

Ahsay Online Backup Manager v8

Quick Start Guide for Synology NAS

Ahsay Systems Corporation Limited

30 April 2021

Copyright Notice

© 2021 Ahsay Systems Corporation Limited. All rights reserved.

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

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

Trademarks

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

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

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

Dropbox is a registered trademark of Dropbox Inc.

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

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

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

MariaDB is a registered trademark of MariaDB Corporation AB.

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

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

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

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

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

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

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

Ubuntu is a registered trademark of Canonical Ltd.

ShadowProtect is a registered trademark of StorageCraft Technology Corporation.

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

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

Disclaimer

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

Revision History

Date	Descriptions	Type of modification
3 January 2020	Modified the diagram for the Overview on the Backup Process and added a diagram for the Detailed Process of Periodic Data Integrity Check in Ch. 8	New / Modification
6 February 2020	Modified the Data Integrity Check in Ch. 6 and added the TCP port requirement in Ch. 2	New / Modification
30 July 2020	Updated Best Practices and Recommendations in Ch. 2.12; Updated Backup Set Settings – Backup Schedule in Ch. 6.6.1; Updated Backup Set Settings – Compression in Ch. 6.6.1; Updated Data Integrity Check in Ch. 6.10.1; Updated Create a Backup Set in Ch. 7; Updated PDIC diagram in Ch. 8;	New / Modifications
23 September 2020	Updated PDIC diagram in Ch. 8	Modification
7 April 2021	Updated Ch. 8; added sub-chapters for the detailed process diagrams in Ch. 8.1, 8.2, 8.2.1, 8.2.2 and 8.3	Modification
30 April 2021	Updated description of Data Integrity Check in Ch. 6.10.1; Updated description of Delete Backup Data in Ch. 6.10.2; Added notes for Periodic Data Integrity Check (PDIC) in Ch. 8.1	New / Modifications

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.....	2
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	3
2.11	Limitations	4
2.12	Best Practices and Recommendations.....	4
2.13	Supported Features from AhsayCBS Web Console	5
3	Get started with AhsayOBM	6
4	Download and Install AhsayOBM	7
4.1	Download AhsayOBM.....	7
4.2	Install AhsayOBM	8
4.3	AhsayOBM Scheduler Service Check.....	12
5	Start AhsayOBM	14
5.1	Add an AhsayOBM Shortcut Icon to the Desktop.....	14
5.2	Login to AhsayOBM.....	16
6	AhsayOBM Overview	21
6.1	Profile	22
6.2	Online Help.....	29
6.3	Language.....	30
6.4	Information.....	30
6.5	Backup.....	31
6.6	Backup Sets	34
	Backup Set Settings.....	34
6.7	Report.....	45

6.7.1 Backup.....	45
6.7.2 Restore	49
6.8 Restore	50
6.9 Settings.....	52
6.9.1 Scheduler.....	52
6.9.2 Proxy	53
6.10 Utilities	54
6.10.1 Data Integrity Check.....	54
6.10.2 Delete Backup Data	66
7 Create a Backup Set	70
8 Overview on the Backup Process	78
8.1 Periodic Data Integrity Check (PDIC) Process	79
8.2 Backup Set Index Handling Process	81
8.2.1 Start Backup Job	81
8.2.2 Completed Backup Job.....	82
8.3 Data Validation Check Process.....	83
9 Run Backup Jobs	84
9.1 Login to AhsayOBM	84
9.2 Start a Manual Backup.....	84
10 Restore Data.....	87
10.1 Login to AhsayOBM	87
10.2 Restore Data.....	87
11 Contact Ahsay	95
11.1 Technical Assistance	95
11.2 Documentation.....	95
Appendix.....	96
Appendix A: Cloud Storage as Backup Destination	96
Appendix B: Uninstall AhsayOBM.....	98
Appendix C: Scheduler Scenarios	100
Appendix D: Create Free Trial Account in AhsayOBM	104

1 Overview

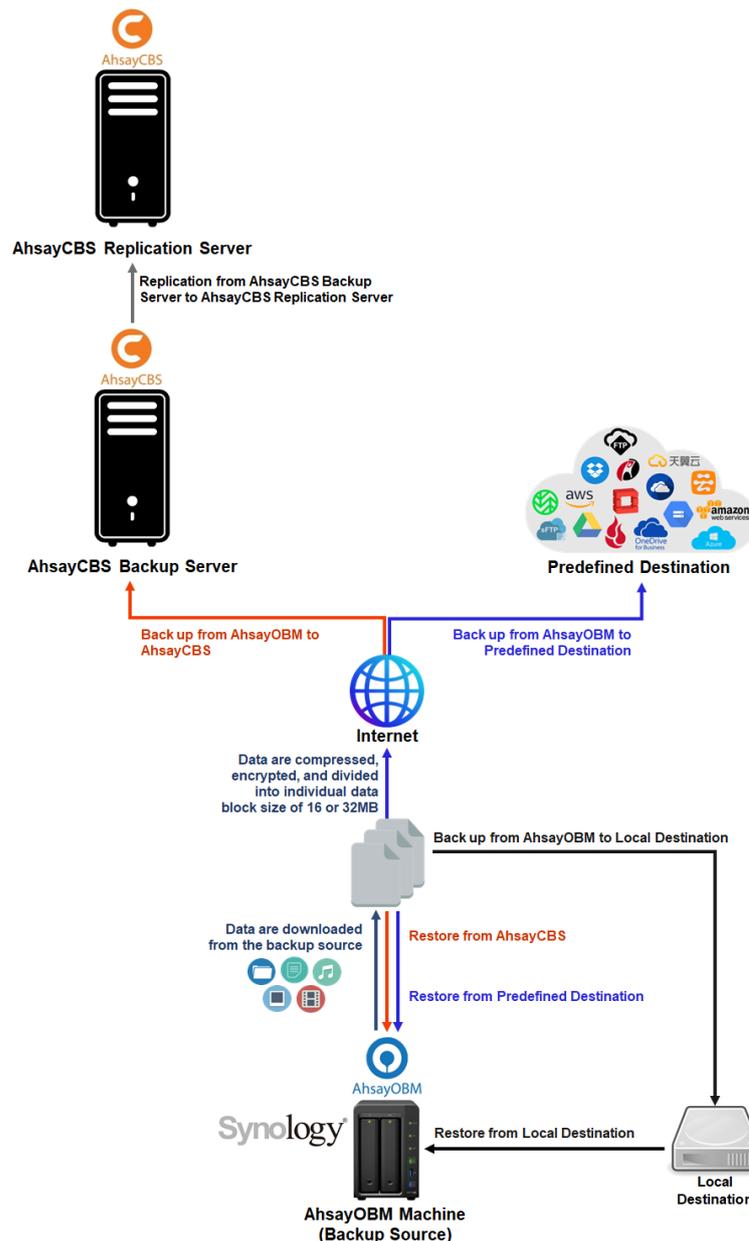
1.1 What is this software?

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.

The screenshot shows the 'Backup Client Settings' tab for a user. The 'Backup Client' is set to 'AhsayOBM User'. Under 'Add-on Modules', the following modules are listed with their status:

Module	Status
Microsoft Exchange Server	<input type="checkbox"/>
MySQL Database Server	<input type="checkbox"/>
Lotus Lotus Domino	<input type="checkbox"/>
Windows System Backup	<input type="checkbox"/>
VMware	<input type="checkbox"/>
Microsoft Exchange Mailbox	<input type="checkbox"/>
Continuous Data Protection	<input type="checkbox"/>
Mobile	<input type="checkbox"/>
Volume Shadow Copy	<input type="checkbox"/>
OpenDirect / Granular Restore	<input type="checkbox"/>
Microsoft SQL Server	<input type="checkbox"/>
Oracle Database Server	<input type="checkbox"/>
Lotus Lotus Notes	<input type="checkbox"/>
Windows System State Backup	<input type="checkbox"/>
Hyper-V	<input type="checkbox"/>
ShadowProtect System Backup	<input type="checkbox"/>
NAS - Synology	<input checked="" type="checkbox"/>
NAS - QNAP	<input type="checkbox"/>
In-File Delta	<input checked="" type="checkbox"/>
Office 365 Backup	<input type="checkbox"/>

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.

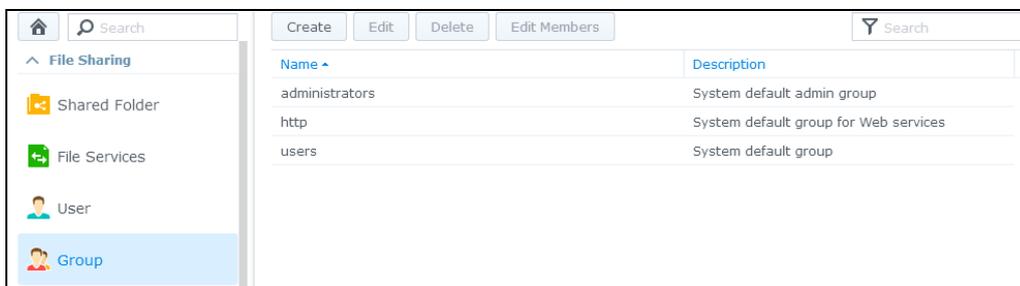
2.8 TCP Port Requirement

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.

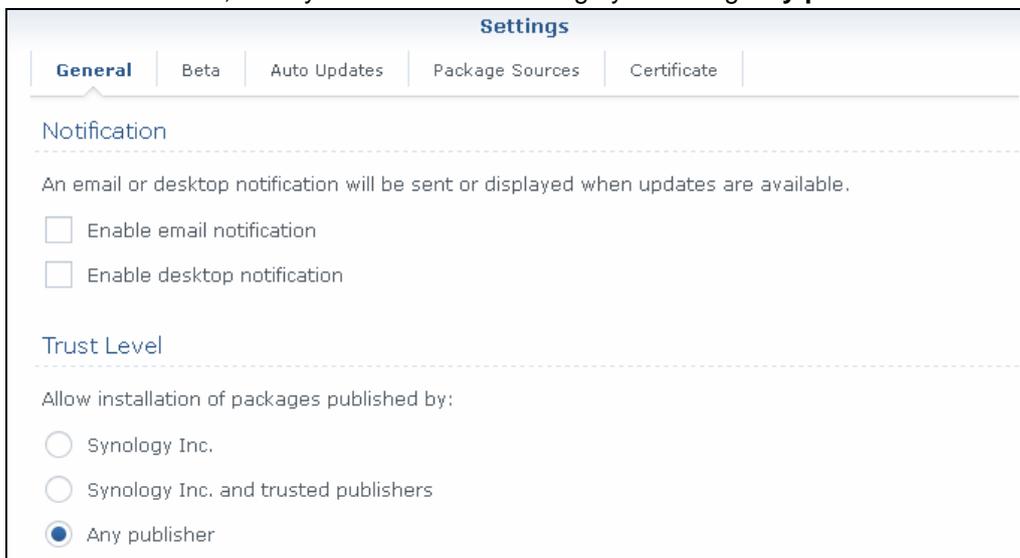
2.9 Synology NAS User Account Permission

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 Limitations

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

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

2.12 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
- **Network** – make sure to have enough network bandwidth to accommodate the volume of data within the backup interval.
- **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 take into account the retention policy settings and retention area storage management which can grow because of the changes in the backup data for each backup job.

2.13 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 Statics Report**

3 Get started with AhsayOBM

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

Download and Install

Download and install AhsayOBM on your Synology NAS

Launch the App

Launch and log in to AhsayOBM

Create a Backup Set

Create a backup set according to your preferences

Run Backup Jobs

Run a backup job to back up your data

Restore Data

Restore your backed-up data

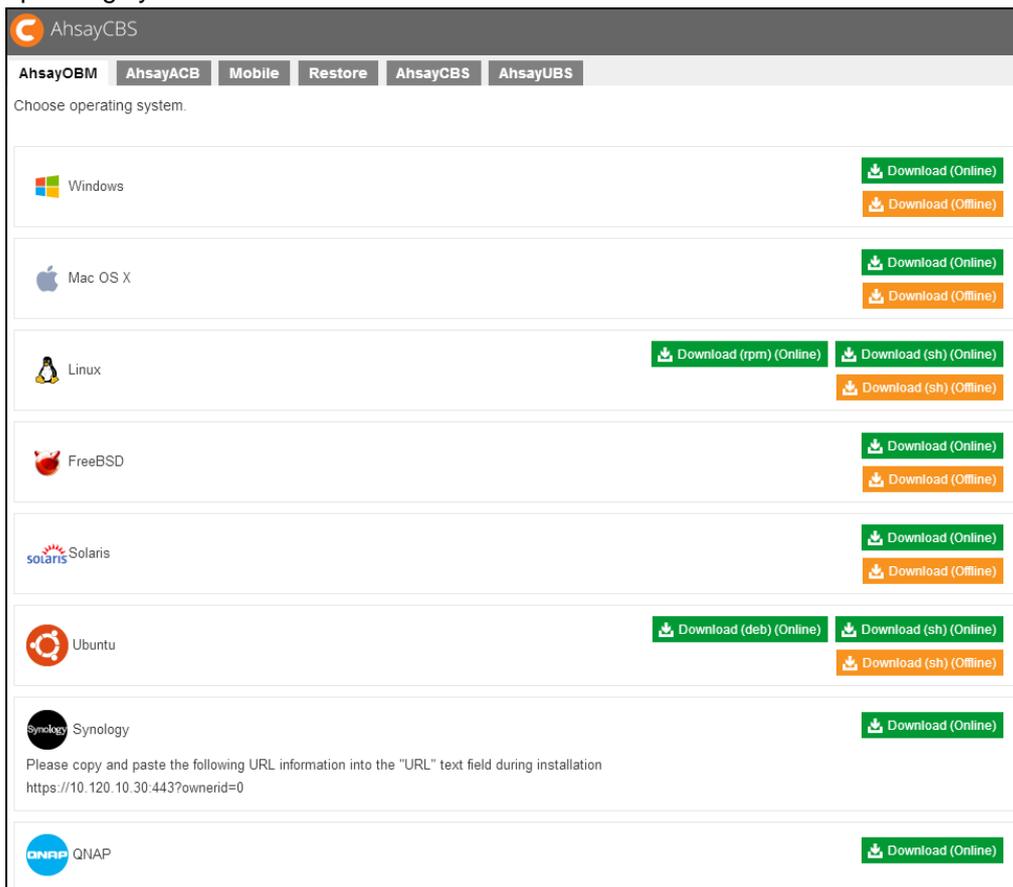
4 Download and Install AhsayOBM

4.1 Download AhsayOBM

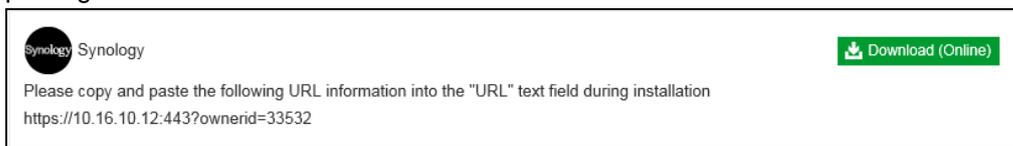
1. In a web browser, click the blue icon on the top right corner to open the download page for the AhsayOBM installation package file from your backup service provider's website.



2. In the **AhsayOBM** tab of the download page, you can choose the AhsayOBM installer by operating system.



3. In the Synology section, click the **Download** icon to download the AhsayOBM installation package.



4.2 Install 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

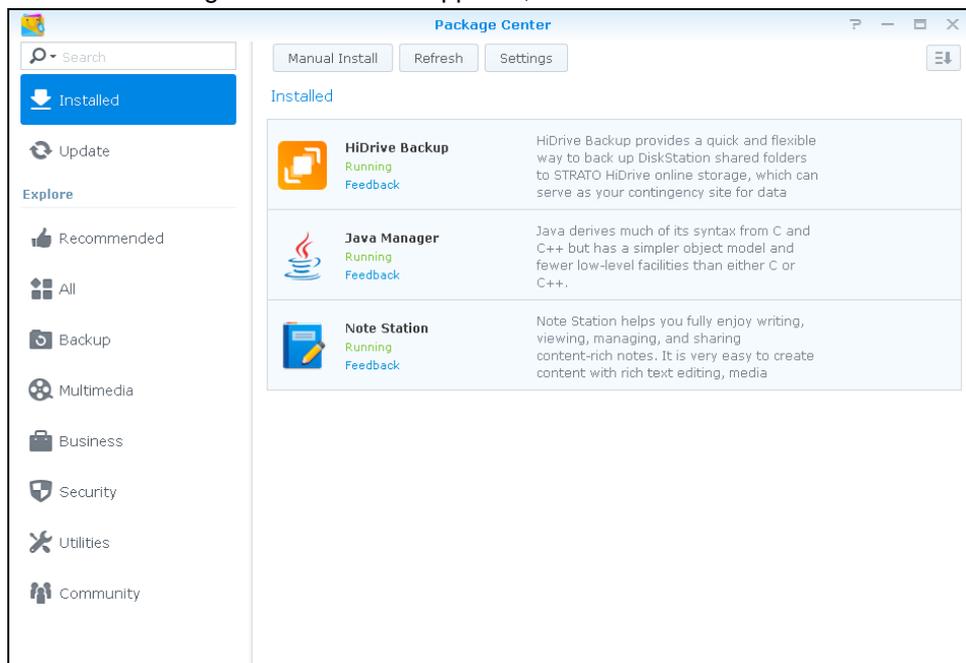
https://nas_hostname:5000

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

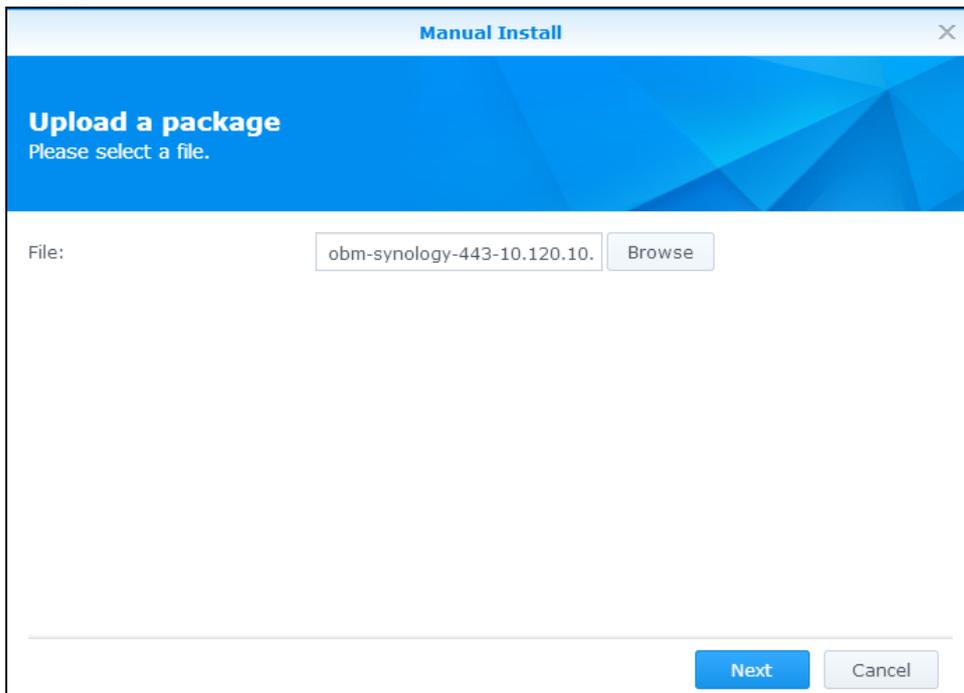
2. To install AhsayOBM on Synology NAS, click the Package Center icon from the desktop.



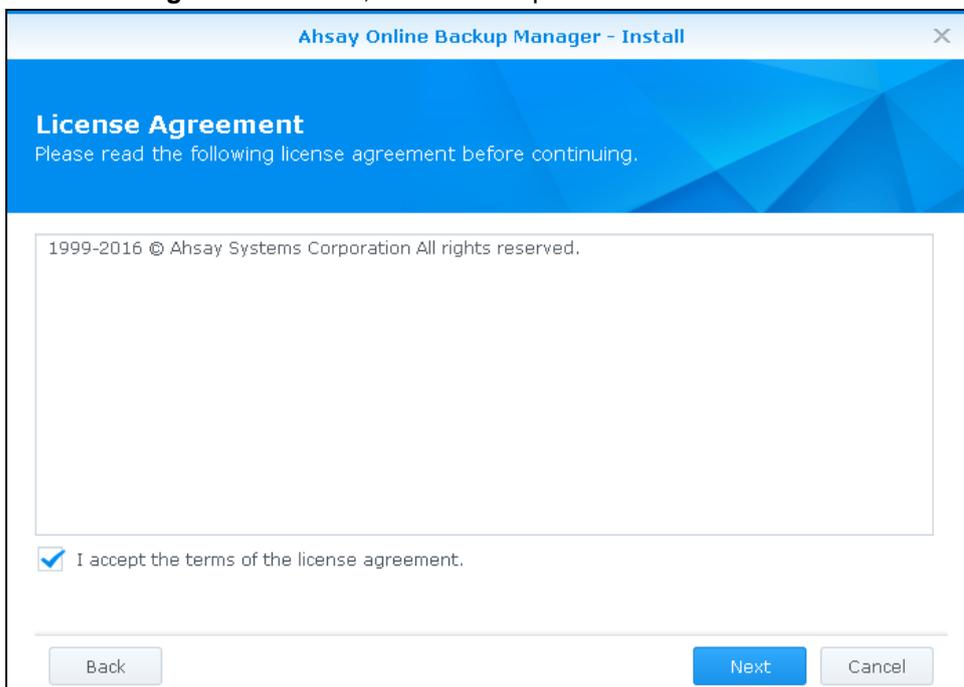
3. When the Package Center window appears, select **Manual Install**.



4. When the Manual Install window appears, click **Browse** to select the AhsayOBM package file which you have downloaded (e.g. obm-synology-443-backup service provider IP address-https-00.spk). Then, click **Next** to proceed.

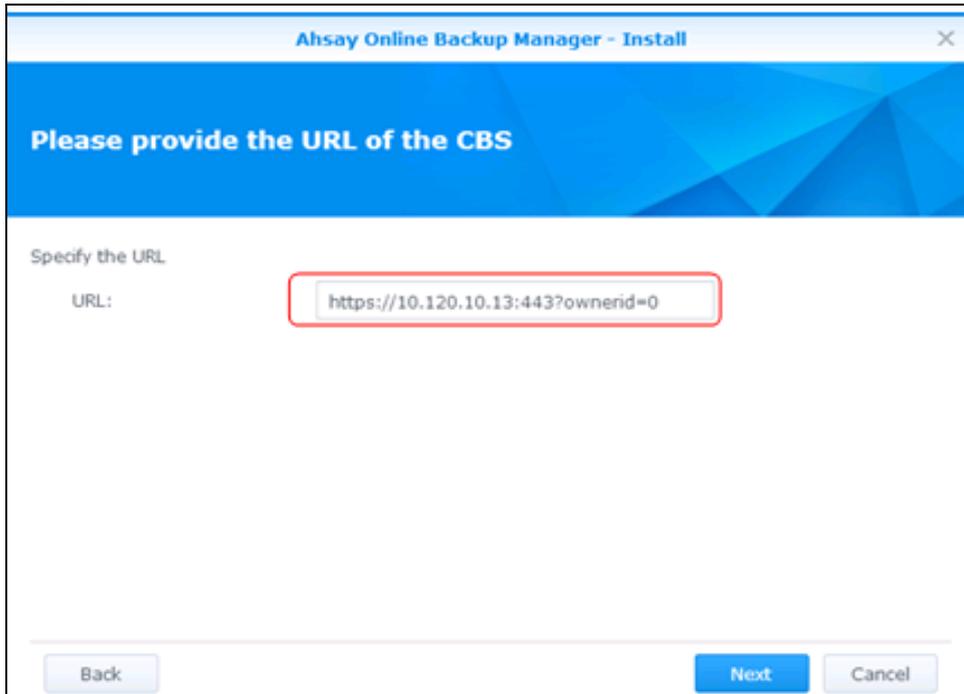


5. After reading the License Agreement carefully, tick the checkbox next to **I accept the terms of the license agreement**. Then, click **Next** to proceed.

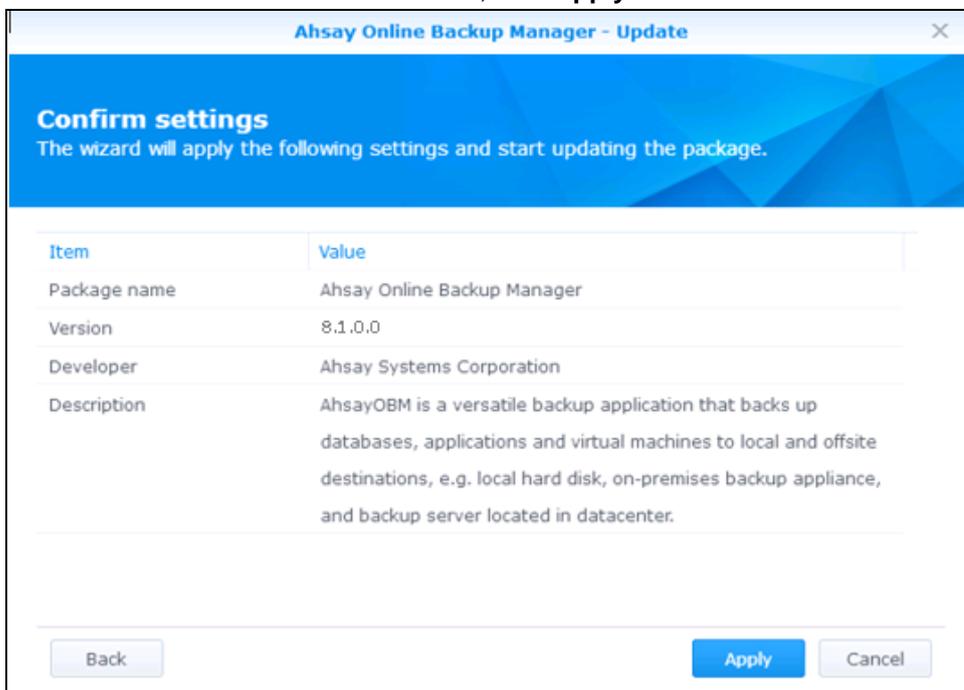


6. Copy and paste the URL information for installing on Synology shown in the download page. Then, click **Next** to proceed.

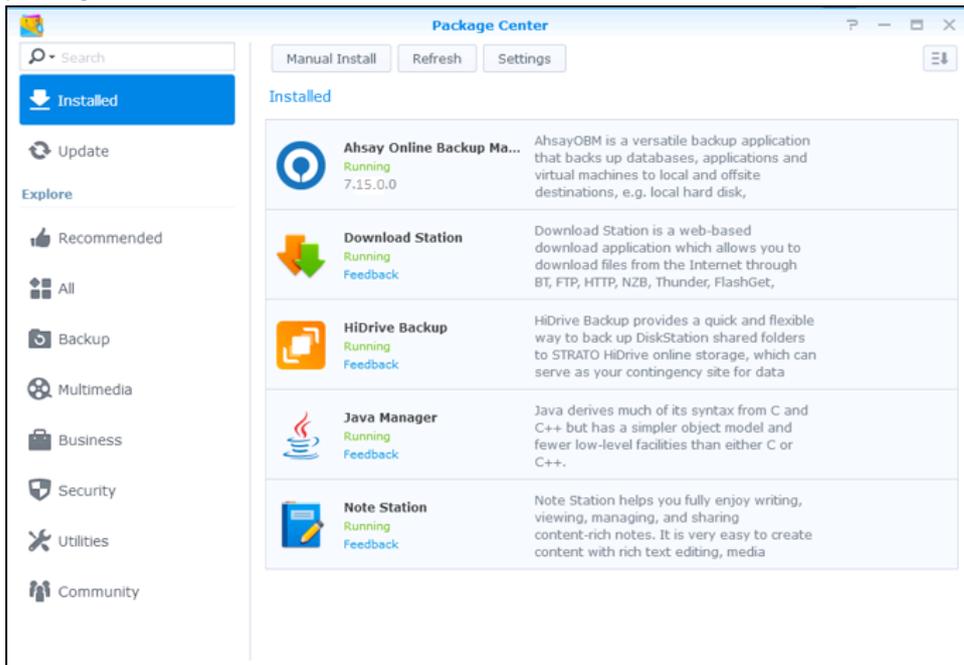




7. Review the information on screen. Then, click **Apply** to start the installation of AhsayOBM.



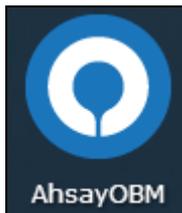
- Upon successful installation, Ahsay Online Backup Manager will be listed in the Installed packages.



- You can click the Main Menu icon on the top left corner of your desktop.



