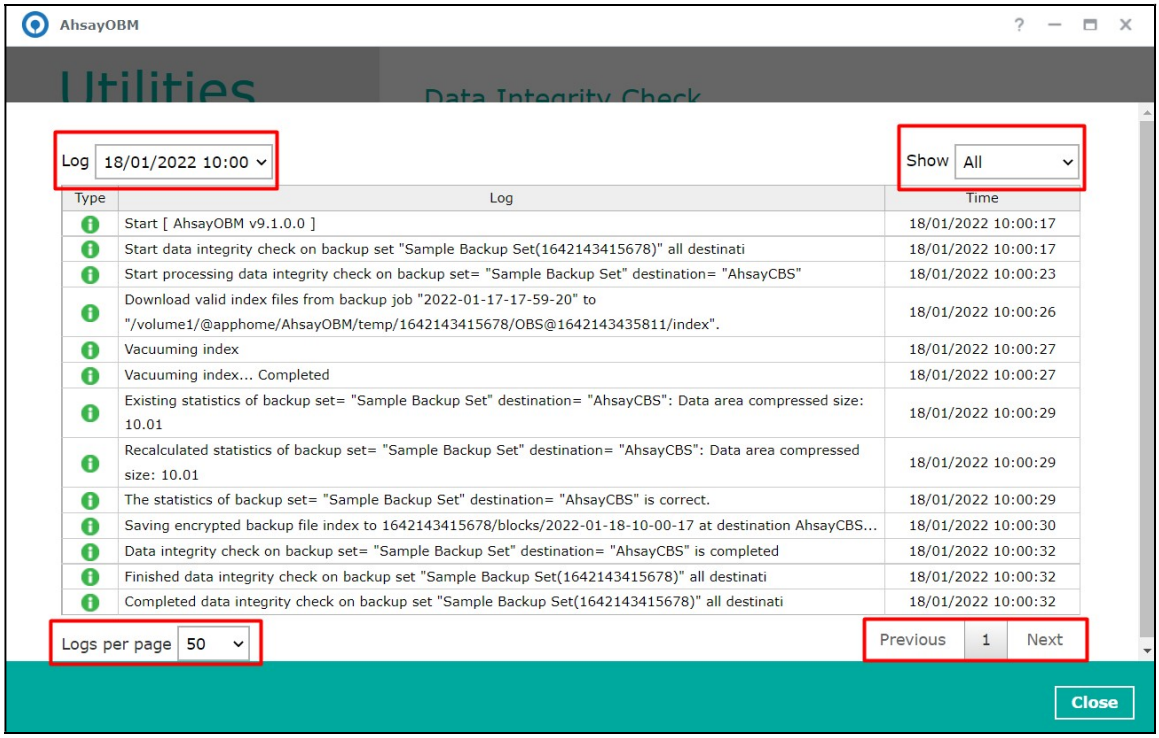


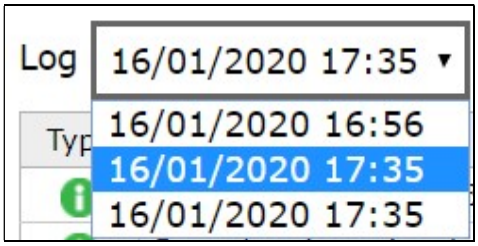
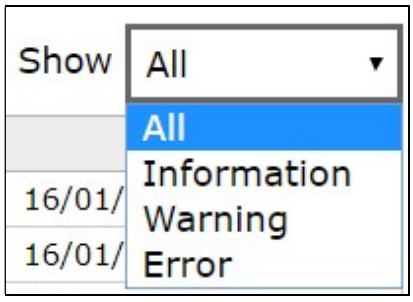
7. The detailed log of Data Integrity Check process will be displayed.

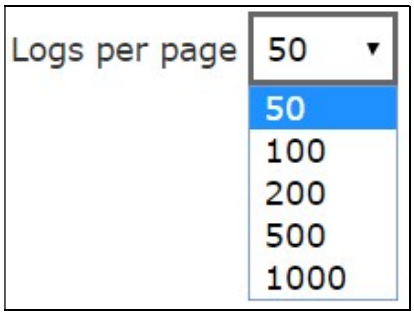


The following options can be used for further viewing of the detailed DIC log:

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



Option	Screenshot	Function
Log filter		This option can be used to display logs of the previous Data Integrity Check jobs.
Show filter		This option can be used to sort the Data Integrity Check log by its status (i.e., All, Information, Warning, and Error). With this filter, it will be easier to sort the DIC logs by its status especially for longer Data Integrity Check logs.

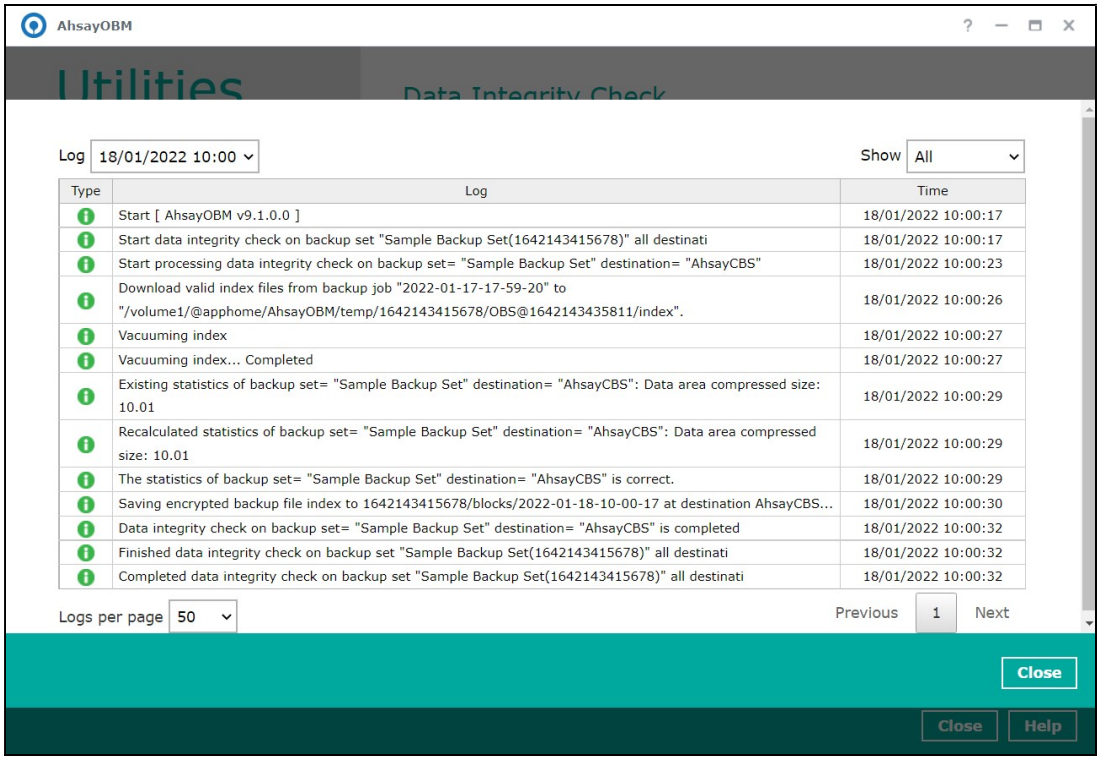
Logs per page		This option allows user to control the displayed number of logs per page.
Page		This option allows user to navigate the logs to the next page(s).

Data Integrity Check Result

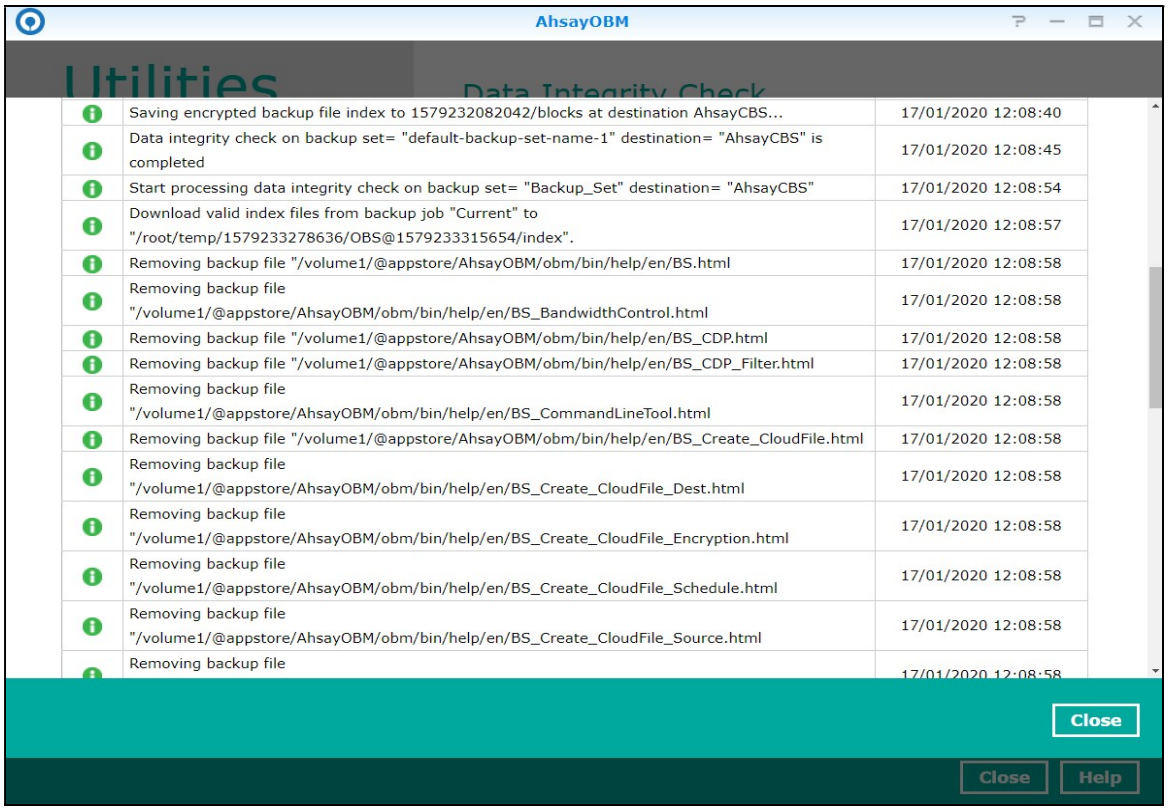
There are two possible outcomes after the completion of a Data Integrity Check:

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

The screenshot below shows an example of a Data Integrity Check log with NO data corruption/issues detected.



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).



NOTE

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

The (TEST MODE) confirmation screen is not supported 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 Data Integrity Check 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:

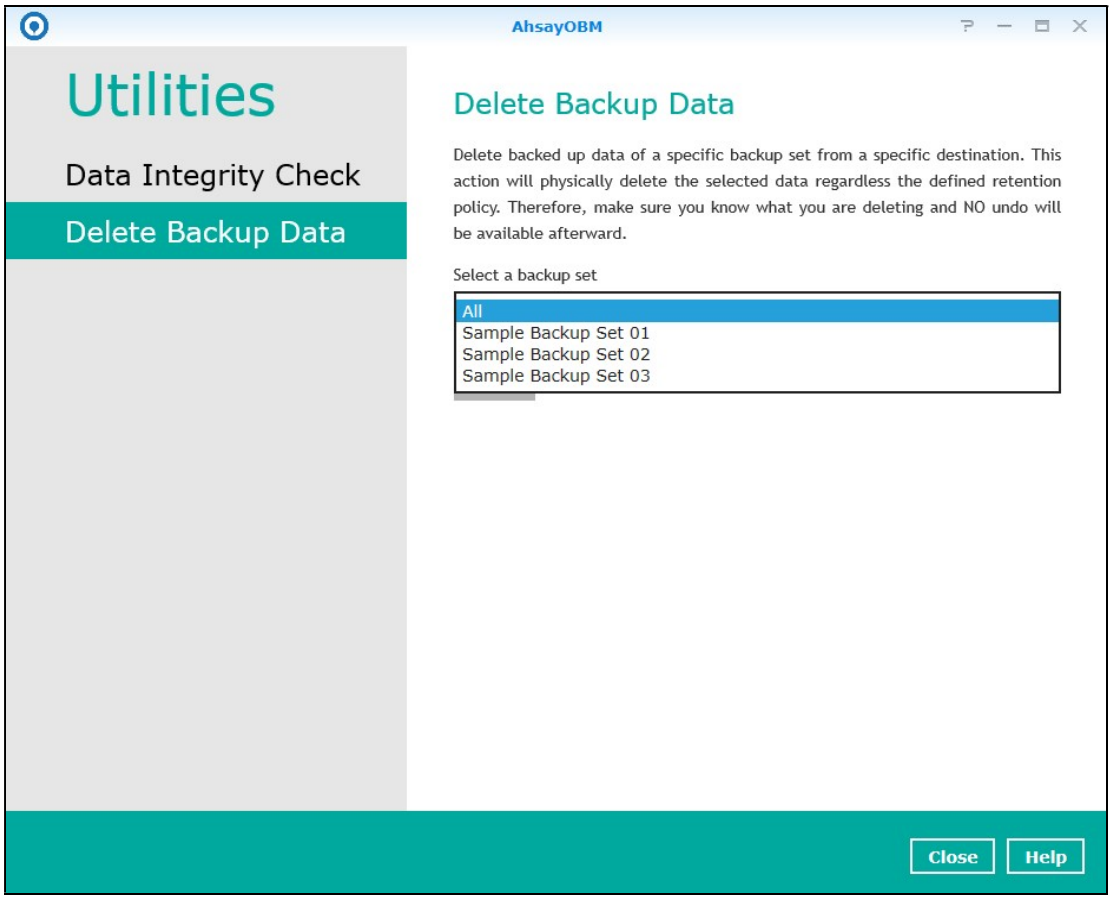
/volume_id/@appstore/product_name/.obm/system/IntegrityCheck

6.10.2 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.

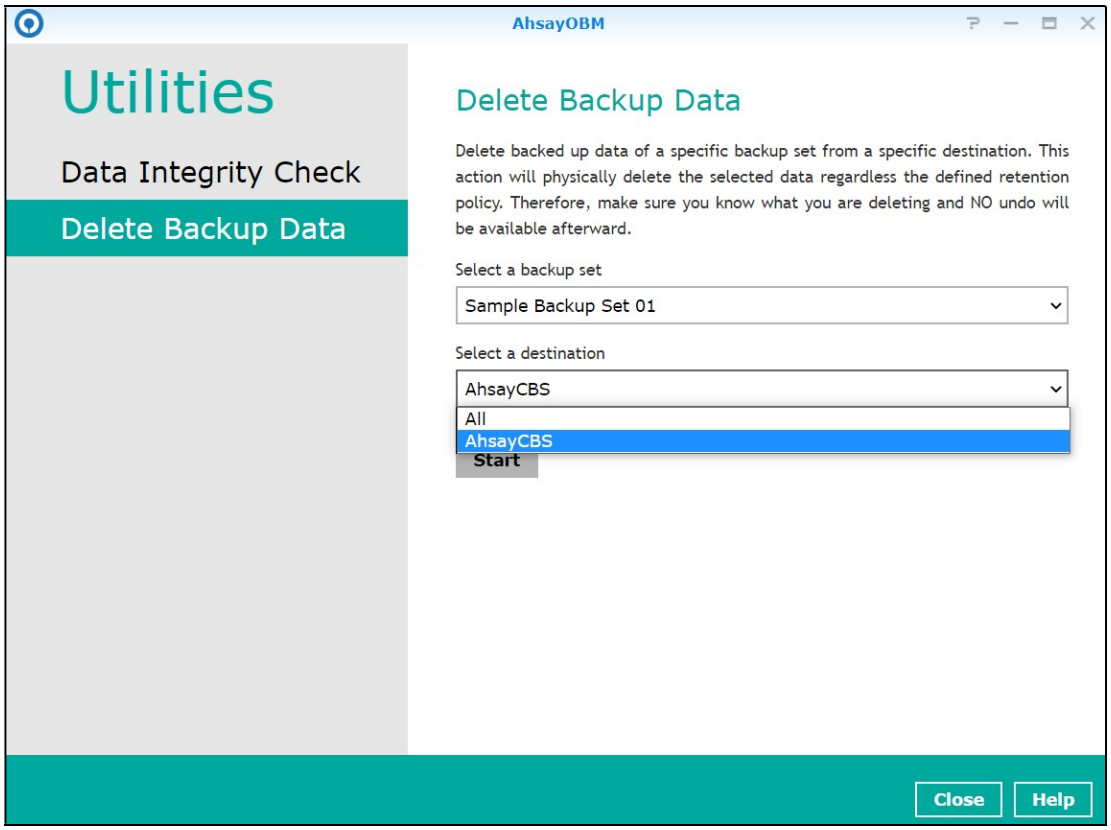
To perform deletion of backup data, follow the instructions below:

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

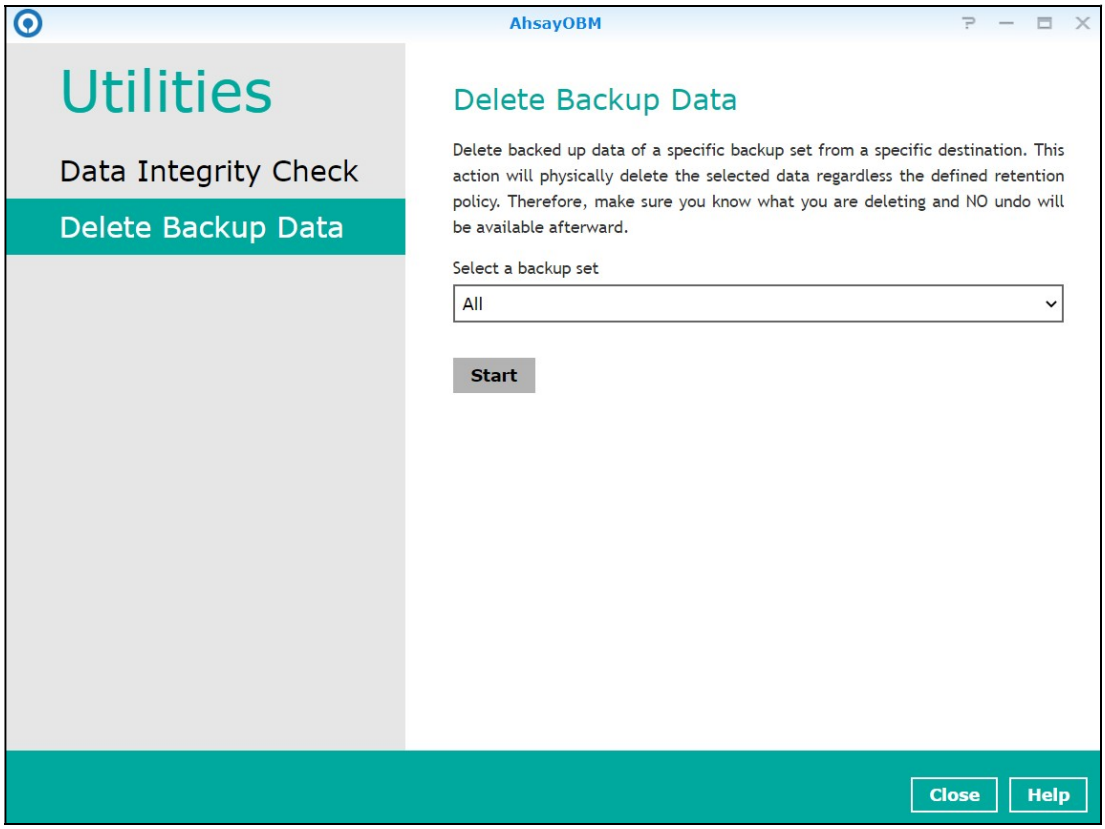


NOTE: This will only delete the backed up files in a backup set(s) and destination(s), but the backup set and destination will remain.