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



- 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
```

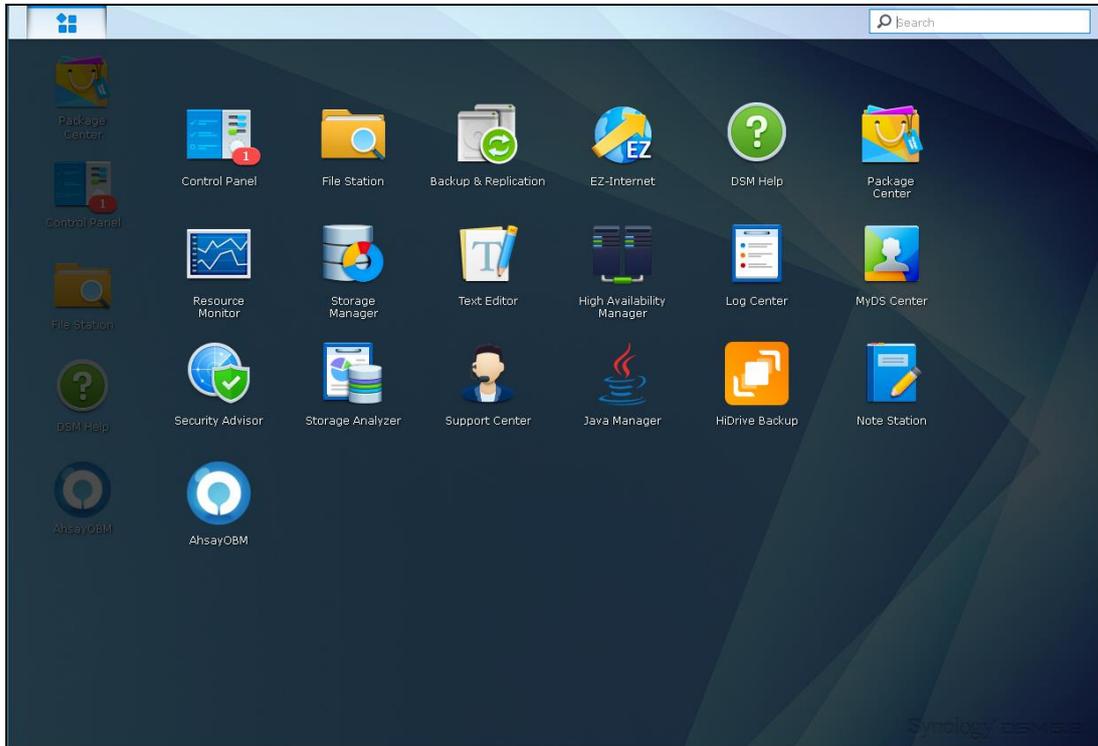
5 Start AhsayOBM

5.1 Add an AhsayOBM Shortcut Icon to the Desktop

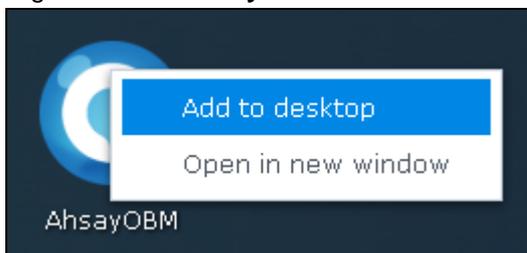
1. In the DiskStation Manager (DSM) console, click the **Main Menu** icon on the top left corner of the desktop to open it.



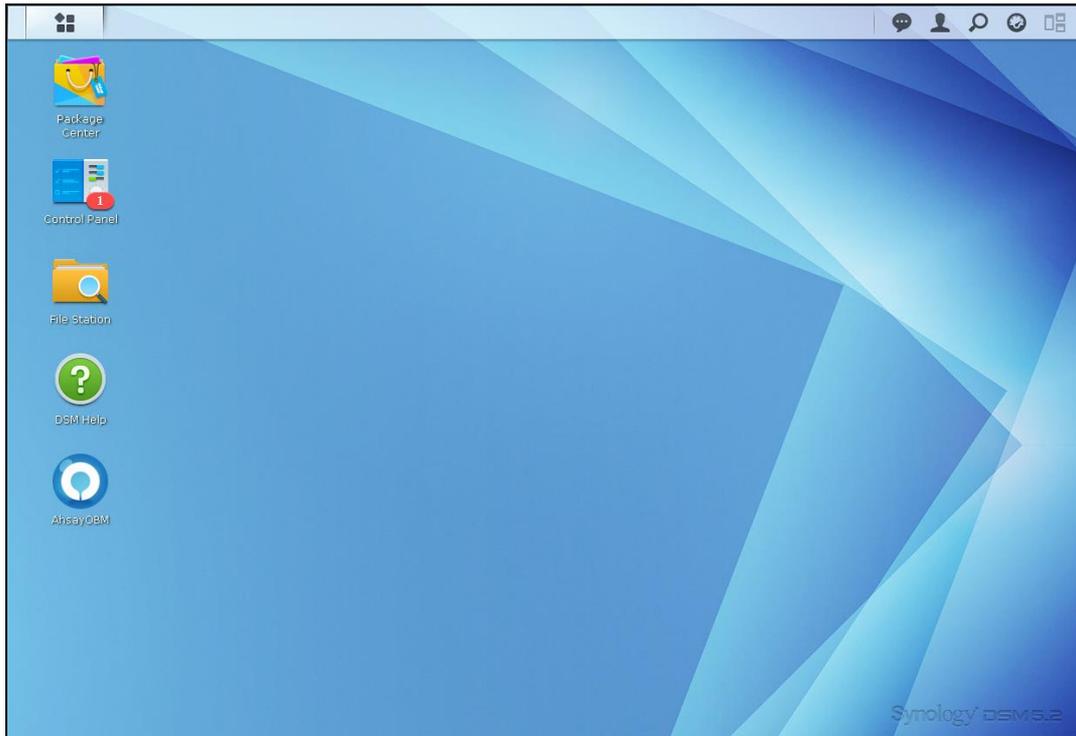
2. All application icons will be shown. Look for the **AhsayOBM** icon.



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

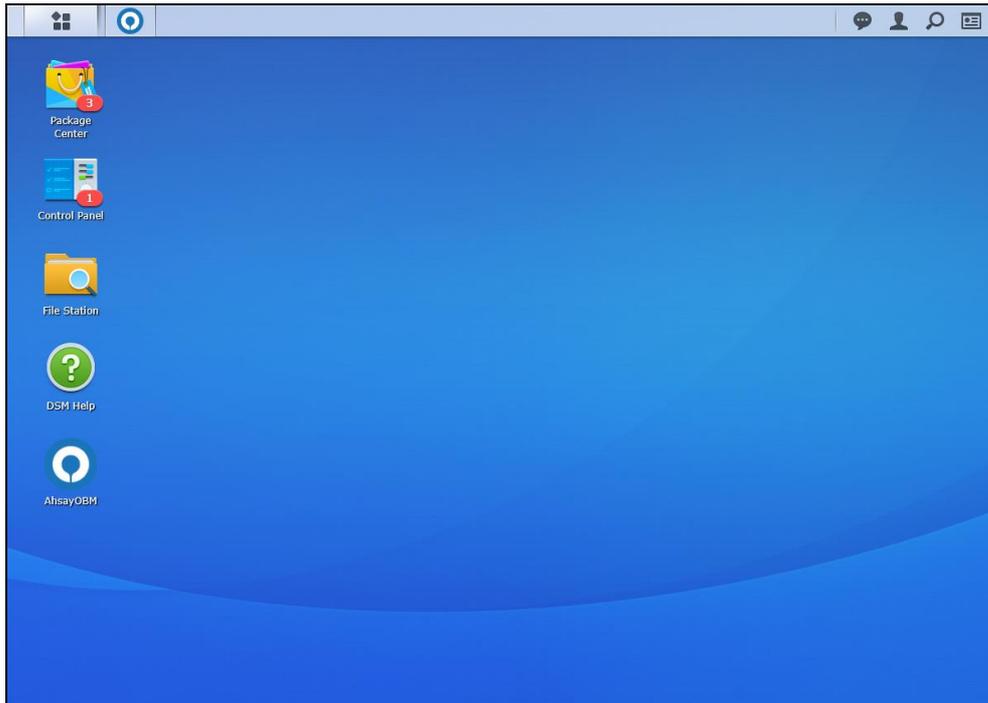


4. The AhsayOBM shortcut icon will be added to the desktop.

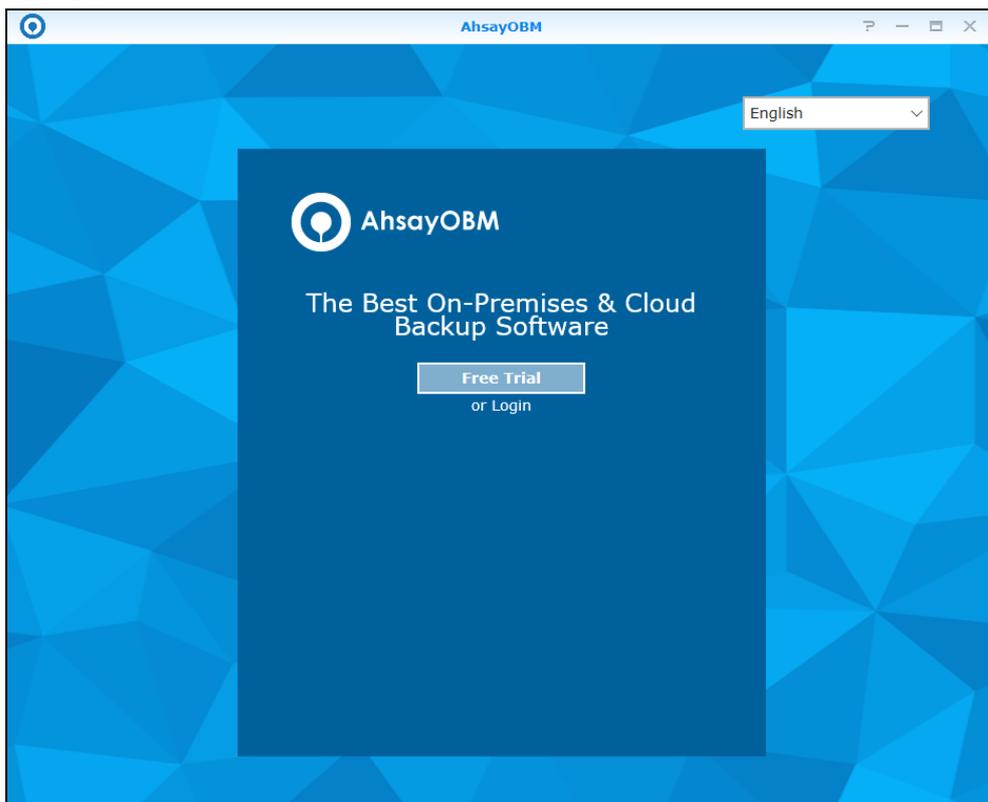


5.2 Login to AhsayOBM

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

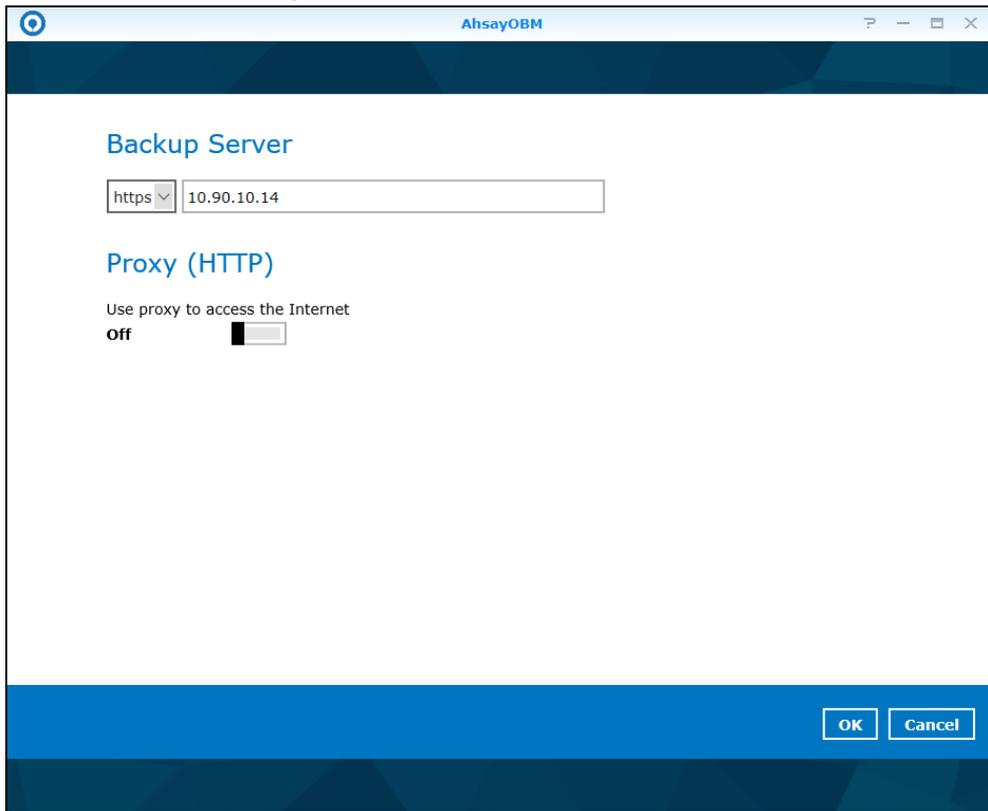


2. The Free Trial Registration menu may be displayed when you login for the first time. Click **Login** if you already have an AhsayOBM account or click [Free Trial](#) to register for a trial backup account.



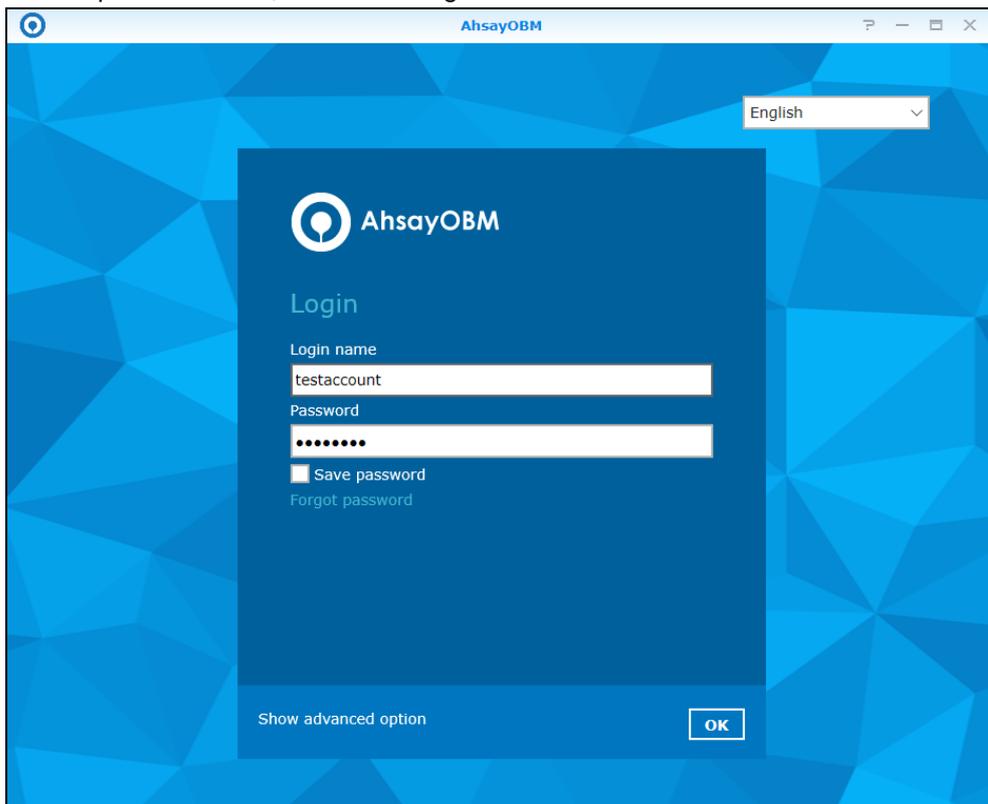
Note: The free trial registration menu will be displayed if your service provider has enabled free trial registration on the backup server.

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



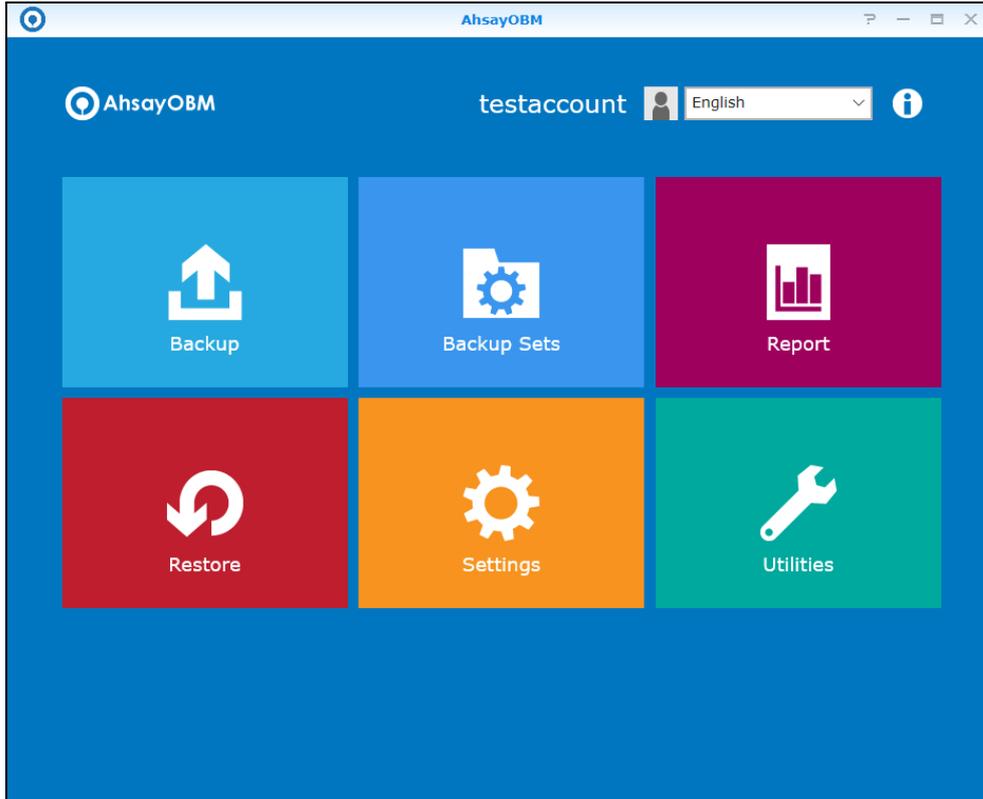
The screenshot shows a dialog box titled "AhsayOBM" with a "Backup Server" section. It features a dropdown menu set to "https" and a text input field containing "10.90.10.14". Below this is a "Proxy (HTTP)" section with the text "Use proxy to access the Internet" and a toggle switch labeled "Off". At the bottom right, there are "OK" and "Cancel" buttons.

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



The screenshot shows the AhsayOBM login interface. It features a dark blue background with a geometric pattern. A central dark blue box contains the AhsayOBM logo and the text "Login". Below the logo are two input fields: "Login name" with the text "testaccount" and "Password" with masked characters. There is a "Save password" checkbox and a "Forgot password" link. At the bottom left of the login box is a "Show advanced option" link, and at the bottom right is an "OK" button. In the top right corner of the main window, there is a language dropdown menu set to "English".

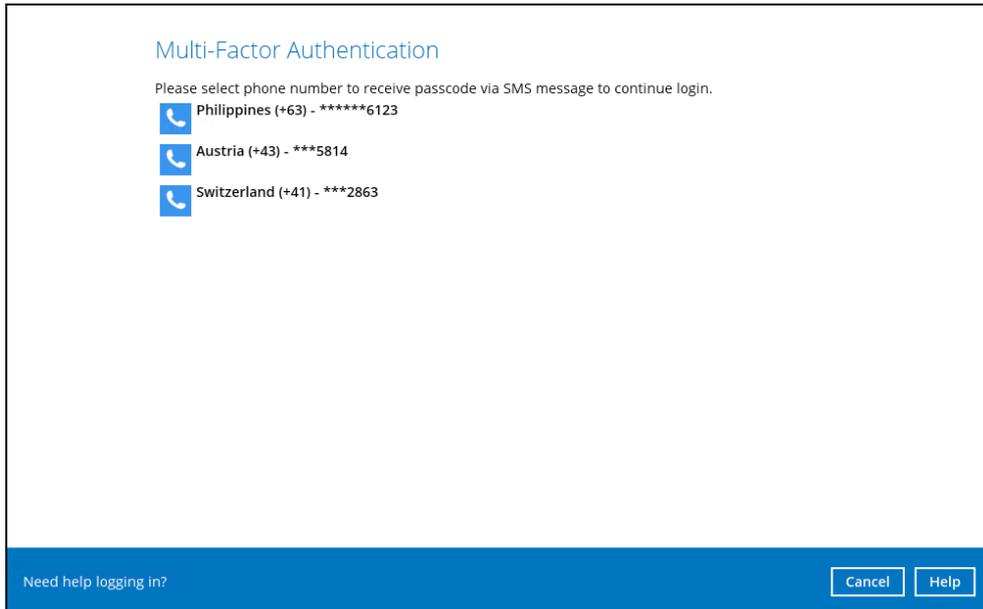
5. Upon successful login, the following screen will appear.



6. If Multi-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.

The image shows a 'Multi-Factor Authentication' setup screen. The title is 'Multi-Factor Authentication'. Below the title, there is a message: 'Multi-Factor Authentication is enabled for helping safeguard access to your account. Please provide a phone number to setup in the first-time login.' This is followed by the instruction: 'You will receive a passcode in the SMS message'. There is a dropdown menu for country codes with 'Andorra (+376)' selected, and an adjacent text input field for the phone number. Below this, another message states: 'There is no contact email address defined in your account. Please enter an email address for account recovery.' followed by an empty text input field. At the bottom right, there are three buttons: 'Send', 'Cancel', and 'Help'.

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



Multi-Factor Authentication

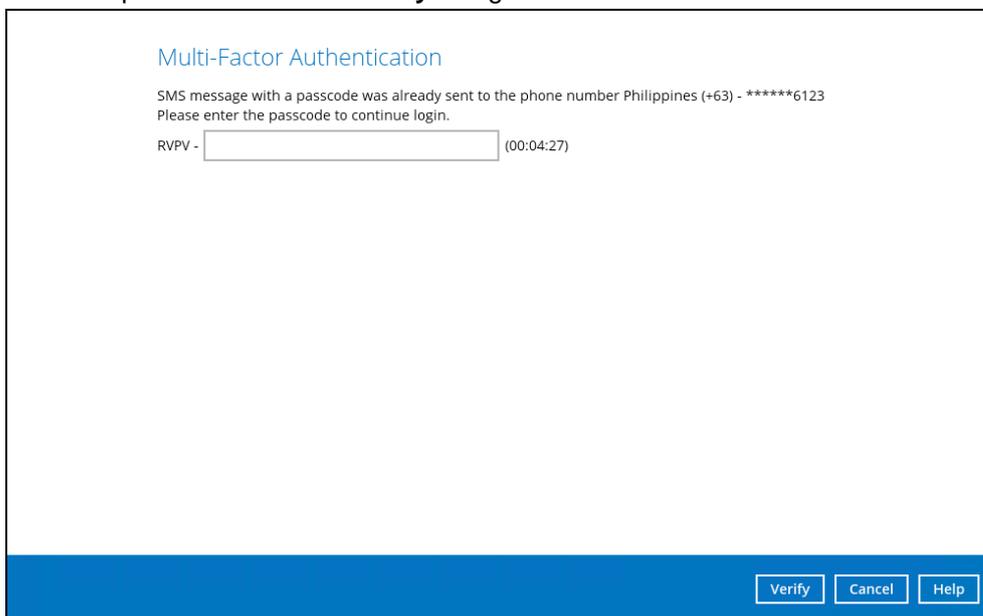
Please select phone number to receive passcode via SMS message to continue login.

-  Philippines (+63) - *****6123
-  Austria (+43) - ***5814
-  Switzerland (+41) - ***2863

Need help logging in? Cancel Help

Note: If **Need help logging in?** is clicked, enter the email address where login instructions will be sent.

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



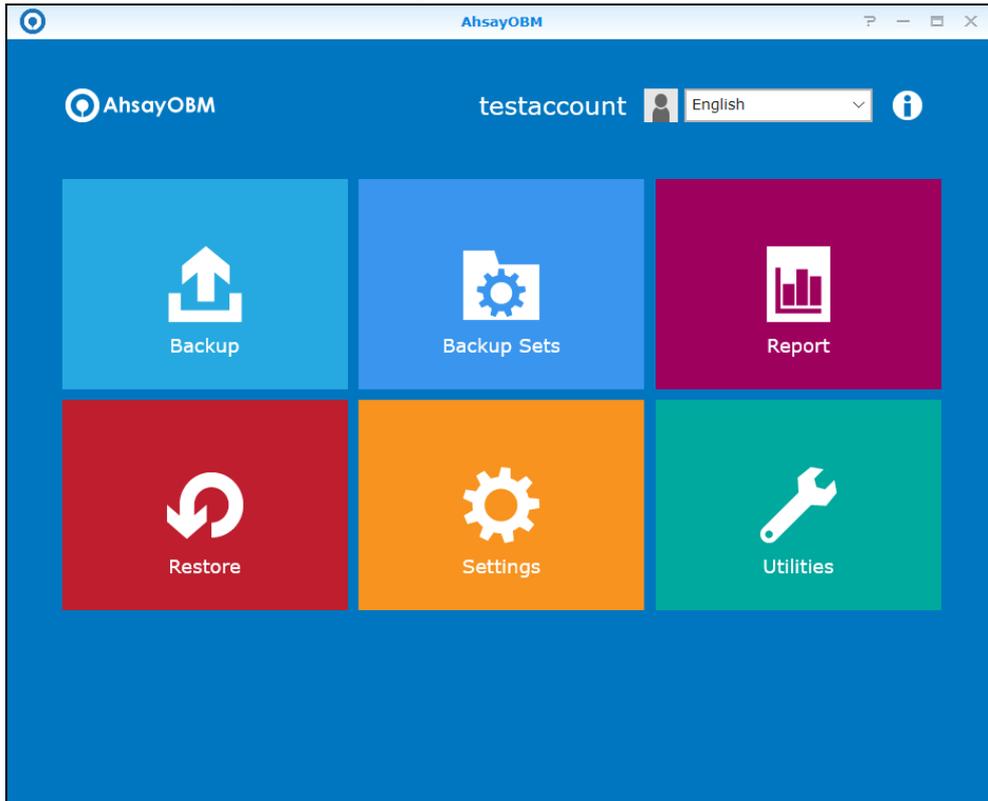
Multi-Factor Authentication

SMS message with a passcode was already sent to the phone number Philippines (+63) - *****6123
Please enter the passcode to continue login.

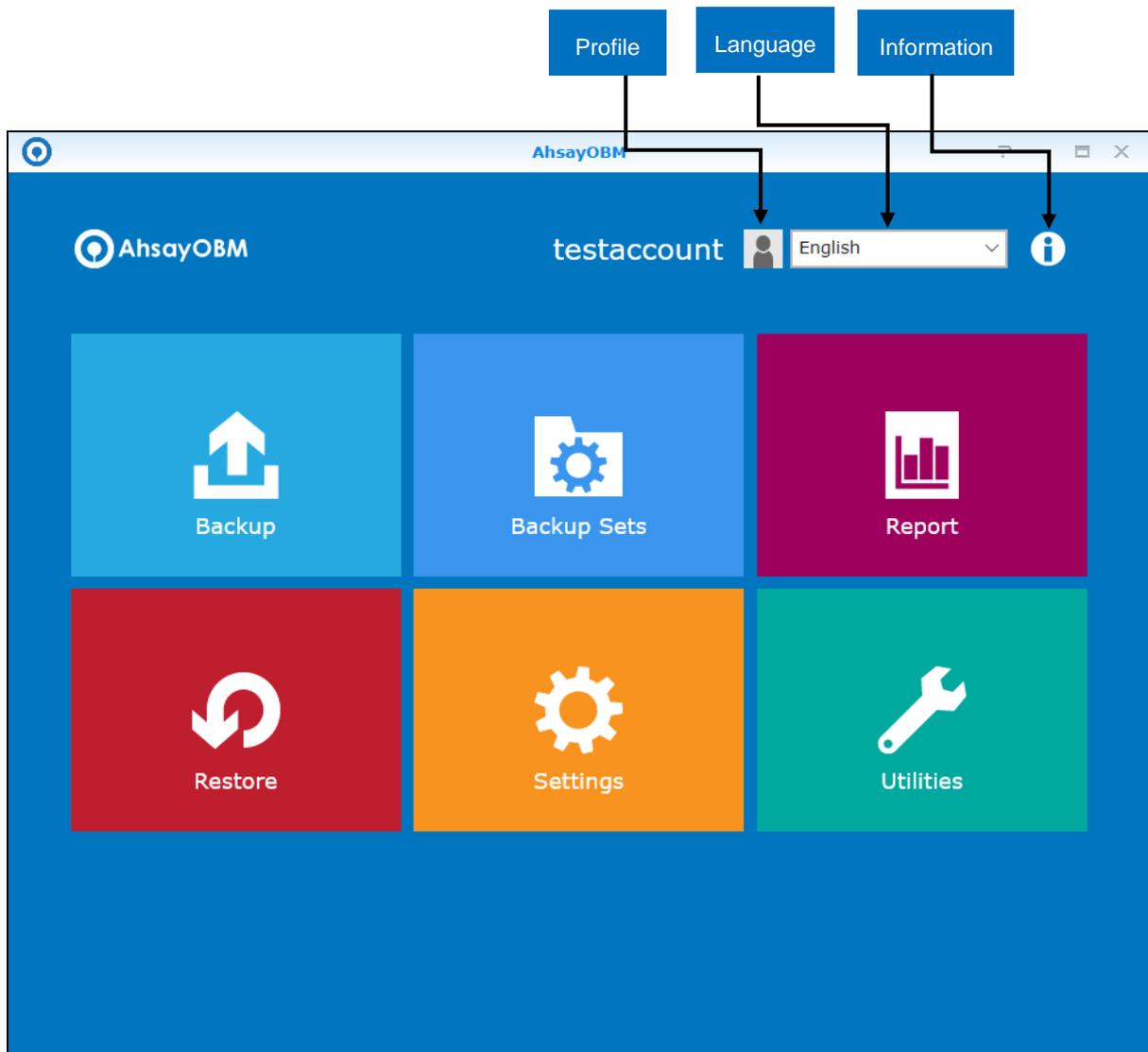
RVPV - (00:04:27)

Verify Cancel Help

8. 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, namely:

- **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.



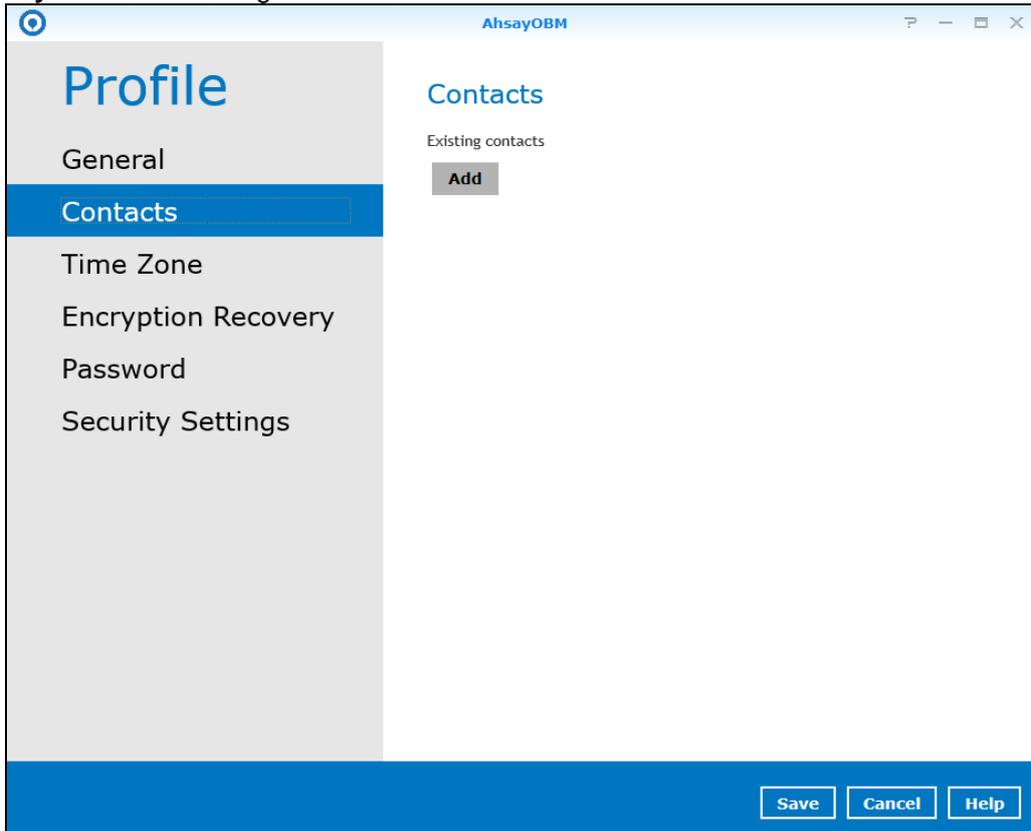
Profile has five (5) features:

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

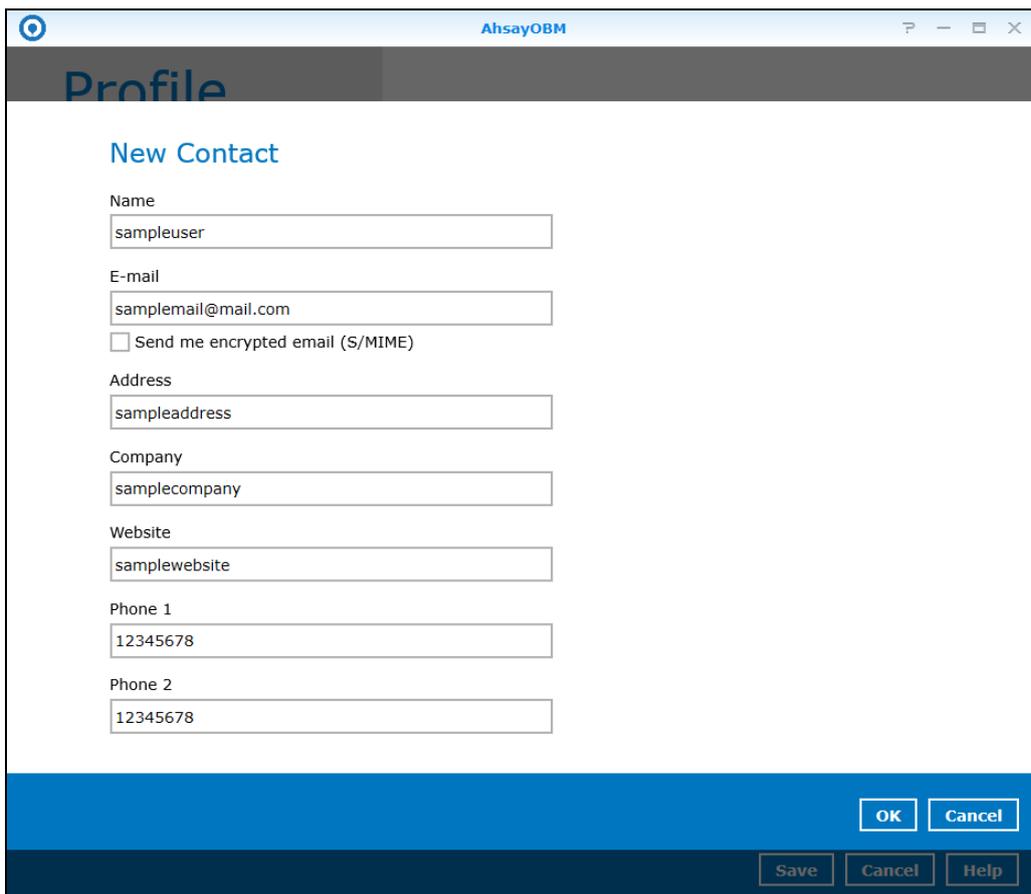
The **General** tab displays the **user information**.

- 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.

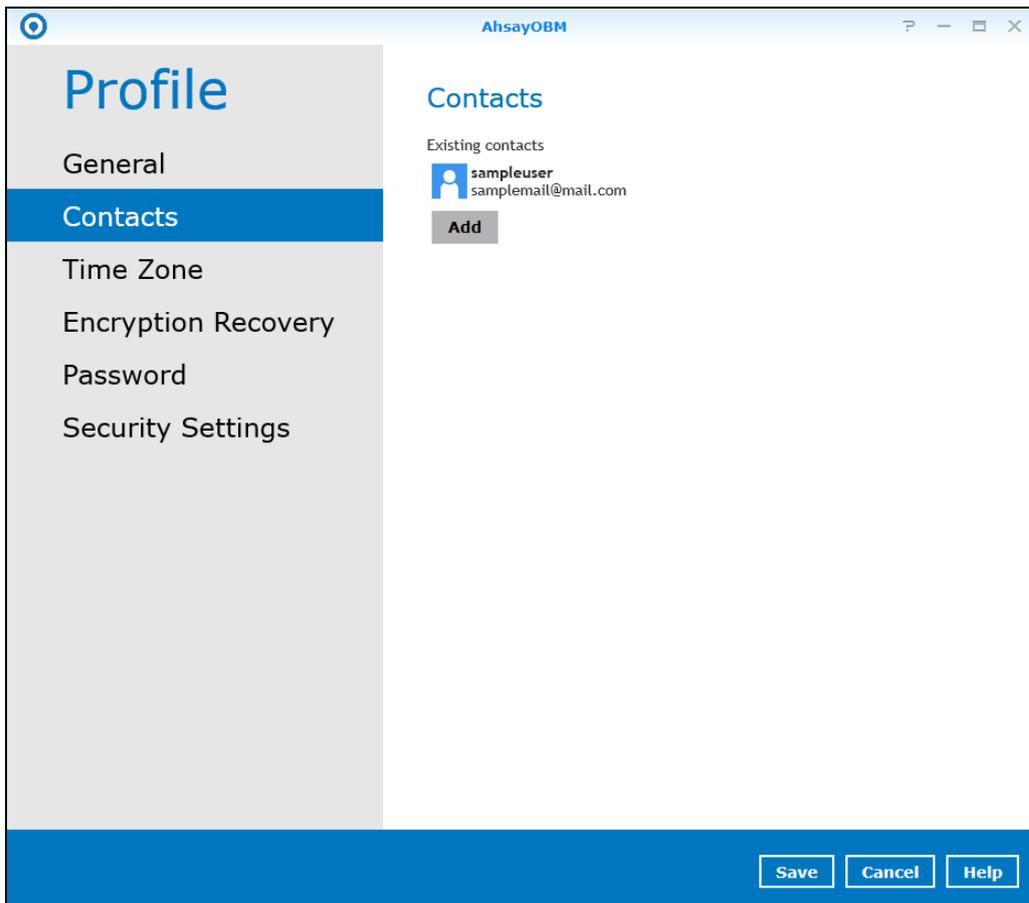
You can add or modify the email address of the **contact person** here. Having this filled in will help us to know where to send the **backup** and **daily reports**, and the **recovered backup set encryption key** in case it was forgotten or lost.



The screenshot shows the AhsayOBM web interface. The top navigation bar includes the AhsayOBM logo and window controls. The main content area is titled "Profile" and has a sidebar menu with options: General, Contacts (selected), Time Zone, Encryption Recovery, Password, and Security Settings. The "Contacts" section is active, showing "Existing contacts" and an "Add" button. At the bottom, there are "Save", "Cancel", and "Help" buttons.

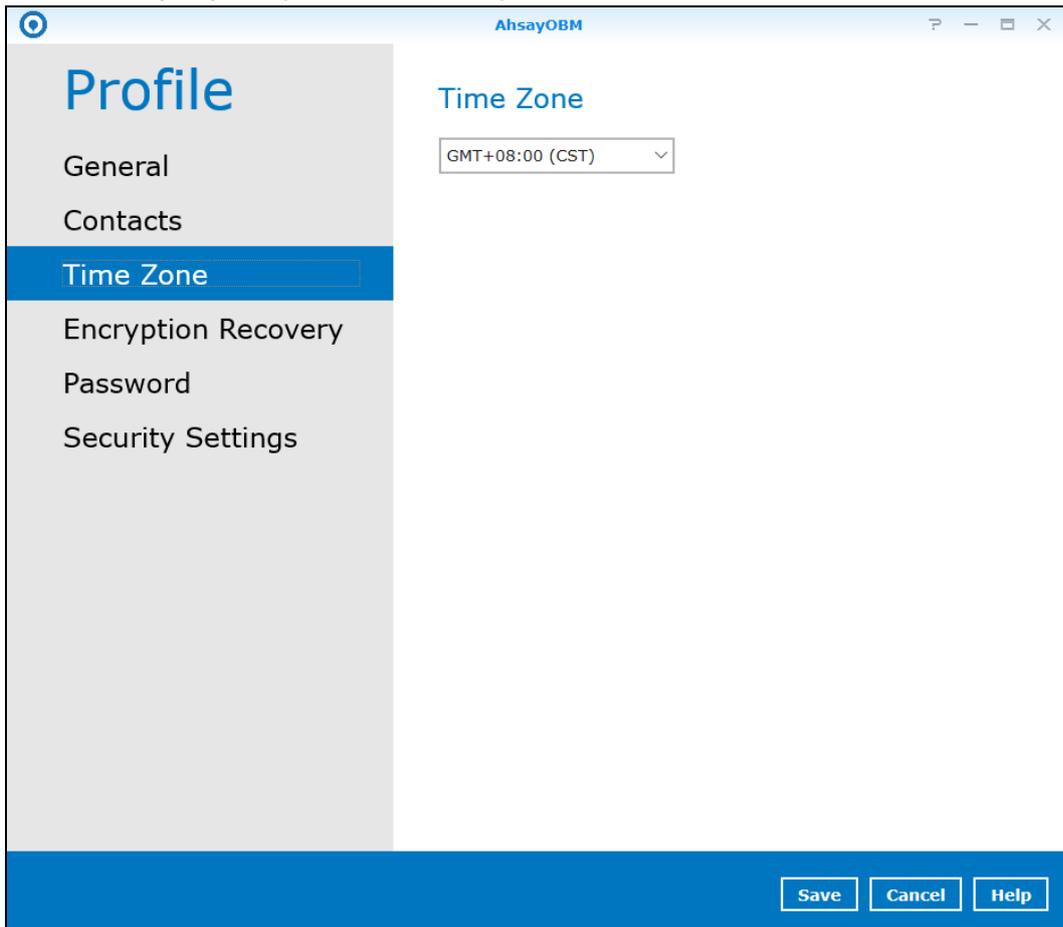


The screenshot shows the "New Contact" form in the AhsayOBM web interface. The form fields are: Name (sampleuser), E-mail (samplemail@mail.com), a checkbox for "Send me encrypted email (S/MIME)", Address (sampleaddress), Company (samplecompany), Website (samplewebsite), Phone 1 (12345678), and Phone 2 (12345678). The "OK" and "Cancel" buttons are visible at the bottom of the form area, and "Save", "Cancel", and "Help" buttons are at the very bottom of the page.



Note: You can add multiple contacts here.

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, setup the correct time.

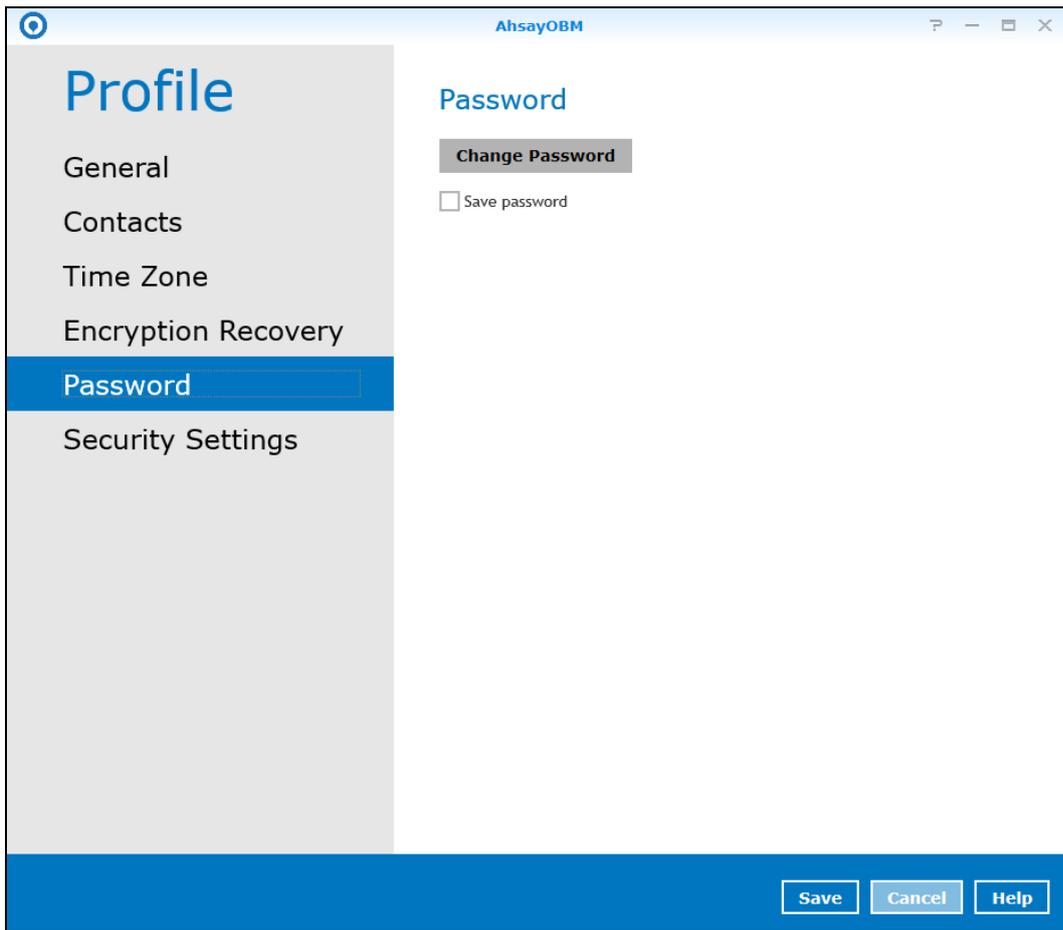


Backup set encryption key can be recovered by turning this feature on.

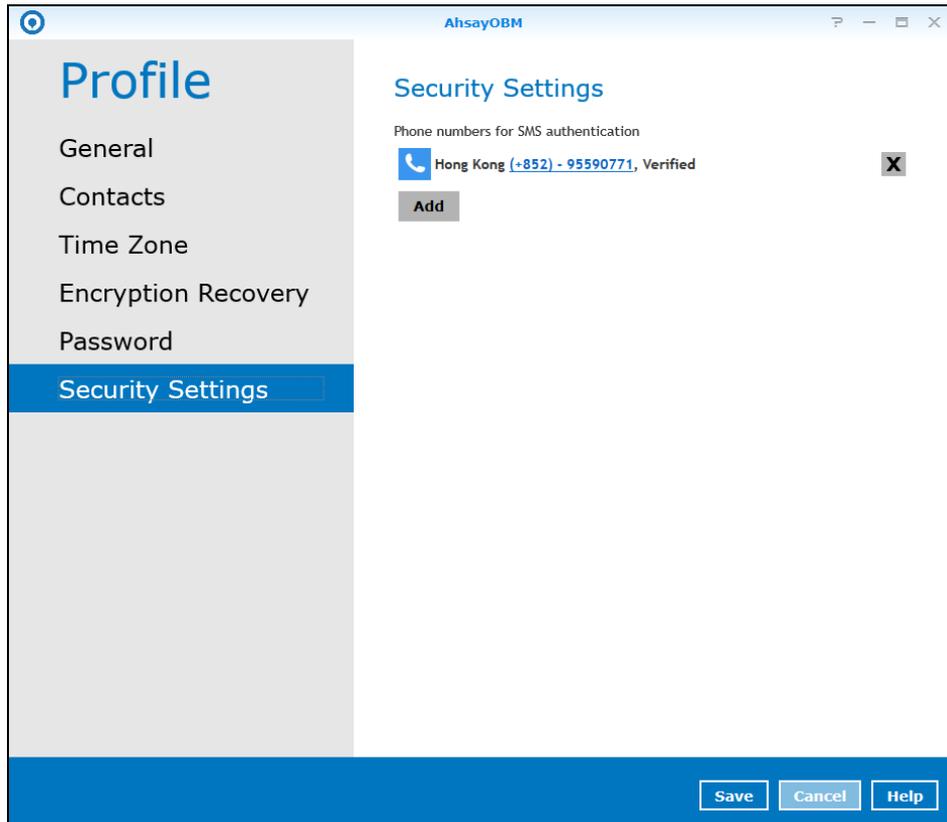


Note: This option may not be available. Please contact your backup service provider for details.

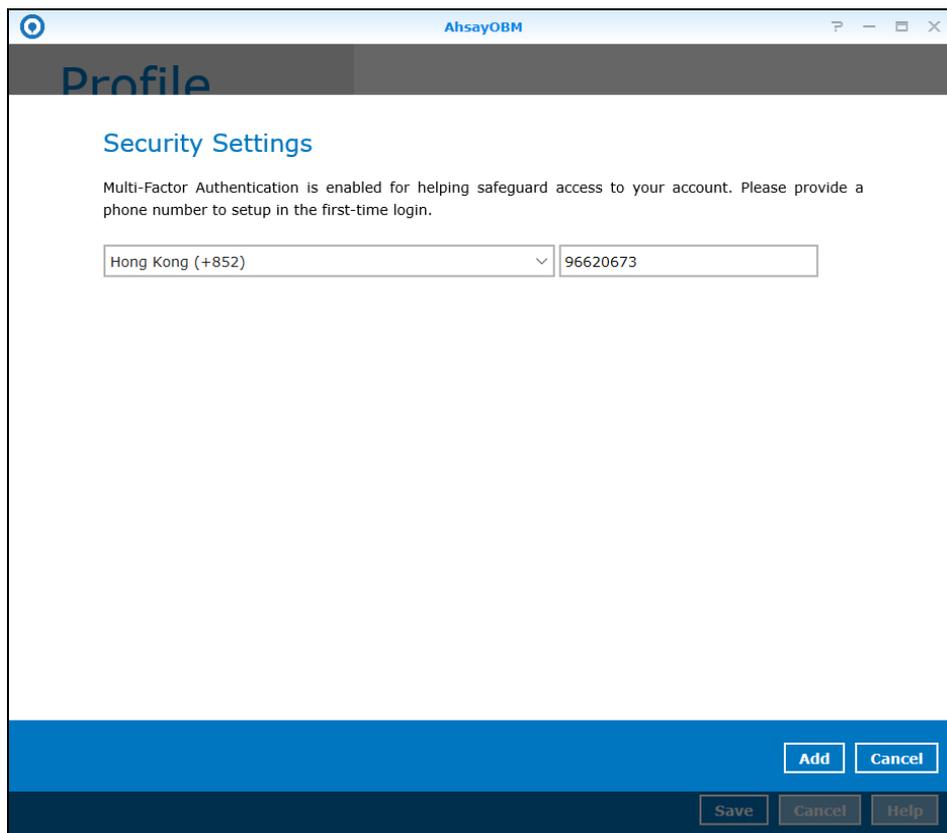
Login password can be modified anytime. You can also tick the **save password** box to bypass the password entry when opening the AhsayOBM interface.



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

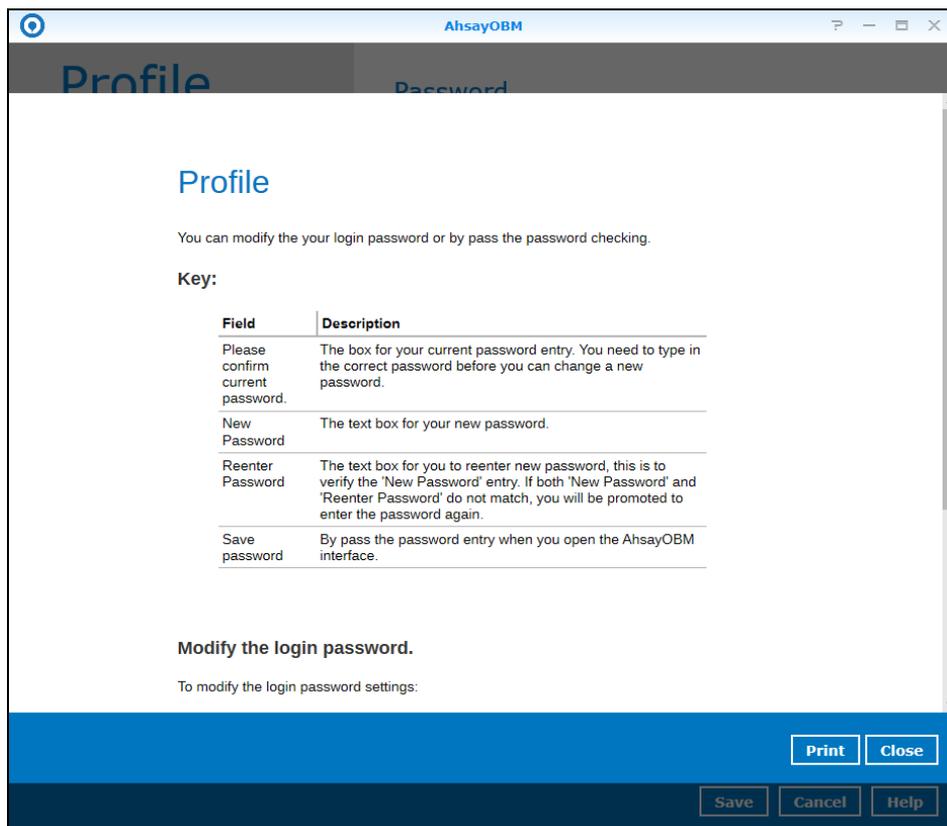
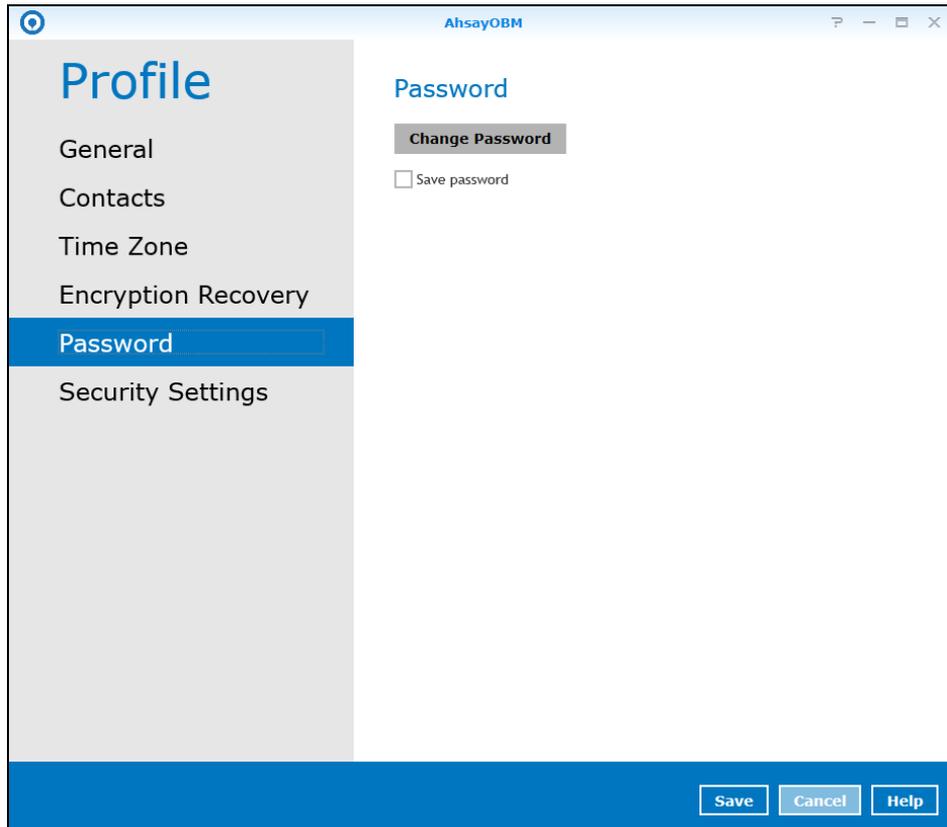


Select the country and enter the phone number, then click **Add**.



6.2 Online Help

Clicking on the **help** tab will show you the information and instructions you may need.



6.3 Language

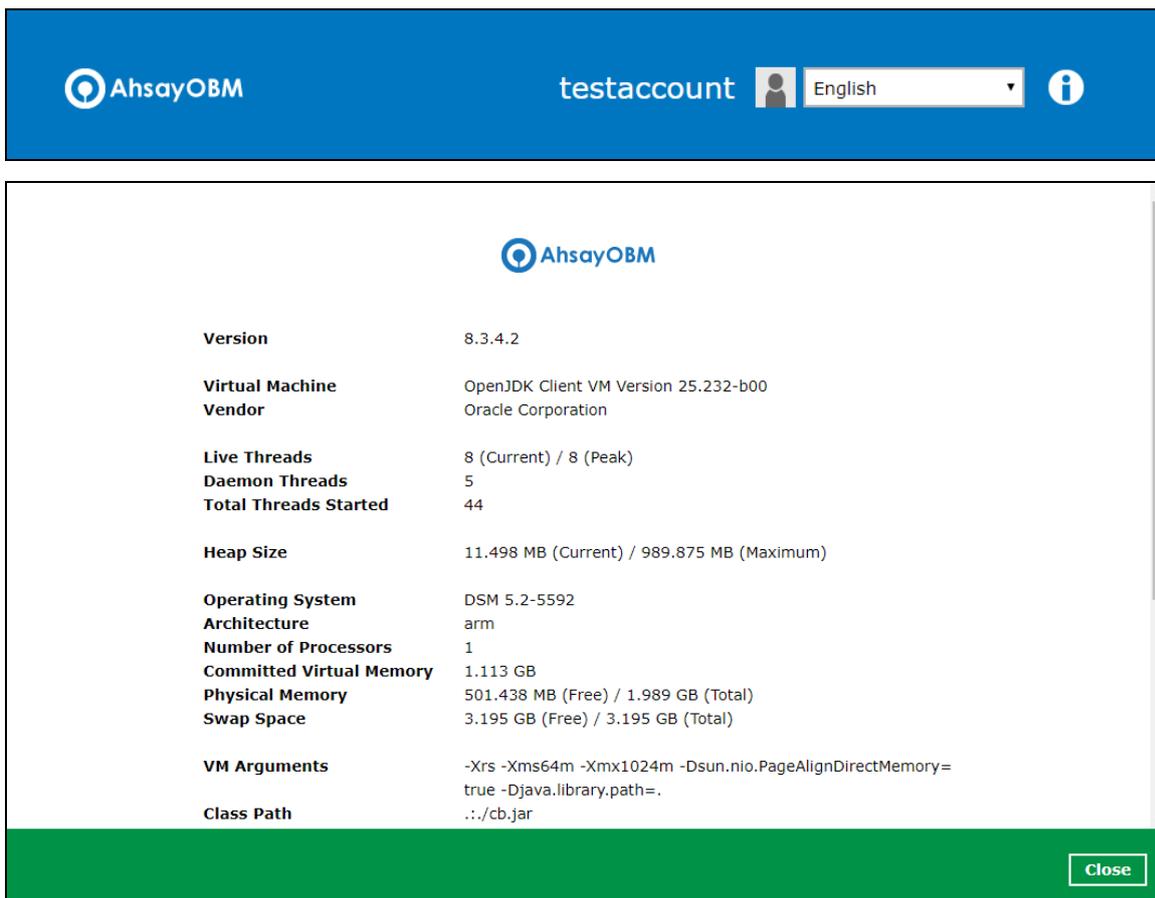
This option is used to change the language of the user interface. The list of available languages depends on the backup service provider.



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

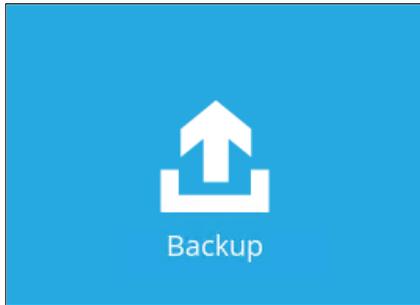
6.4 Information

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

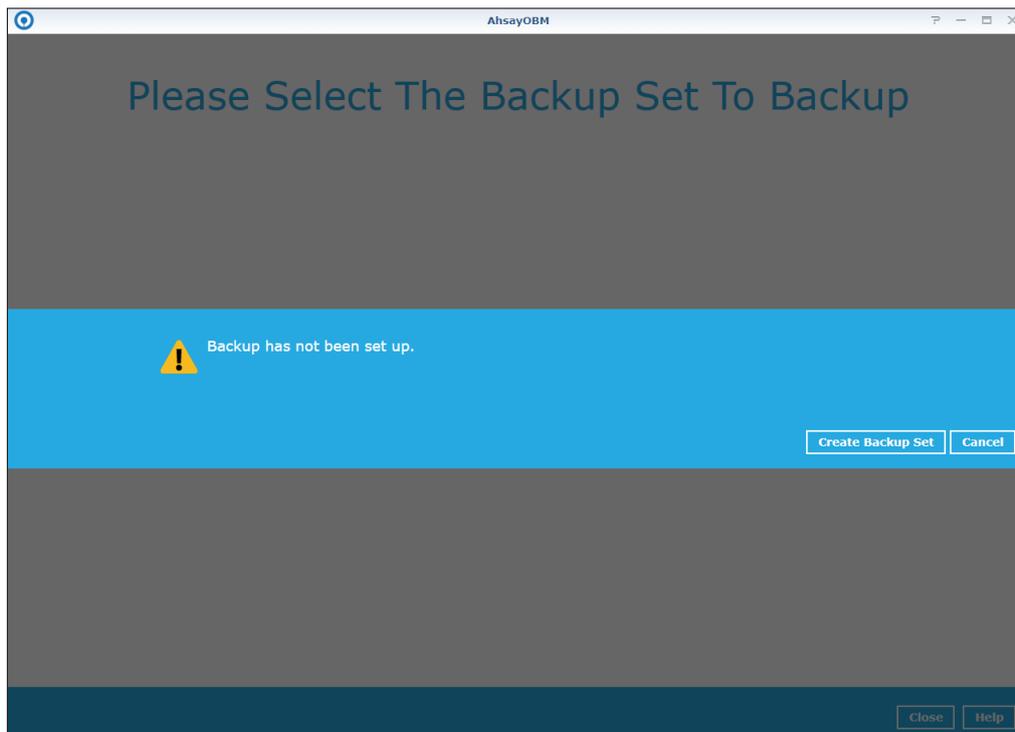


6.5 Backup

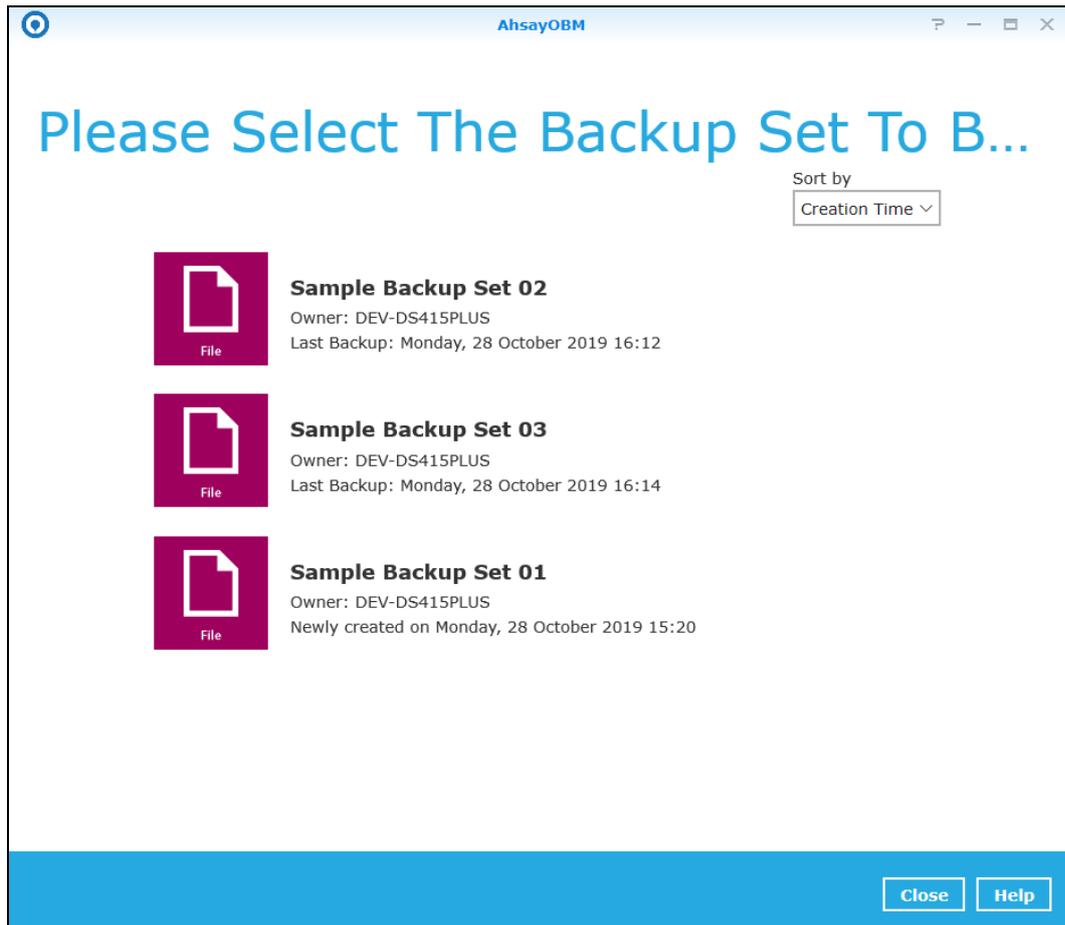
This feature is used to run your backup set(s).

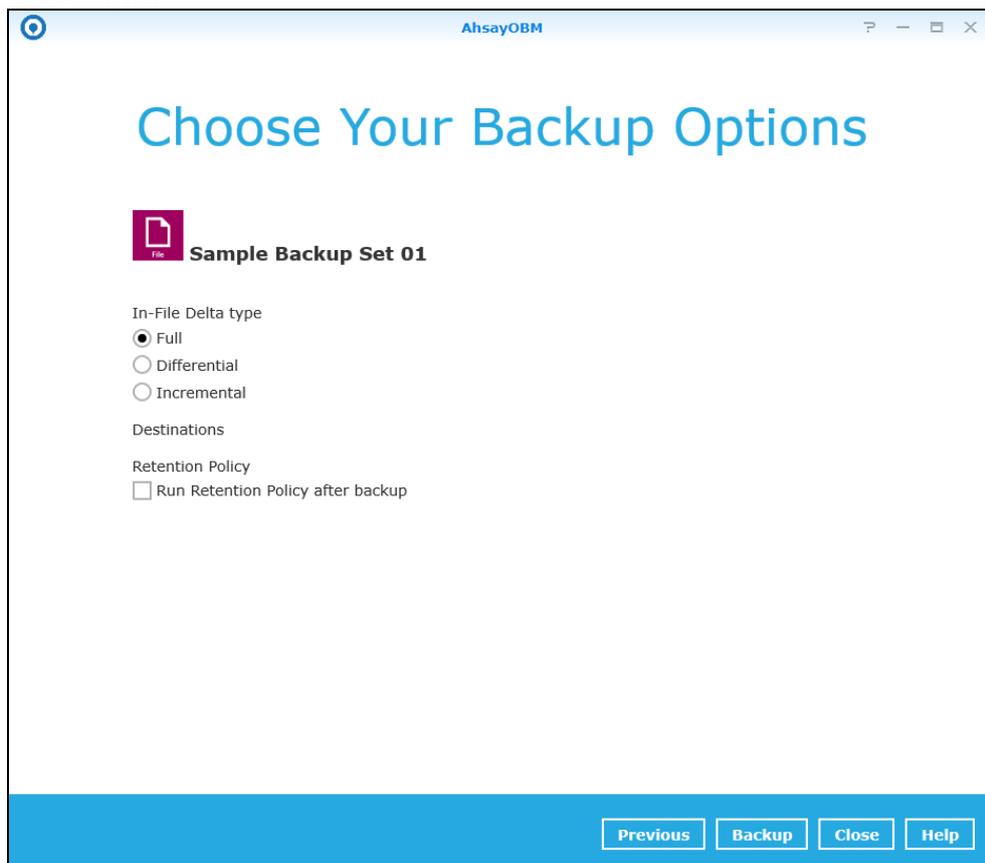


When using AhsayOBM for the first time, you will be asked to create a new backup set first.



If there is an existing backup set or after a backup set is created, choose the backup set you want to backup.





There are three (3) options in the In-File Delta type section:

- **Full** – this type of backup will capture all the data that you want to secure. When you run a backup job for the first time, AhsayOBM will run a full backup regardless of the in-file delta setting.
- **Differential** – this type of backup captures only the changes made as compared with the last uploaded full file only and not since the last differential backup.
- **Incremental** – this type of backup captures only the changes compared with the last uploaded full or delta file.

The **destination** depends on the selected destination storage(s) during the creation of backup set.

Enabling the **retention policy** will help you save hard disk quota in the long run.

Click **backup** to start the backup job.

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 Creating a File Backup Set](#).

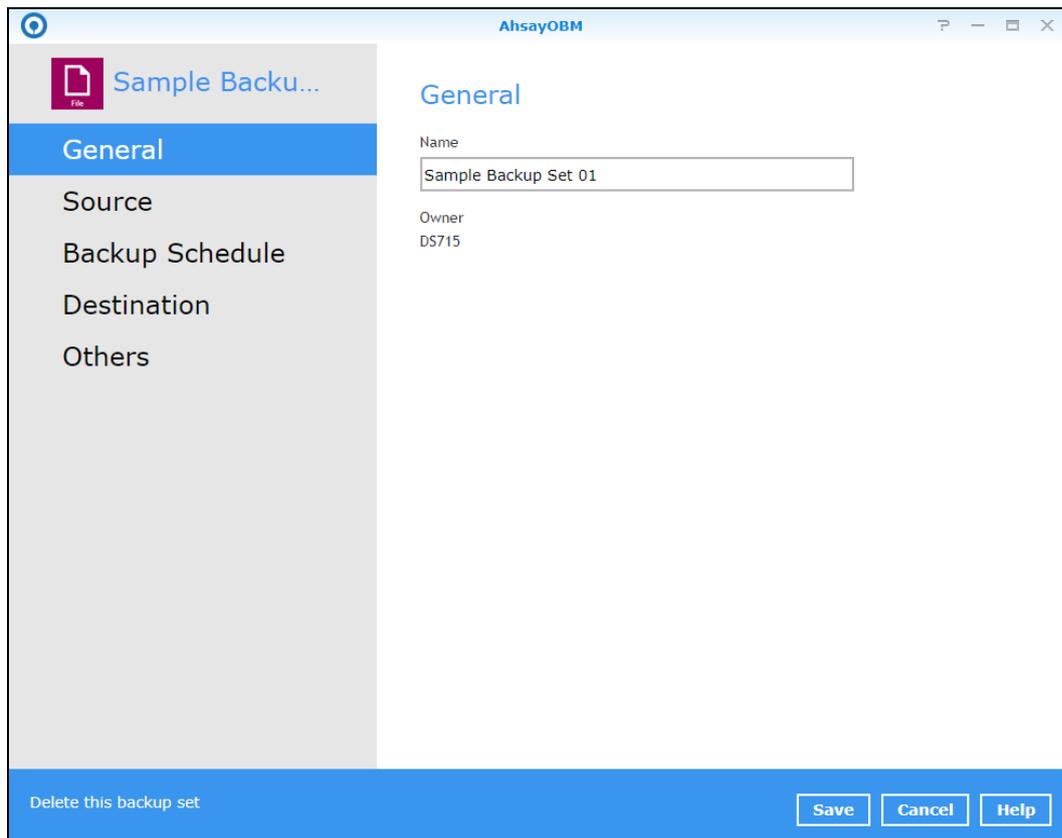
Backup Set Settings

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

- [General](#)
- [Source](#)
- [Backup Schedule](#)
- [Destination](#)
- [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.

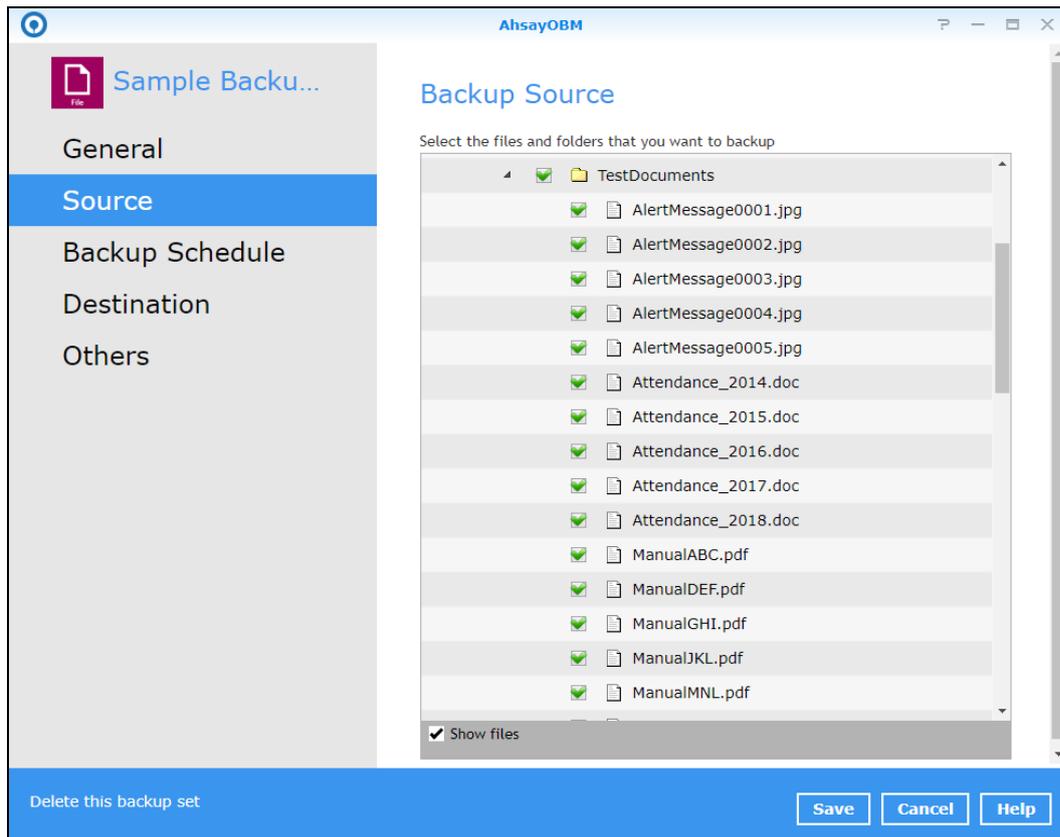


To modify the backup set name, follow the instructions below:

1. Select [General].
2. Enter the 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 NAS device.

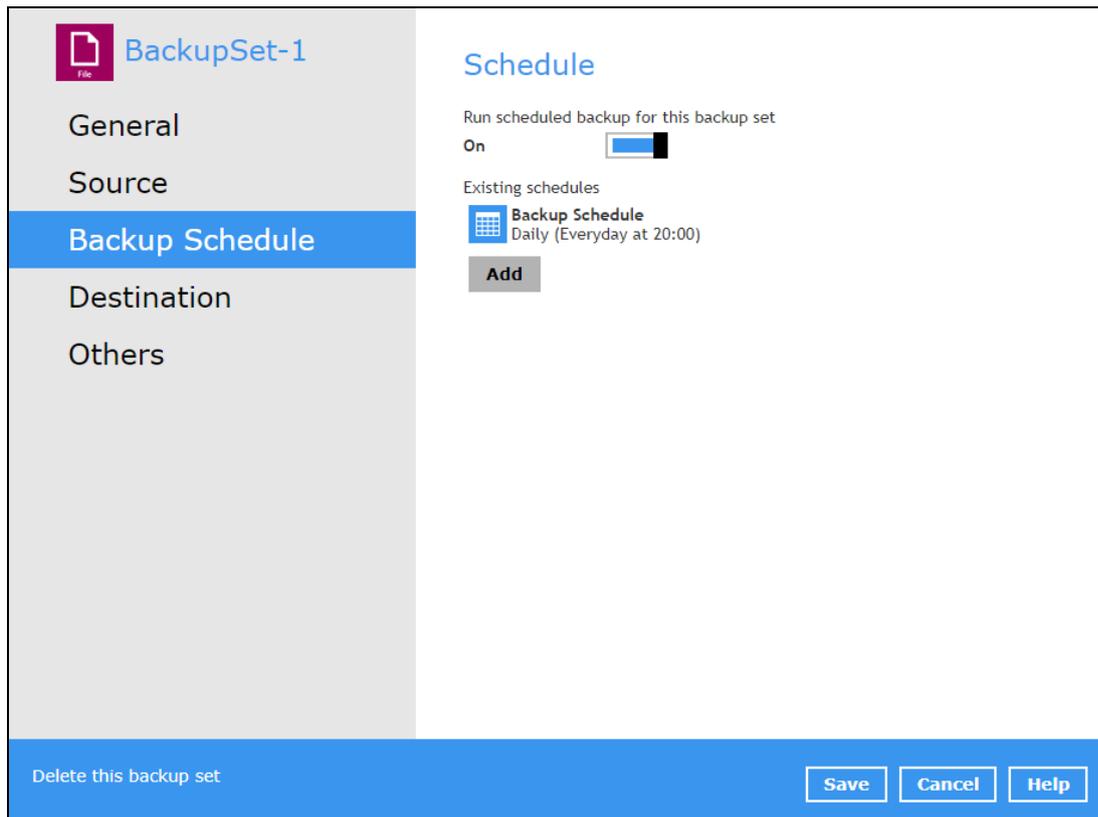


To add backup source, follow the instructions below:

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

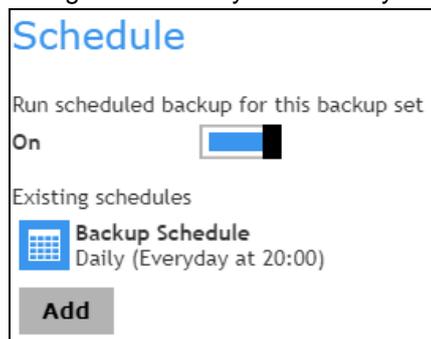
Backup Schedule

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

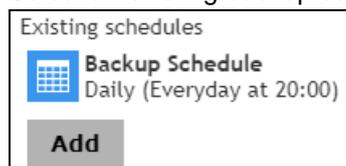


To configure a backup schedule, follow the steps below:

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



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



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

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

Backup Schedule

Name
Daily-1

Type
Daily ▾

Start backup
at ▾ 18 ▾ : 00 ▾

Stop
until full backup completed ▾

Run Retention Policy after backup

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

Backup Schedule

Name
Weekly-1

Type
Weekly ▾

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

Start backup
at ▾ 19 ▾ : 00 ▾

Stop
until full backup completed ▾

Run Retention Policy after backup

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

Backup Schedule

Name
Monthly-1

Type
Monthly ▾

Backup on the following day every month
 Day 1 ▾
 Last ▾ Sunday ▾

Start backup at
20 ▾ : 00 ▾ on the selected days

Stop
until full backup completed ▾

Run Retention Policy after backup

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

Backup Schedule

Name

Type

Backup on the following day once

Start backup at
 :

Stop

Run Retention Policy after backup

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

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

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

- **until full backup completed** – this option will stop a backup job once it is complete. This is the configured stop time of the backup job by default.
- **after (defined no. of hrs.)** – this option will stop a backup job after a certain number of hours regardless of whether the backup job has completed or not. This can range from 1 to 24 hrs.

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

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

The partially backed up data will have to be removed by running the [data integrity check](#).

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

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

5. Click the **[OK]** button to save the configured backup schedule settings.
6. Click the **[Save]** button to save settings.
7. Multiple backup schedules can be created.

Schedule

Run scheduled backup for this backup set

On

Existing schedules

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

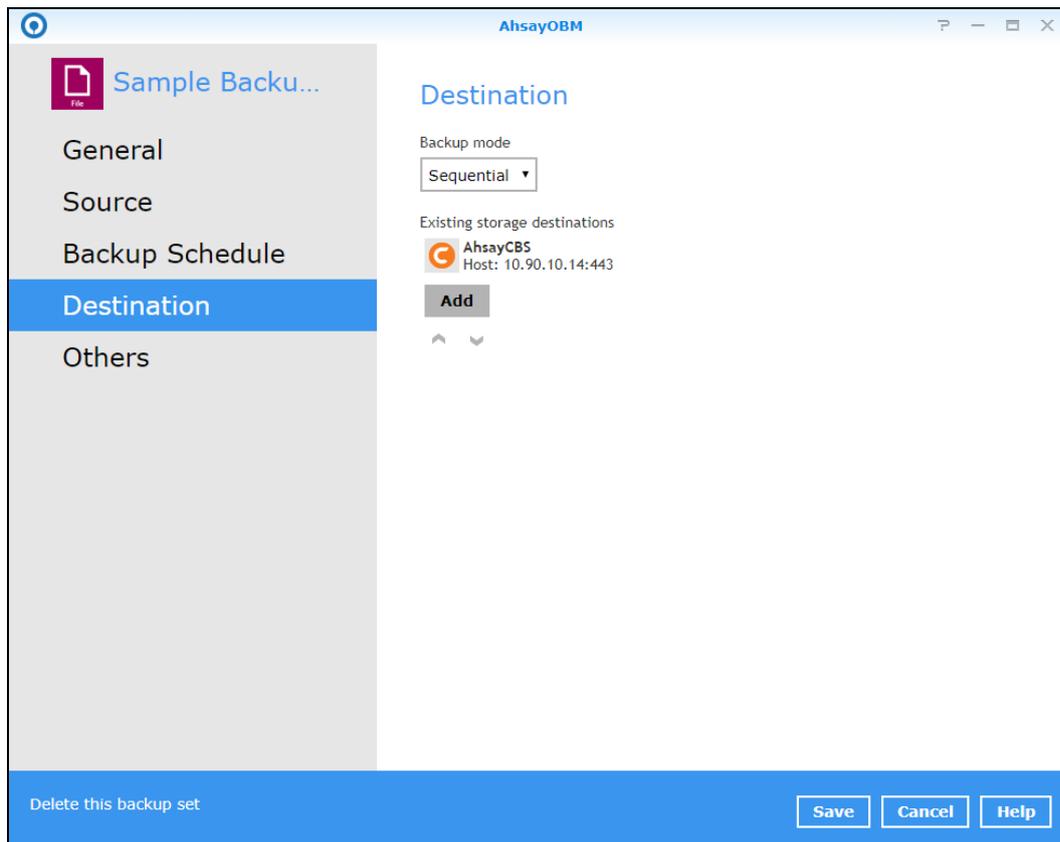
Add

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.



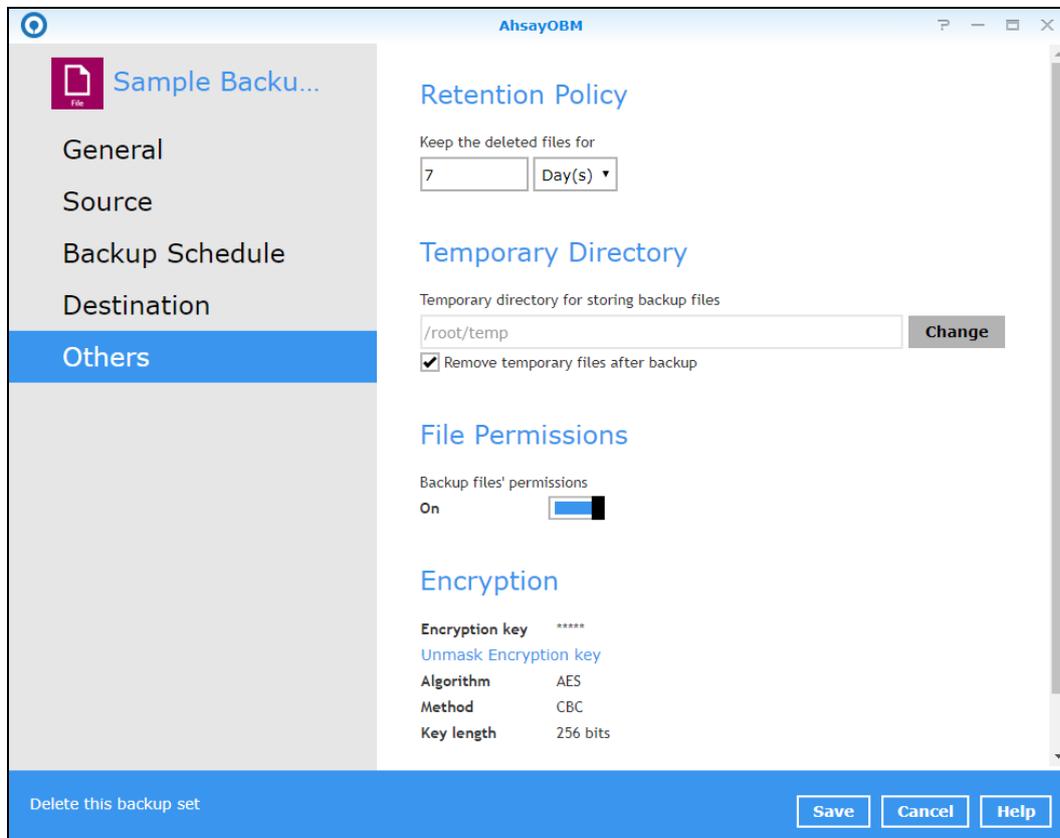
To add a destination, follow the instructions below:

1. Select [Destination].
2. Click the [Add] button.
3. Complete the following fields:
 - Name
 - Destination Storage
4. Click the [OK] button to add the new schedule.
5. Click the [Save] button to save the changes made.

Others

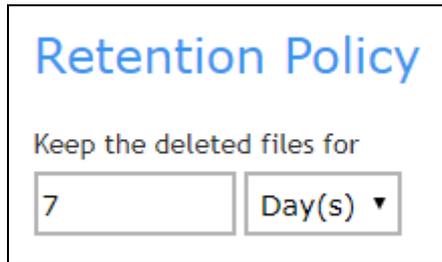
These are the list of other backup set settings that can be configured.