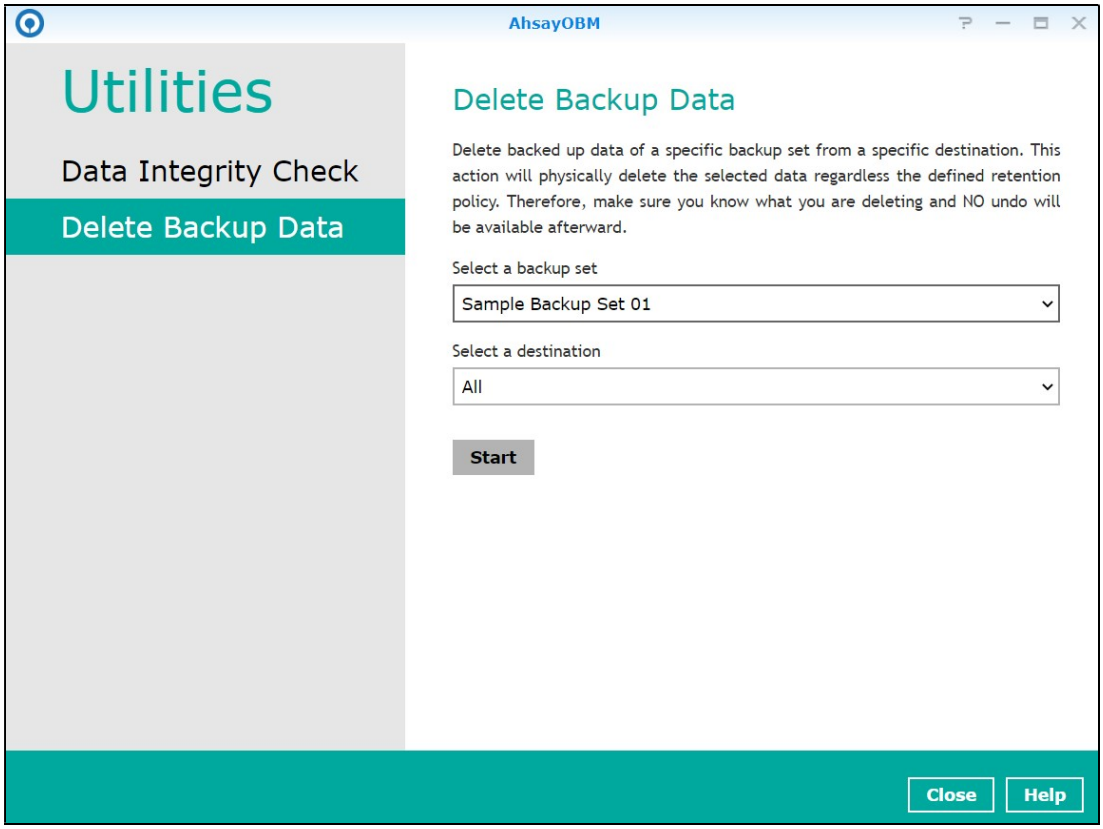
If you select a specific backup set, then you will also have to select a specific destination or all destinations.

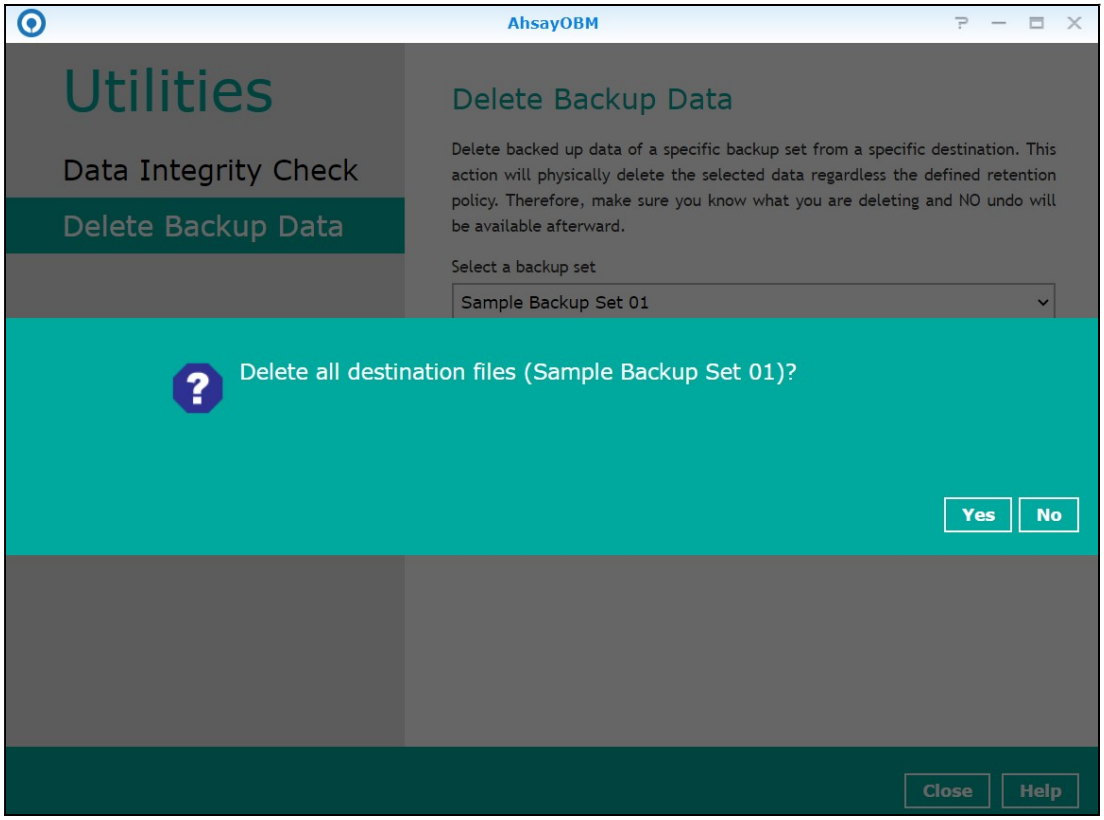


If you select **All** backup sets, then there is no need to select a destination.

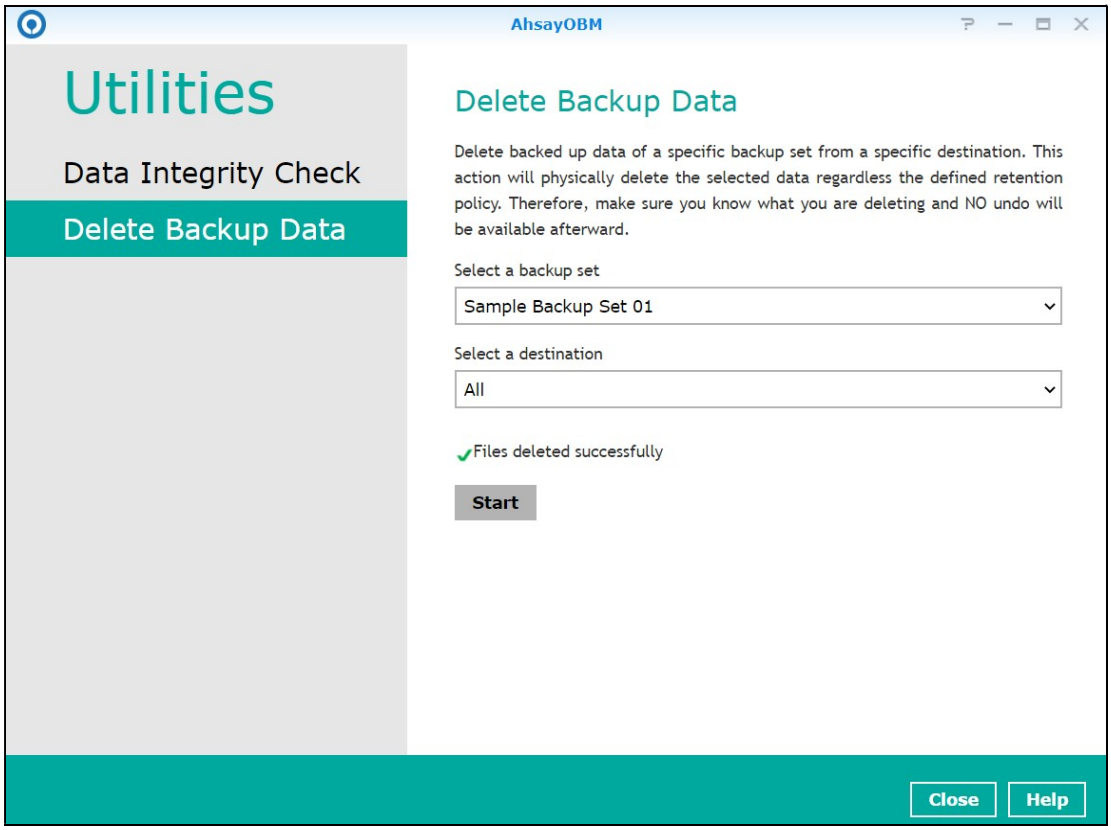


2. Click the **Start** button, then click **Yes** to proceed. This process will delete backed up data on the selected backup set(s) and destination(s).





3. Files are successfully deleted.

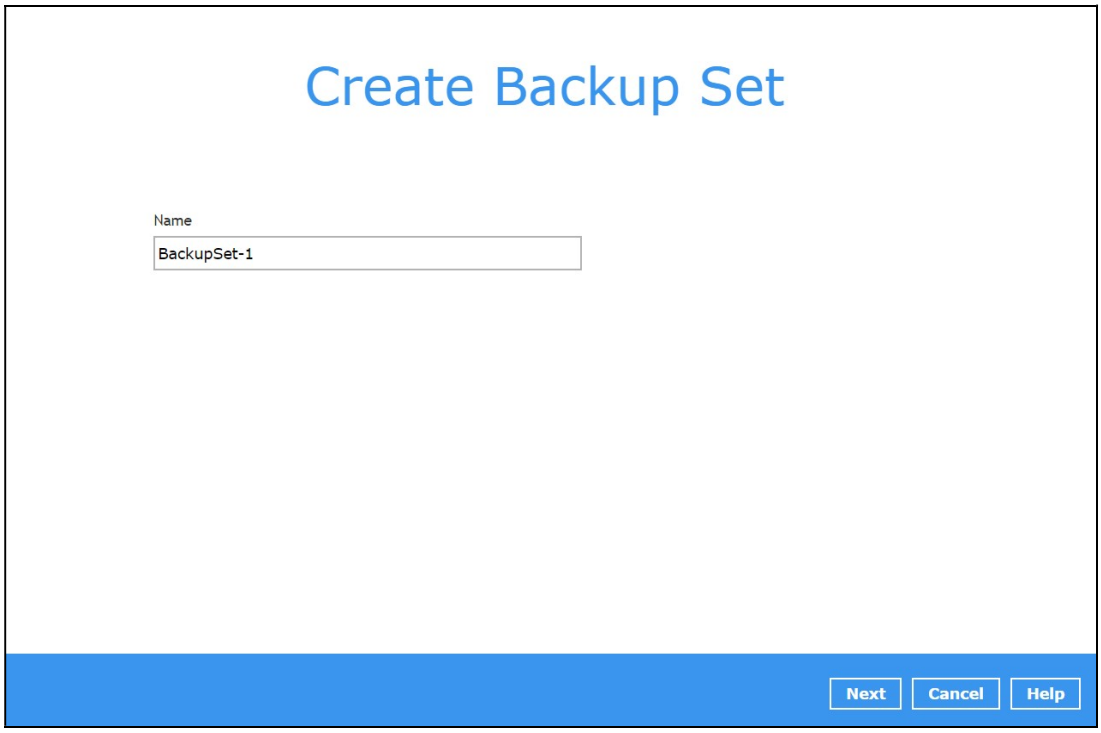


7 Create a Backup Set

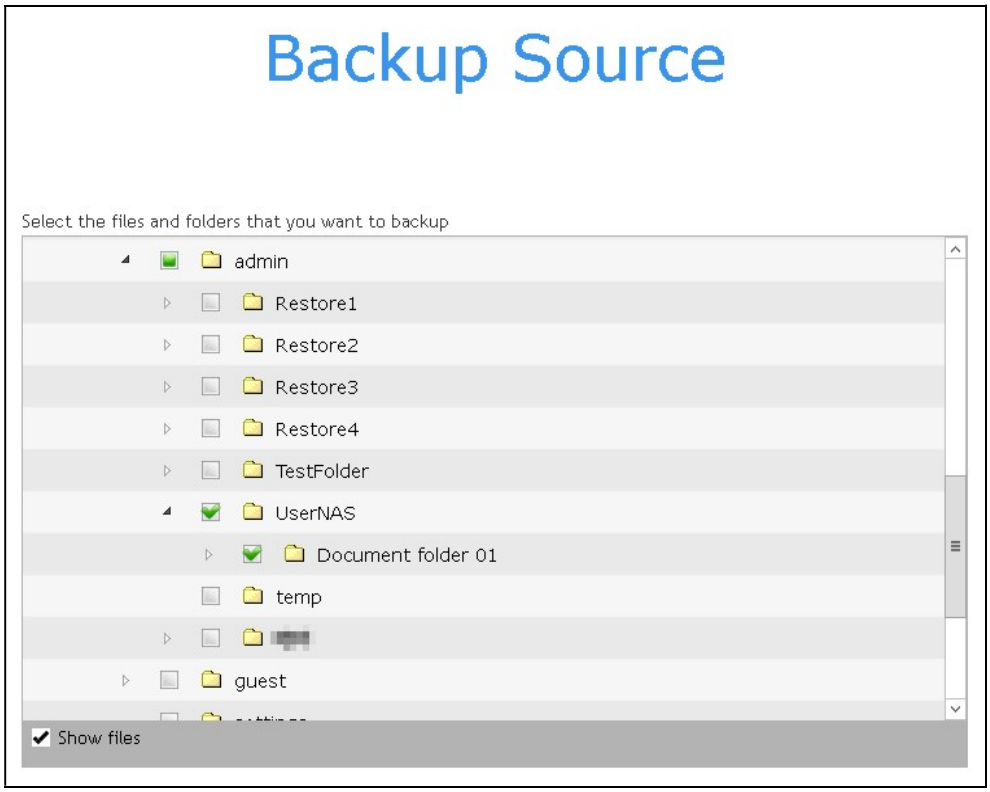
1. Click the **Backup Sets** icon on the main interface of AhsayOBM.

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

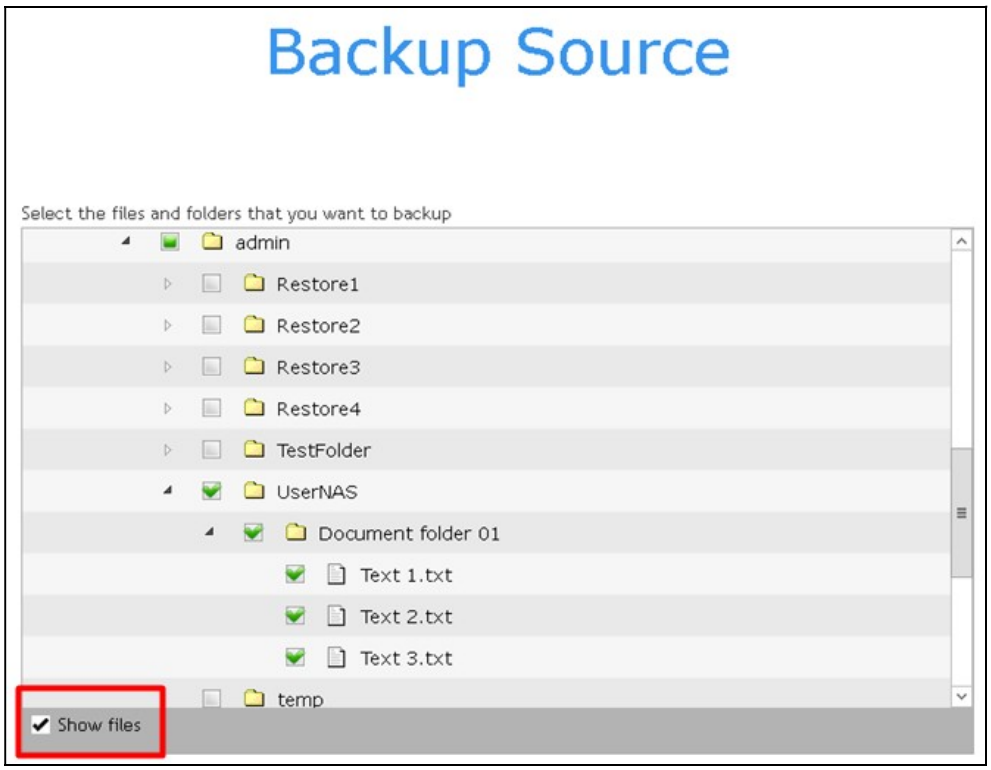
3. When the Create Backup Set window appears, name your new backup set, then click **Next** to proceed.



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.

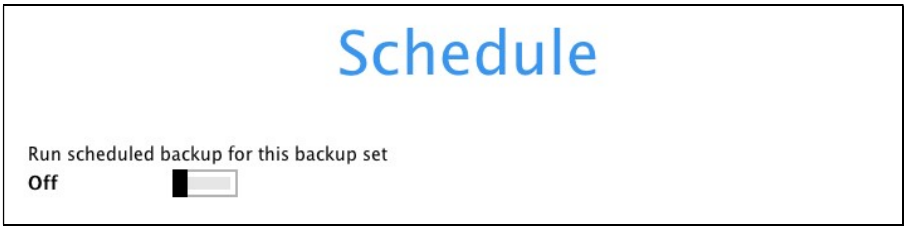


NOTE: *AhsayOBM can only back up files or folders displayed under the File Station on the DiskStation Manager.*

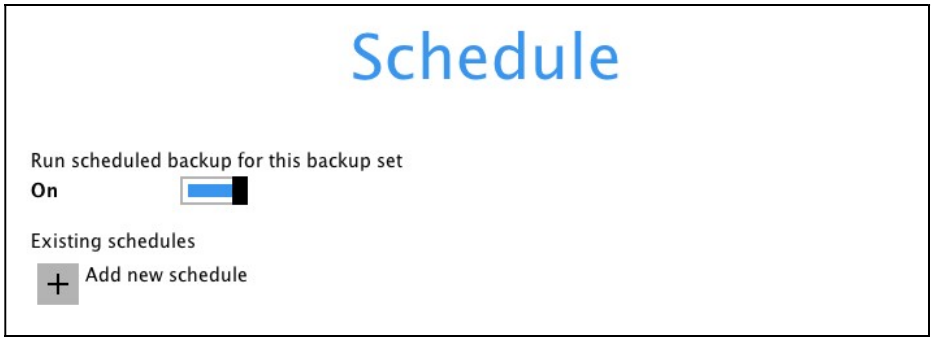
6. In the Backup Source window, click **Next** to proceed.

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

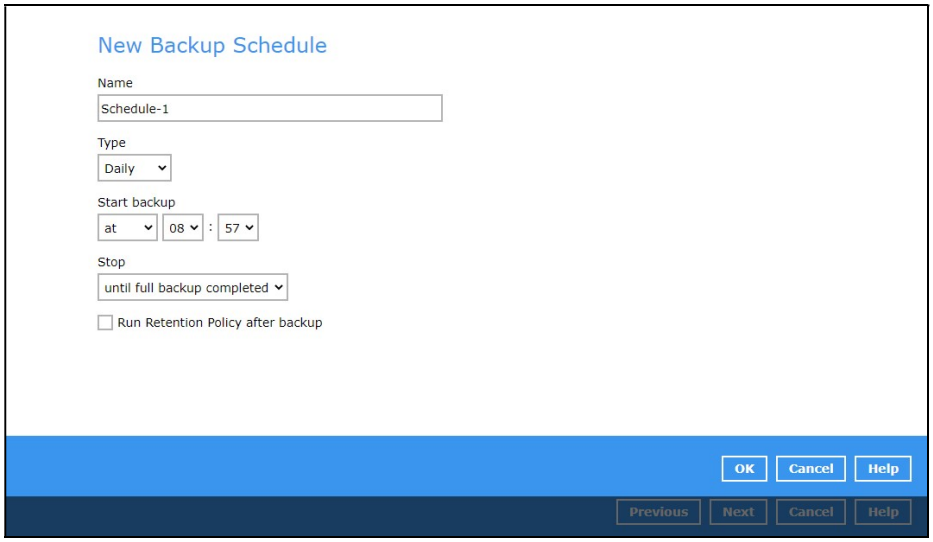
   - In the Schedule window, the Run scheduled backup for this backup set is **Off** by default. You can leave it as is if you want to add a schedule later.



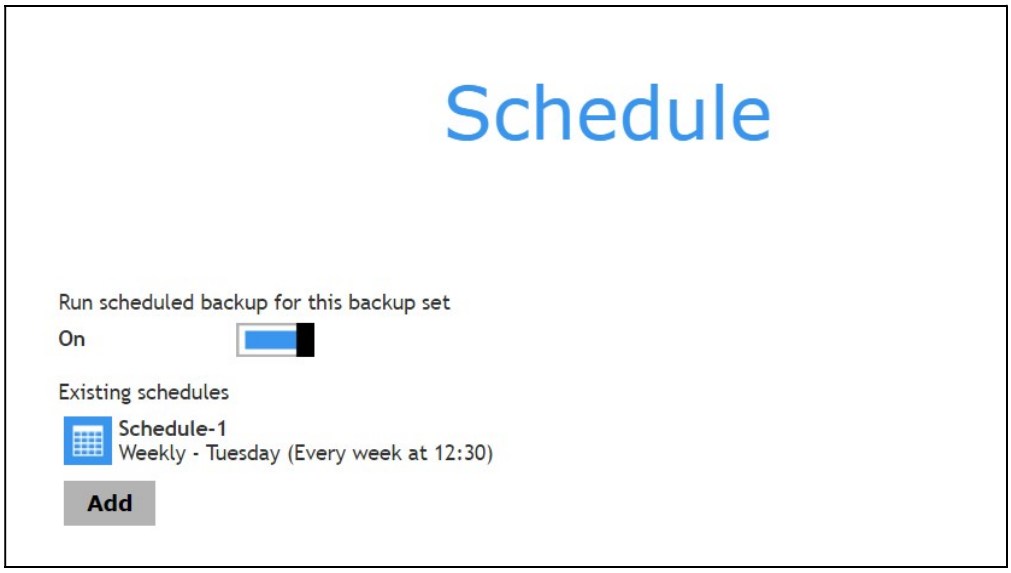
   If you want to add a schedule now, switch on **Run scheduled backup for this backup set**. Then, click "**+**" next to Add New schedule.



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



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.



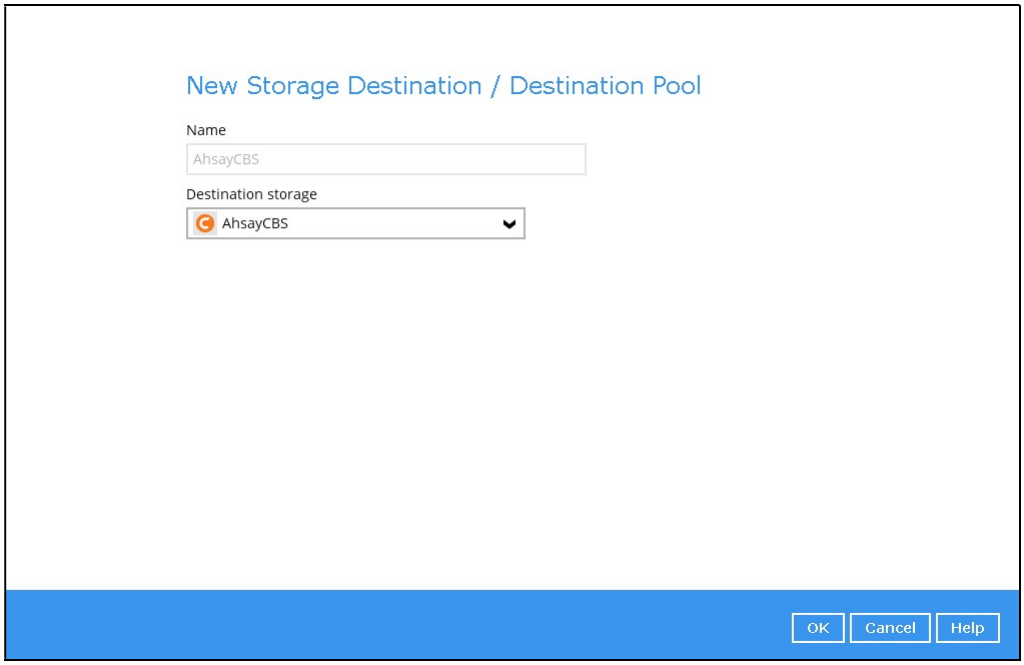
9. Configure the backup destination.

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.

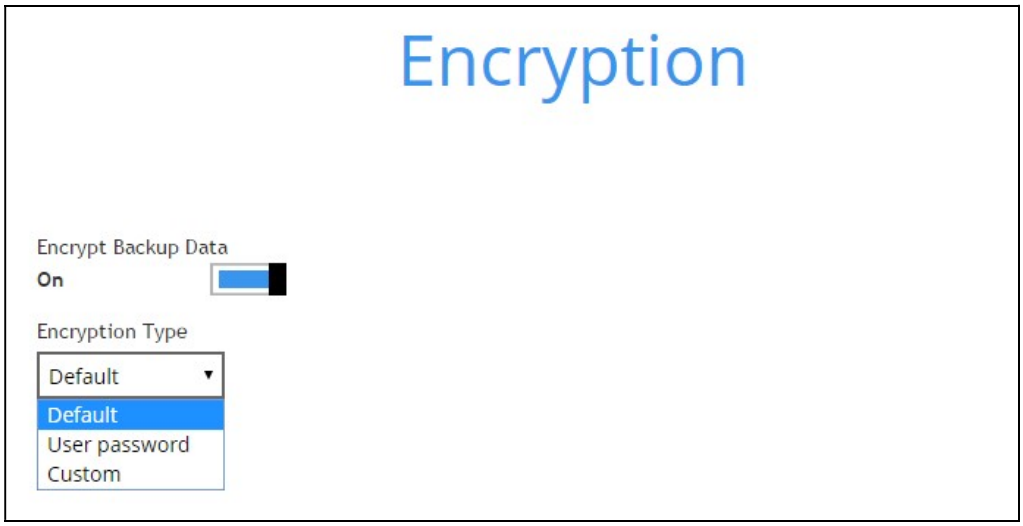
10. In the New Storage Destination / Destination Pool window, select the destination type and destination storage. Then, click **OK** to confirm your selection.



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

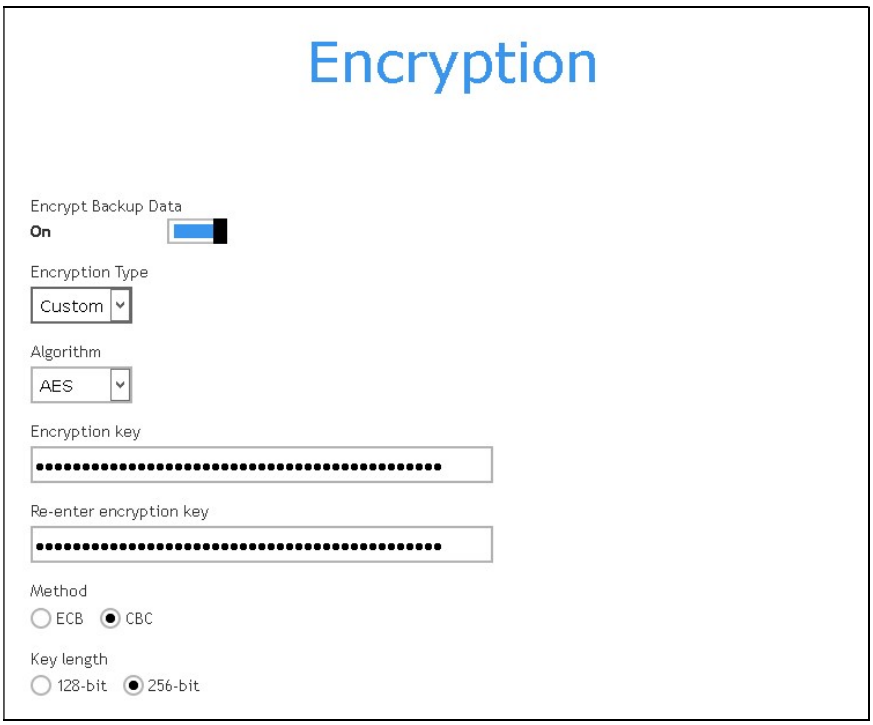
11. In the Destination window, your selected storage destination will be shown. Click **Next** to proceed.

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.



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

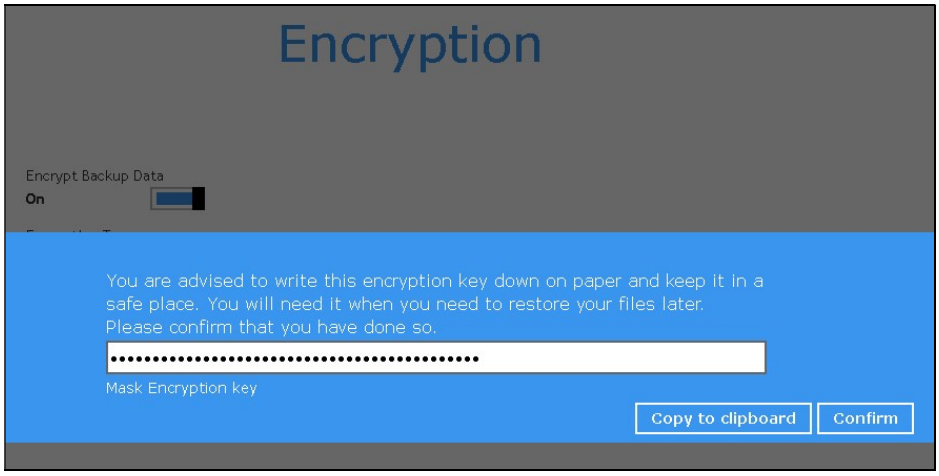
- **Default** – an encryption key with 44 alphanumeric characters will be randomly generated by the system.
- **User password** – the encryption key will be the same as the login password of your AhsayOBM at the time when this backup is created. Please be reminded that if you change the AhsayOBM login 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.



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

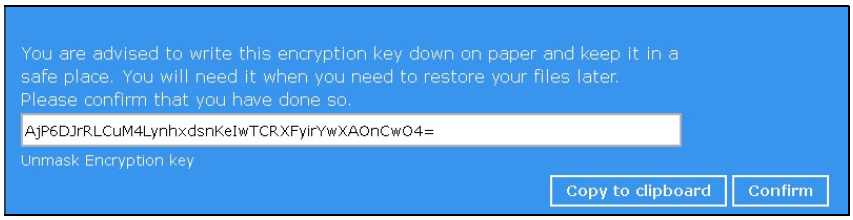
Click **Save** when you are done with the settings.

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.



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

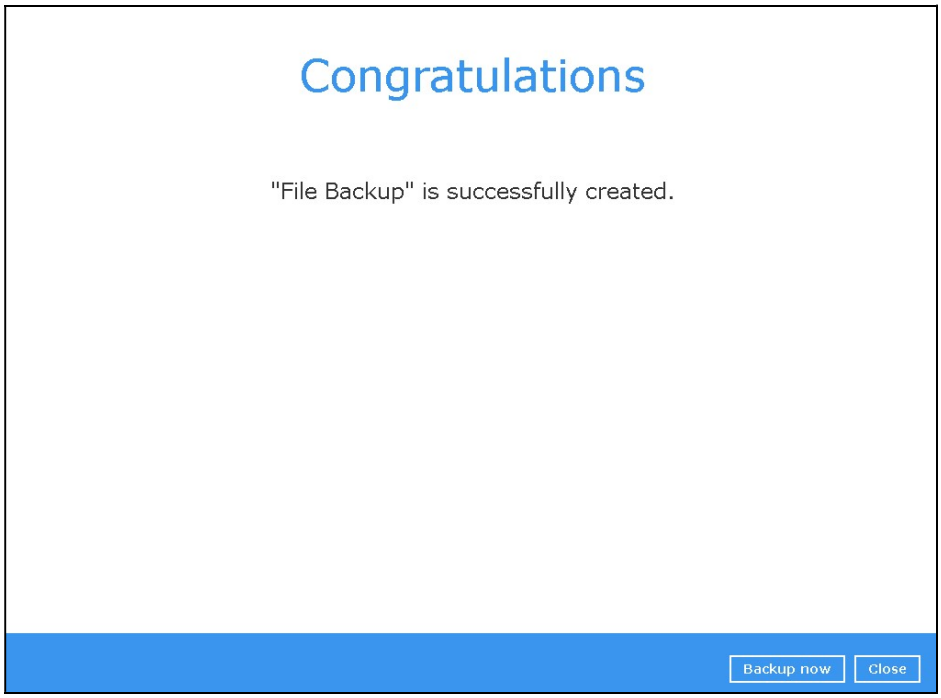
- **Unmask encryption key** – The encryption key is masked by default. Click this option to show the encryption key.



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

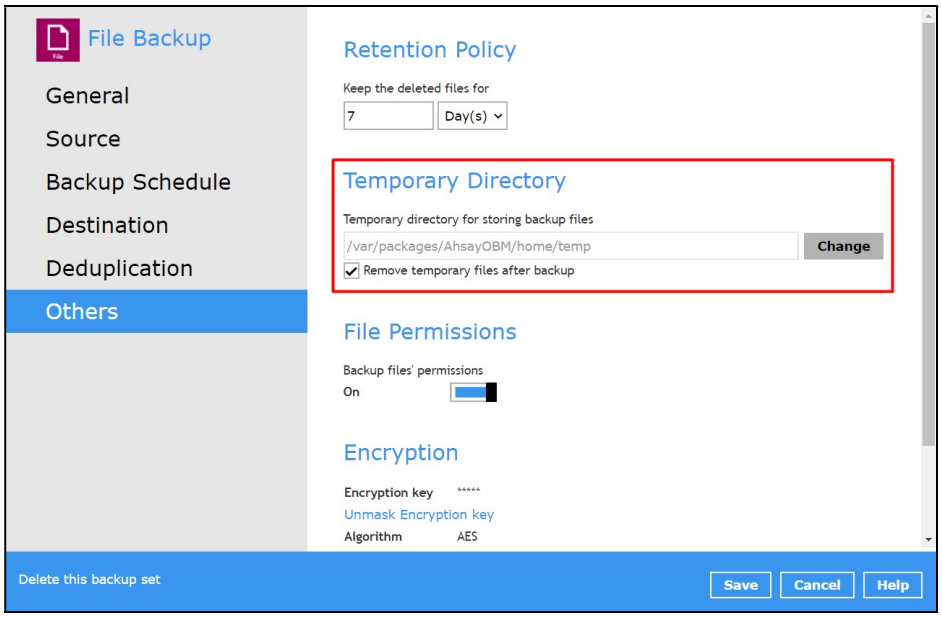
- **Confirm** – Click to exit this pop-up window and proceed to the next step.

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.



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

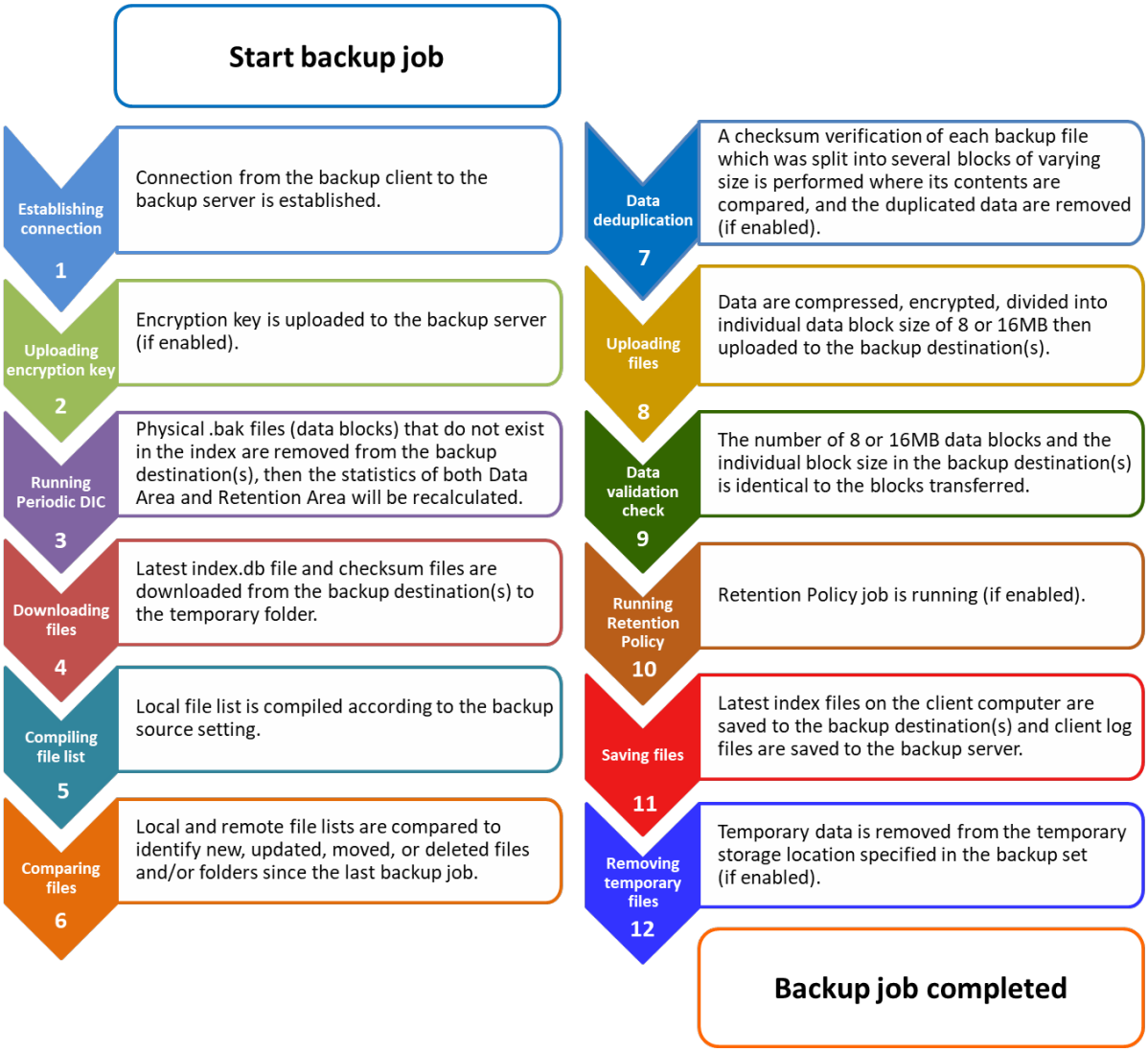
    Go to **Others** > **Temporary Directory**. Click **Change** to browse for another location.