- [Retention Policy](#)
- [Temporary Directory](#)
- [File Permissions](#)
- [Encryption](#)



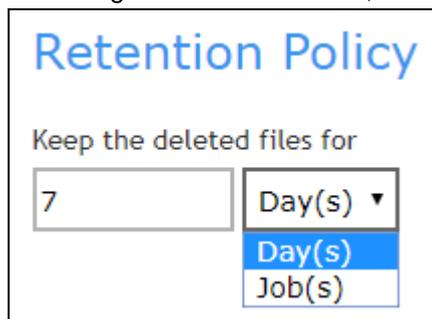
Retention Policy

This allows the user to retain the deleted files based on the selected retention type policy.



To modify the retention policy, follow the instructions below:

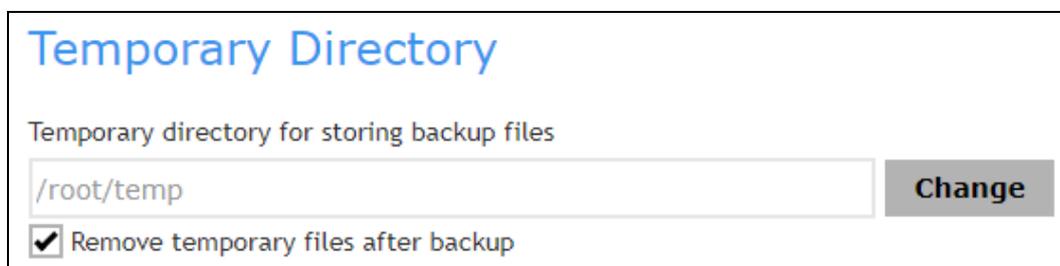
1. Select [Others].
2. On the right side of the screen, select from the two (2) options: Day(s) or Job(s).



3. Input a valid number for the Day(s) or Job(s).
4. Click the [Save] button to save the settings made.

Temporary Directory

This allows the user to configure the temporary directory of spooled files, remote file list, and other temporary backup files.

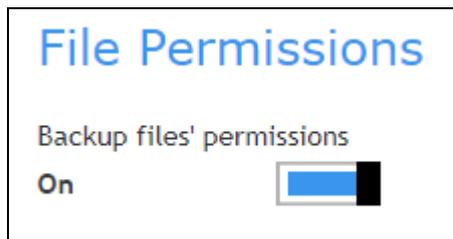


To configure the temporary directory, follow the instructions below:

1. Click the [Change] button to select a directory path for storing the temporary data.
2. You also have an option to check or uncheck the [Remove temporary files after backup].
3. Click the [Save] button to save the settings.

File Permissions

This allows the user to enable or disable the backup file permission which backs up the operating system file permission of the data selected as backup source.



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

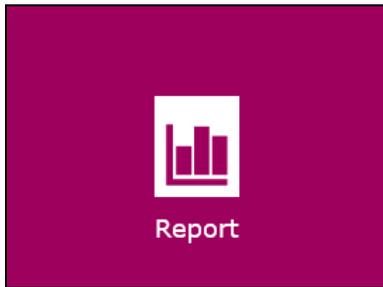
Encryption

This allows the user to view the current encryption settings. For more details about the encryption, check [Chapter 7 Creating a File Backup Set](#).



6.7 Report

This feature allows user to run and view **backup** and **restore reports**.



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

- Backup
- Restore

6.7.1 Backup

This feature is used for viewing backup report(s). There are four (4) filters that can be applied on this feature, namely:

- Time
- Backup set
- Destination
- Status

The screenshot shows the AhsayOBM application window. On the left is a navigation sidebar with a "Report" header and two options: "Backup" (highlighted in purple) and "Restore". The main content area is titled "Backup Report" and features a date range selector with "From" (22 Oct 2019) and "To" (29 Oct 2019) fields, and a "Go" button. Below this is a table with columns for "Backup set", "Destination", "Completion", and "Status".

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

At the bottom right of the window are "Close" and "Help" buttons.

By setting the **time**, you will see the list of all backup report(s) within that period.

Backup Report

From: 22 Oct 2019 To: 29 Oct 2019 **Go**

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

Backup report(s) can be sorted alphabetically by using the **backup up set** filter.

Backup Report

From: 22 Oct 2019 To: 29 Oct 2019 **Go**

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

You can view all the backup report(s) in your storage location by sorting the **destination** filter

Backup Report

From: 22 Oct 2019 To: 29 Oct 2019 **Go**

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

You can sort all backup reports with the same status by using the **status** filter.

Backup Report

From: 22 Oct 2019 To: 29 Oct 2019 **Go**

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

You can apply filter on the status of the event by clicking the drop-down list.

The screenshot shows the AhsayOBM Backup Report interface. A 'Show' dropdown menu is open, displaying options: 'All', 'Information', 'Warning', and 'Error'. The 'All' option is currently selected. Below the menu is a table with columns for 'Type', 'Log', and a date/time column. The table contains various log entries such as 'Start [AhsayOBM v8.3.0.30]', 'Saving encrypted backup set encryption keys to server...', and 'Start Backup ... [In-File Delta: Full]'. At the bottom right, there are 'Close' and 'Help' buttons.

Type	Log	28/10/2019 16:14:30
[i]	Start [AhsayOBM v8.3.0.30]	28/10/2019 16:14:30
[i]	Saving encrypted backup set encryption keys to server...	28/10/2019 16:14:30
[i]	Start Backup ... [In-File Delta: Full]	28/10/2019 16:14:31
[i]	Using Temporary Directory /root/temp/1572250178351/OBS@1572250195445	28/10/2019 16:14:31
[i]	Start running pre-commands	28/10/2019 16:14:33
[i]	Finished running pre-commands	28/10/2019 16:14:33
[i]	Downloading server file list...	28/10/2019 16:14:33
[i]	Downloading server file list... Completed	28/10/2019 16:14:35
[i]	Reading backup source from hard disk...	28/10/2019 16:14:36
[i]	[New Directory]... /	28/10/2019 16:14:36
[i]	[New Directory]... /volume1	28/10/2019 16:14:36
[i]	[New Directory]... /volume1/Manyfiles	28/10/2019 16:14:36
[i]	[New Directory]... /volume1/Manyfiles/#recycle	28/10/2019 16:14:36
[i]	[New Directory]... /volume1/Manyfiles/1000x100K1	28/10/2019 16:14:36
[i]	[New File]... 100% of "/volume1/Manyfiles/#recycle/desktop.ini"	28/10/2019 16:14:36
[i]	[New File]... 24% of "/volume1/Manyfiles/1000x100K1/100KB_1"	28/10/2019 16:14:37
[i]	[New File]... 40% of "/volume1/Manyfiles/1000x100K1/100KB_1"	28/10/2019 16:14:37
[i]	[New File]... 56% of "/volume1/Manyfiles/1000x100K1/100KB_1"	28/10/2019 16:14:37
[i]	[New File]... 72% of "/volume1/Manyfiles/1000x100K1/100KB_1"	28/10/2019 16:14:37

You can choose to view the number of logs per page by clicking the drop-down list.

The screenshot shows the AhsayOBM Backup Report interface with a pagination control. A dropdown menu for 'Logs per page' is set to '50'. Below it, there are 'Previous', '1', '2', '3', '4', '5', '...', '324', and 'Next' buttons. The table displays a list of log entries, each starting with '[New File]...' and showing a percentage of completion for a file. At the bottom right, there are 'Close' and 'Help' buttons.

[i]	[New File]... 56% of "/volume1/Manyfiles/1000x100K1/100KB_100"	28/10/2019 16:14:37
[i]	[New File]... 72% of "/volume1/Manyfiles/1000x100K1/100KB_100"	28/10/2019 16:14:37
[i]	[New File]... 88% of "/volume1/Manyfiles/1000x100K1/100KB_100"	28/10/2019 16:14:37