8 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)**



8.1 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:

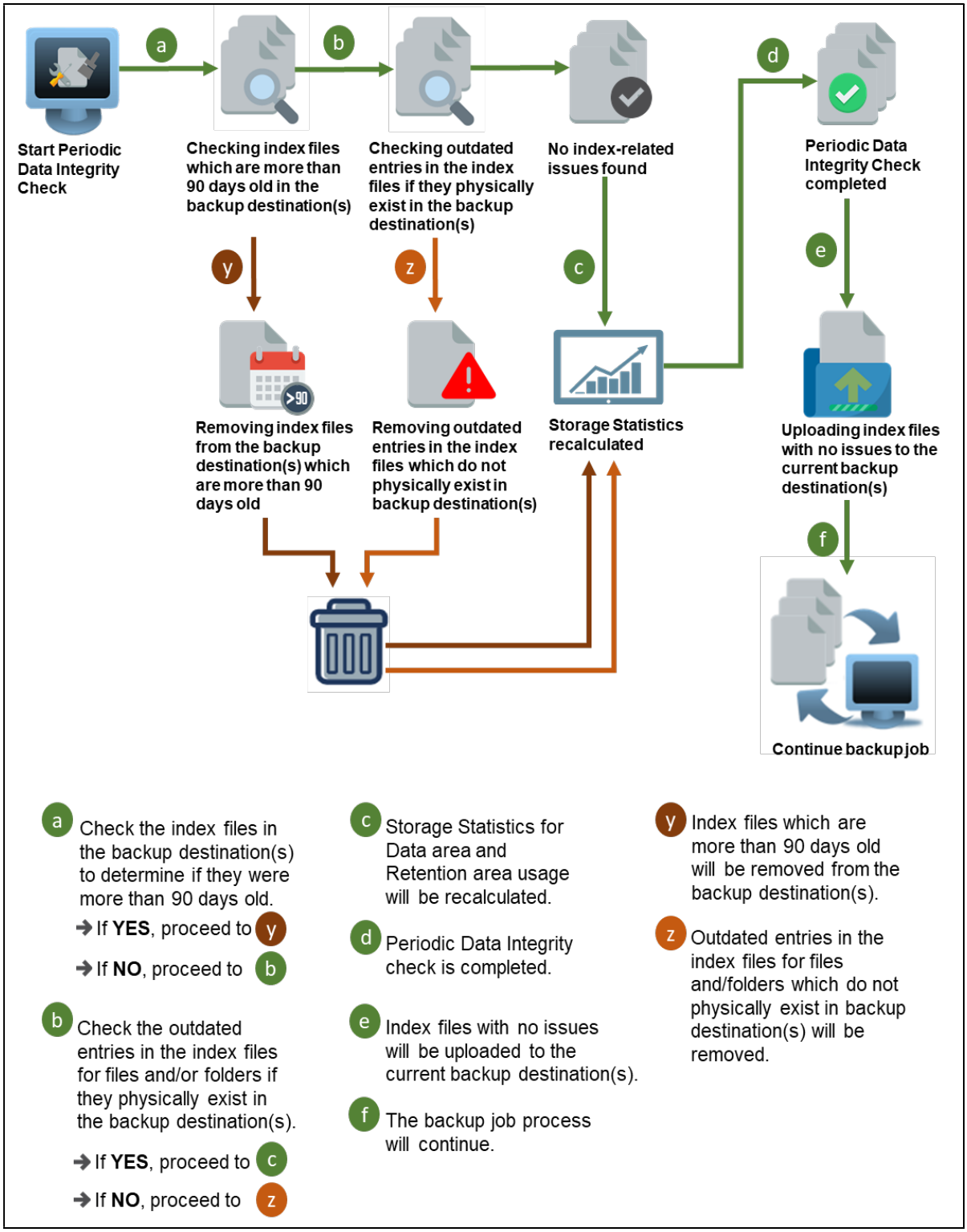
- the PDIC will run on the first backup job that falls on Wednesday; or
- if there is no active backup job(s) running from Monday to Friday, then the PDIC will run on the next available backup job.

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.



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.

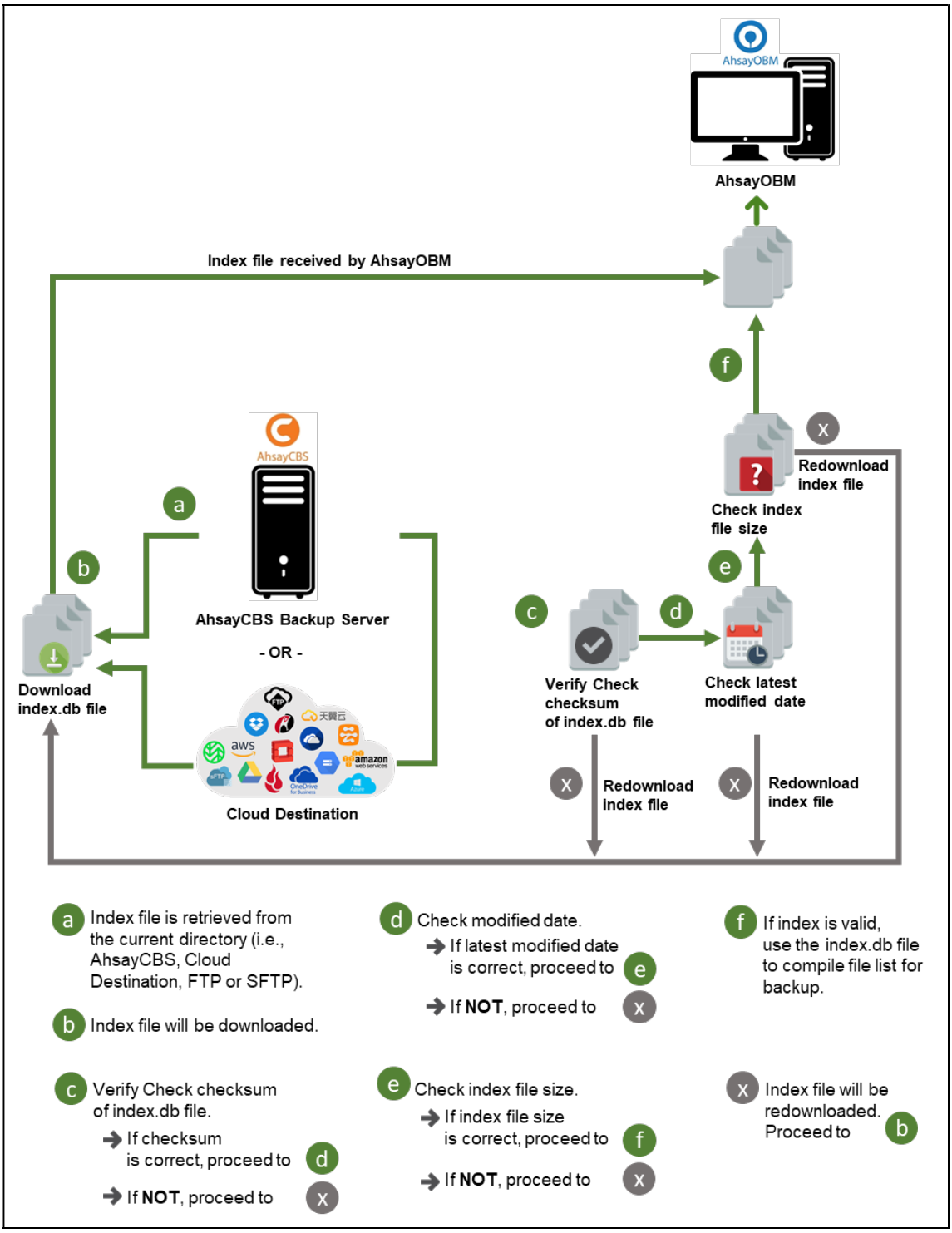
y Index files which are more than 90 days old will be removed from the backup destination(s).

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

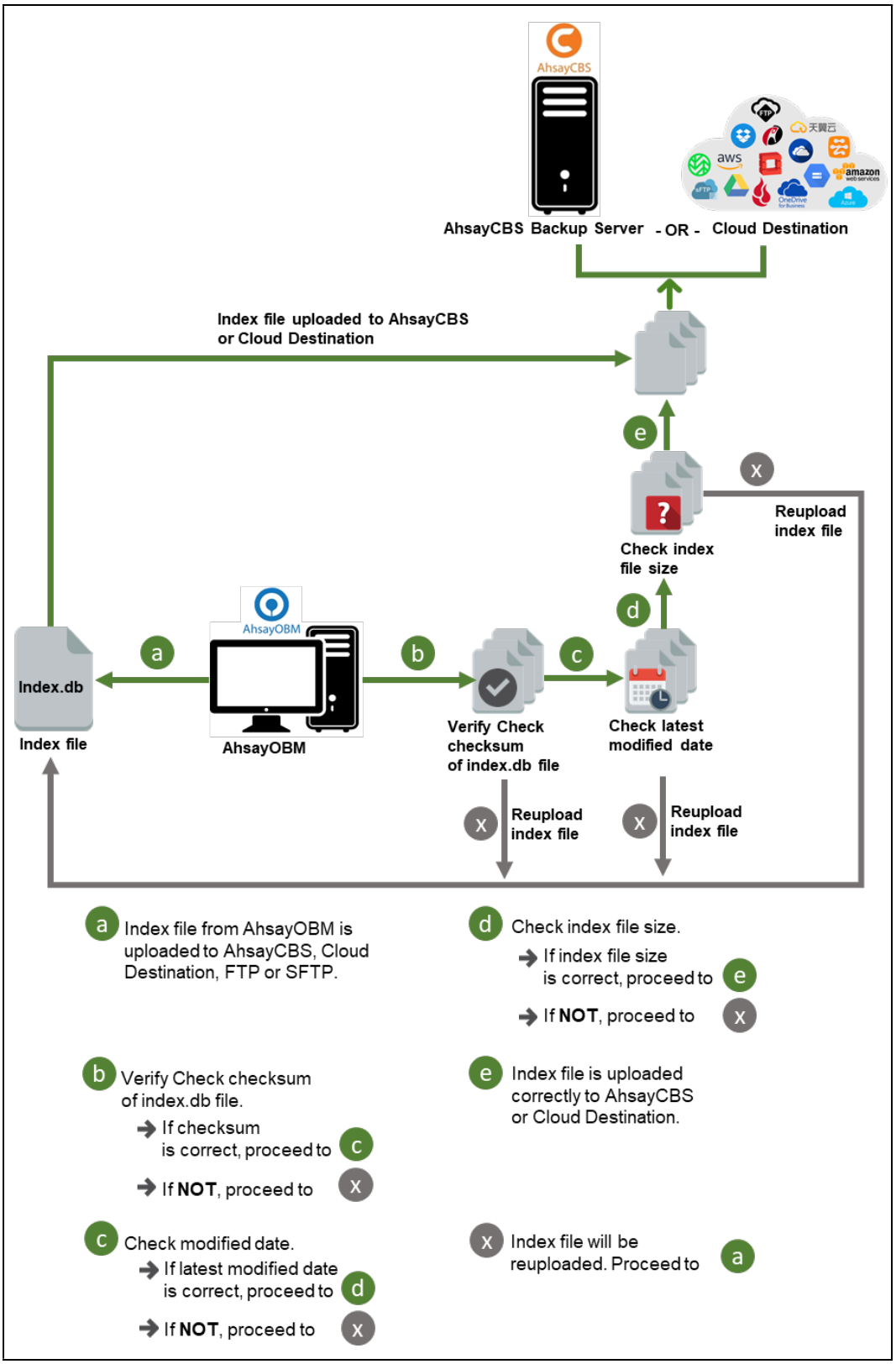
8.2 Backup Set Index Handling Process

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.

8.2.1 Start Backup Job

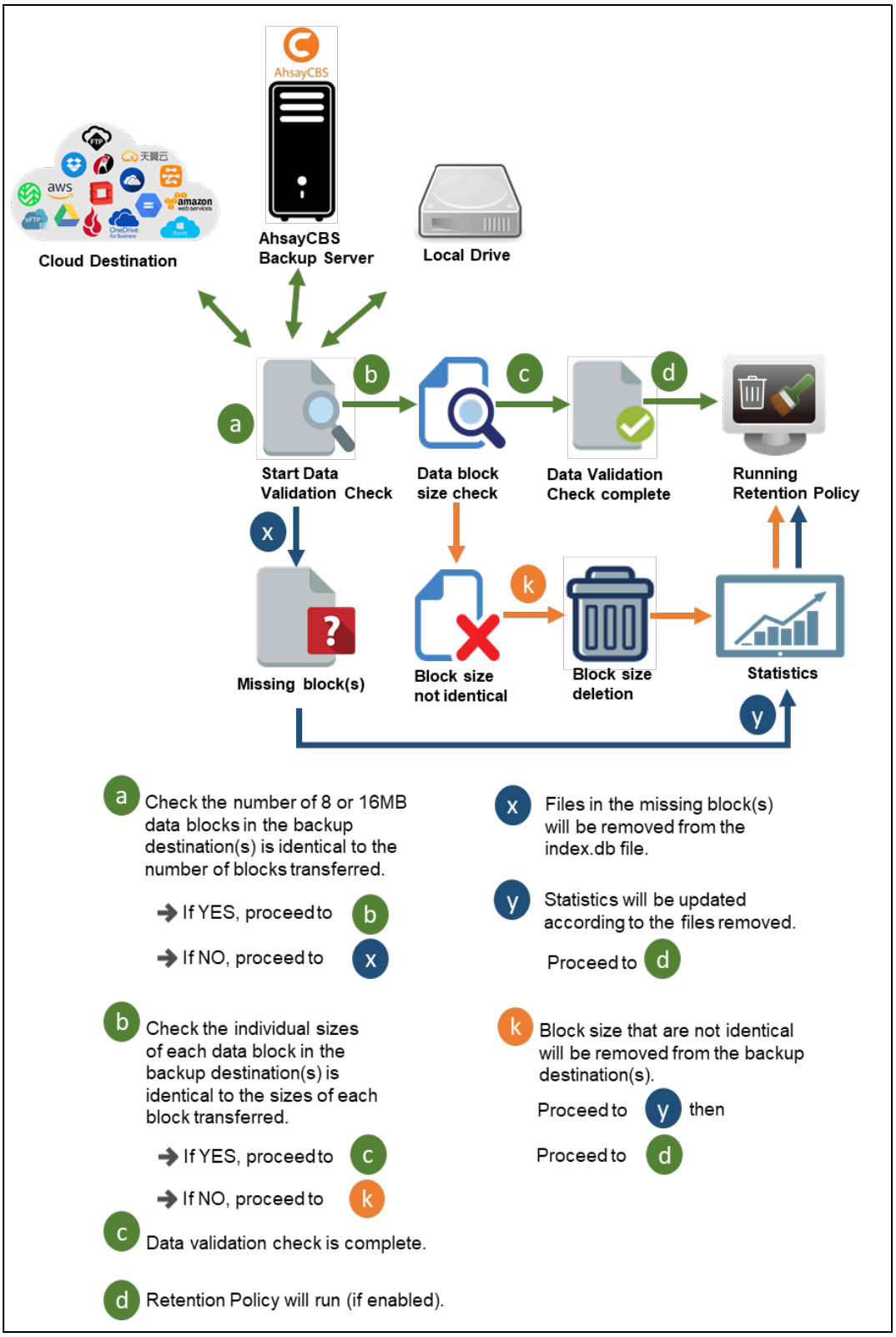


8.2.2 Completed Backup Job



8.3 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.



9 Run Backup Jobs

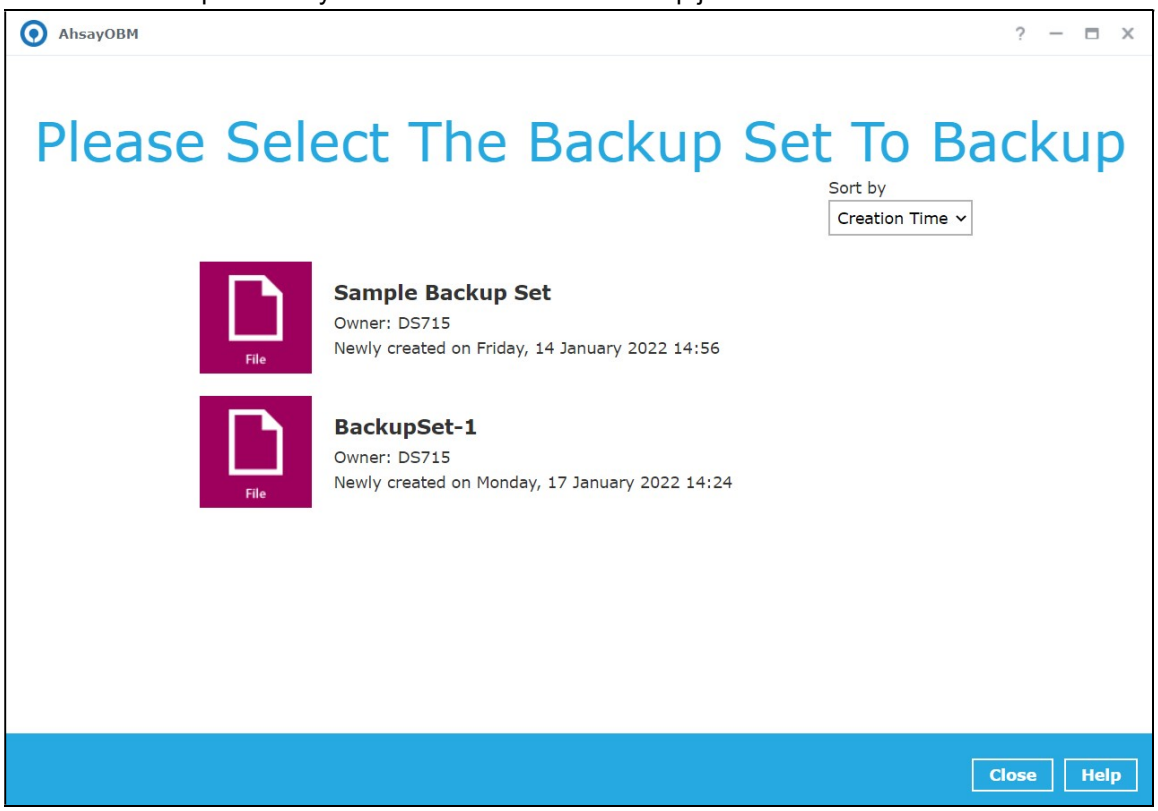
9.1 Login to AhsayOBM

Login to the AhsayOBM application according to the instructions provided in Chapter 5.2 Login to AhsayOBM.