[i]	[New File]... 100% of "/volume1/Manyfiles/1000x100K1/100KB_100"	28/10/2019 16:14:37
[i]	[New File]... 24% of "/volume1/Manyfiles/1000x100K1/100KB_101"	28/10/2019 16:14:37
[i]	[New File]... 40% of "/volume1/Manyfiles/1000x100K1/100KB_101"	28/10/2019 16:14:37
[i]	[New File]... 56% of "/volume1/Manyfiles/1000x100K1/100KB_101"	28/10/2019 16:14:37
[i]	[New File]... 72% of "/volume1/Manyfiles/1000x100K1/100KB_101"	28/10/2019 16:14:37
[i]	[New File]... 88% of "/volume1/Manyfiles/1000x100K1/100KB_101"	28/10/2019 16:14:37
[i]	[New File]... 100% of "/volume1/Manyfiles/1000x100K1/100KB_101"	28/10/2019 16:14:37
[i]	[New File]... 24% of "/volume1/Manyfiles/1000x100K1/100KB_1000"	28/10/2019 16:14:37
[i]	[New File]... 40% of "/volume1/Manyfiles/1000x100K1/100KB_1000"	28/10/2019 16:14:37
[i]	[New File]... 56% of "/volume1/Manyfiles/1000x100K1/100KB_1000"	28/10/2019 16:14:37
[i]	[New File]... 72% of "/volume1/Manyfiles/1000x100K1/100KB_1000"	28/10/2019 16:14:37
[i]	[New File]... 88% of "/volume1/Manyfiles/1000x100K1/100KB_1000"	28/10/2019 16:14:37
[i]	[New File]... 100% of "/volume1/Manyfiles/1000x100K1/100KB_1000"	28/10/2019 16:14:37
[i]	[New File]... 24% of "/volume1/Manyfiles/1000x100K1/100KB_102"	28/10/2019 16:14:37
[i]	[New File]... 40% of "/volume1/Manyfiles/1000x100K1/100KB_102"	28/10/2019 16:14:37
[i]	[New File]... 56% of "/volume1/Manyfiles/1000x100K1/100KB_102"	28/10/2019 16:14:37
[i]	[New File]... 72% of "/volume1/Manyfiles/1000x100K1/100KB_102"	28/10/2019 16:14:37
[i]	[New File]... 88% of "/volume1/Manyfiles/1000x100K1/100KB_102"	28/10/2019 16:14:37

6.7.2 Restore

This feature is used for viewing restore report(s). You can also apply filter on **time**, **backup set**, **destination** and **status** here.

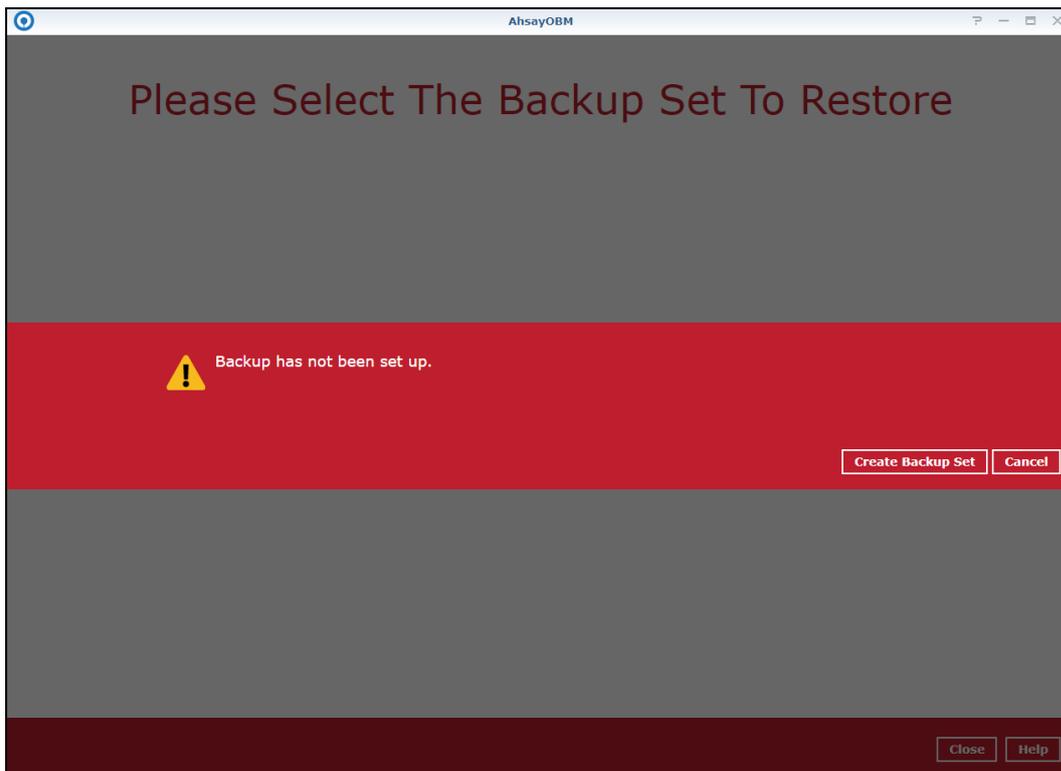
Backup set	Destination	Job	Status
Sample Backup Set 03	AhsayCBS	28/10/2019 16:28	Completed
Sample Backup Set 03	AhsayCBS	28/10/2019 16:27	Completed

6.8 Restore

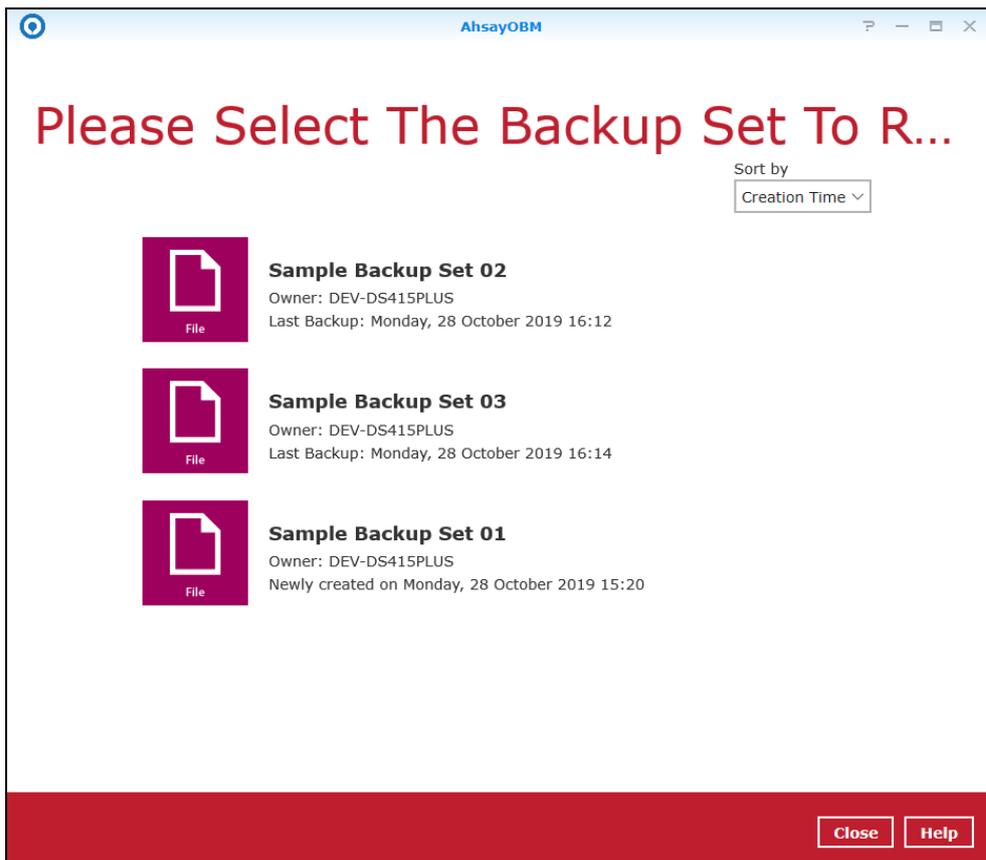
This feature is used to copy the backed-up file(s) from the backup set and restoring it to its original location or new location.



If using AhsayOBM for the first time, you will be asked to create a backup set first. A restore cannot be performed unless you already run a backup.

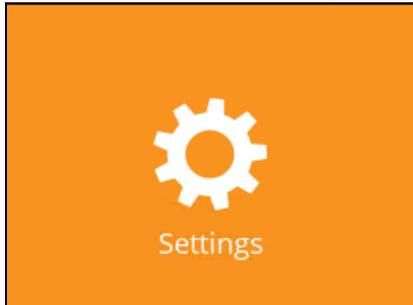


After a backup job has been performed, select a backup set you wish to restore.



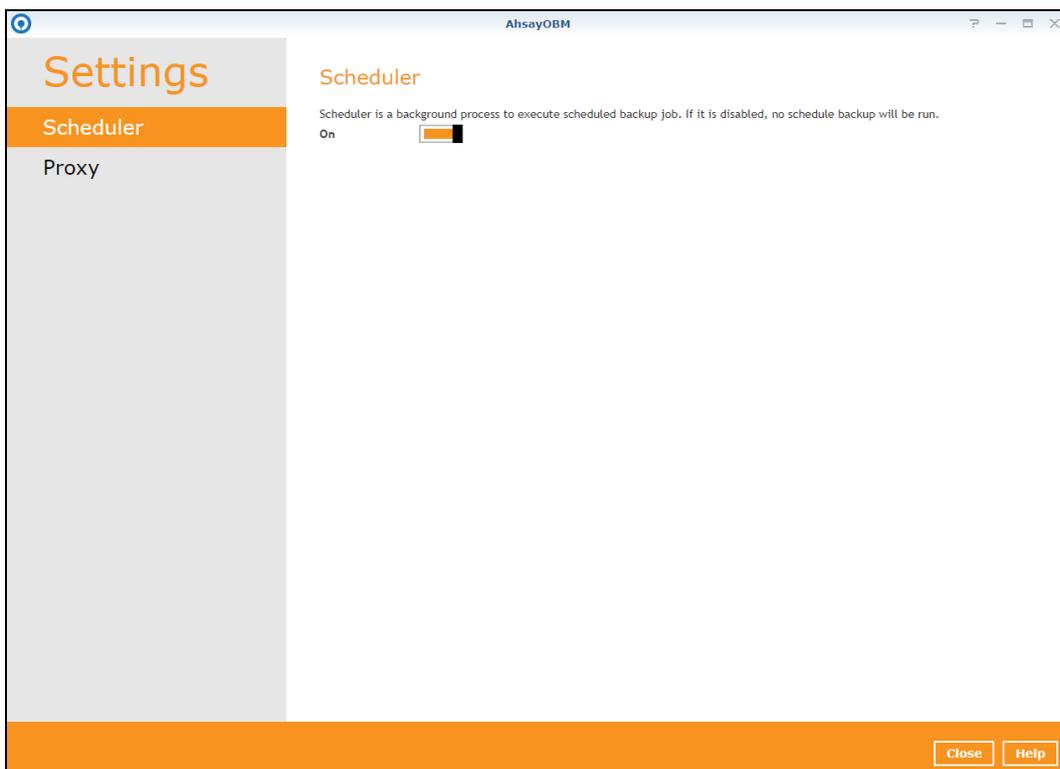
6.9 Settings

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.

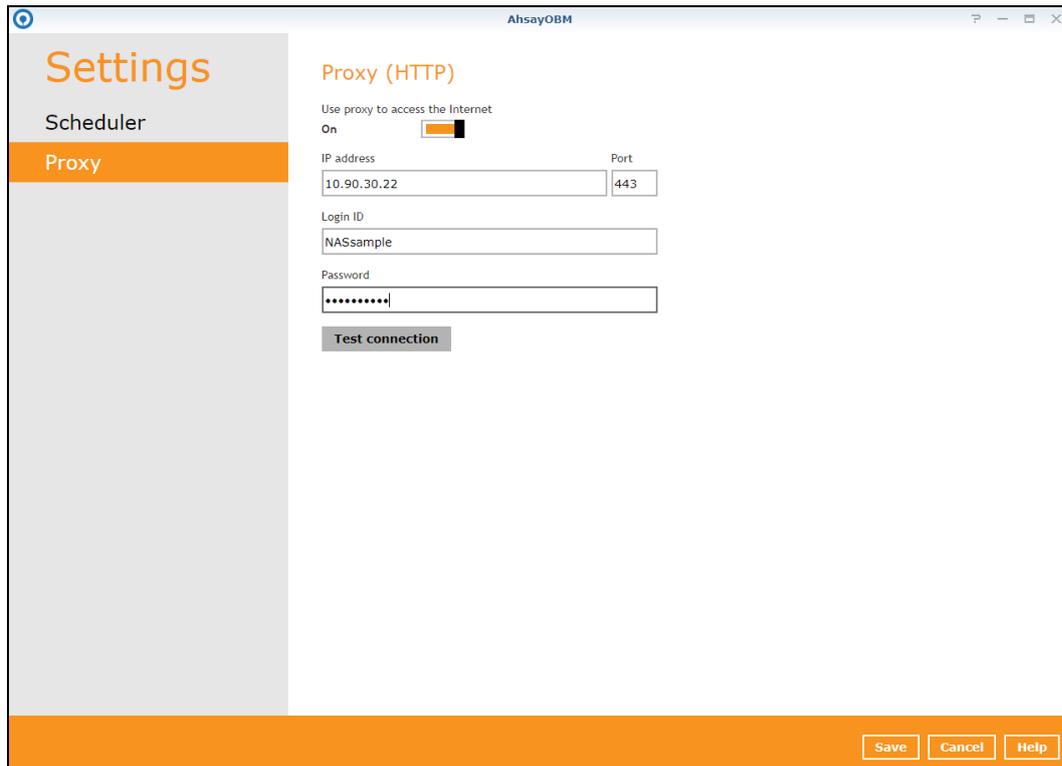


Note

For more details on the scenario for the Scheduler under Settings, refer to [Appendix C: Scheduler Scenarios](#).

6.9.2 Proxy

This feature is used to allow AhsayOBM to gain access to the internet.



The screenshot shows the 'Proxy (HTTP)' settings window in AhsayOBM. The window title is 'AhsayOBM'. On the left, there is a sidebar with 'Settings' at the top, followed by 'Scheduler' and 'Proxy' (which is highlighted in orange). The main content area is titled 'Proxy (HTTP)' and contains the following fields and controls:

- 'Use proxy to access the Internet' with a toggle switch set to 'On'.
- 'IP address' field containing '10.90.30.22'.
- 'Port' field containing '443'.
- 'Login ID' field containing 'NASsample'.
- 'Password' field containing masked characters '*****'.
- 'Test connection' button.

At the bottom right of the window, there are three buttons: 'Save', 'Cancel', and 'Help'.

6.10 Utilities

This allows the user to perform quality check on the backed up data and 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).

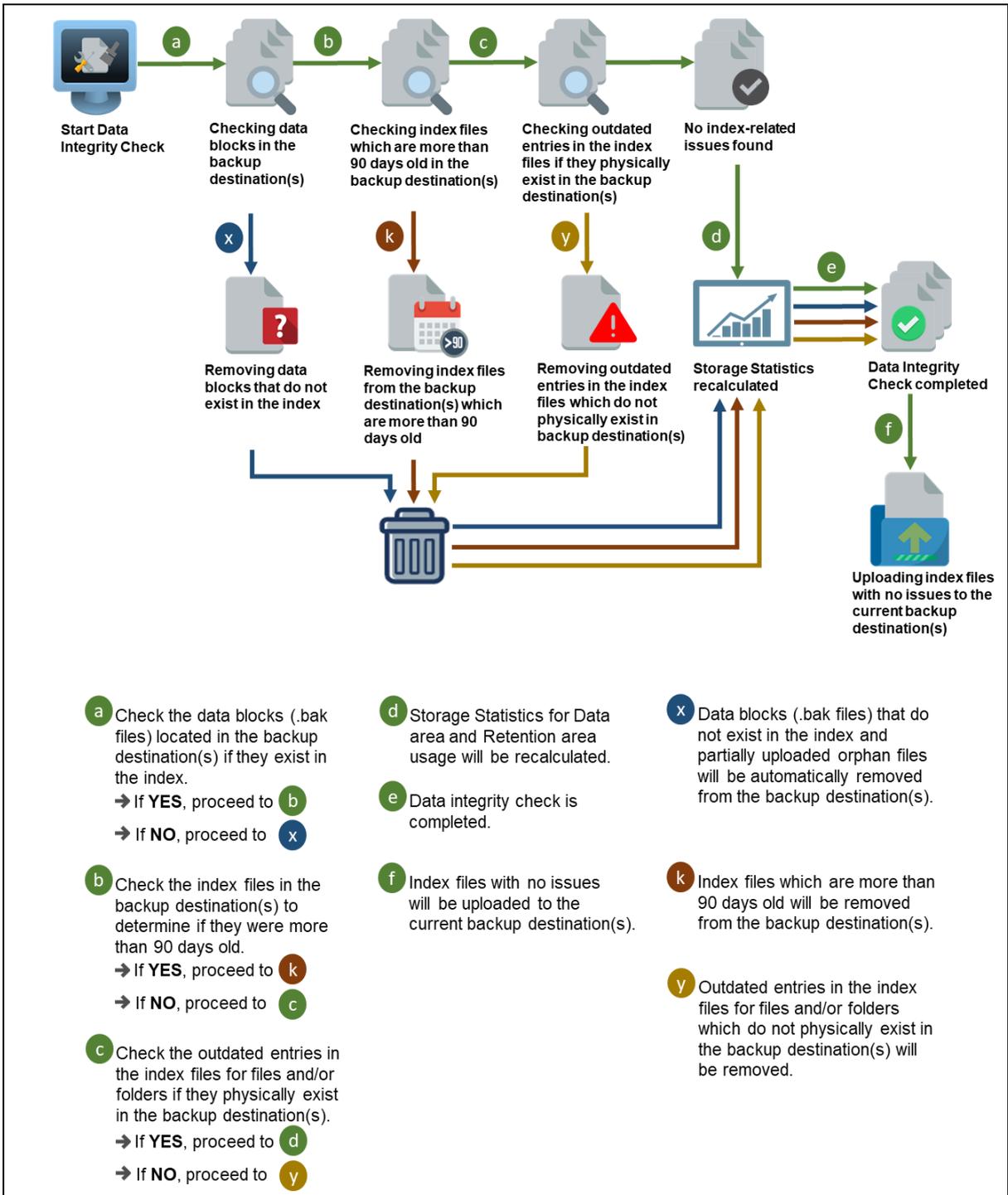
There are two (2) options in performing the Data Integrity Check:

<p>Option 1</p> <p><input type="checkbox"/> Run Cyclic Redundancy Check (CRC) during data integrity check</p> <p>Start</p>	For checking of index and data.
<p>Option 2</p> <p><input checked="" type="checkbox"/> Run Cyclic Redundancy Check (CRC) during data integrity check</p> <p>Start</p>	For checking of index and integrity of files against the checksum file generated at the time of the backup job.

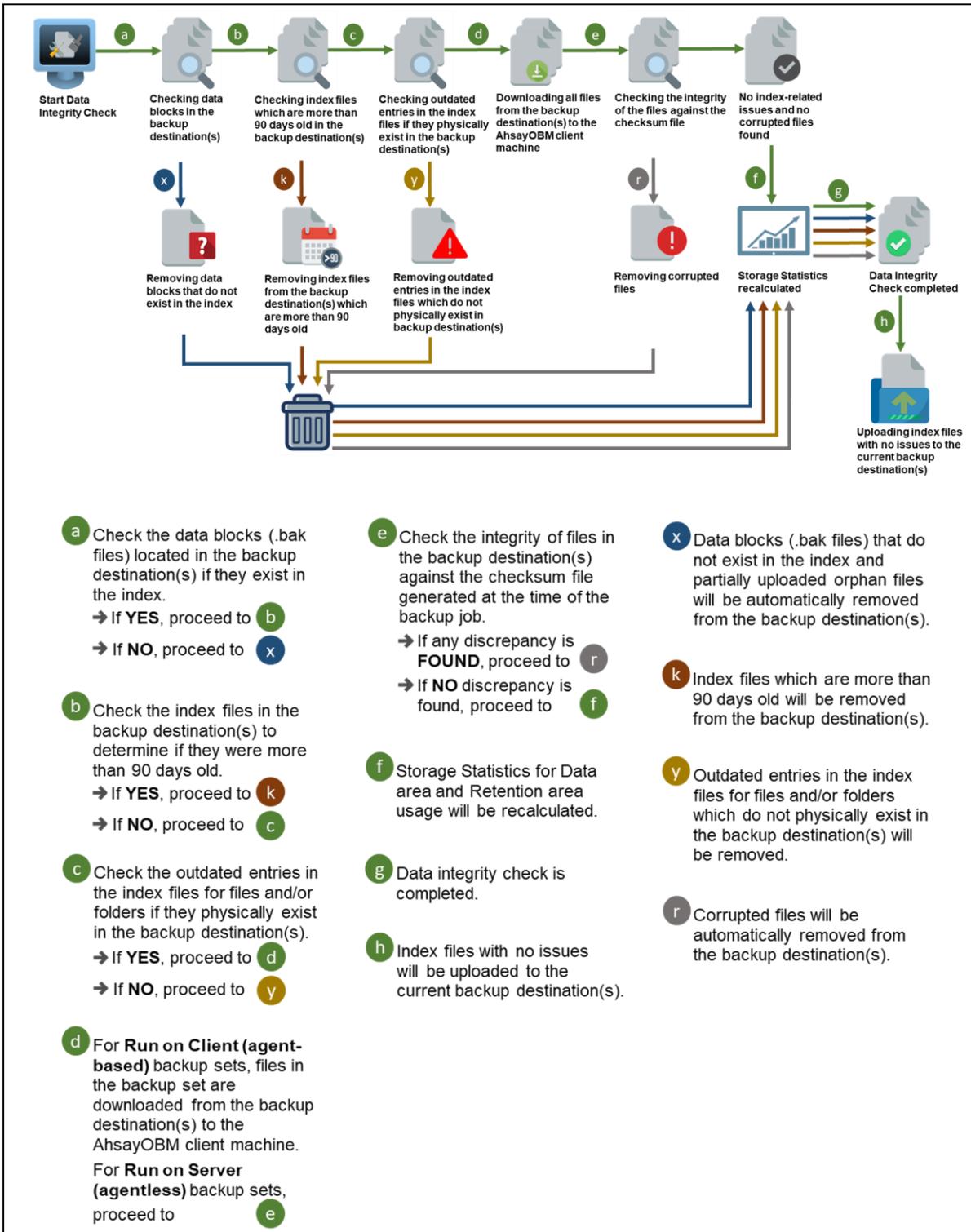
The following diagrams show the detailed process of the Data Integrity Check (DIC) in two (2) modes:

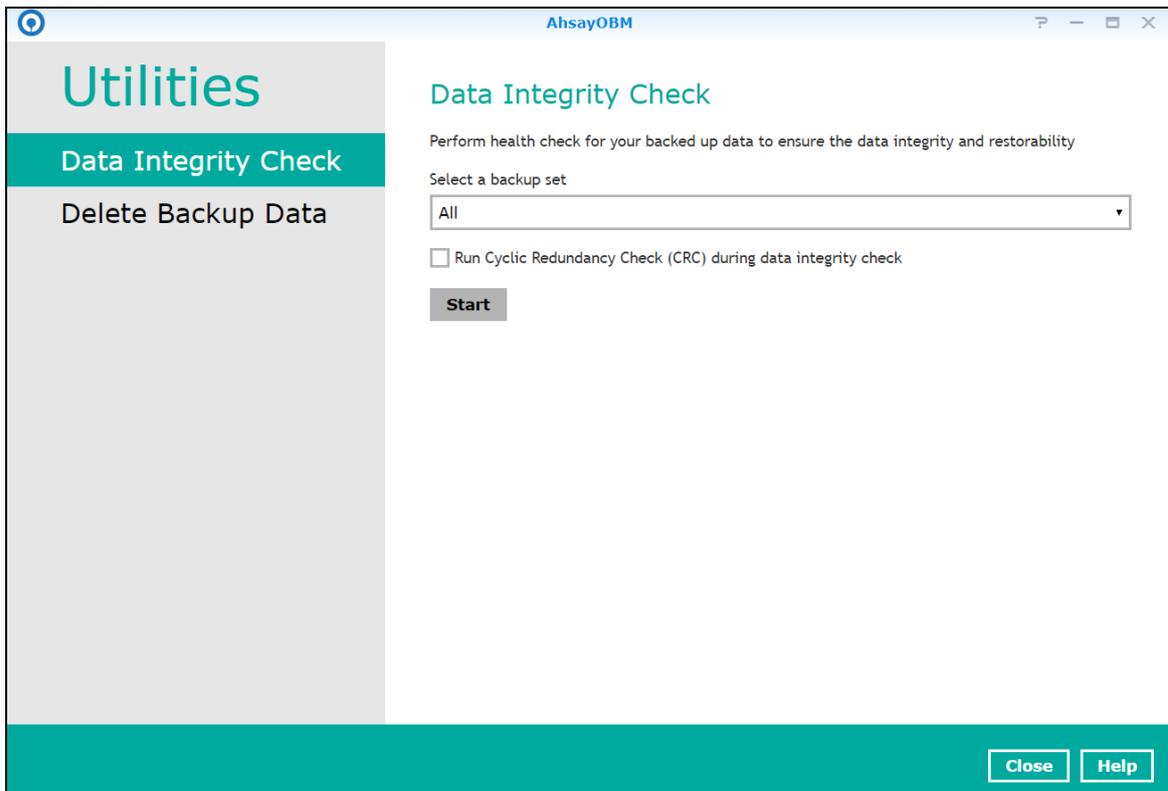
- **Option 1**
Disabled Run Cyclic Redundancy Check (CRC) - **(Default mode)**
- **Option 2**
Enabled Run Cyclic Redundancy Check (CRC)

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



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

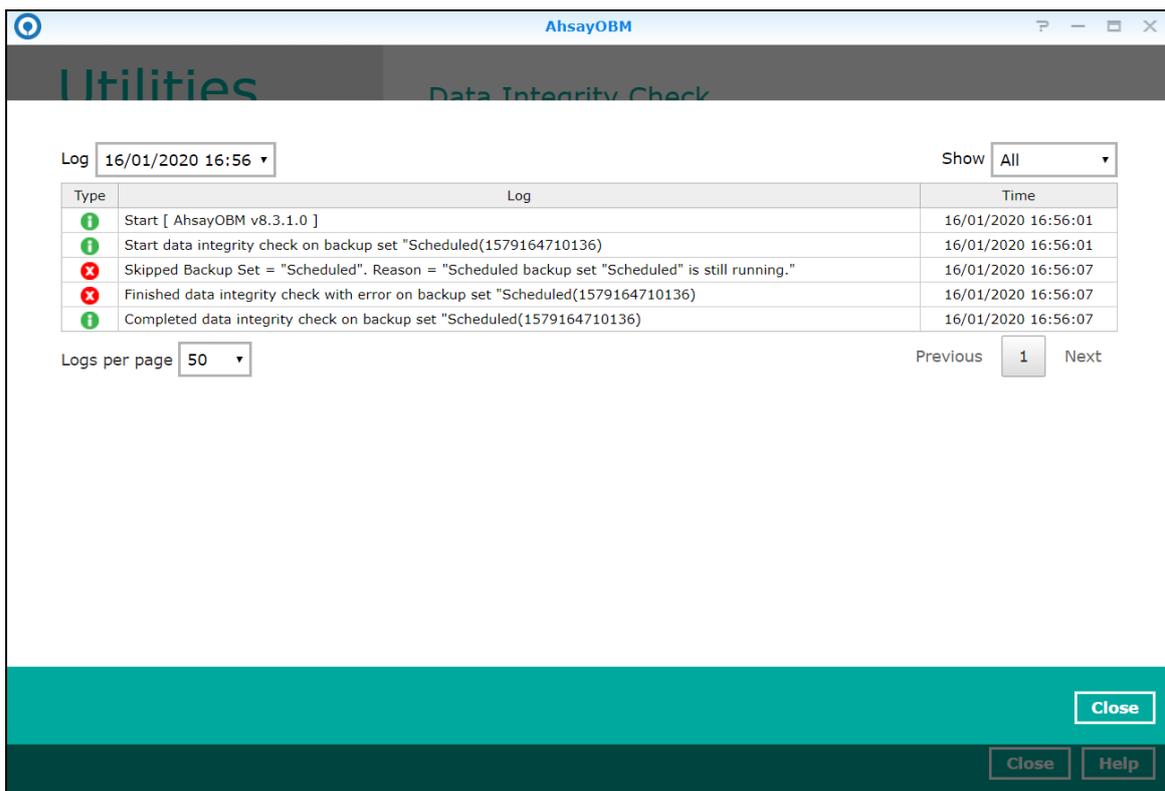
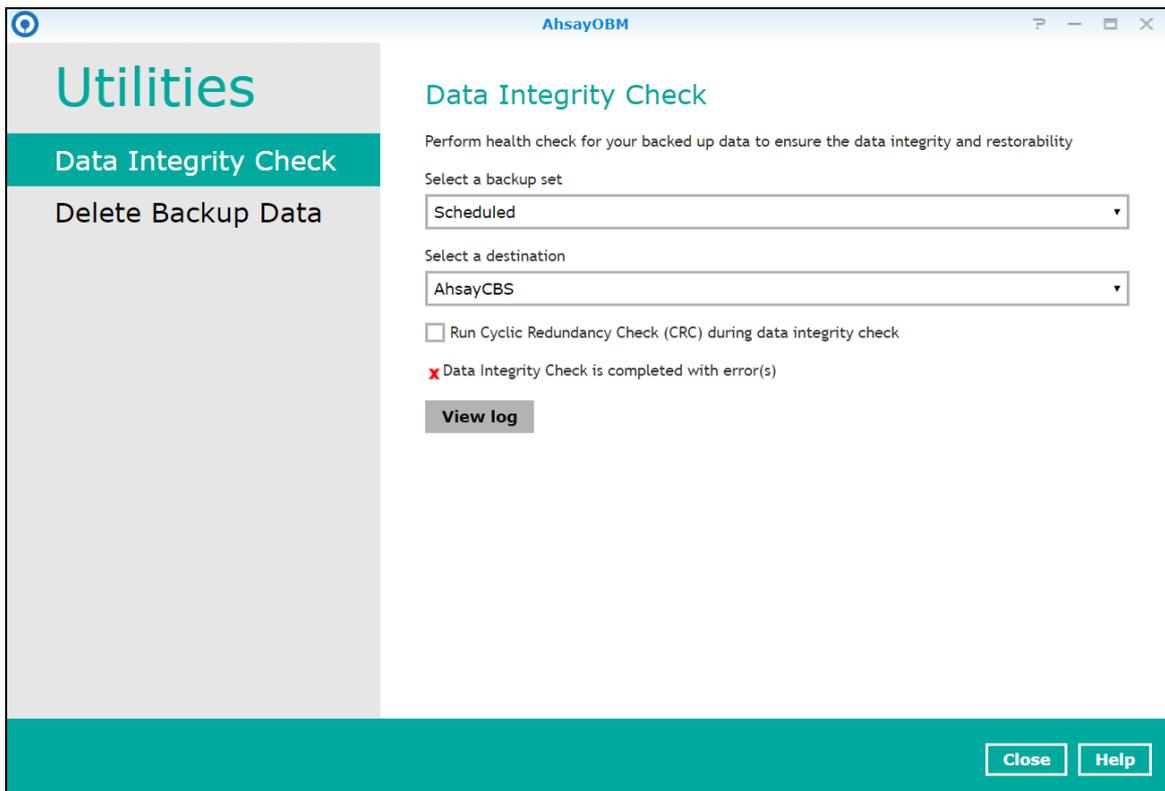




NOTES

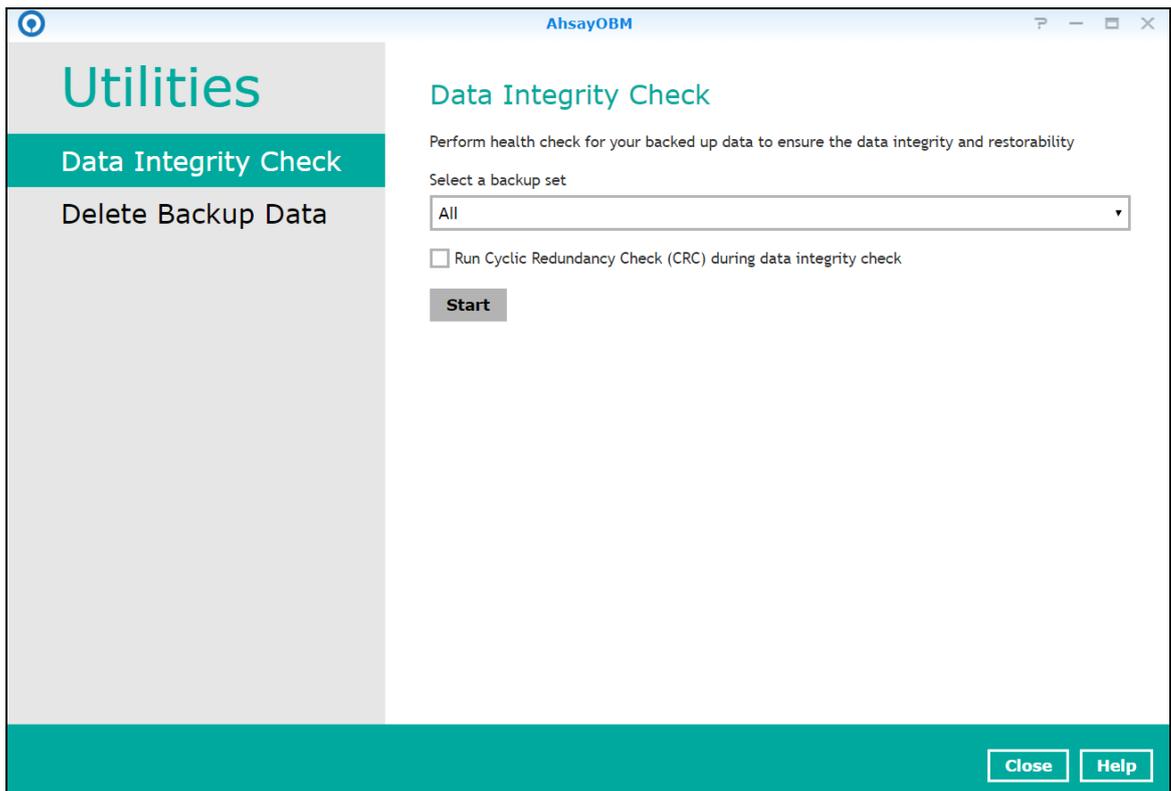
1. Data Integrity Check CANNOT fix or repair files that are already corrupted.
2. Data Integrity Check can only be started if there is NO active backup or restore job(s) running on the backup set selected for the DIC job. As the **backup**, **restore** and **data integrity check** are using the same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

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

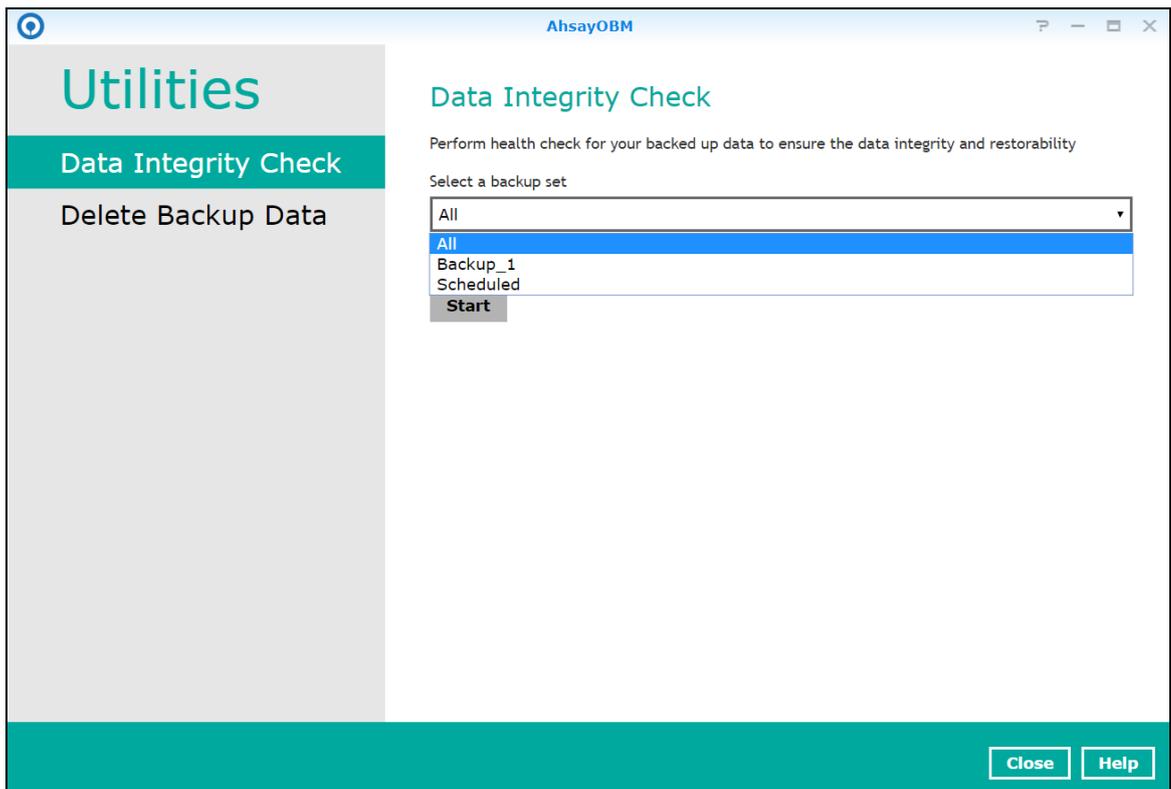


To perform a Data Integrity Check, follow the instructions below:

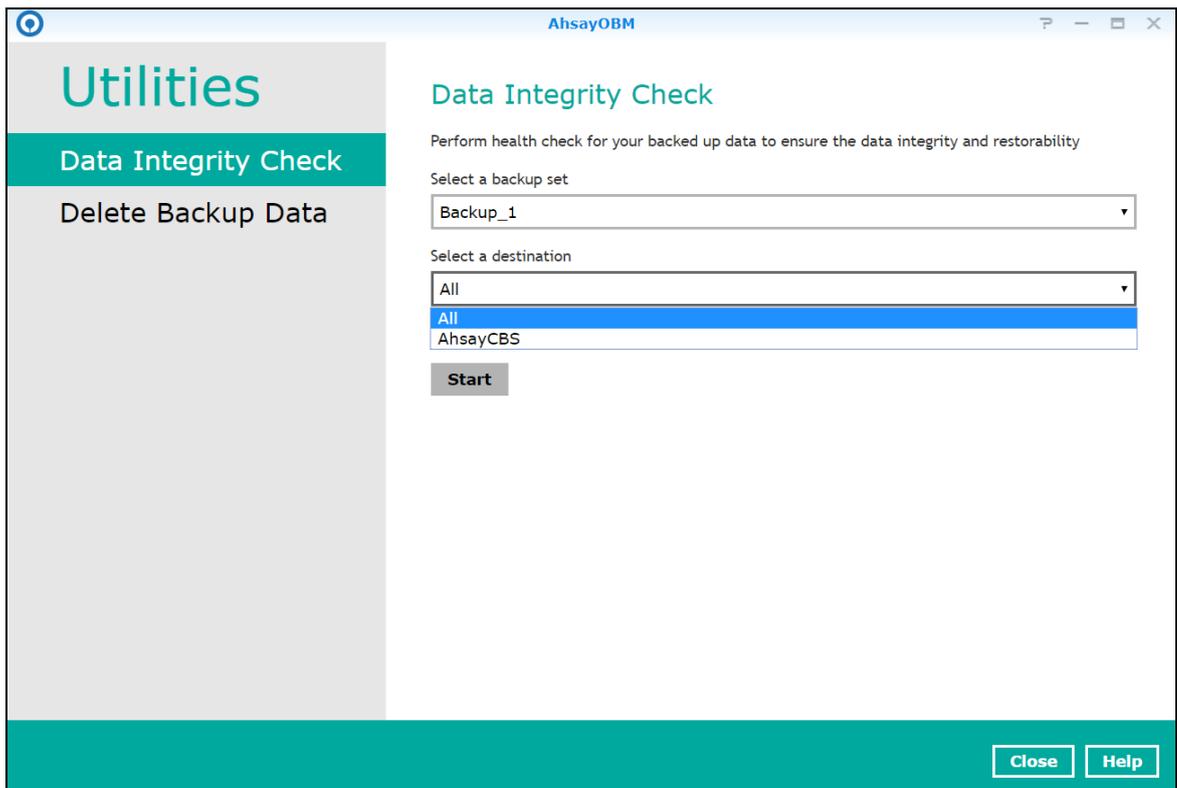
1. Go to the Data Integrity Check tab in the Utilities menu.



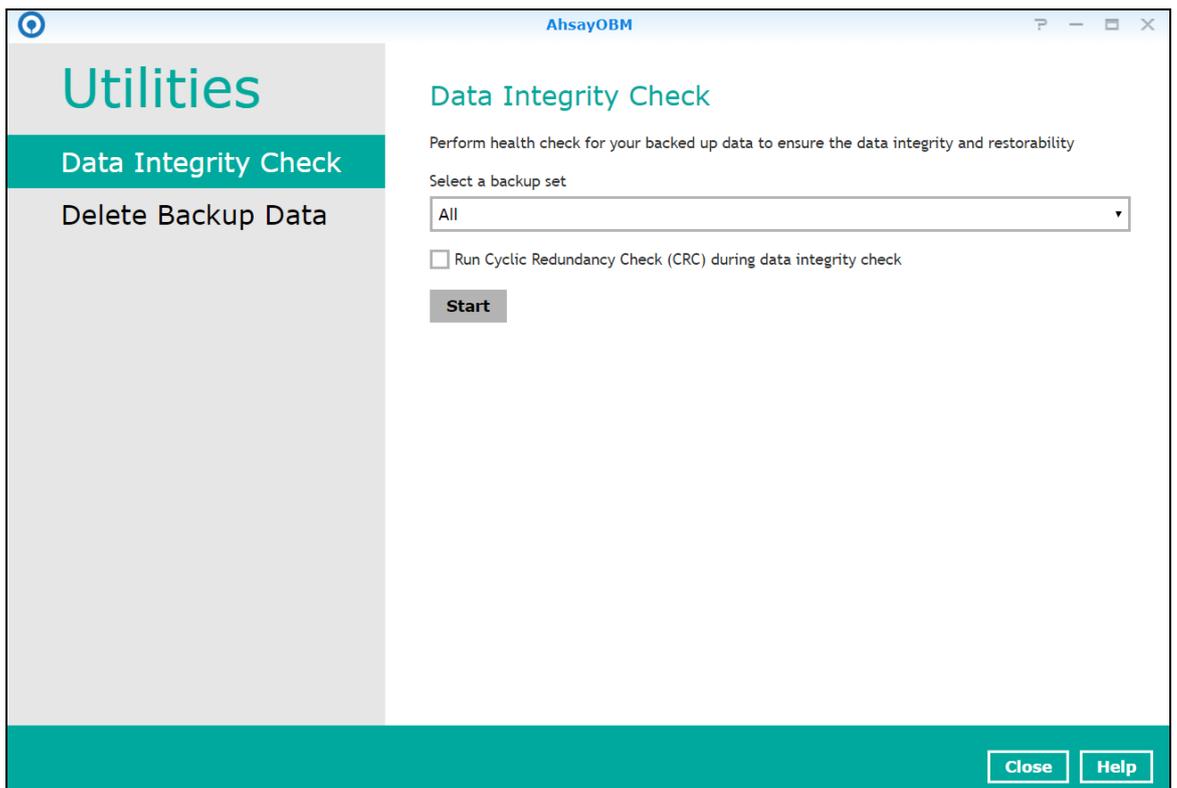
2. Click the drop-down button to select a backup set.



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



4. Unchecked Run Cyclic Redundancy Check (CRC) 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.

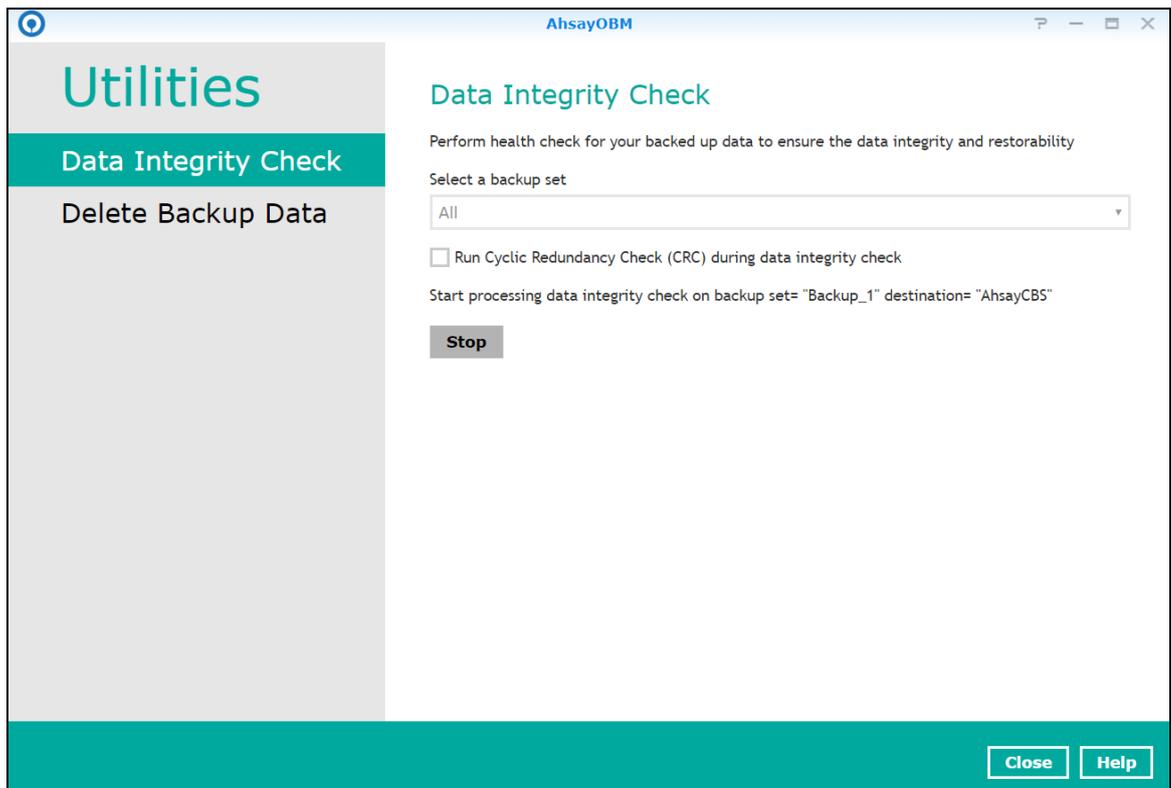
The time required to complete a data integrity check depends on the number of factors such as:

- 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

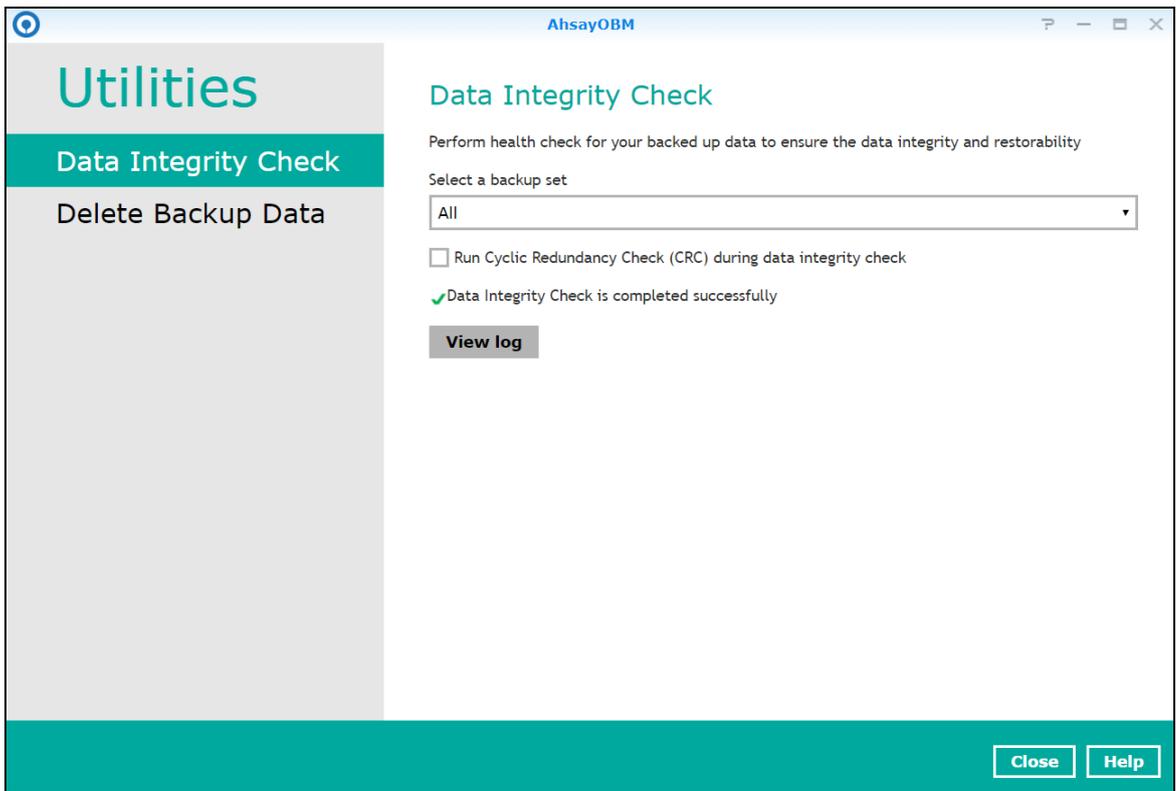
NOTE

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.

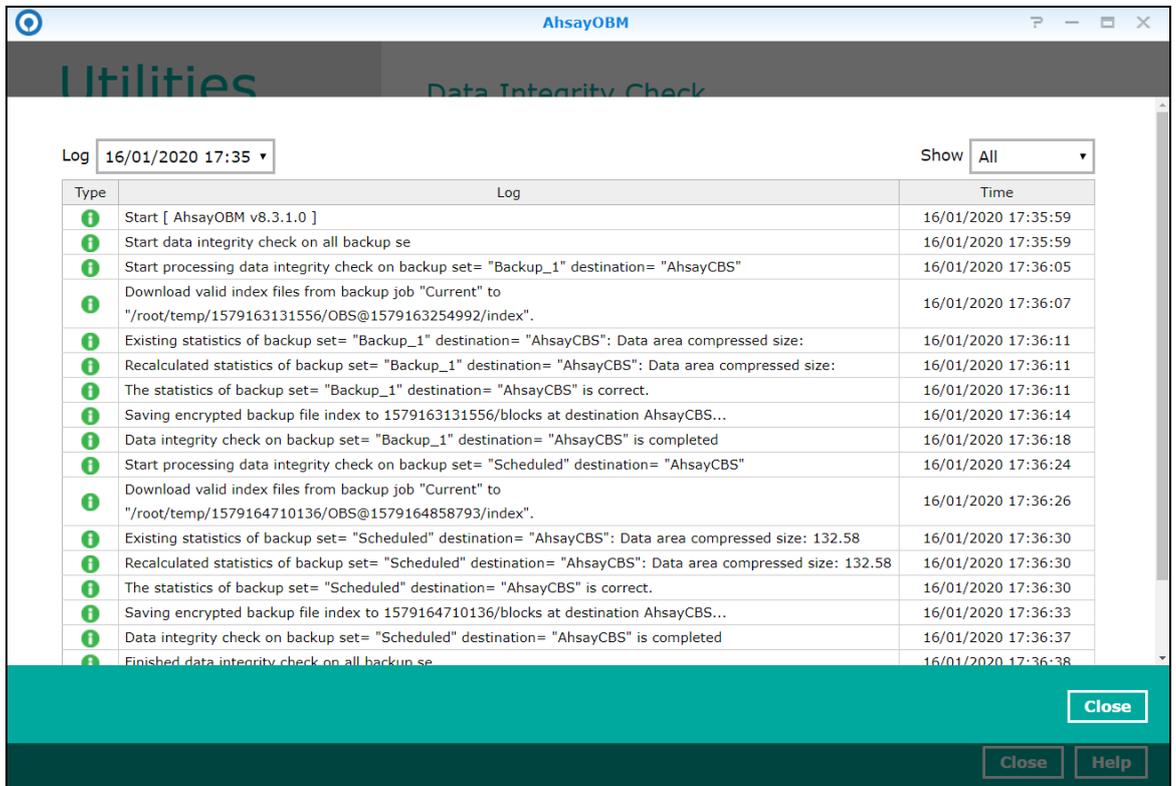
5. Click the [Start] button to begin the Data Integrity Check.
6. Data Integrity Check will start running on the selected backup set(s) and backup destination(s).



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

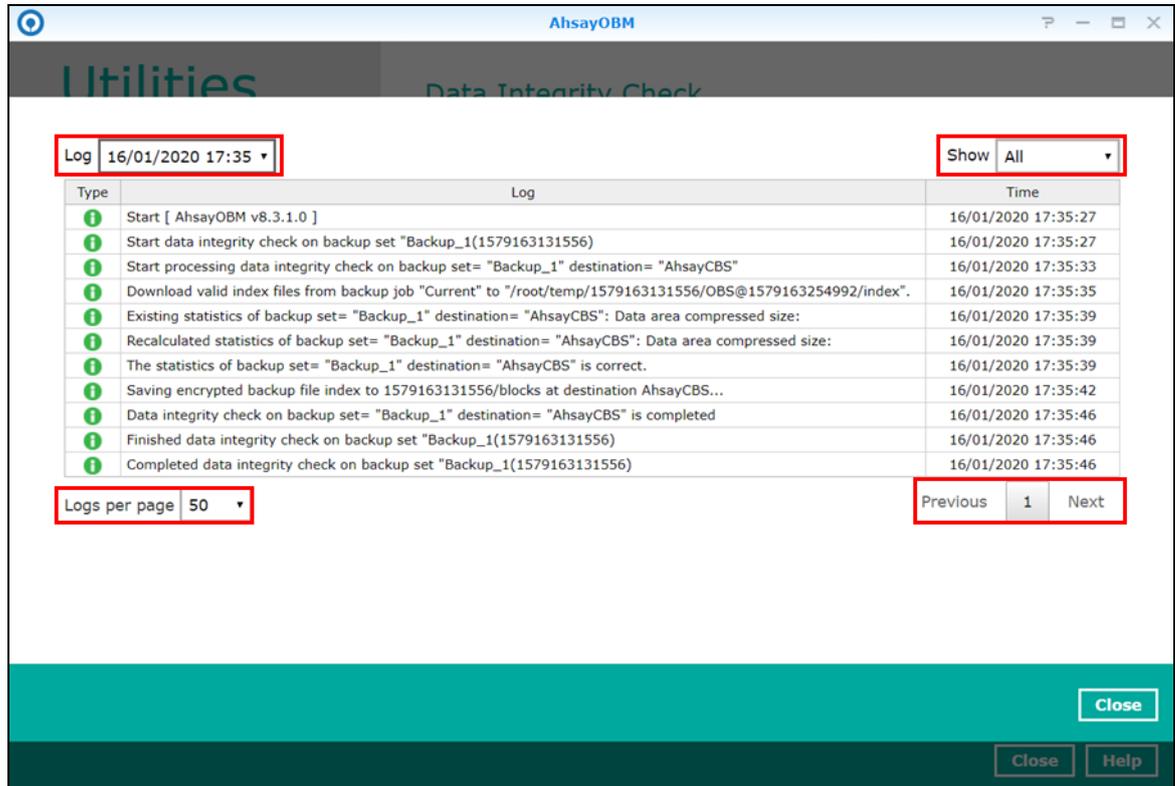


8. The detailed log of data integrity check process will be displayed.

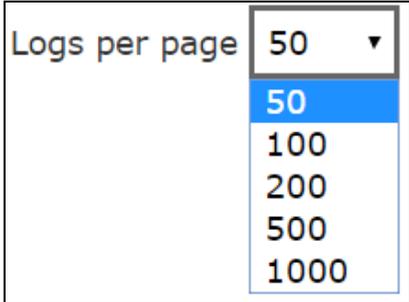


The following options can be used for further viewing of the detailed DIC log:

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



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

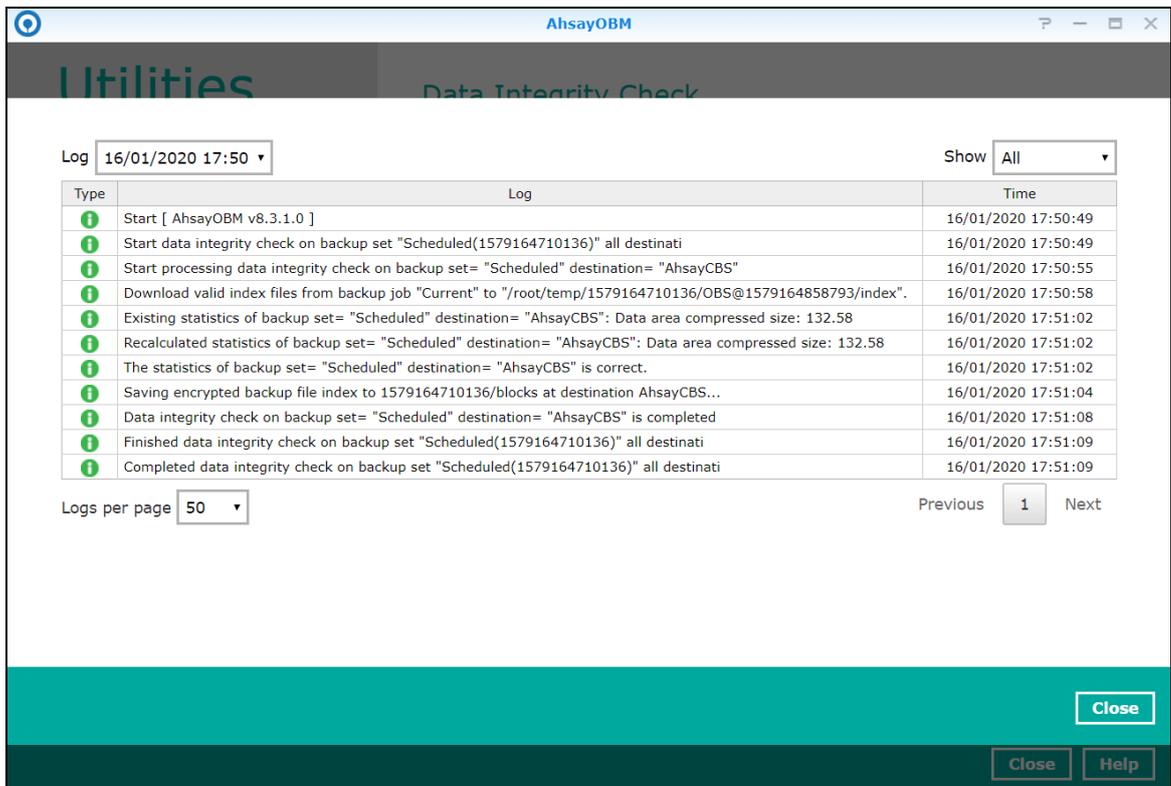
Logs per page		This option allows user to control the displayed number of logs per page.
Page		This option allows user to navigate the logs to the next page(s).

Data Integrity Check 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.



Log 16/01/2020 17:50 Show All

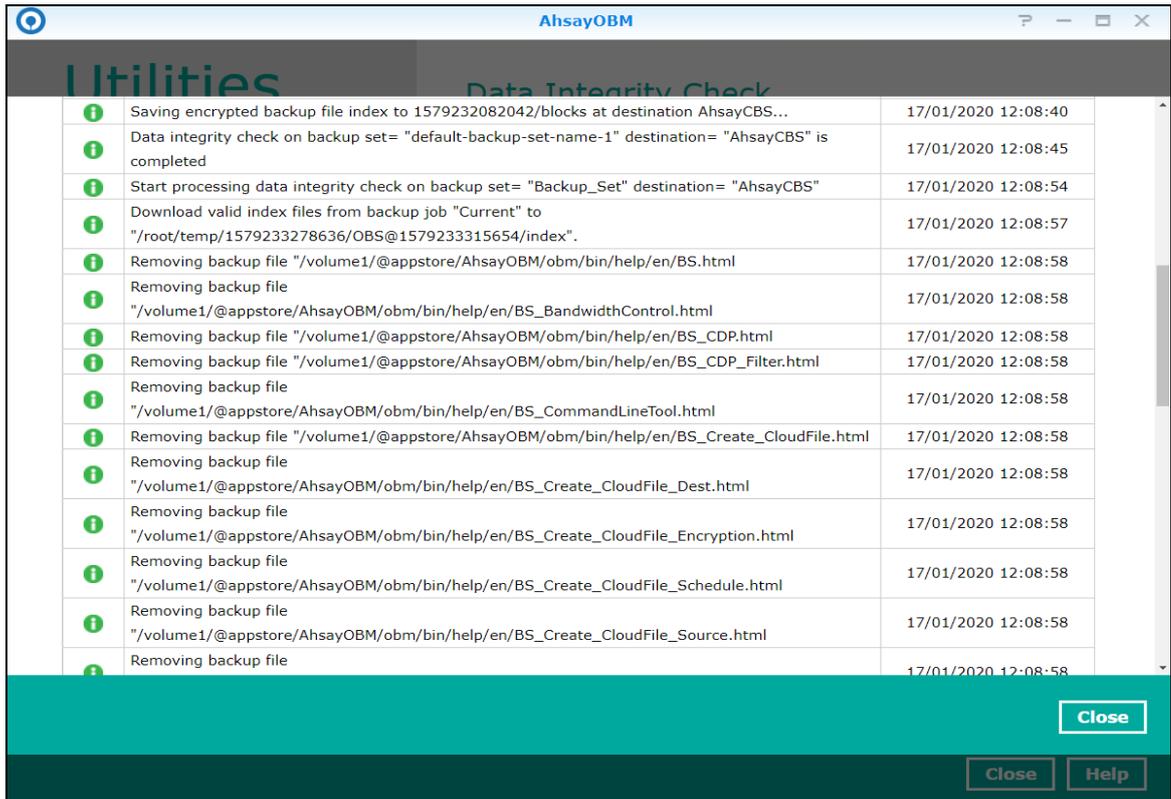
Type	Log	Time
i	Start [AhsayOBM v8.3.1.0]	16/01/2020 17:50:49
i	Start data integrity check on backup set "Scheduled(1579164710136)" all destinati	16/01/2020 17:50:49
i	Start processing data integrity check on backup set= "Scheduled" destination= "AhsayCBS"	16/01/2020 17:50:55
i	Download valid index files from backup job "Current" to "/root/temp/1579164710136/OBS@1579164858793/index".	16/01/2020 17:50:58
i	Existing statistics of backup set= "Scheduled" destination= "AhsayCBS": Data area compressed size: 132.58	16/01/2020 17:51:02
i	Recalculated statistics of backup set= "Scheduled" destination= "AhsayCBS": Data area compressed size: 132.58	16/01/2020 17:51:02
i	The statistics of backup set= "Scheduled" destination= "AhsayCBS" is correct.	16/01/2020 17:51:02
i	Saving encrypted backup file index to 1579164710136/blocks at destination AhsayCBS...	16/01/2020 17:51:04
i	Data integrity check on backup set= "Scheduled" destination= "AhsayCBS" is completed	16/01/2020 17:51:08
i	Finished data integrity check on backup set "Scheduled(1579164710136)" all destinati	16/01/2020 17:51:09
i	Completed data integrity check on backup set "Scheduled(1579164710136)" all destinati	16/01/2020 17:51:09

Logs per page 50 Previous 1 Next

Close

Close Help

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:

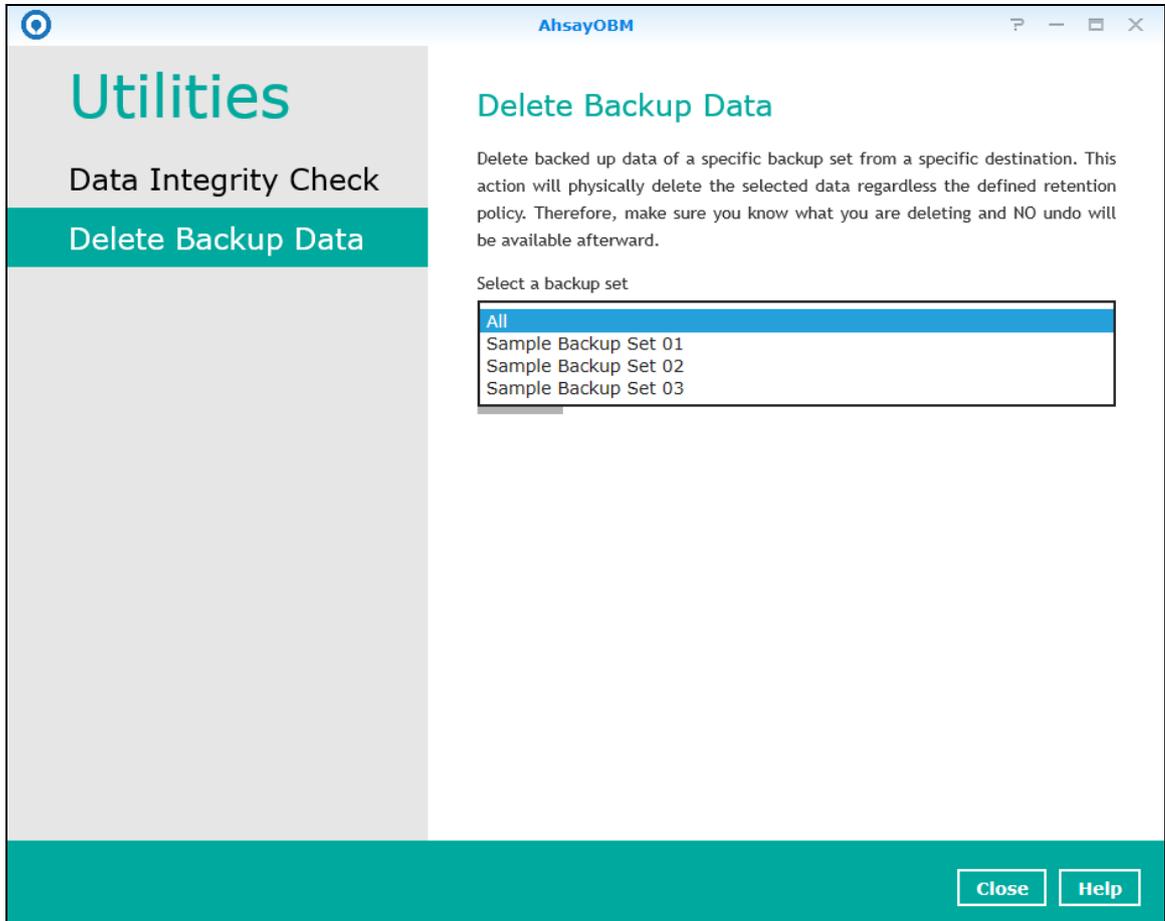
/volume_id/@appstore/product_name/.obm/system/IntegrityCheck

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.

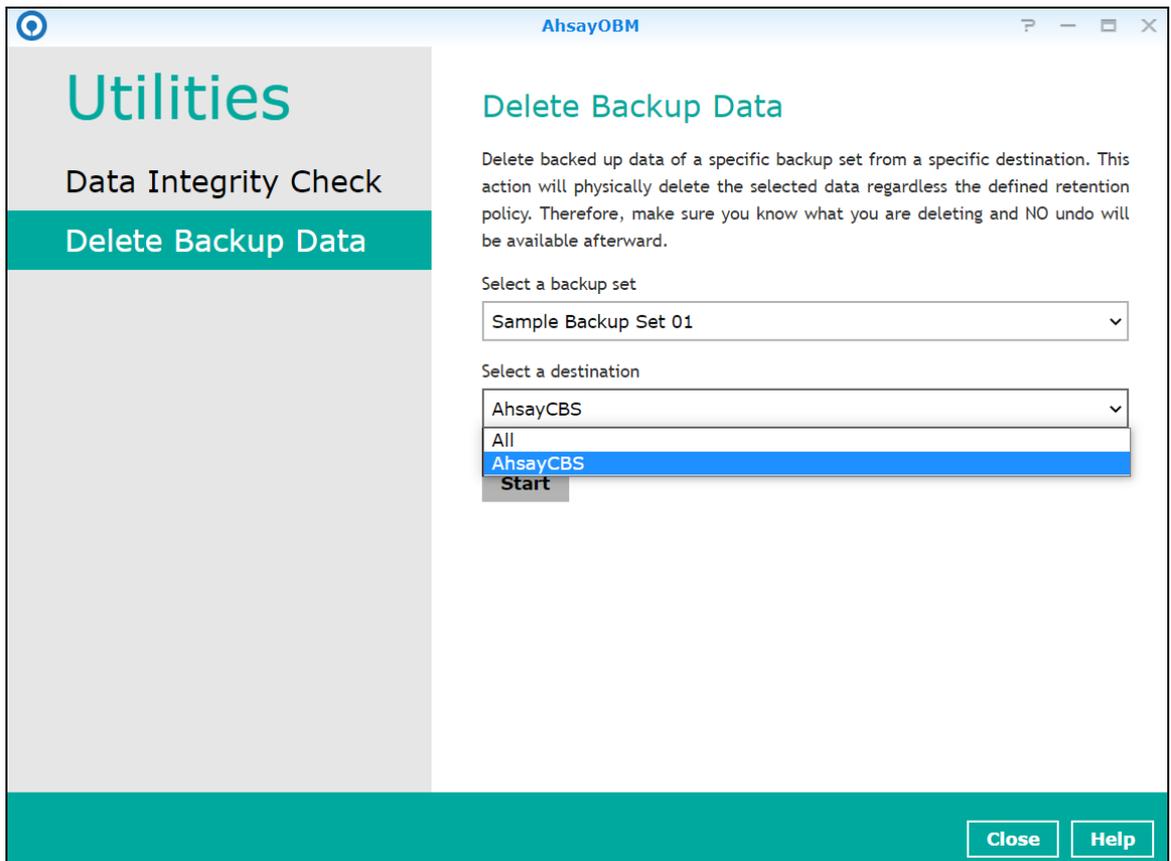
To perform deletion of backup data, follow the instructions below:

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

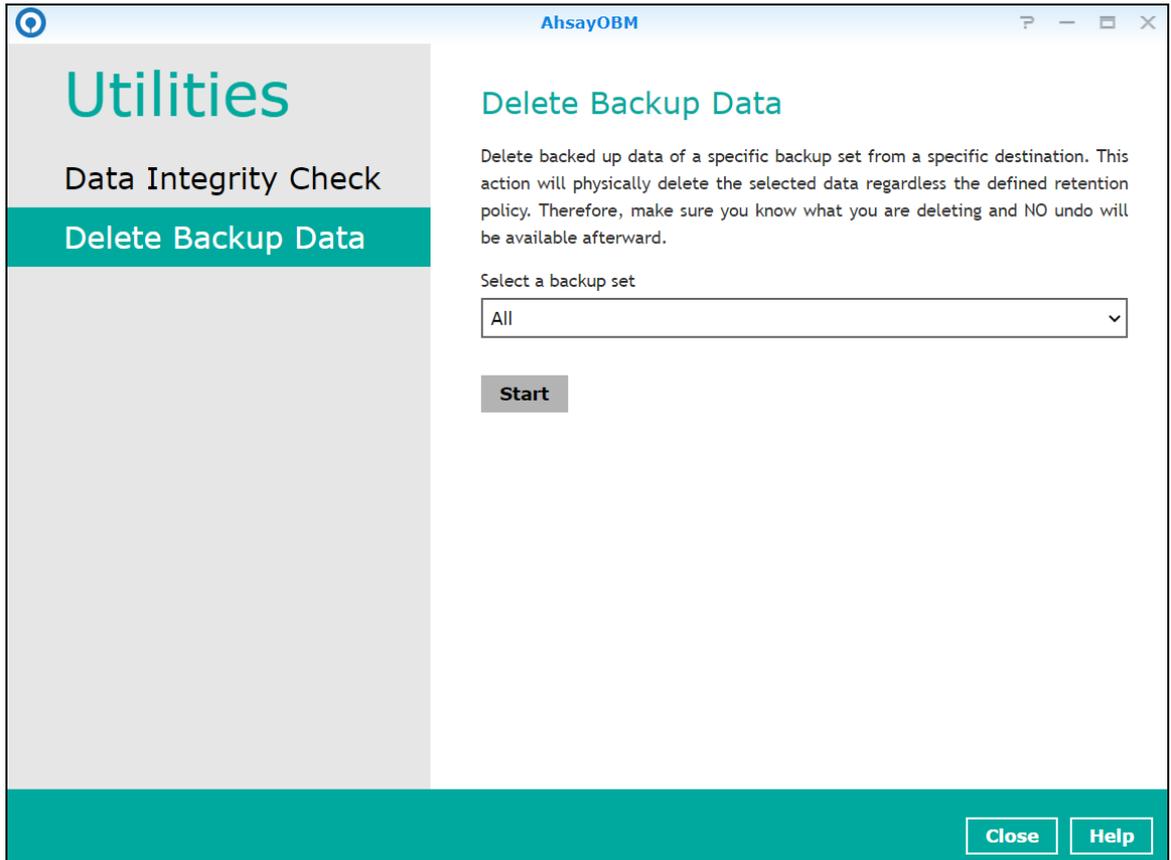


NOTE: This will only delete the backed up files in a backup set(s) and destination(s), but the backup set and destination will remain.

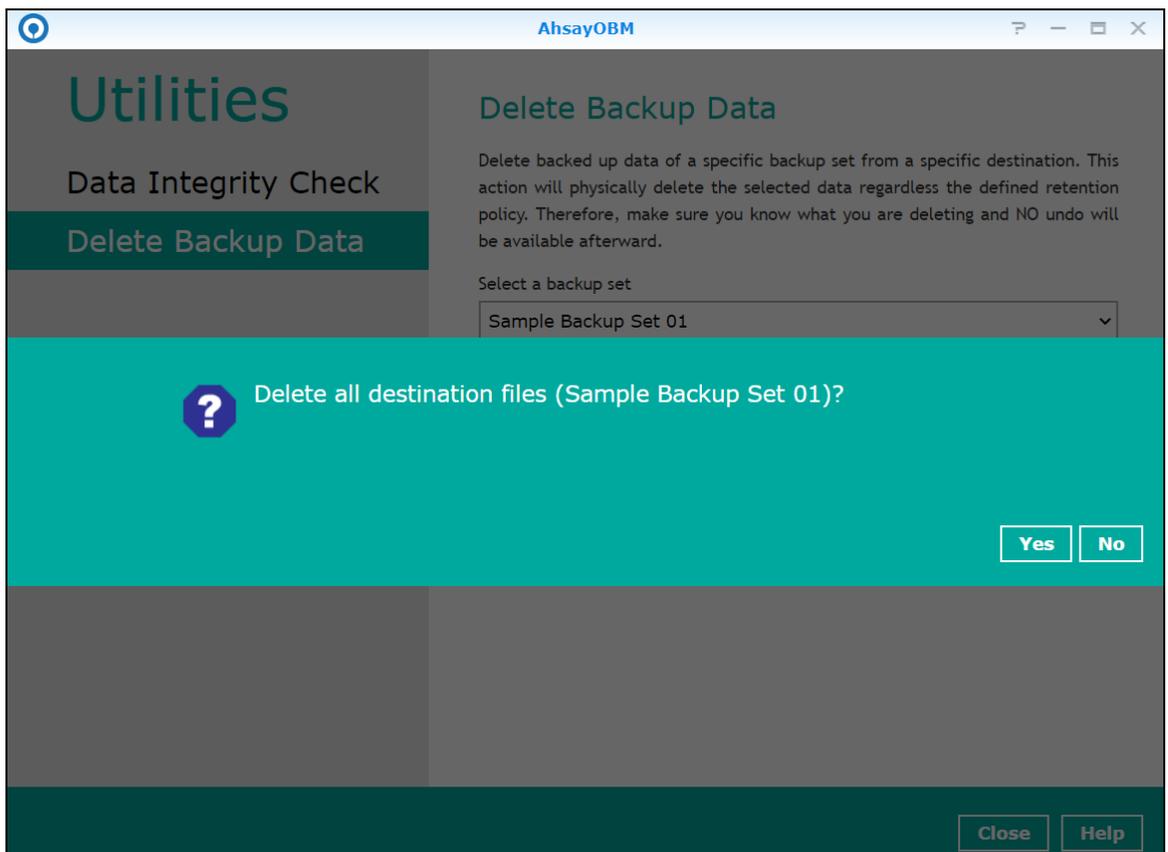
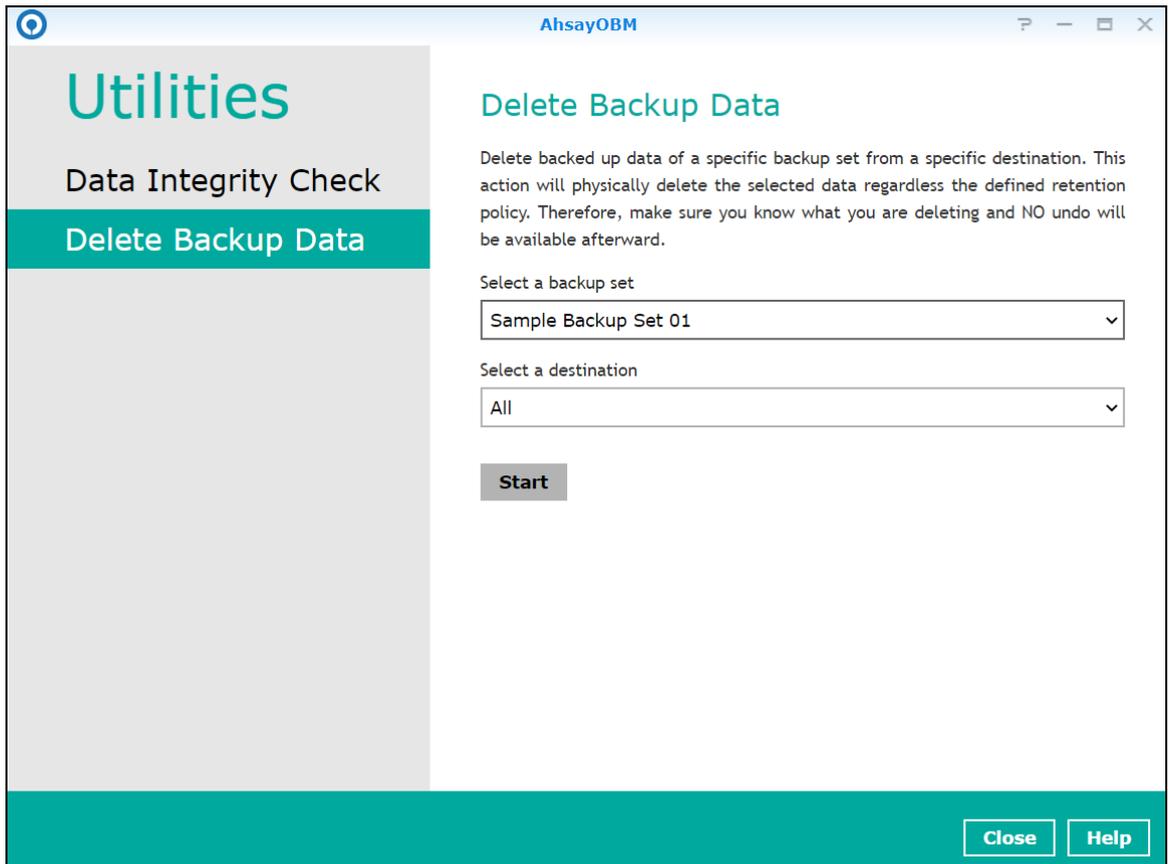
If you select a specific backup set, then you will also have to select a specific destination or all destinations.



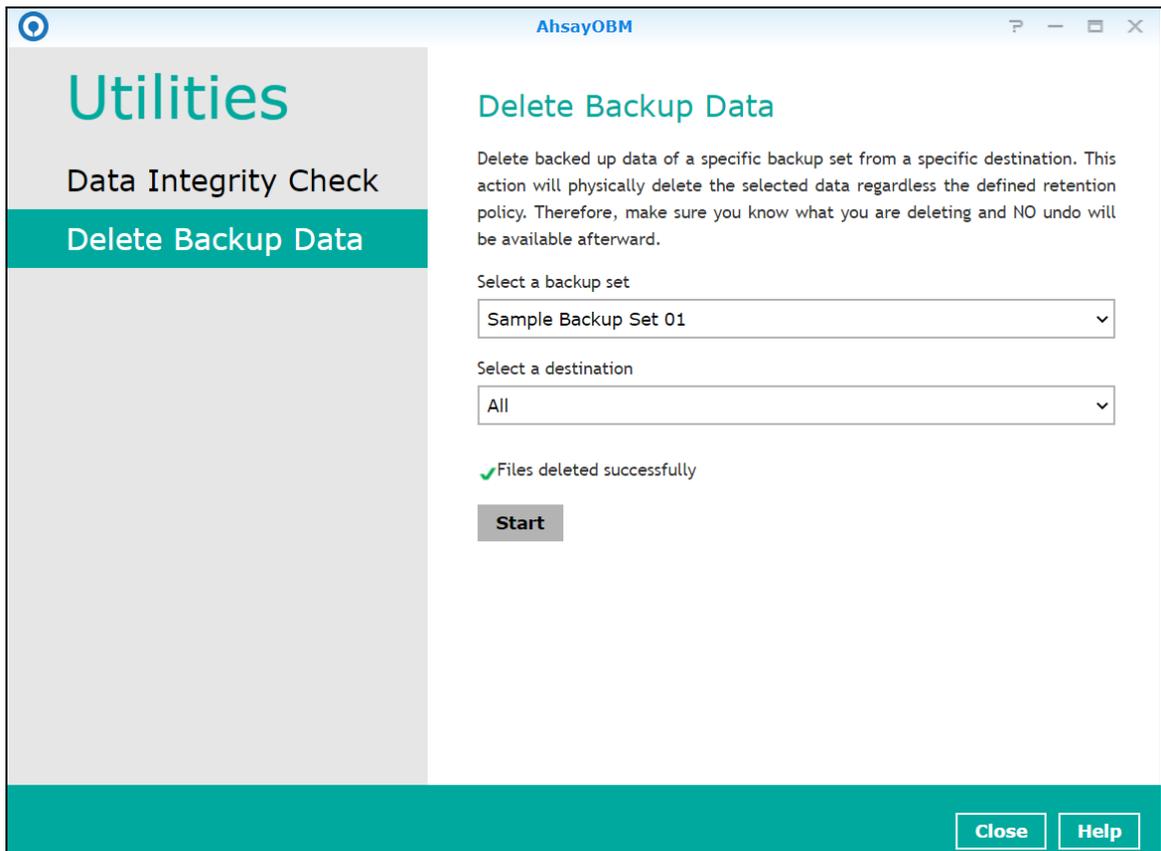
If you select **All** backup sets, then there is no need to select a destination.



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).



- Files are successfully deleted.



7 Create a Backup Set

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



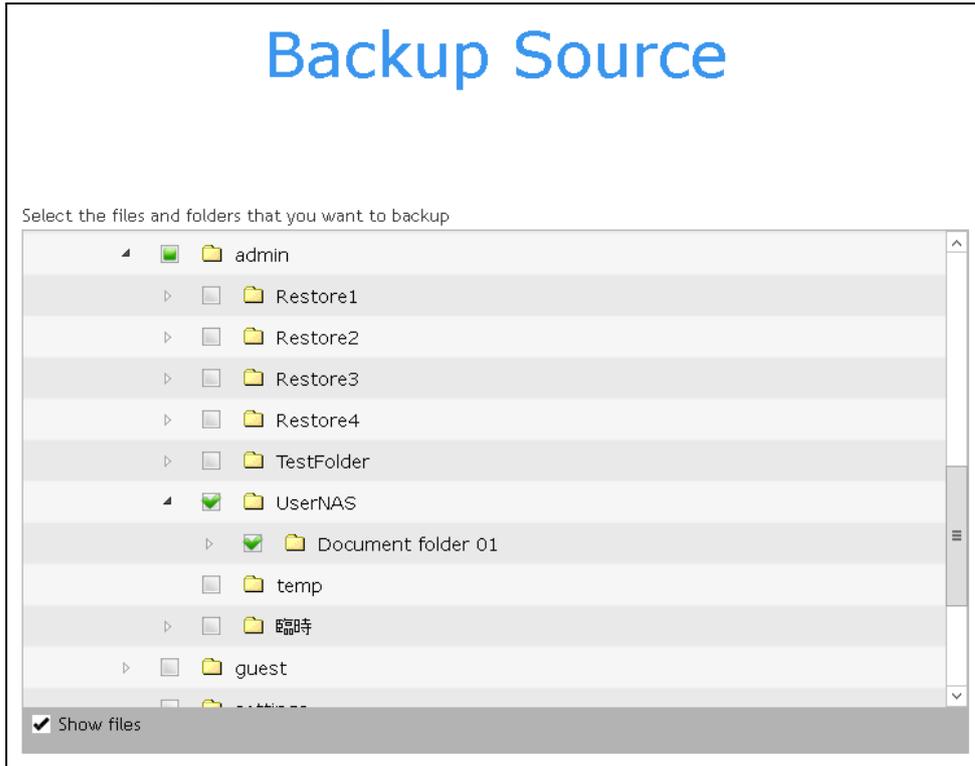
2. Create a backup set by clicking "+ Add new backup set".



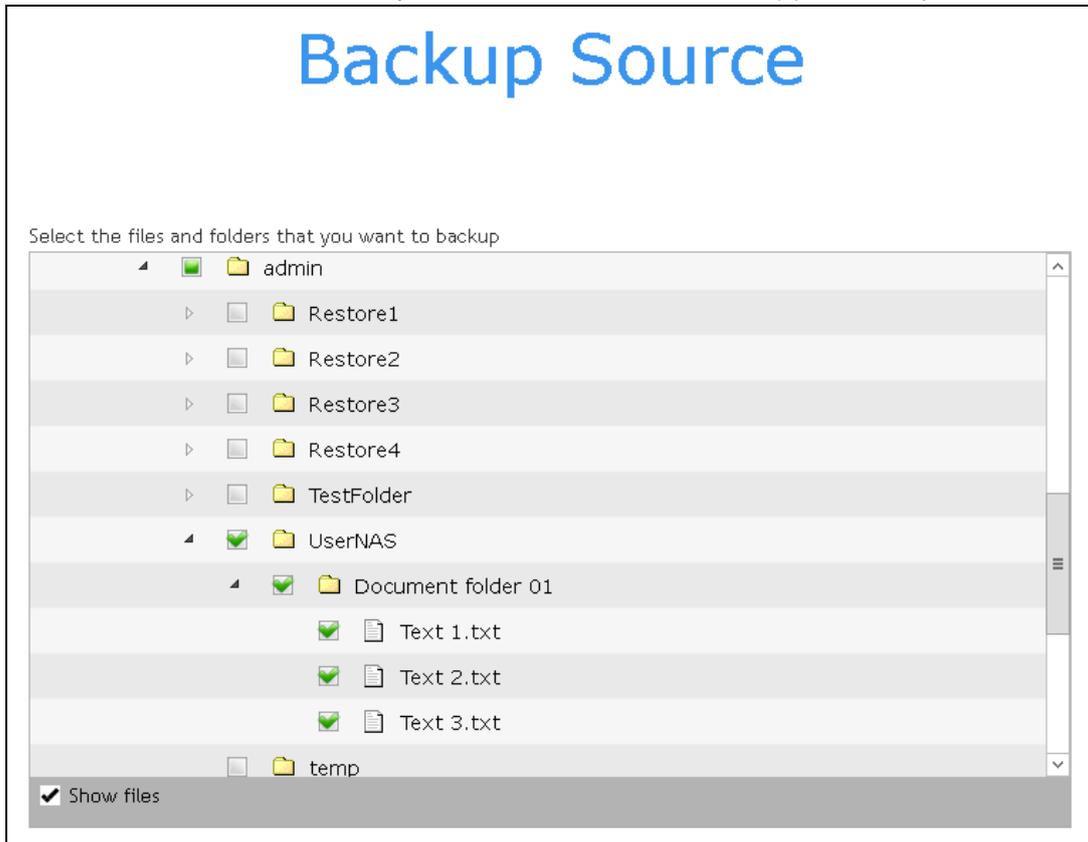
3. When the Create Backup Set window appears, name your new backup set, then click **Next** to proceed.



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



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

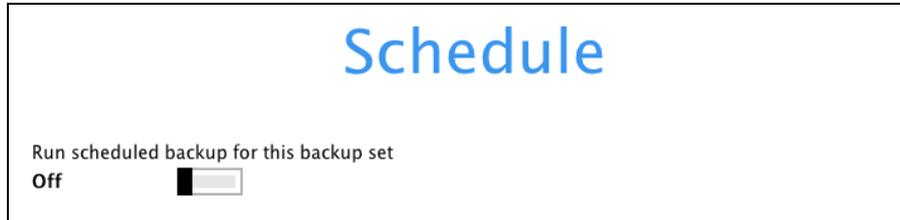


Note: AhsayOBM can only back up files or folders displayed under the File Station on the DiskStation Manager.

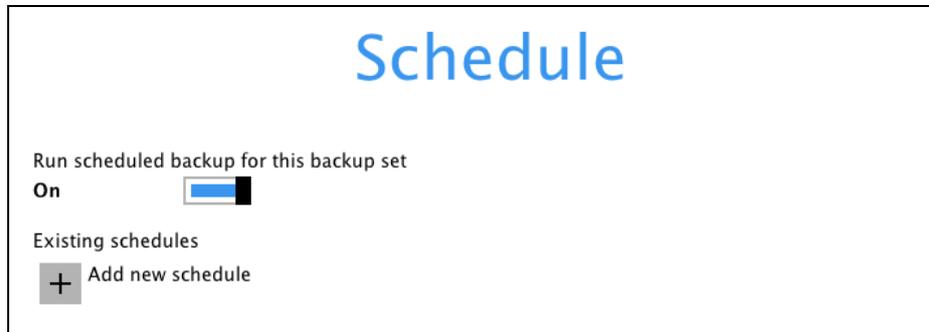
For more details, refer to the following Wiki article:

http://wiki.ahsay.com/doku.php?id=public:8019_faq:faq_about_synologyobm

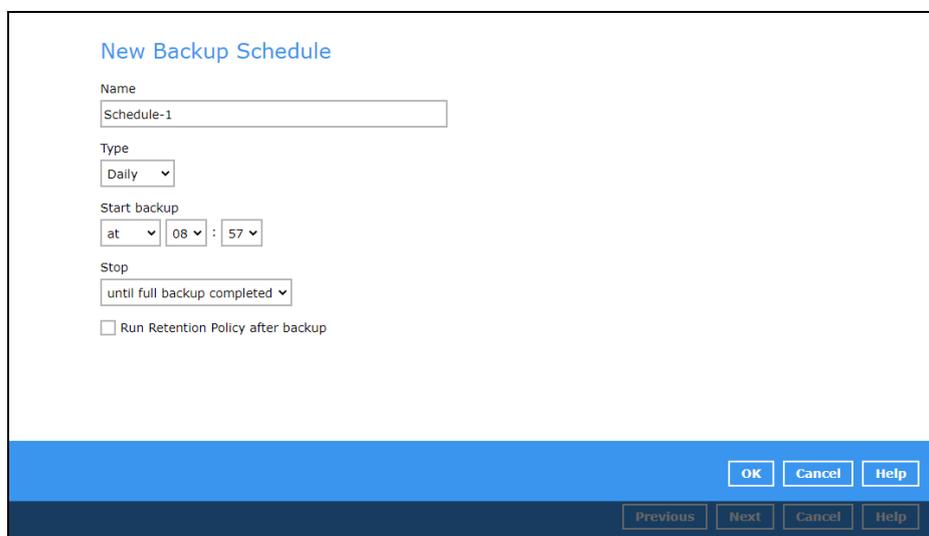
- In the Backup Source window, click **Next** to proceed.
- When the Schedule window appears, you can configure a backup schedule to automatically run a backup job at your specified time interval.
 - In the Schedule window, the Run scheduled backup for this backup set is **Off** by default.
You can leave 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.

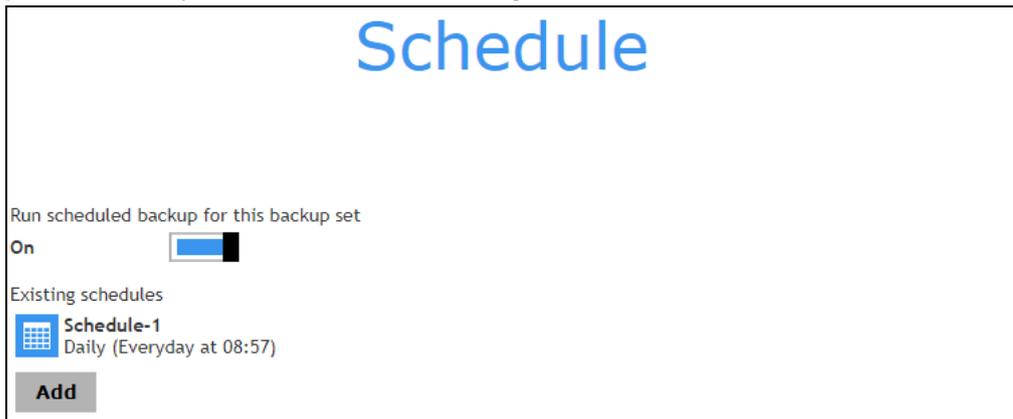


When the **New Backup Schedule** window appears, specify your backup schedule. Then, click **OK** to save your changes and close the New Backup Schedule window.



Note: For details about the options from the dropdown menus, please refer to [Configure Backup Schedule for Automated Backup](#).

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



9. The Destination window will appear.

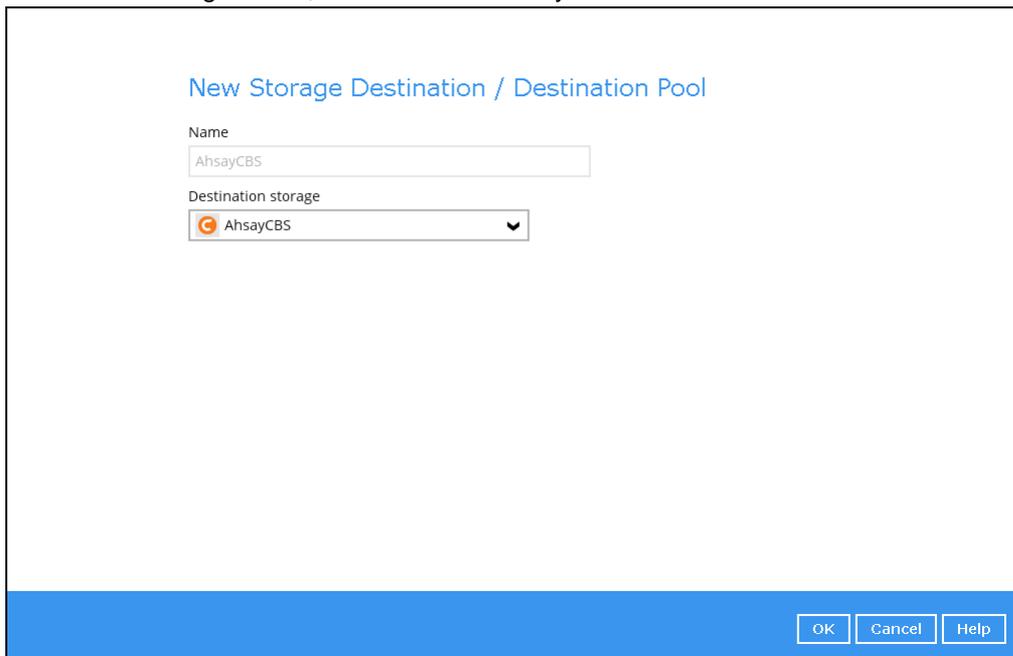


Select the appropriate option from the **Backup mode** drop down menu.

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

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

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



New Storage Destination / Destination Pool

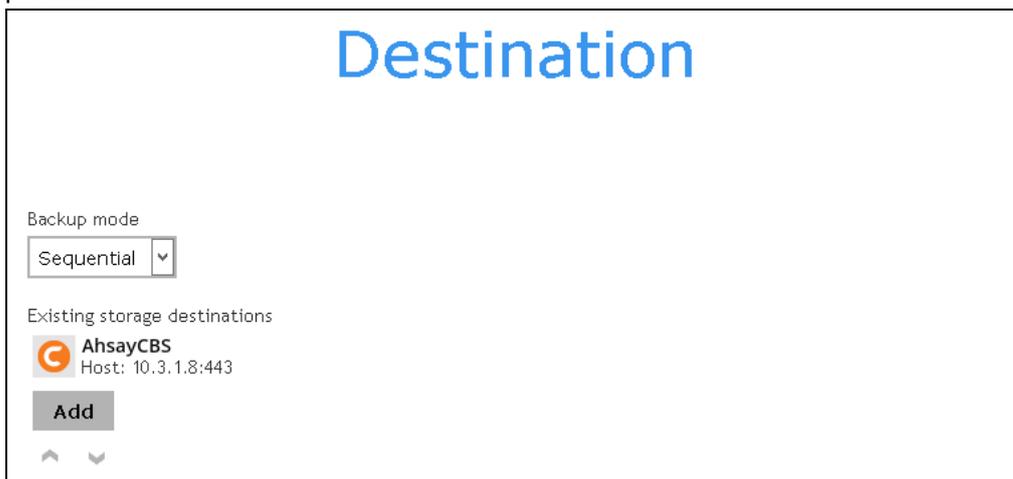
Name
AhsayCBS

Destination storage
AhsayCBS

OK Cancel Help

Note: For more details on configuration of cloud storage as backup destination, refer to [Appendix A](#) in this guide.

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



Destination

Backup mode
Sequential

Existing storage destinations
AhsayCBS
Host: 10.3.1.8:443

Add

^ v

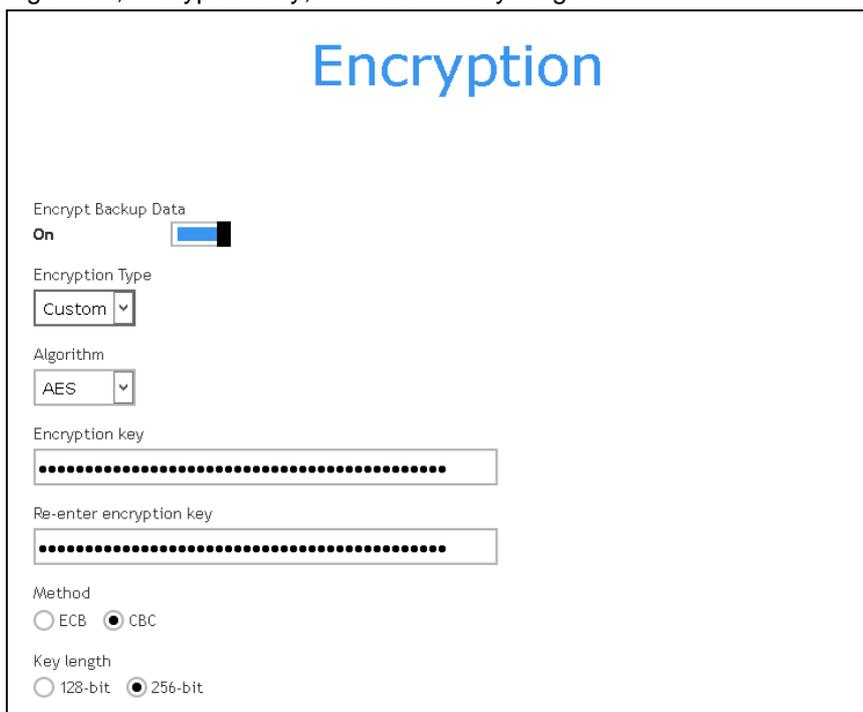
12. In the Encryption window, the default **Encrypt Backup Data** option is enabled with an encryption key preset by the system which provides the most secure protection.



The screenshot shows the 'Encryption' window. At the top, the word 'Encryption' is displayed in a large blue font. Below it, the 'Encrypt Backup Data' option is set to 'On', indicated by a blue slider. Underneath, the 'Encryption Type' dropdown menu is open, showing four options: 'Default' (selected), 'Default', 'User password', and 'Custom'.