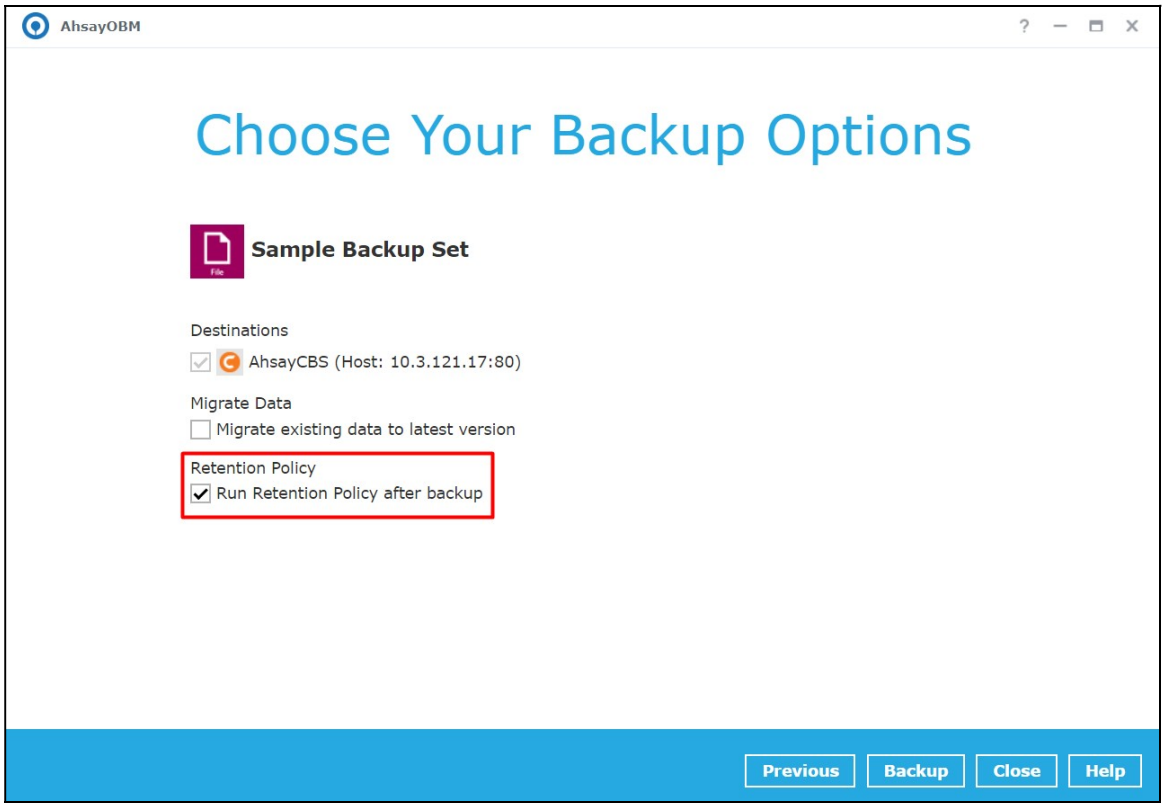
9.2 Start a Manual Backup

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

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



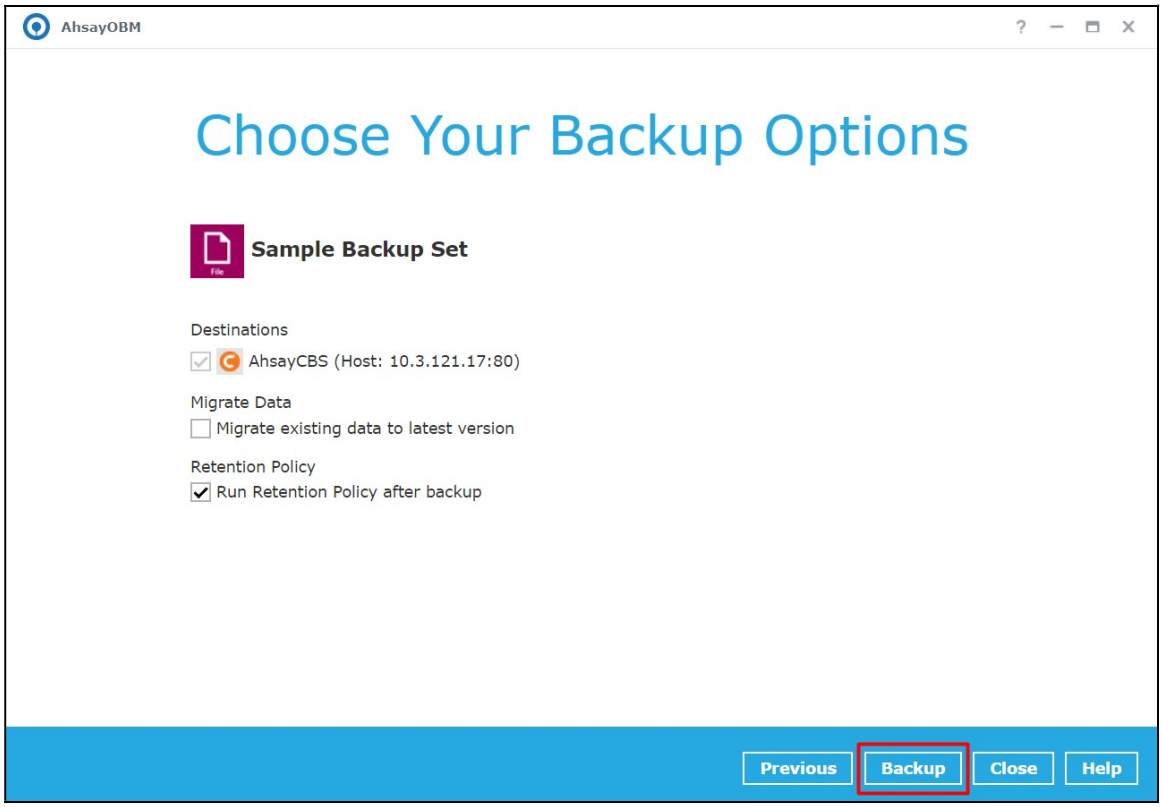
3. When the following screen is displayed, it is recommended to enable the **Run Retention Policy after backup**. This will help you save hard disk quota in the long run.



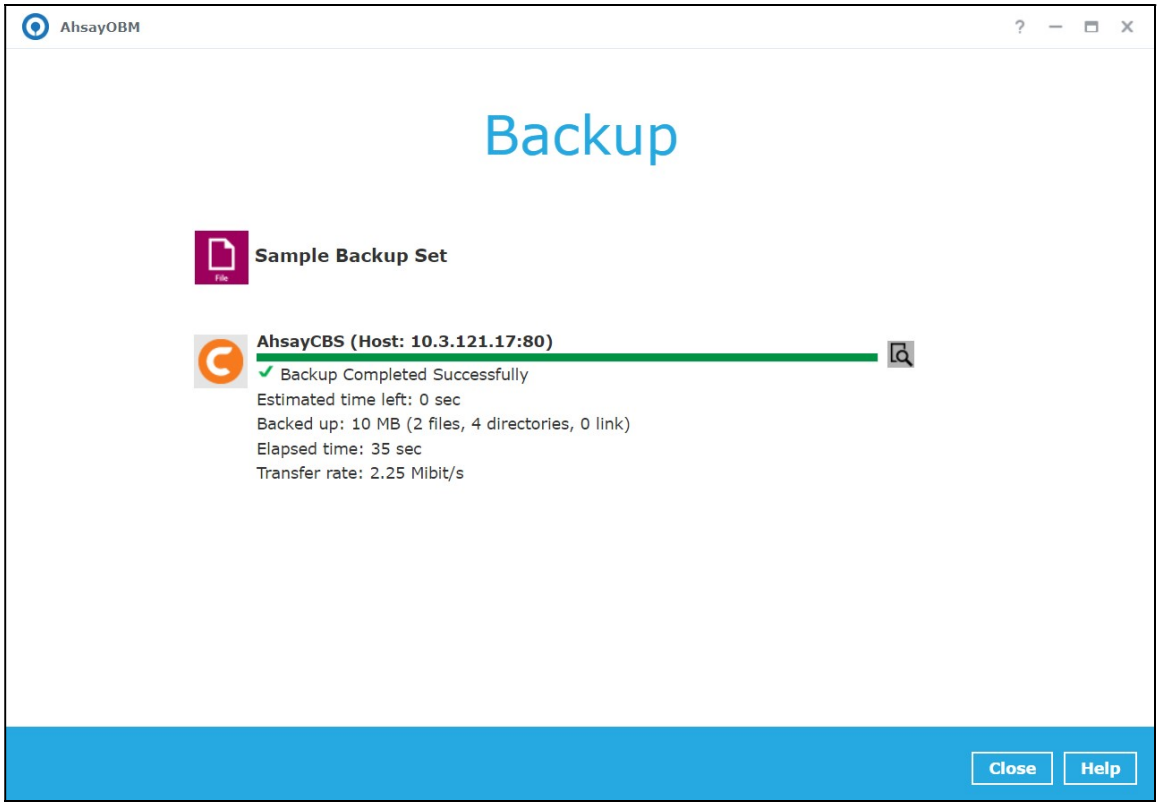
NOTE

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

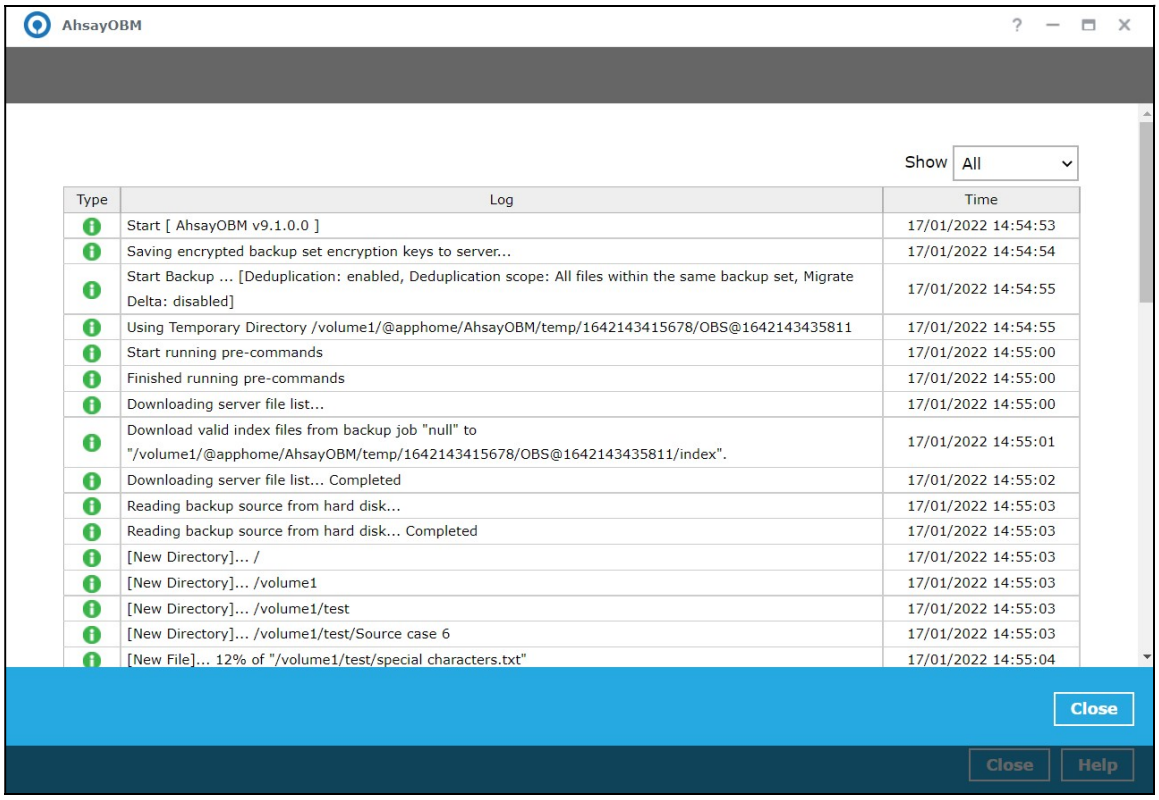
4. Once done with the settings, click the **Backup** button to start the backup job.



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.



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



10 Restore Data

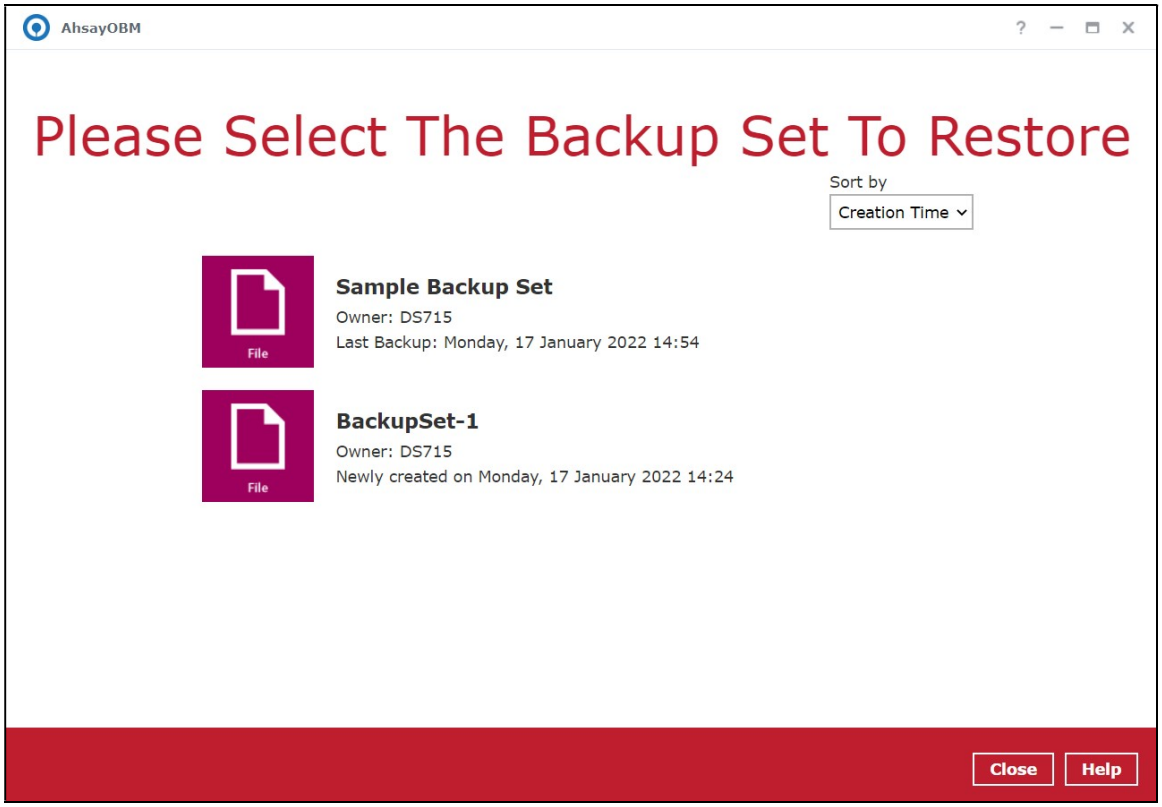
10.1 Login to AhsayOBM

Login to the AhsayOBM application according to the instructions provided in Chapter 5.2 Login to AhsayOBM.

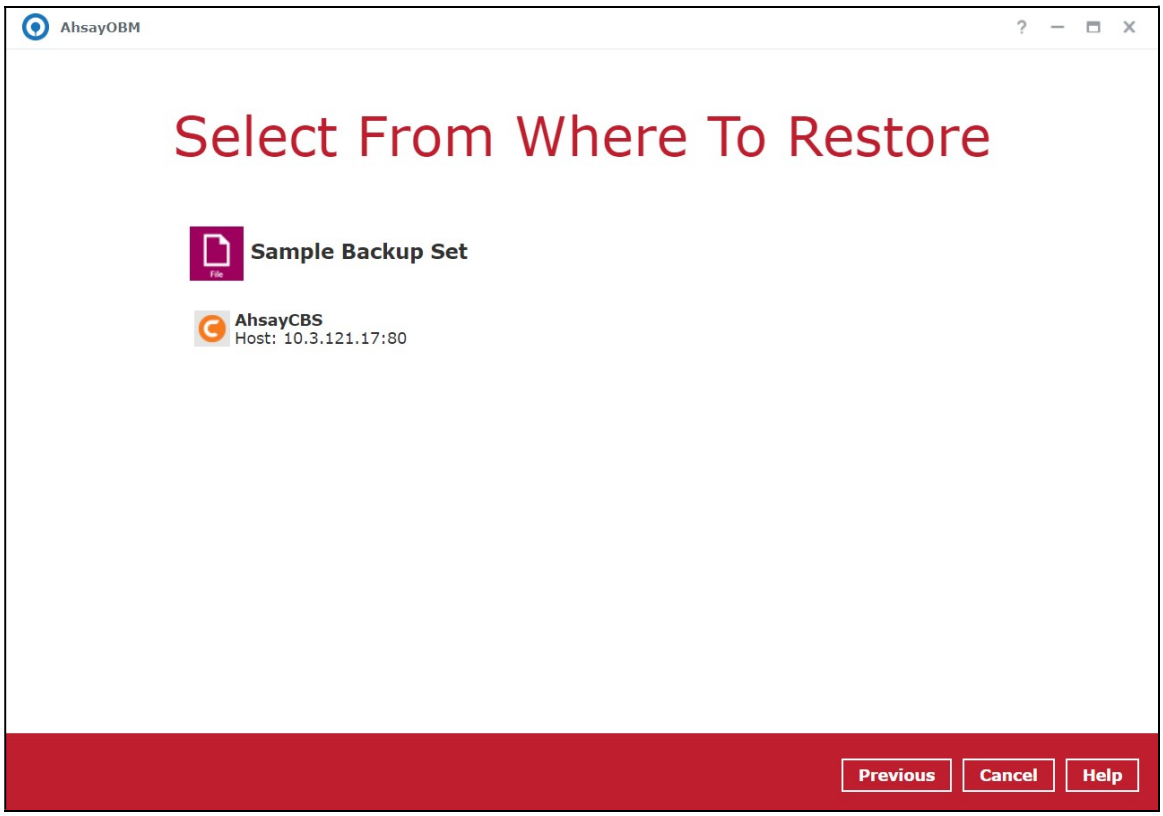
10.2 Restore Data

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

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



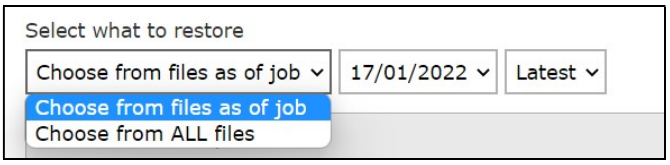
3. Select the destination where you would like to restore your data from.

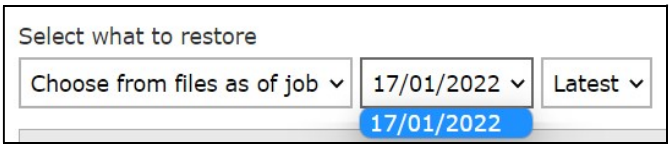


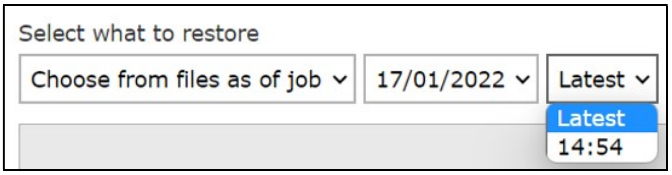
4. Select to restore files from a specific backup job, or from ALL files available. Then, select the files or folders that you would like to restore.

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

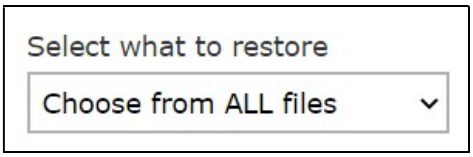
   - Choose **from files as of job** – This option allows you to select a backup version from a specific date and time to restore.

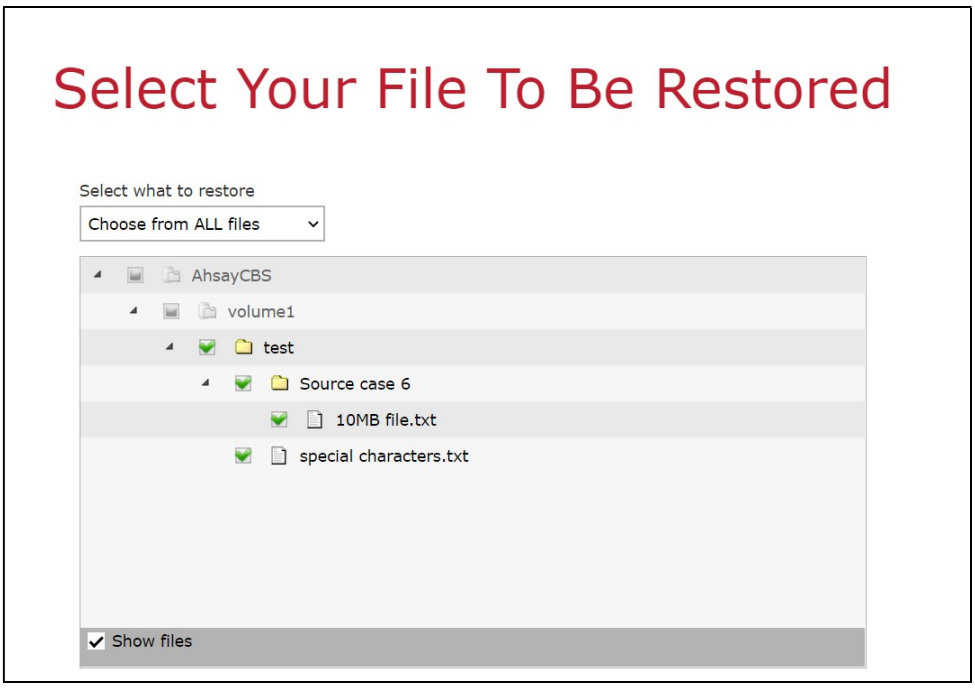




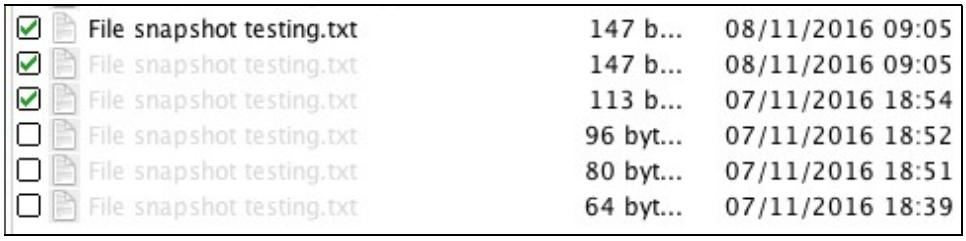


- **Choose from ALL files** – This option allows you to restore all the available backup versions for this backup set. Among all the available backup versions, you can also select only some of the backup versions of a file to restore.