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

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



The screenshot shows the 'Encryption' window with 'Encrypt Backup Data' set to 'On'. The 'Encryption Type' dropdown is set to 'Custom'. Below it, the 'Algorithm' dropdown is set to 'AES'. There are two input fields for the 'Encryption key', both filled with dots. At the bottom, the 'Method' section has radio buttons for 'ECB' and 'CBC', with 'CBC' selected. The 'Key length' section has radio buttons for '128-bit' and '256-bit', with '256-bit' selected.

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

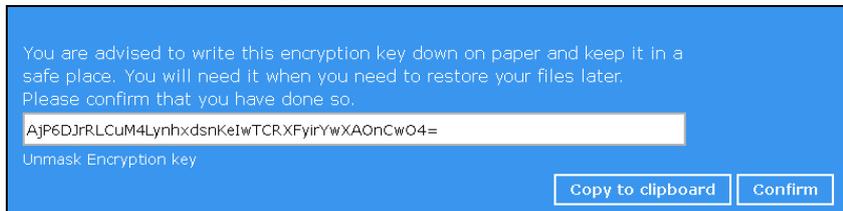
Click **Save** when you are done with the settings.

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



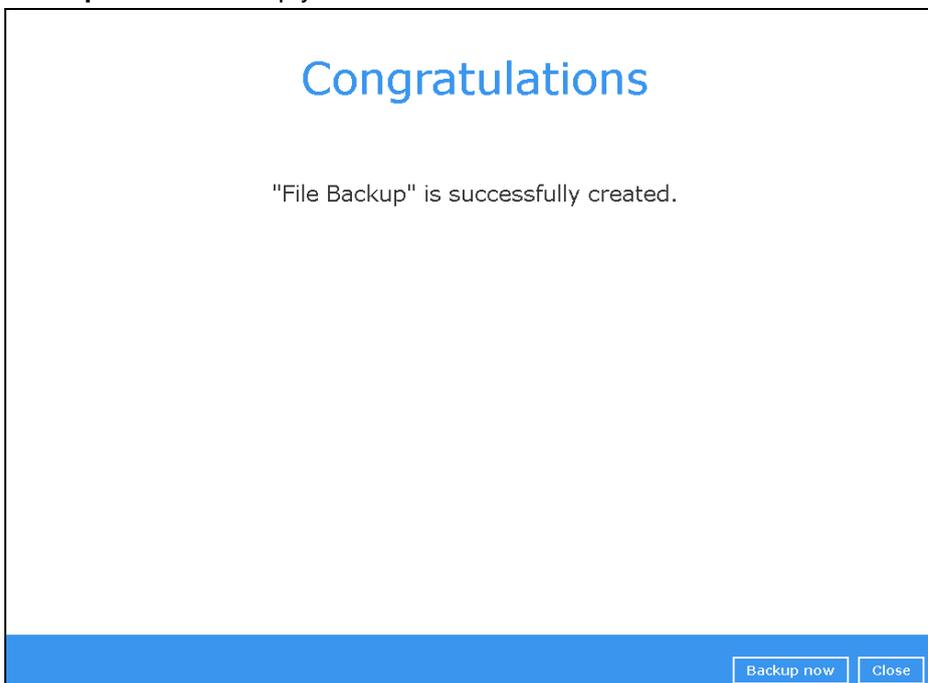
The pop-up window has the following three options to choose from:

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



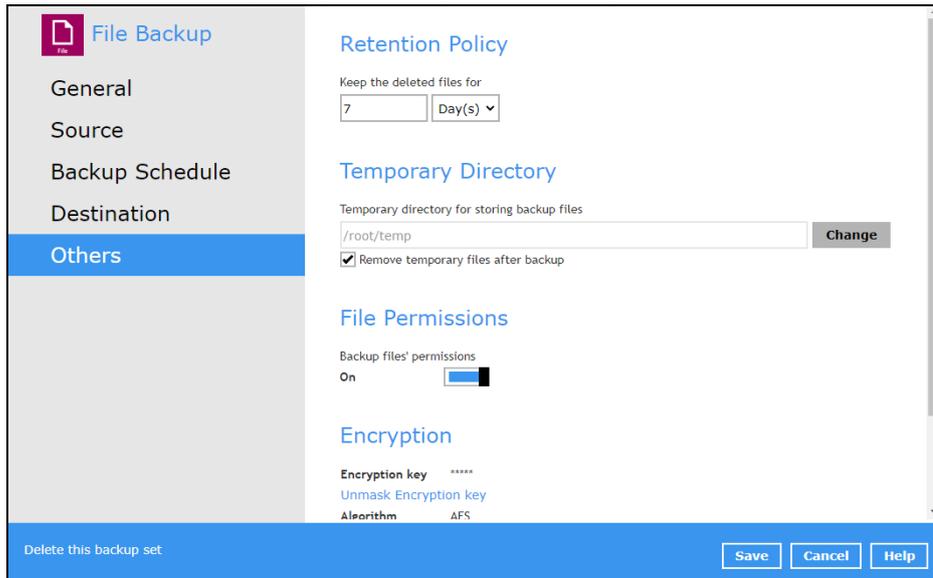
- **Copy to clipboard** – Click to copy the encryption key, then you can paste it in another location of your choice.
- **Confirm** – Click to exit this pop-up window and proceed to the next step.

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.

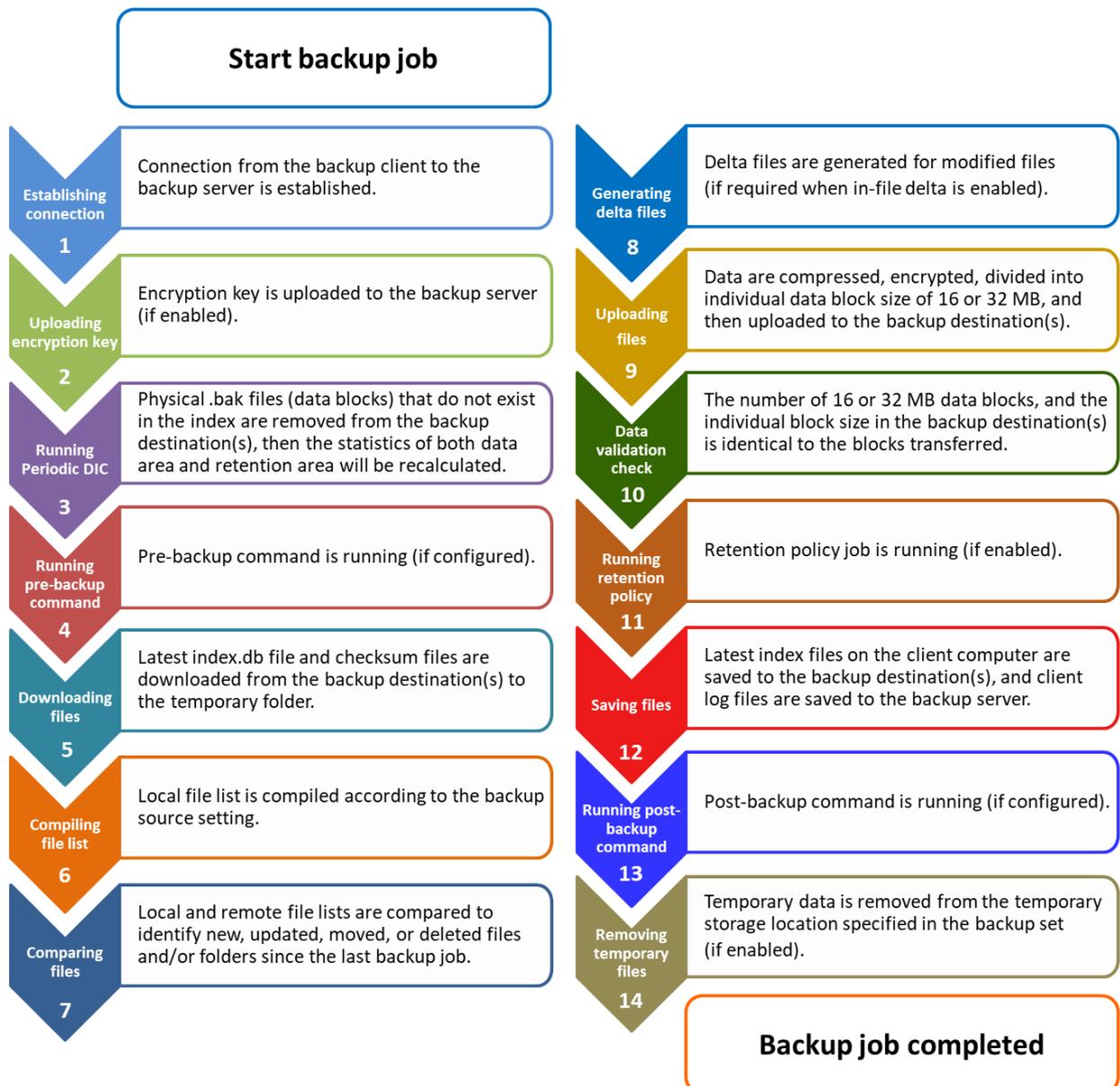
Go to **Others > Temporary Directory**. Click **Change** to browse for another location.



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, 5, 10 and 12, please refer to the following chapters.

- [Periodic Data Integrity Check \(PDIC\) Process \(Step 3\)](#)
- Backup Set Index Handling Process
 - [Start Backup Job \(Step 5\)](#)
 - [Completed Backup Job \(Step 12\)](#)
- [Data Validation Check Process \(Step 10\)](#)



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:

$PDIC\ schedule = \%BackupSetID\% \bmod 5$ or $\%BackupSetID\% \bmod 5$

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: $1594627447932 \bmod 5 = 2$

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

In this example:

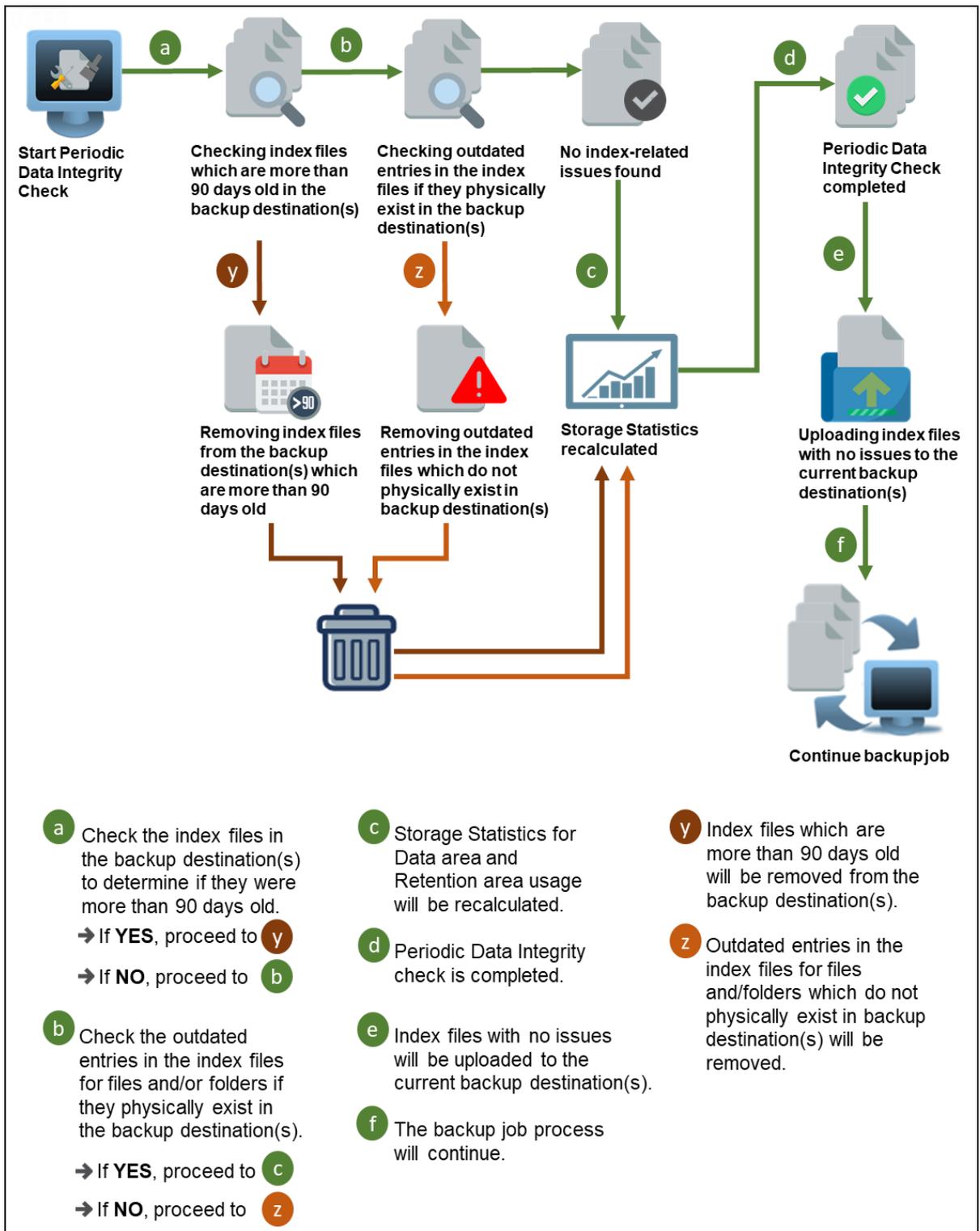
- the PDIC will run on the first backup job that falls on Wednesday; or
- if there is no active backup job(s) running from Monday to Friday, then the PDIC will run on the next available backup job.

NOTE

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

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

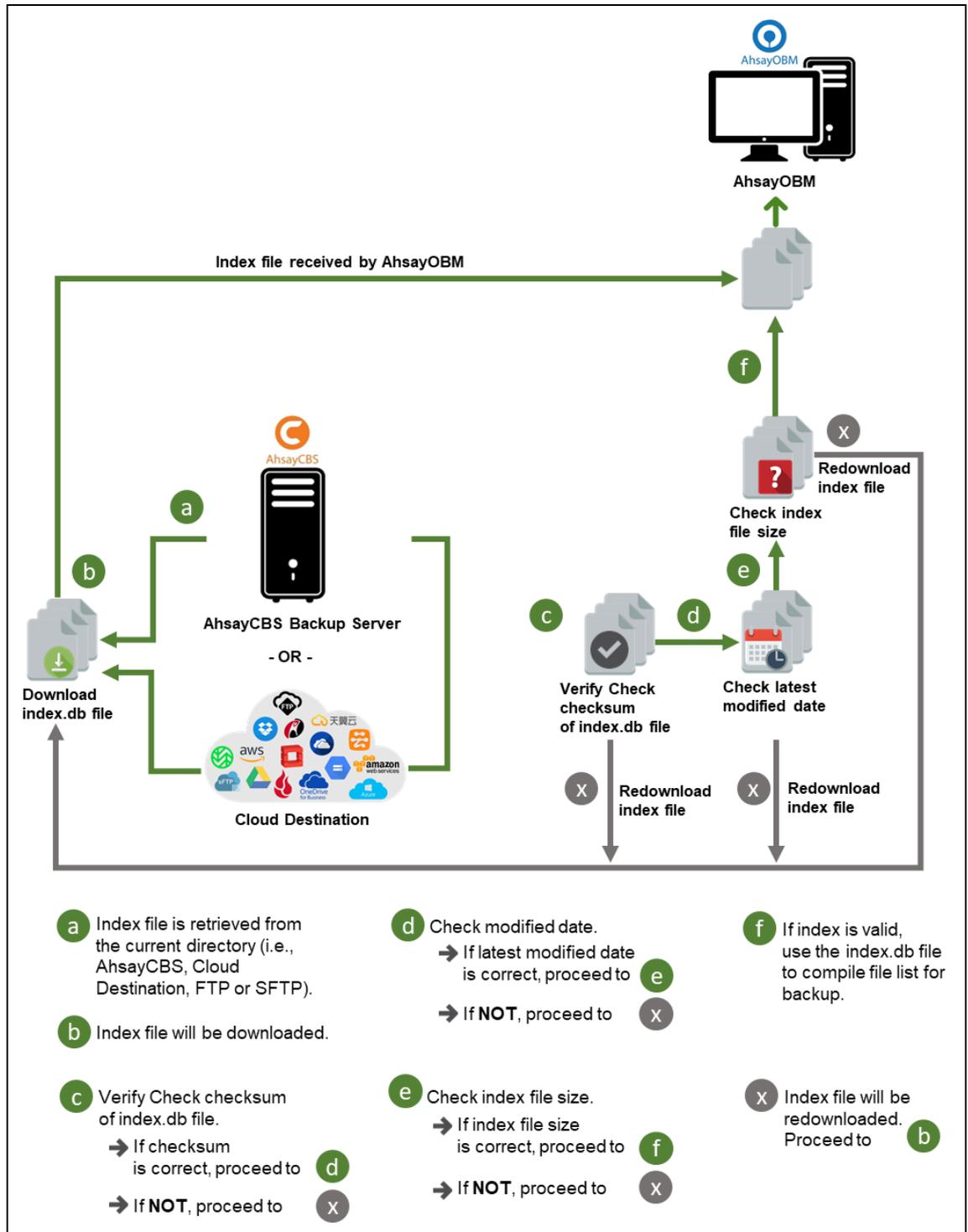
1. If AhsayOBM was upgraded to v8.5 (or above) from an older version v6, v7, or pre-8.3.6.0 version. In this case, the PDIC job will run on the first backup job after upgrade.
2. If backup jobs for a backup set are not run on a regular daily backup schedule (for example: on a weekly or monthly schedule),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



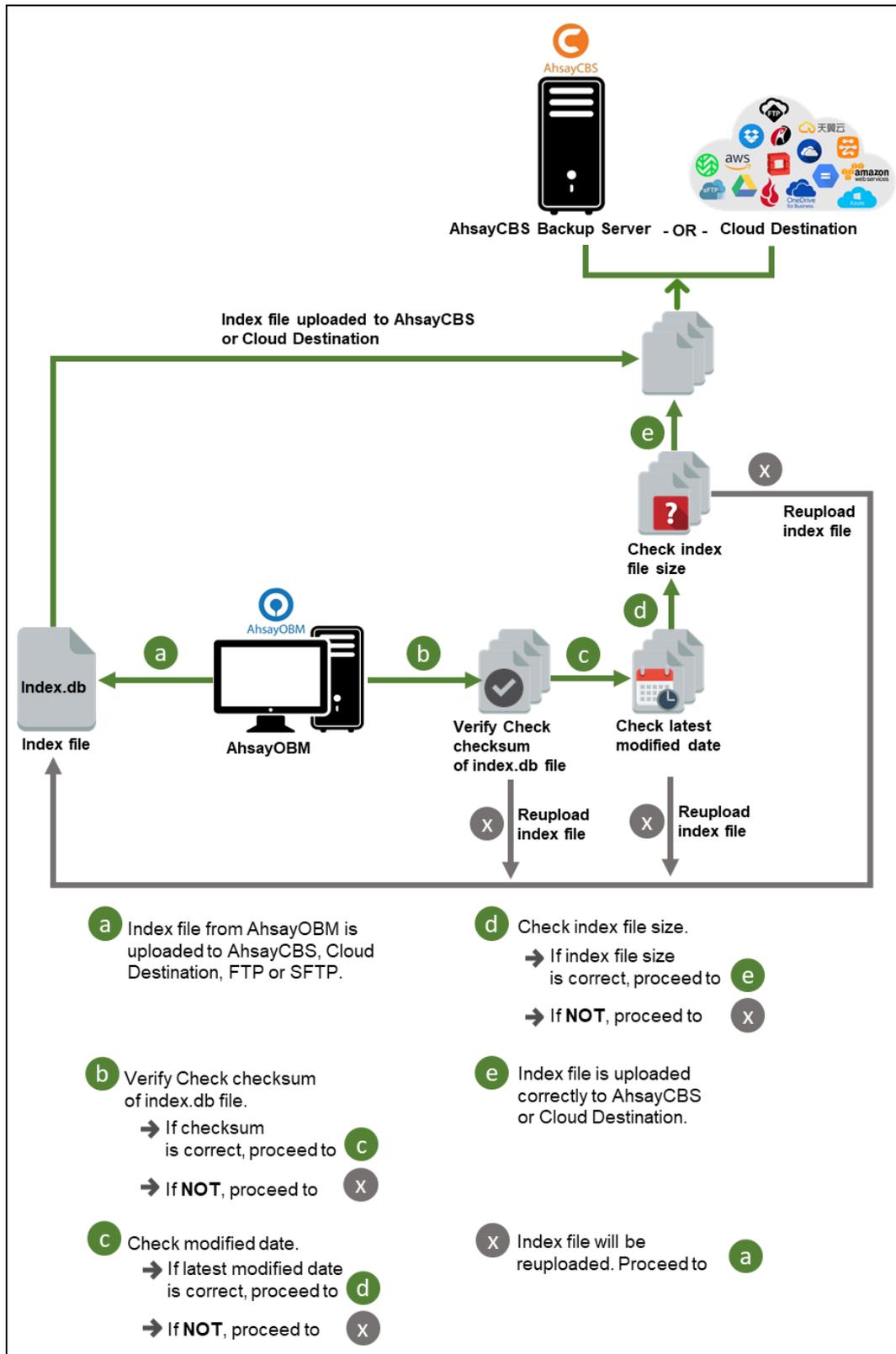
8.2 Backup Set Index Handling Process

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

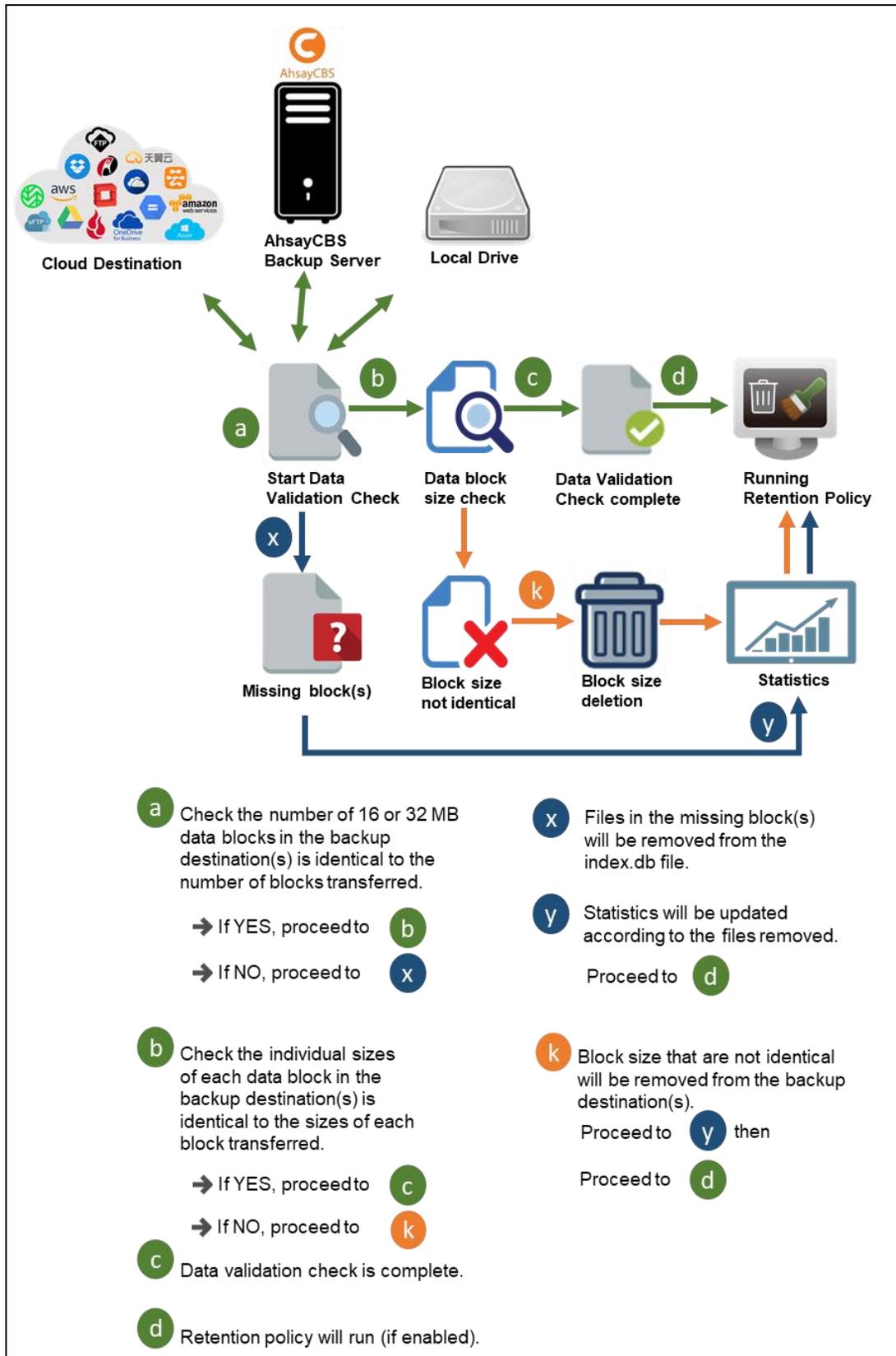


8.2.2 Completed Backup Job



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 16 or 32 MB data block files and the size of each block file are checked again after the files are transferred.



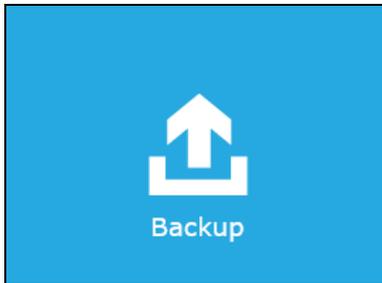
9 Run Backup Jobs

9.1 Login to AhsayOBM

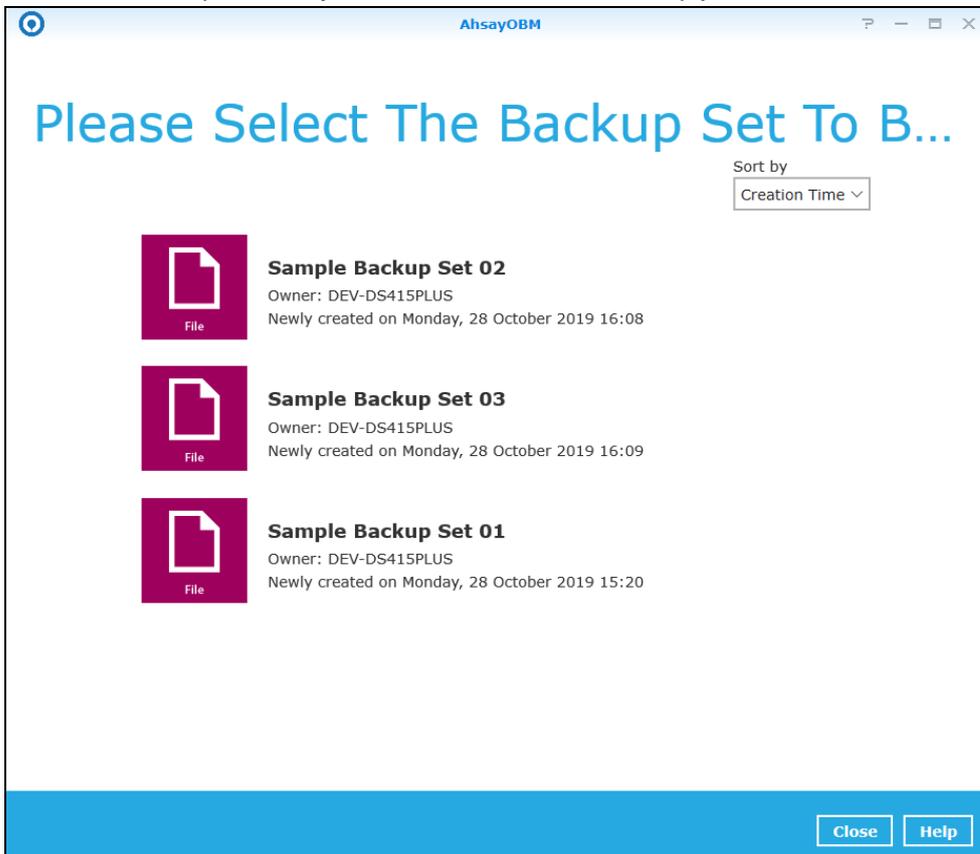
Login to the AhsayOBM application with the instructions provided in [Login to AhsayOBM](#).

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.



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

In-File Delta type

Full

Differential

Incremental

Destinations

 AhsayCBS (Host: 10.90.10.14:443)

Retention Policy

Run Retention Policy after backup

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

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

 **AhsayCBS (Host: 10.90.10.14:443)** 🔍 ✕

Reading backup source from hard disk... /volume1/Manyfiles/1000x100K1/...

Estimated time left: 0 sec

Backed up: 74 B (1 file, 5 directories, 0 link)

Elapsed time: 7 sec

Transfer rate: 0 bit/s

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

 **AhsayCBS (Host: 10.90.10.14:443)** 🔍

 ✓ Backup Completed Successfully

Estimated time left: 0 sec

Backed up: 1 GB (2002 files, 6 directories, 0 link)

Elapsed time: 2 min 40 sec

Transfer rate: 55.5 Mibit/s

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

Type	Log	Time
	Start [AhsayOBM v8.3.0.30]	28/10/2019 16:14:30
	Saving encrypted backup set encryption keys to server...	28/10/2019 16:14:30
	Start Backup ... [In-File Delta: Full]	28/10/2019 16:14:31
	Using Temporary Directory /root/temp/1572250178351/OBS@1572250195445	28/10/2019 16:14:31
	Start running pre-commands	28/10/2019 16:14:33
	Finished running pre-commands	28/10/2019 16:14:33
	Downloading server file list...	28/10/2019 16:14:33
	Downloading server file list... Completed	28/10/2019 16:14:35
	Reading backup source from hard disk...	28/10/2019 16:14:36
	[New Directory]... /	28/10/2019 16:14:36
	[New Directory]... /volume1	28/10/2019 16:14:36
	[New Directory]... /volume1/Manyfiles	28/10/2019 16:14:36
	[New Directory]... /volume1/Manyfiles/#recycle	28/10/2019 16:14:36
	[New Directory]... /volume1/Manyfiles/1000x100K1	28/10/2019 16:14:36
	[New File]... 100% of "/volume1/Manyfiles/#recycle/desktop.ini"	28/10/2019 16:14:36
	[New File]... 24% of "/volume1/Manyfiles/1000x100K1/100KB_1"	28/10/2019 16:14:37
	[New File]... 40% of "/volume1/Manyfiles/1000x100K1/100KB_1"	28/10/2019 16:14:37
	[New File]... 56% of "/volume1/Manyfiles/1000x100K1/100KB_1"	28/10/2019 16:14:37
	[New File]... 72% of "/volume1/Manyfiles/1000x100K1/100KB_1"	28/10/2019 16:14:37
	[New File]... 88% of "/volume1/Manyfiles/1000x100K1/100KB_1"	28/10/2019 16:14:37
	[New File]... 100% of "/volume1/Manyfiles/1000x100K1/100KB_1"	28/10/2019 16:14:37
	[New File]... 24% of "/volume1/Manyfiles/1000x100K1/100KB_10"	28/10/2019 16:14:37