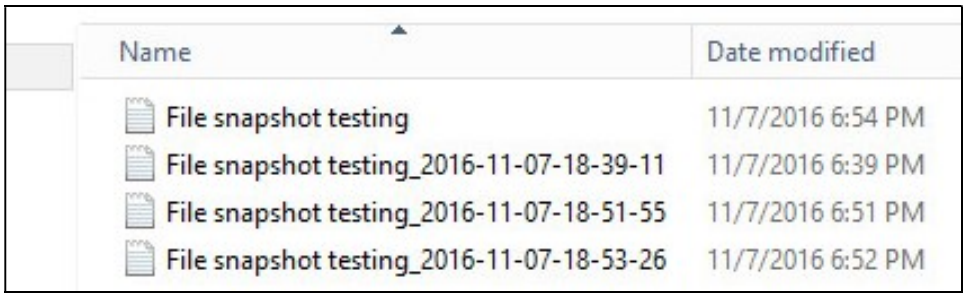




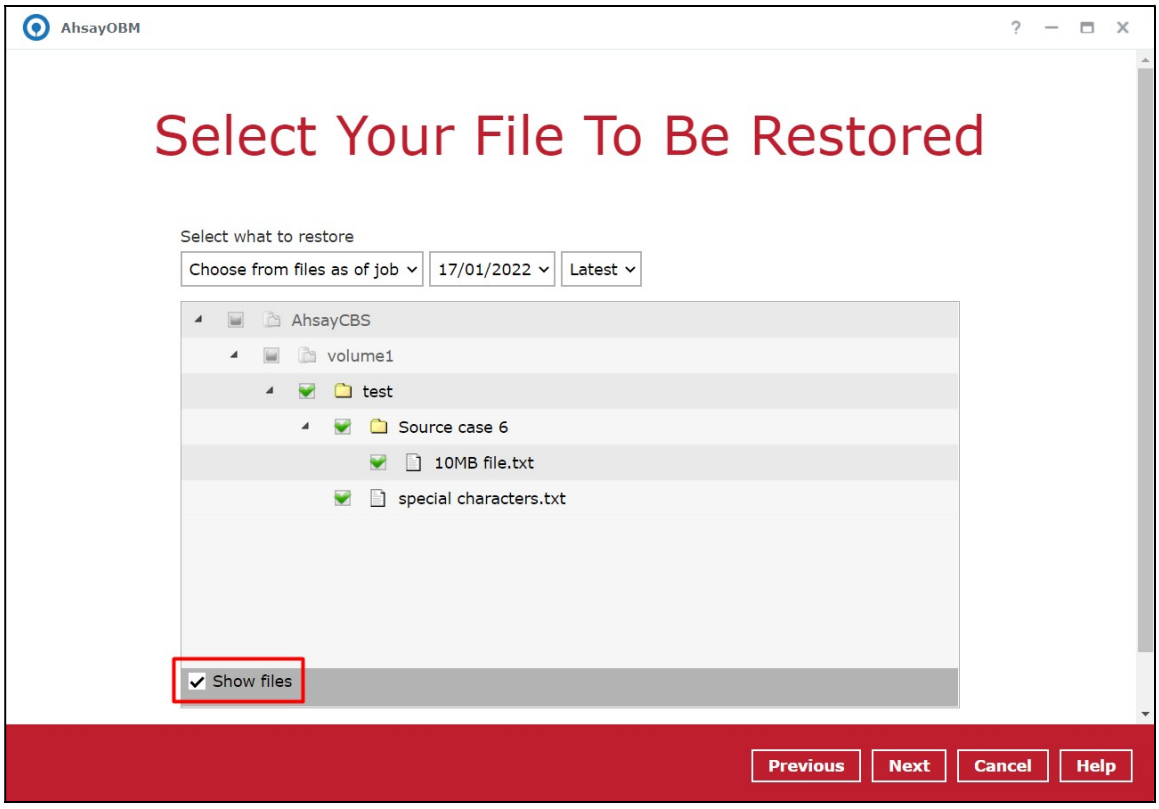
Below is an example showing all the available backup versions of the file **File snapshot testing.txt**. The latest version is shown in solid black color and all the previous versions are shown in grey color. You can identify the file version from the **Date modified** column.



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.



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



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

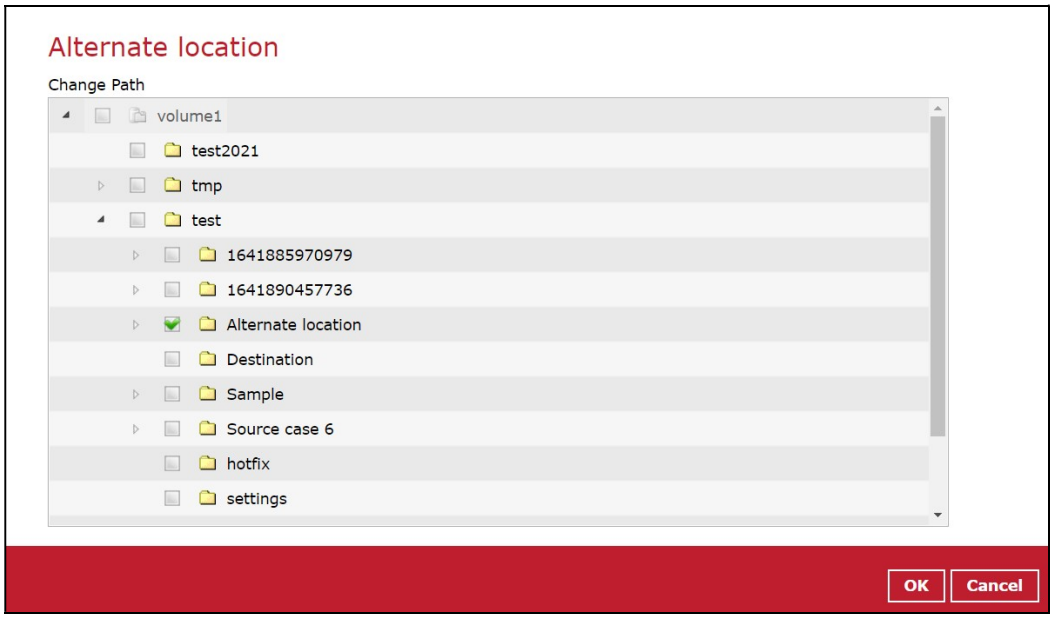
   - **Original location** – the backed-up data will be restored to the computer running the AhsayOBM under the same directory path as on the machine storing the backup source.

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

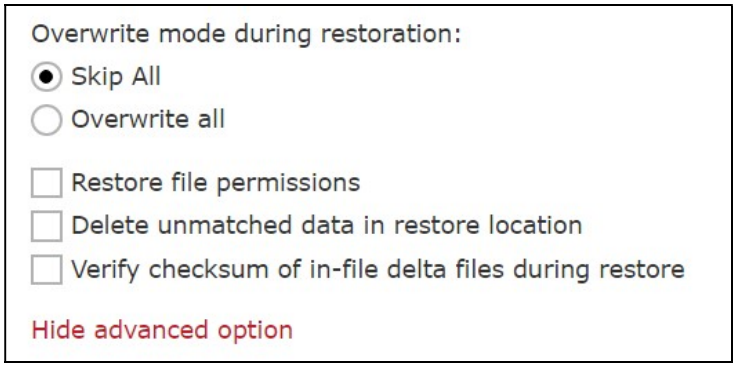
     Users/[User's Name]/Downloads,

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

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



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



- **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**

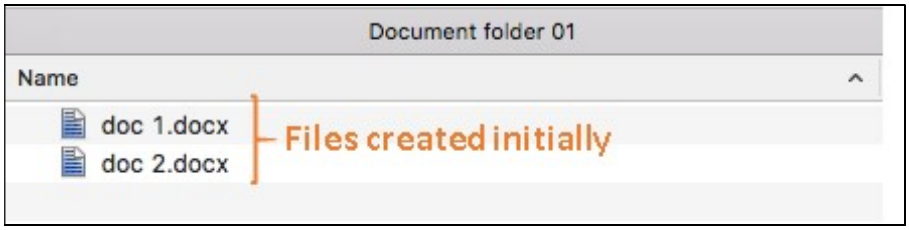
  Restore file permissions is disabled by default. When you perform a file restore on a shared computer, it is recommended that you enable Restore file permissions by ticking the checkbox so that the files restored will not be fully accessible to everyone using the shared computer.

- **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.

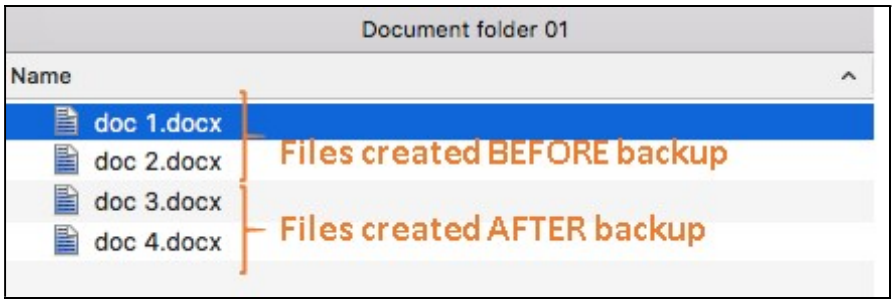
  Example:

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



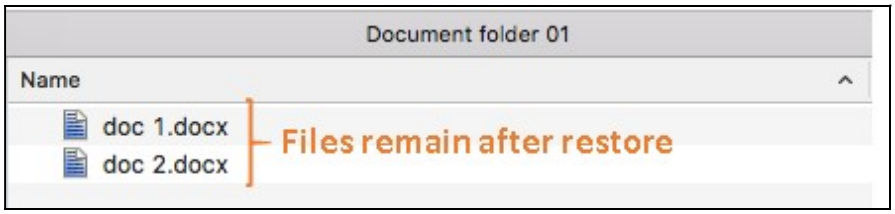
  ii) A backup is performed for folder **Document folder 01**.

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



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

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



WARNING

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

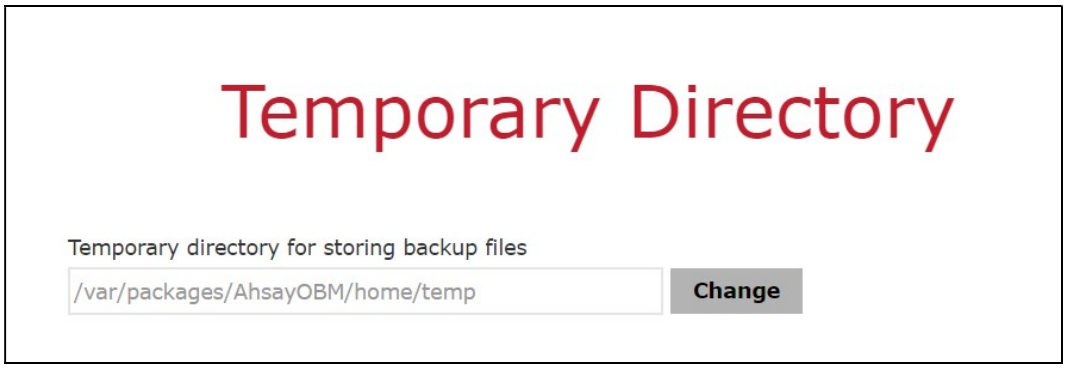
- **Verify checksum of in-file delta files during restore**

  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.

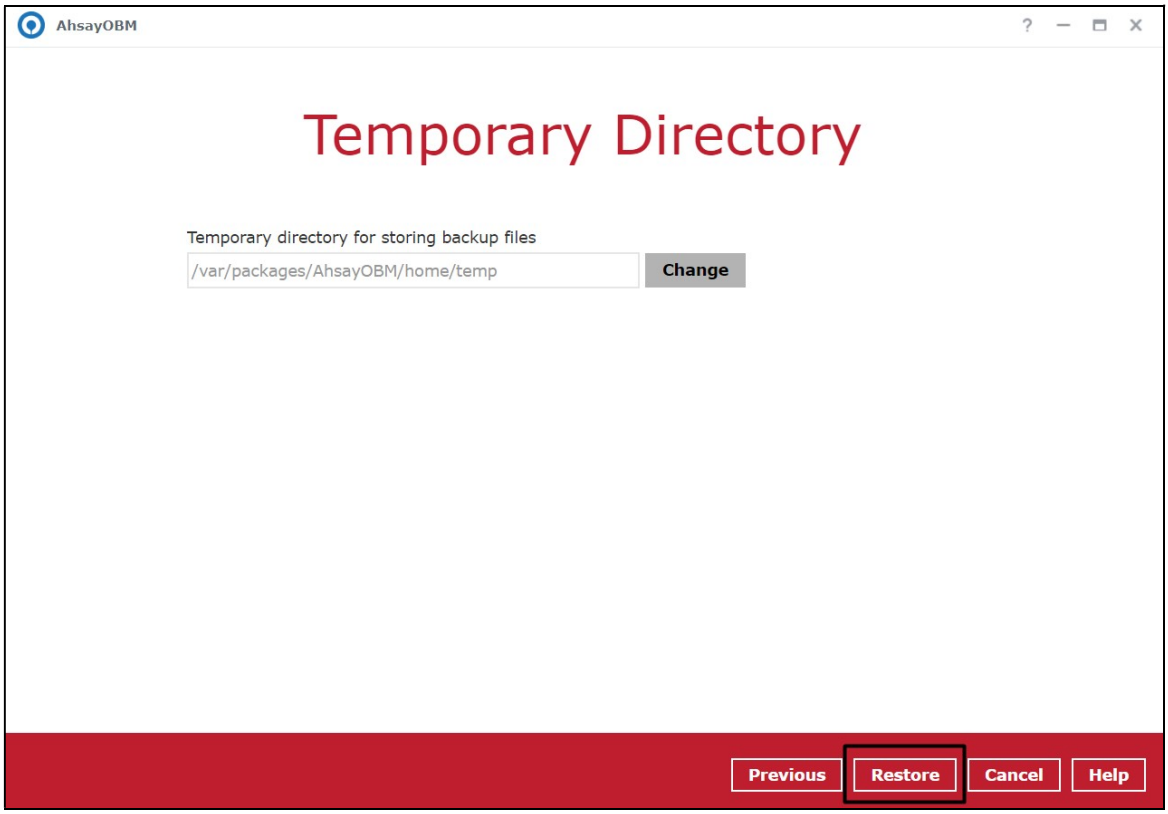
8. Click **Next** to proceed when you are done with the settings.

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

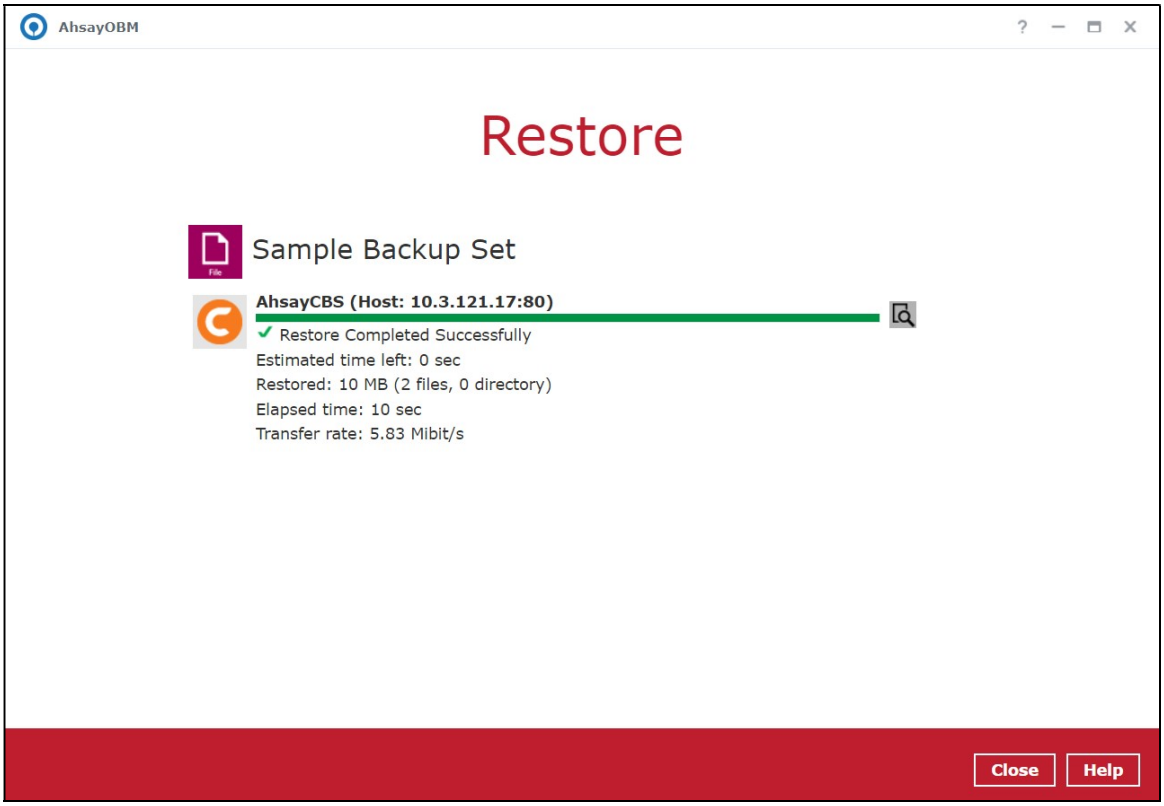
   By default, the temporary files are stored under the temp directory of the user profile directory. In case the same directory path does not exist in the computer where AhsayOBM is running, you have to click **Browse** to define a new location for storing the temporary files. Otherwise, you will not be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



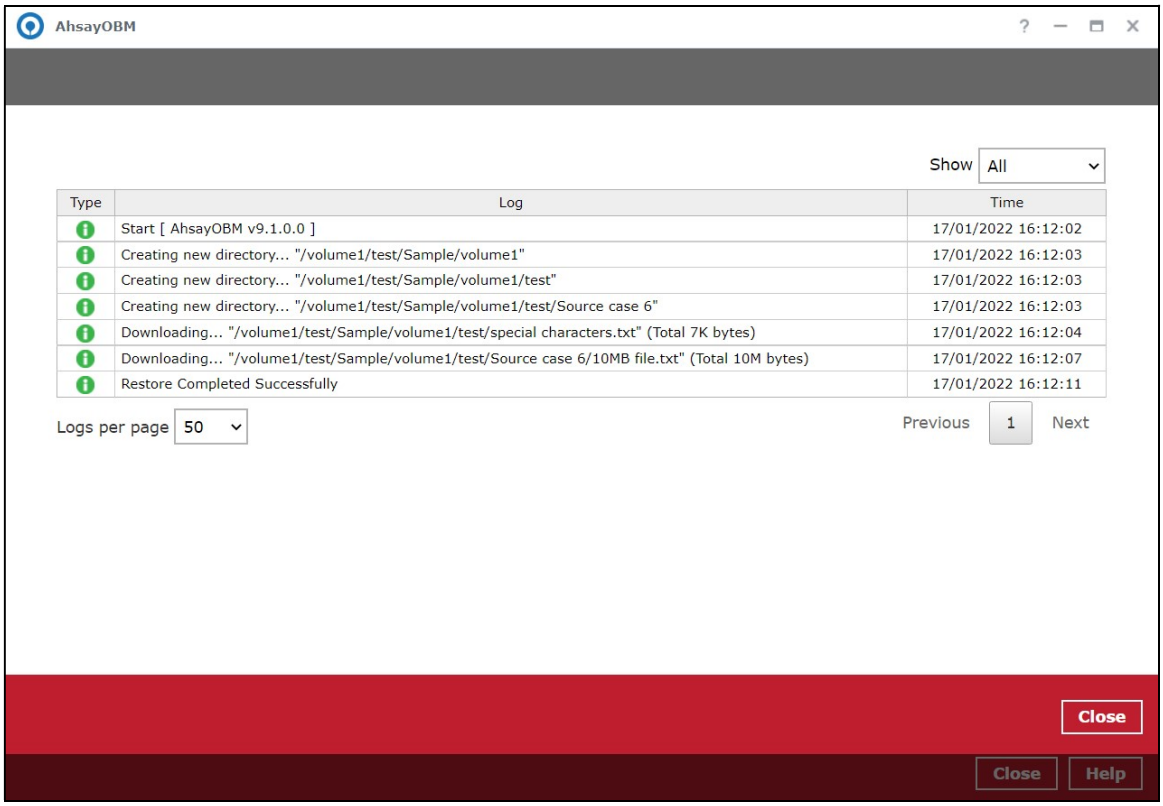
10. Click the **Restore** button to start the restore job.



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.



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



11 Contact Ahsay

11.1 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/

11.2 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

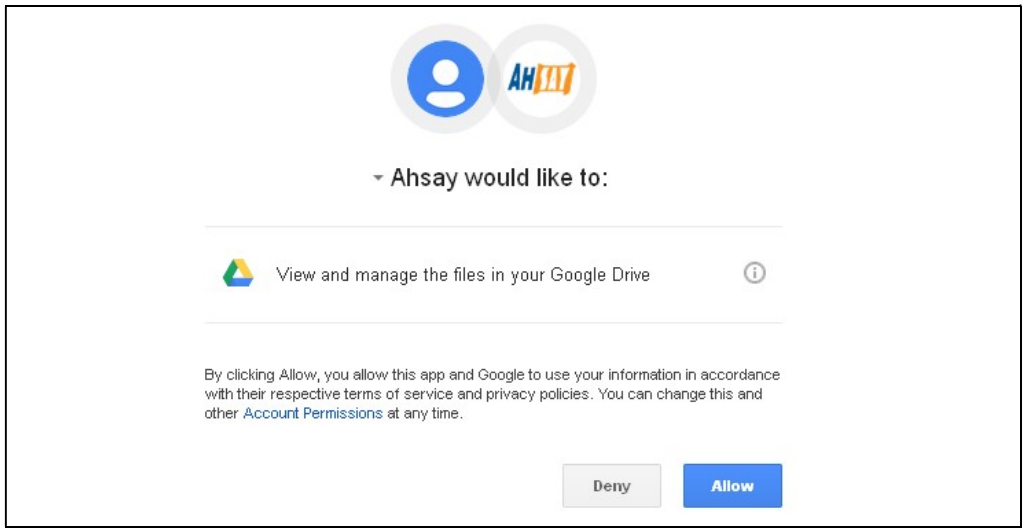
Appendix A: Cloud Storage as Backup Destination

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 log in to the corresponding cloud service.

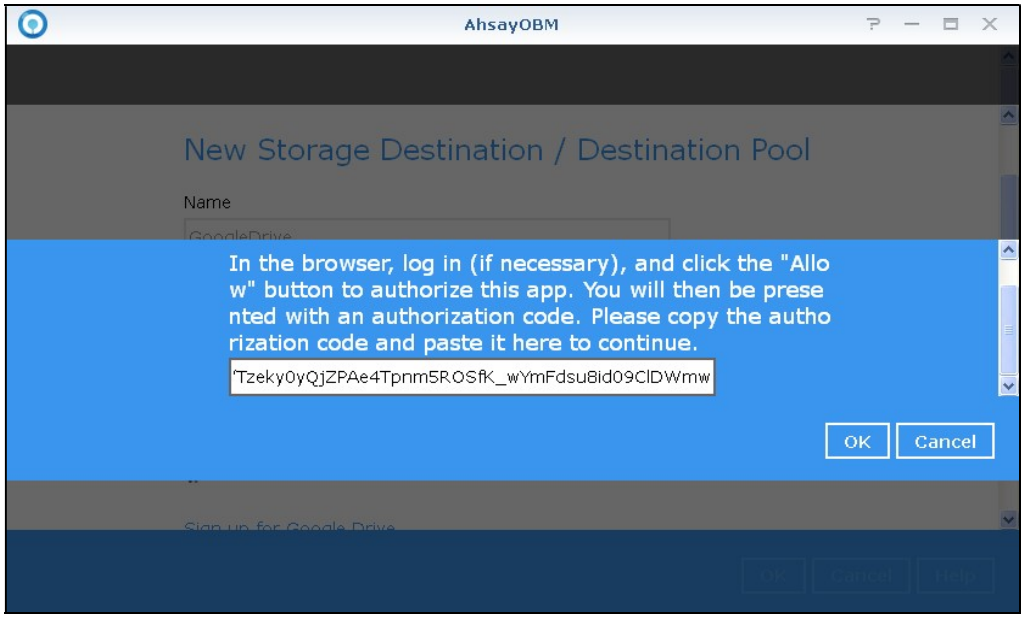
IMPORTANT

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.



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



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

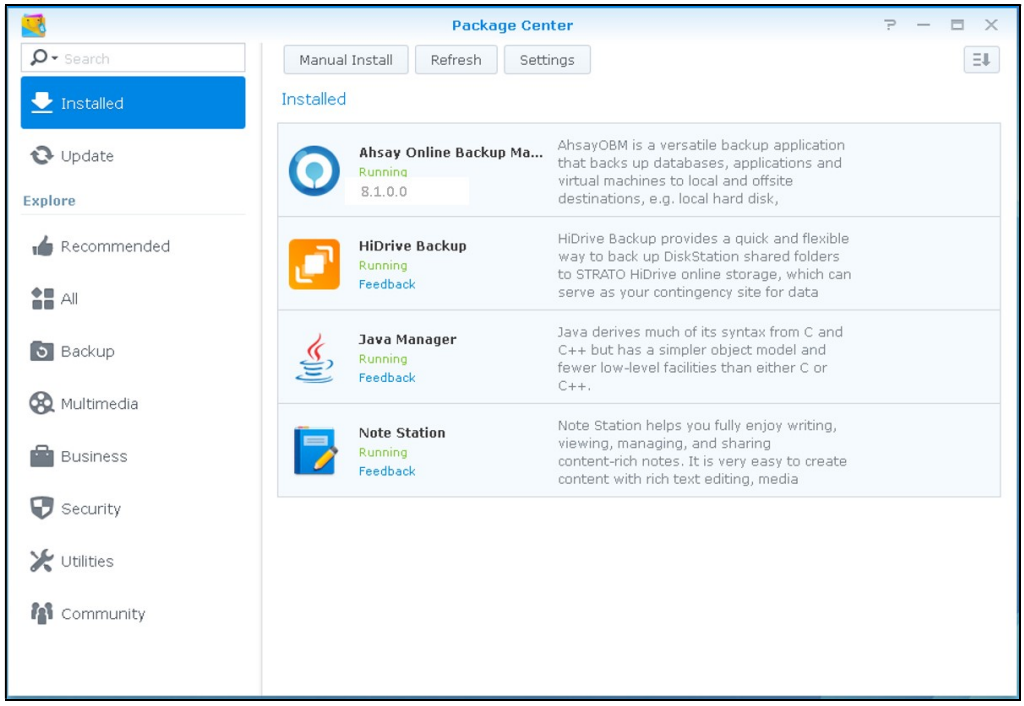
Refer to the following steps to uninstall AhsayOBM.

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

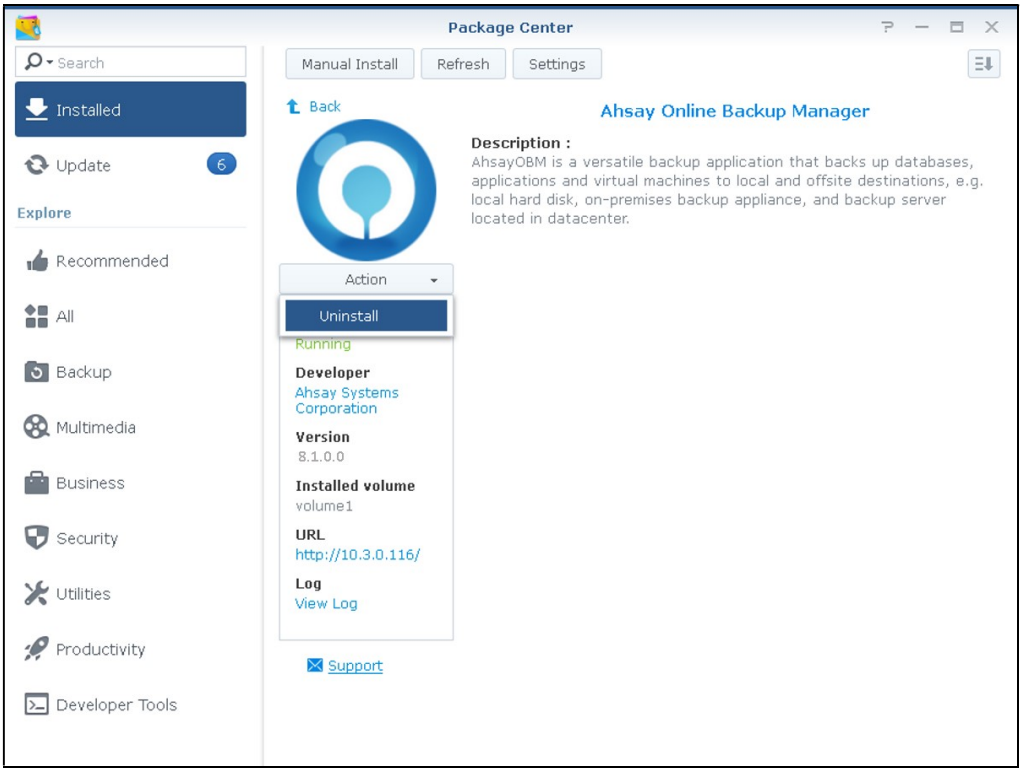
   NOTE: Refer to the following Synology Wiki article for information on how to sign into DSM:
https://www.synology.com/en-us/knowledgebase/DSM/help/DSM/MainMenu/get_started

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.



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



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

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

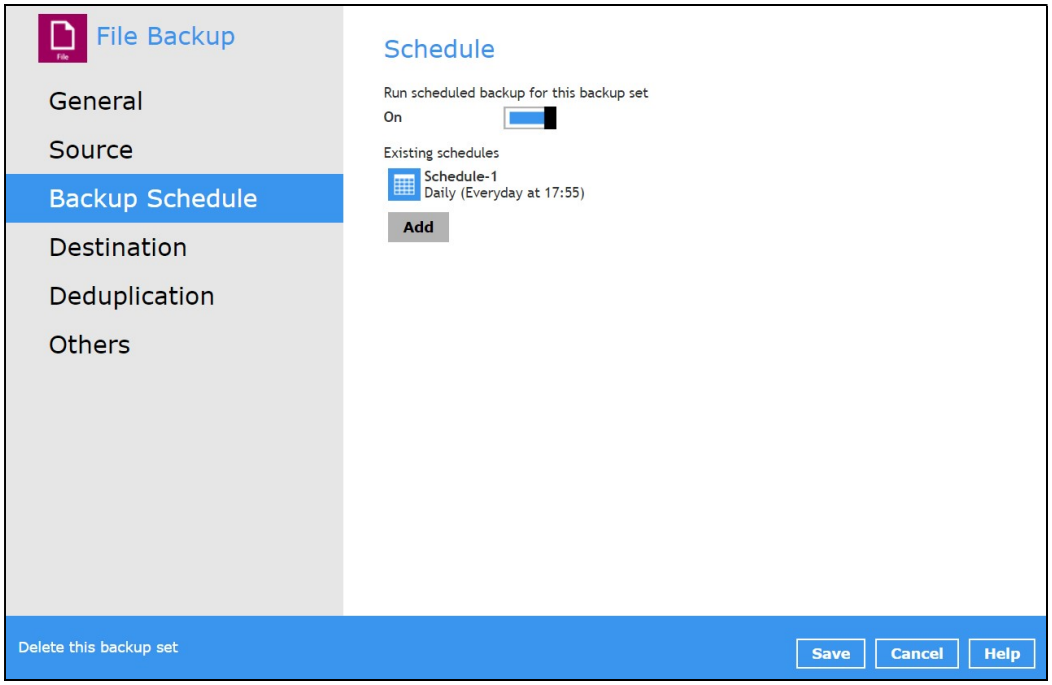
6. When the uninstallation is completed, the following message will appear.

*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:*
/volume1/@appstore/AhsayOBM/.obm
/volume1/@appstore/AhsayOBM/

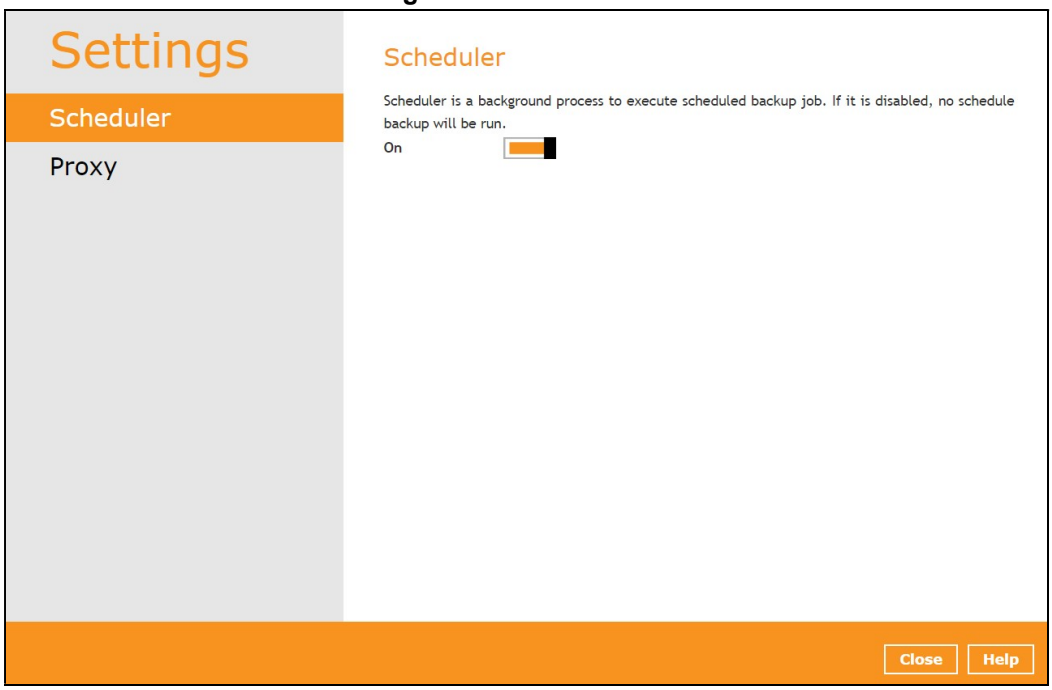
Appendix C: Scheduler Scenarios

NAS Synology has two (2) levels of Scheduler setting for the scheduled backup jobs.

Level 1: Scheduler under Backup Set Settings



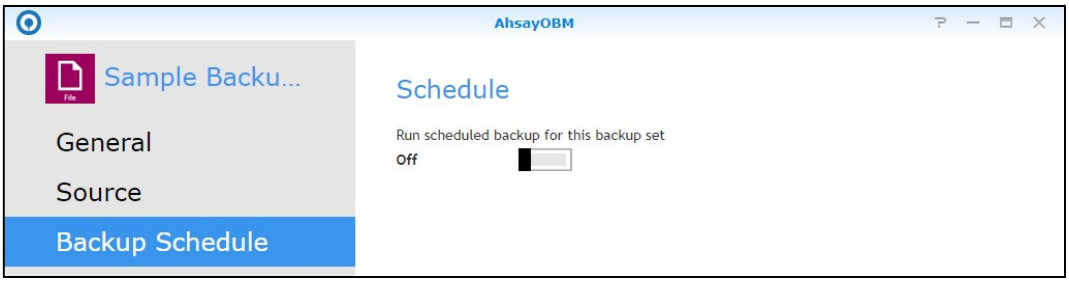
Level 2: Scheduler under Settings



Scenario no. 1: Scheduler under Settings is **On**, and Scheduler under Backup Set Settings is **Off**

Scheduler under Setting

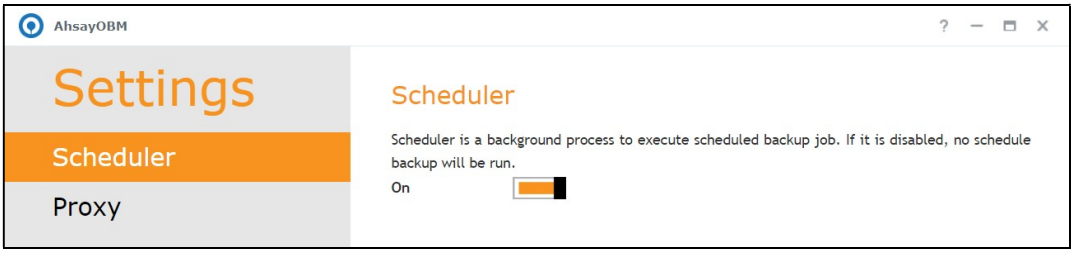
Scheduler under Backup Set Settings



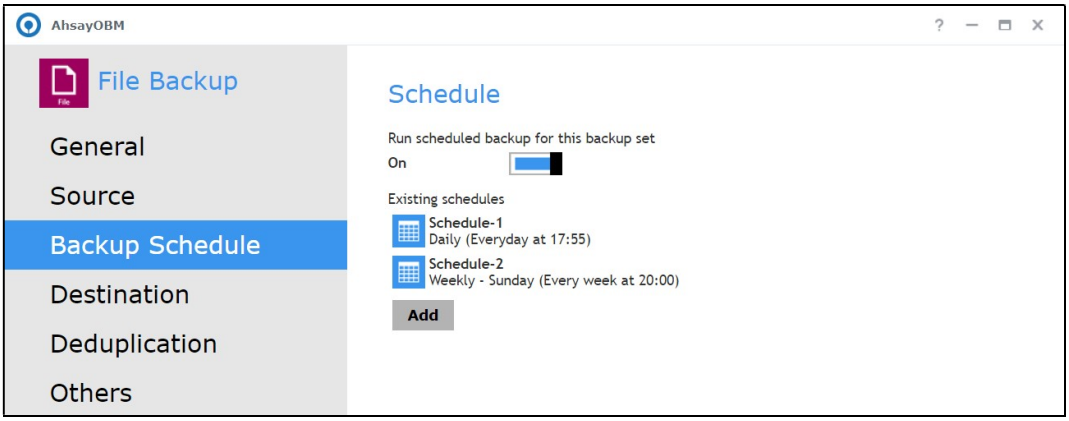
Result: There is no scheduled backup job that will be run for the backup set.

Scenario no. 2: Both the Scheduler under Settings and under Backup Set Settings are **On**

Scheduler under Settings



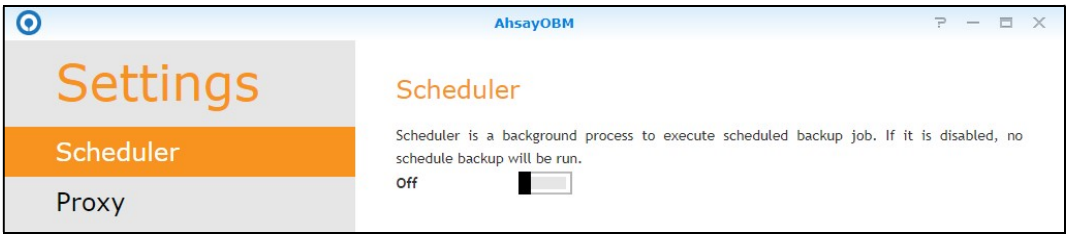
Scheduler under Backup Set Settings



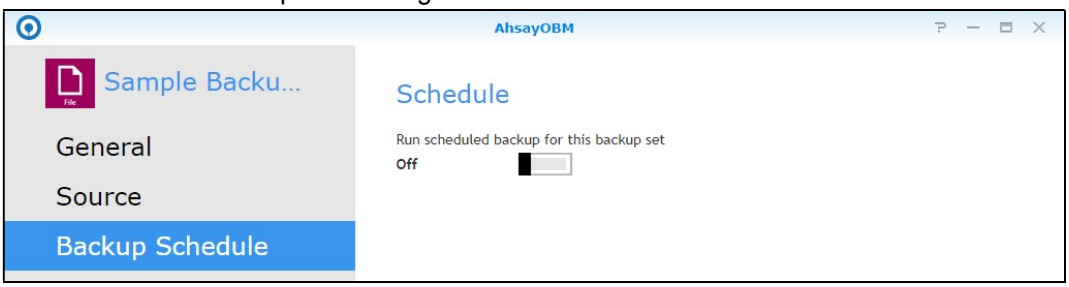
Result: Scheduled backup jobs for the backup set (i.e., Schedule-1 and Schedule-2) will run.

Scenario no. 3: Both the Scheduler under Settings and under Backup Set Settings are **Off**

Scheduler under Settings



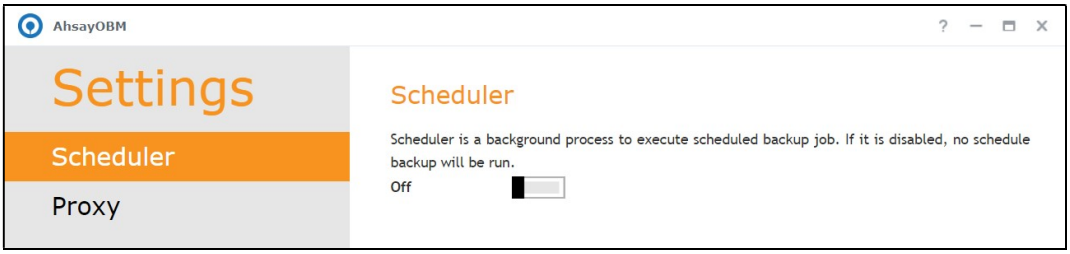
Scheduler under Backup Set Settings



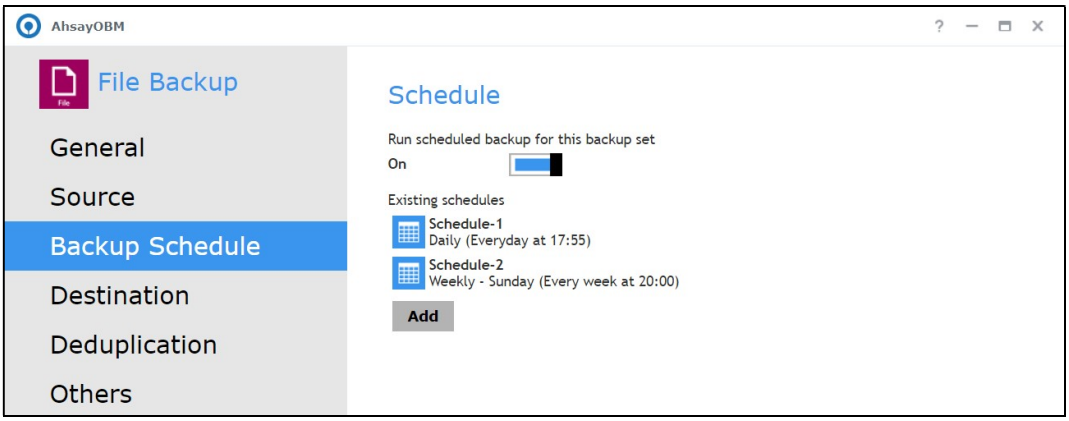
Result: There is no scheduled backup job that will be run for the backup set.

Scenario no. 4: Scheduler under Settings is **Off**, and Scheduler under Backup Set Settings is **On**

Scheduler under Settings



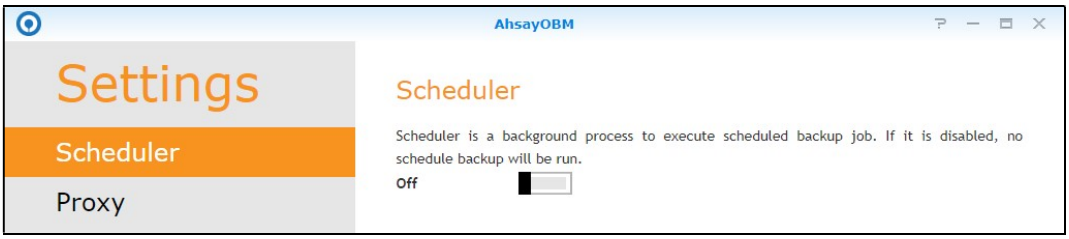
Scheduler under Backup Set Settings



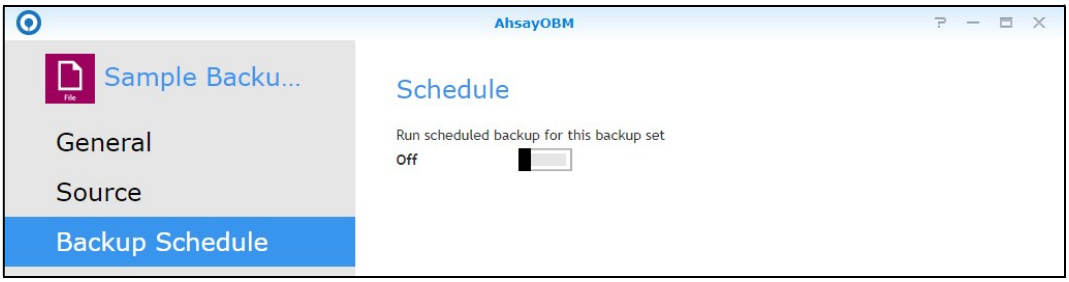
Result: There is no scheduled backup job that will be run for the backup set.

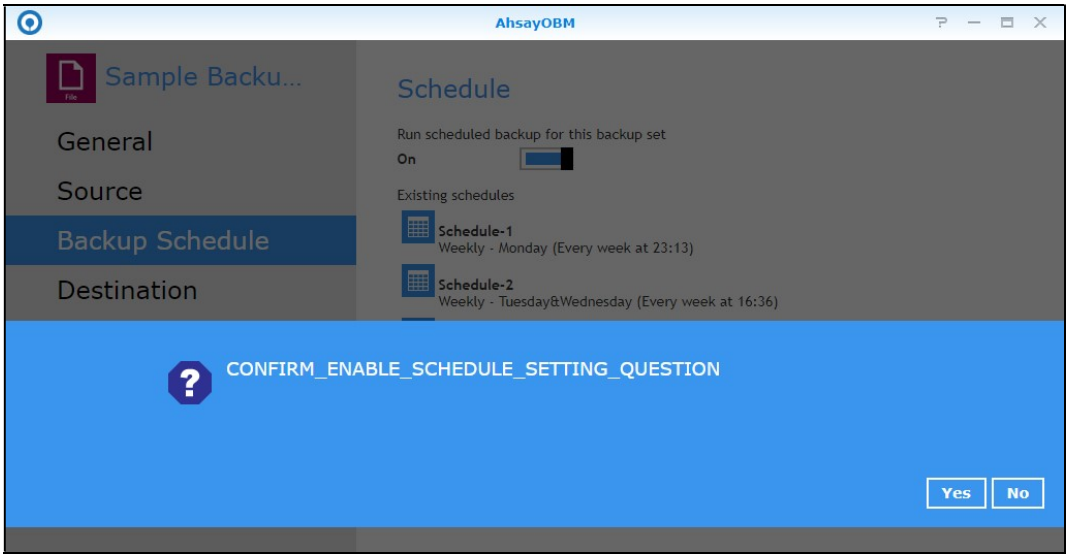
Scenario no. 5: Scheduler under Settings is **Off**, and Scheduler under Backup Set Settings will be switched **On**

Scheduler under Settings



Scheduler under Backup Set Settings





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 remain **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:

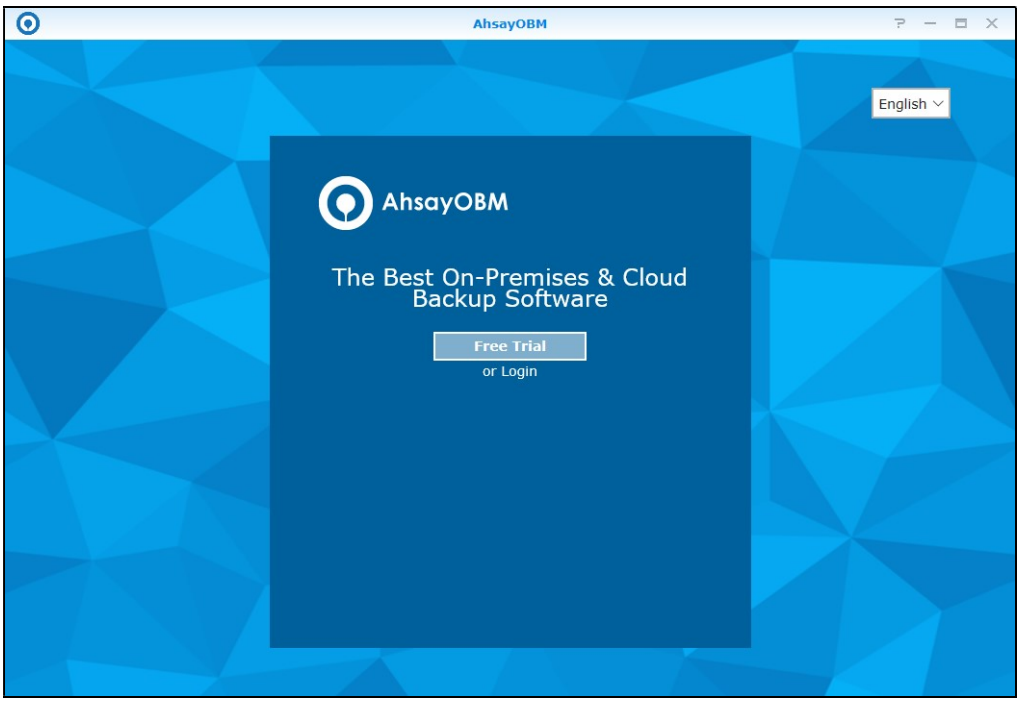
- A valid email address which will be used for receiving notices. A welcome message will also be sent upon creation of the account which specifies the User Setting and Quota set for backup in AhsayCBS.

While here are the limitations of a trial account:

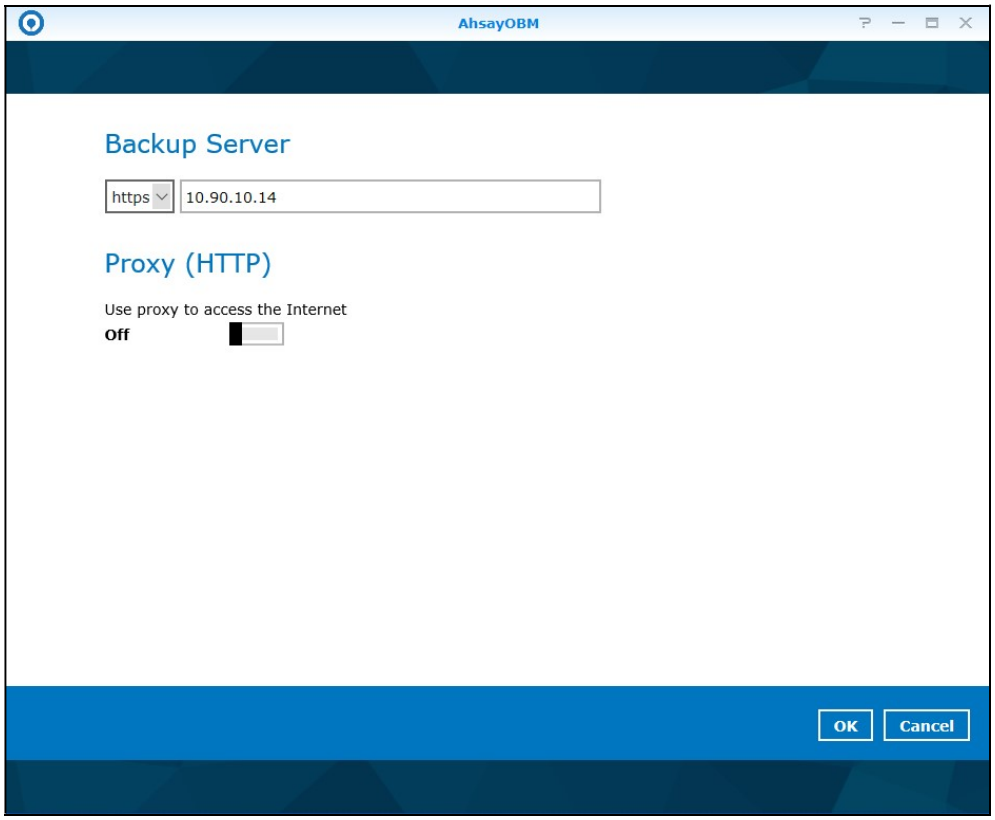
- The Free Trial button will only be displayed once when the user login for the first time. If you cannot create a free trial account kindly contact your backup service provider.
- Only alphanumeric characters and selected special characters, A to Z, 0 to 9, @, - and _, are allowed to be used for the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

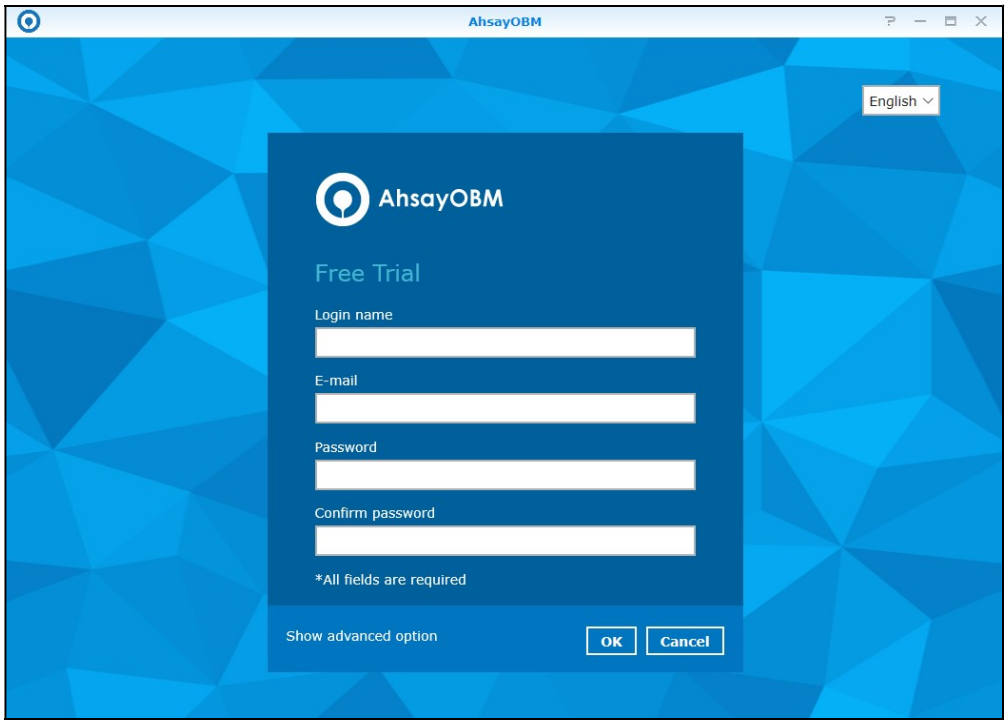
1. Click on **Free Trial**.



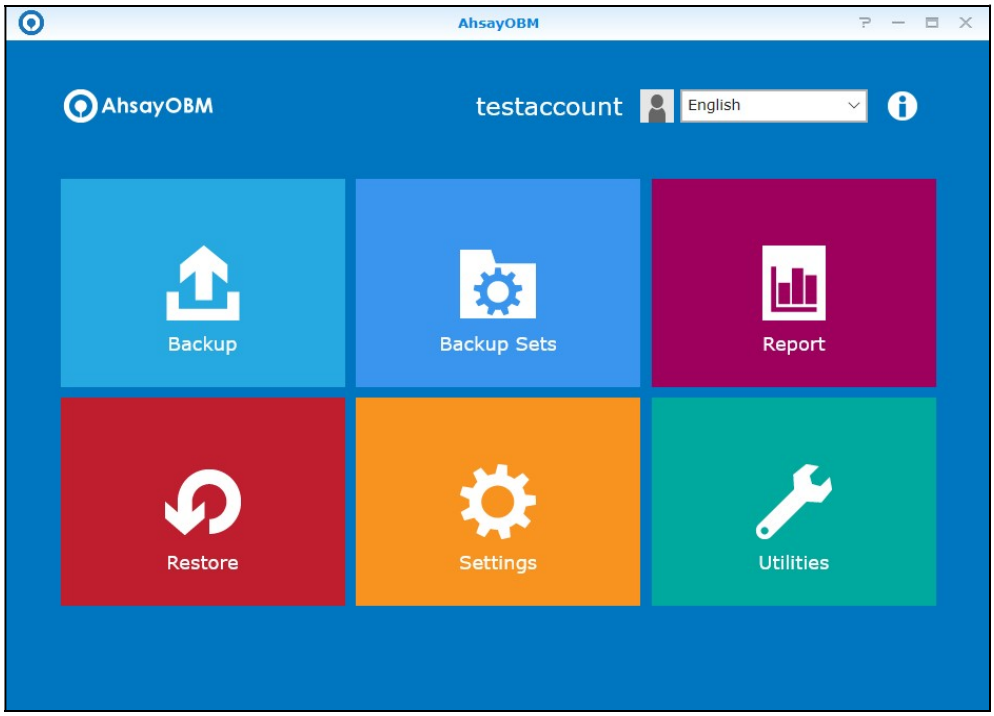
2. Configure your Backup Server settings.



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

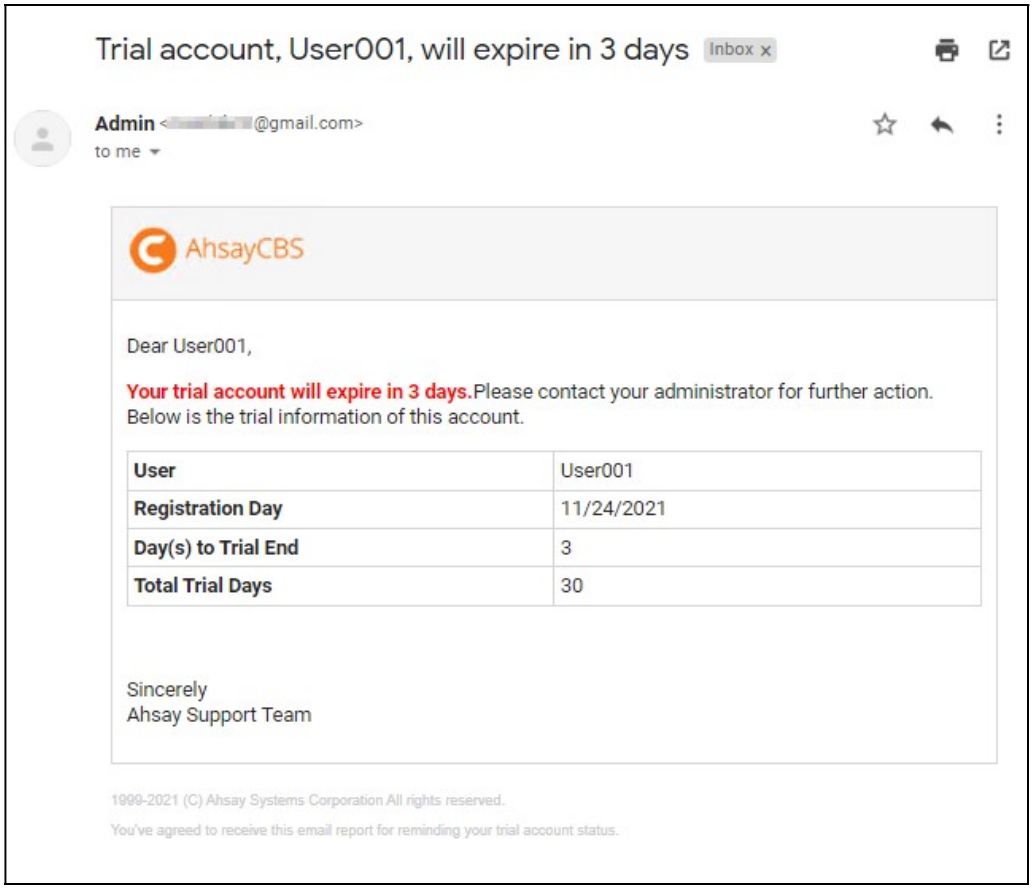


4. Once the trial account is created, this screen will be displayed.



5. 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 Inbox ×

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.