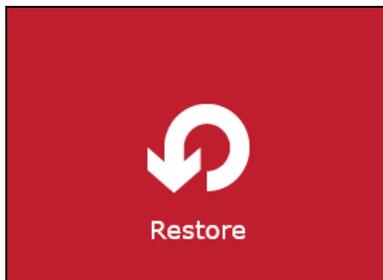
10 Restore Data

10.1 Login to AhsayOBM

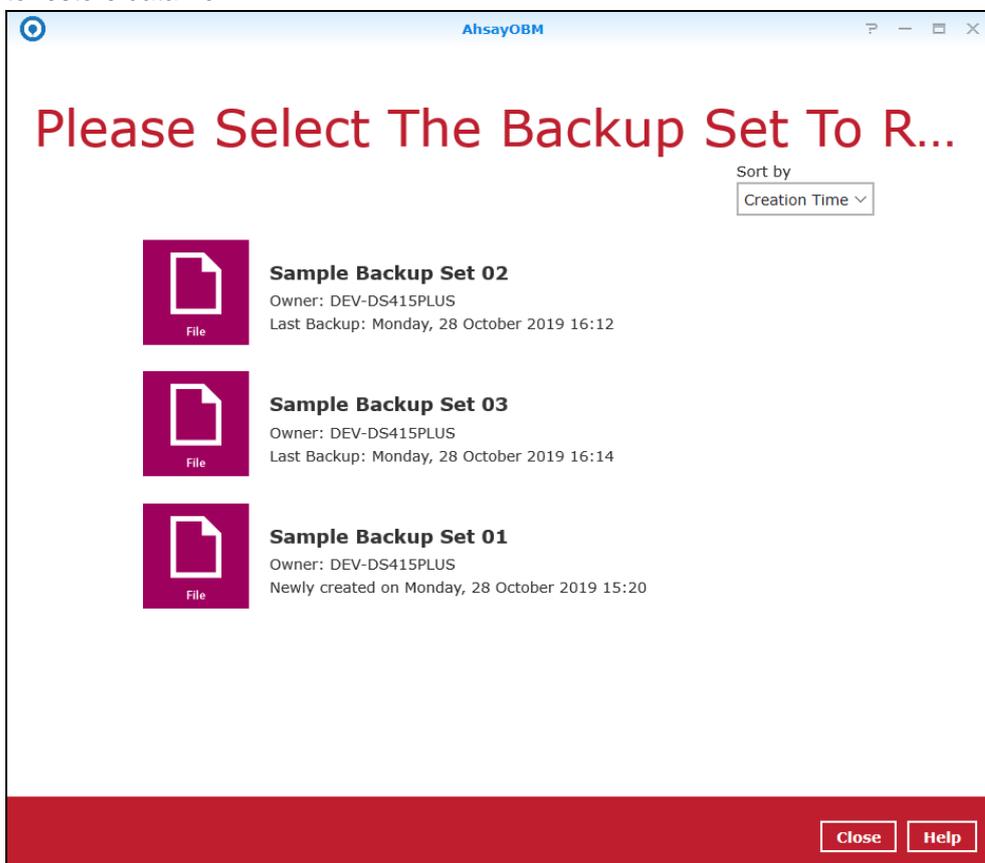
Login to the AhsayOBM application with the instructions provided in [Login to AhsayOBM](#).

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 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.

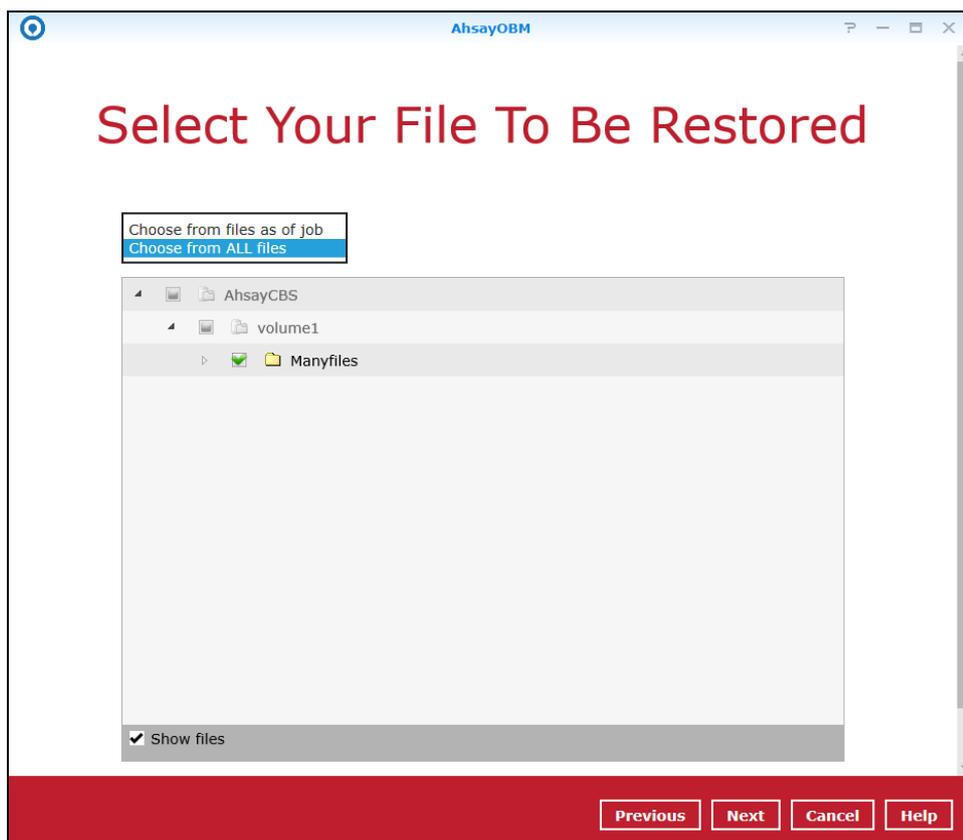
Select what to restore
Choose from files as of job ▾ 28/10/2019 ▾ Latest ▾

Select what to restore
Choose from files as of job ▾ 28/10/2019 ▾ Latest ▾

Select what to restore
Choose from files as of job ▾ 28/10/2019 ▾ Latest ▾

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

Select what to restore
Choose from ALL files ▾



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

<input checked="" type="checkbox"/>	File snapshot testing.txt	147 b...	08/11/2016 09:05
<input checked="" type="checkbox"/>	File snapshot testing.txt	147 b...	08/11/2016 09:05
<input checked="" type="checkbox"/>	File snapshot testing.txt	113 b...	07/11/2016 18:54
<input type="checkbox"/>	File snapshot testing.txt	96 byt...	07/11/2016 18:52
<input type="checkbox"/>	File snapshot testing.txt	80 byt...	07/11/2016 18:51
<input type="checkbox"/>	File snapshot testing.txt	64 byt...	07/11/2016 18:39

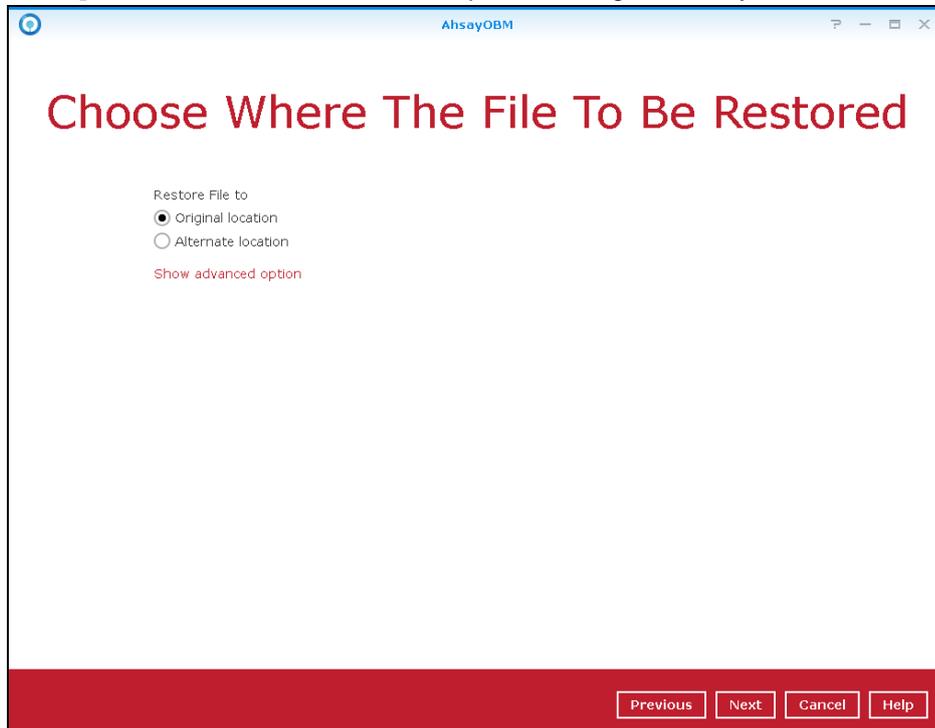
When the restore is done, you will see all the selected backup versions in the restore destination. The latest backup version has the file name as the original file, while the previous versions have the time stamps added to their file names for easy identification.

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

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

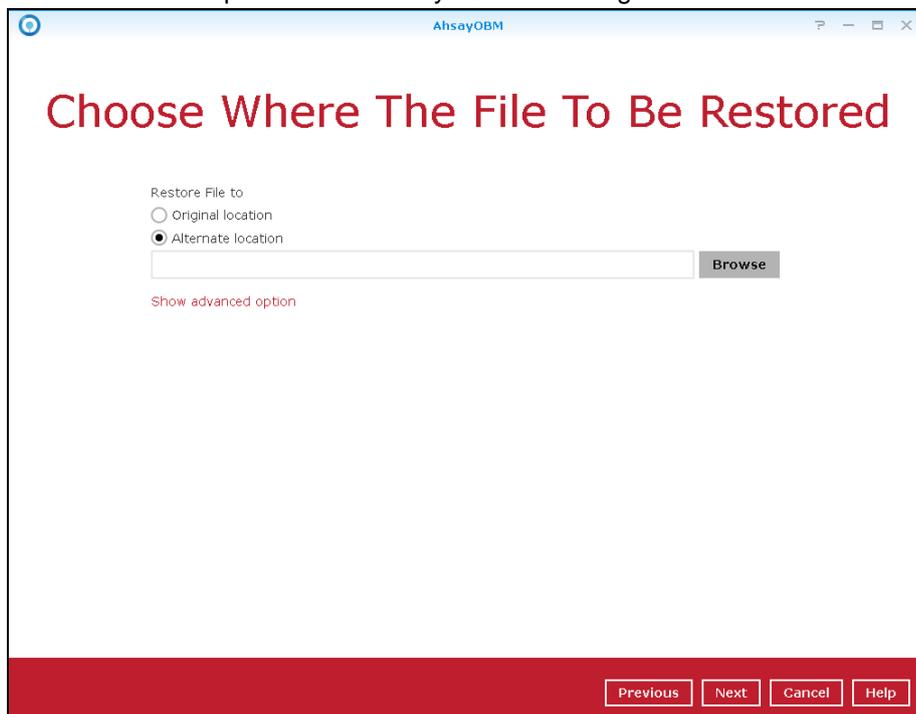
6. Select to restore the files to their **Original location**, or to an **Alternate location**. Then click **Next** to proceed.

- **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 **Users/[User's Name]/Downloads** folder, the data will be restored to **Users/[User's Name]/Downloads** as well on the computer running the AhsayOBM.

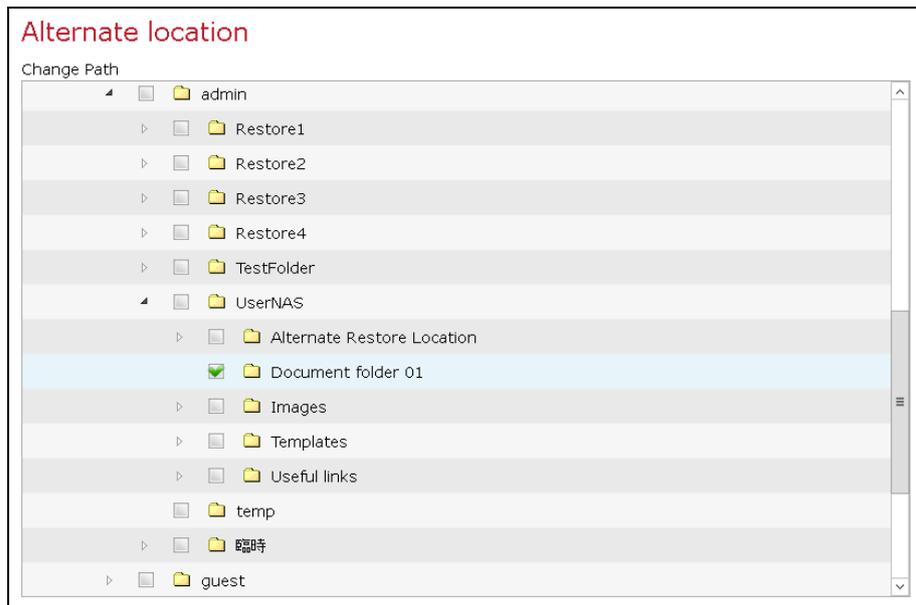


The screenshot shows a window titled "AhsayOBM" with the heading "Choose Where The File To Be Restored". Under "Restore File to", the "Original location" radio button is selected. Below it is an unselected "Alternate location" radio button and a "Show advanced option" link. At the bottom right, there are four buttons: "Previous", "Next", "Cancel", and "Help".

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



The screenshot shows the same "Choose Where The File To Be Restored" dialog box, but now the "Alternate location" radio button is selected. Below the radio buttons is a text input field for a file path, followed by a "Browse" button. The "Show advanced option" link is also present. The "Previous", "Next", "Cancel", and "Help" buttons are at the bottom right.



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

Restore File to

Original location

Alternate location

Show advanced option

Overwrite mode during restoration:

Skip All

Overwrite all

Restore file permissions

Delete extra files

Follow Link

Verify checksum of in-file delta files during restore

Hide advanced option

- Overwrite mode during restoration**

When there are file name conflicts during restoration, you can choose to skip them all or overwrite all existing files in the restore destination.
- Restore file permissions**

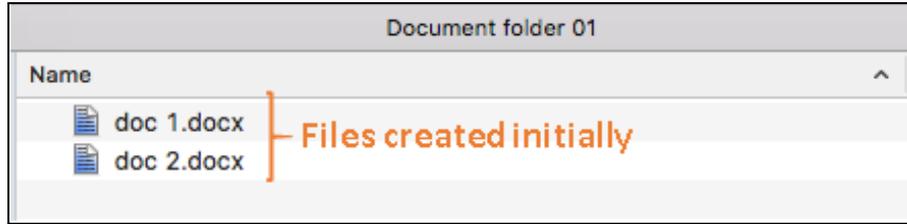
Restore file permissions is disabled by default. When you perform a file restore on a shared computer, it is recommended that you enable Restore file permissions by ticking the checkbox so that the files restored will not be fully accessible to everyone using the shared computer.
- Delete extra files**

Synchronize the selected restore source with the restore destination. 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

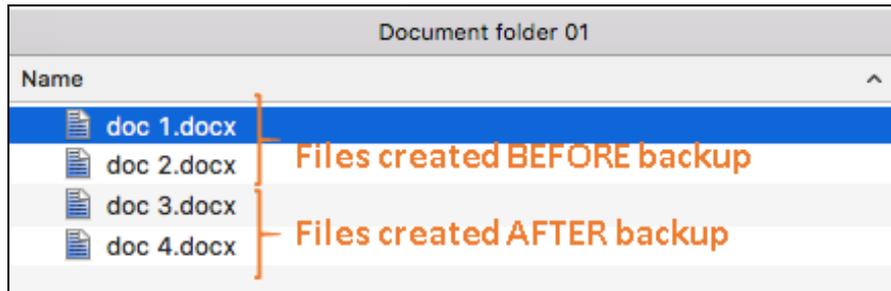
treated as “extra files” and will be deleted from the restore source if this feature is enabled.

Example:

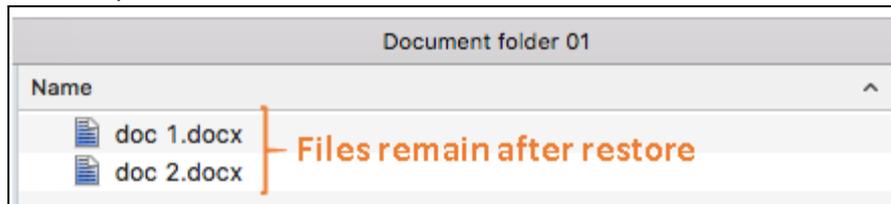
- i) Two files are created under the **Document folder 01**, namely doc 1 & doc 2.



- ii) A backup is performed for folder **Document folder 01**.
- iii) Two new files are created, namely doc 3 & doc 4.



- iv) A restore is performed for the **Document folder 01**, with **Delete extra files** option enabled.
- v) Since doc 3 & doc 4 have never been backed up, therefore they will be deleted from **Document folder 01**, leaving only the two files that have been backed up.



WARNING

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

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

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

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

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

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

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

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

8. Click **Next** to proceed when you are done with the settings.
9. Select the temporary directory for storing temporary files, such as delta files when they are being merged.

Temporary Directory

Temporary directory for storing restore files

Change

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

AhsayCBS (Host: 10.90.10.14:443)
🔍 ✕

Pending

Estimated time left:

Restored:

Elapsed time:

Transfer rate:

- When the restore is completed, the progress bar will be green in color and the message **Restore Completed Successfully** will appear.


AhsayCBS (Host: 10.90.10.14:443)



✓ Restore Completed Successfully
 Estimated time left: 0 sec
 Restored: 1 GB (2002 files, 0 directory)
 Elapsed time: 4 min 40 sec
 Transfer rate: 32.3 Mibit/s

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

Type	Log	Time
	Start [AhsayOBM v8.3.0.30]	28/10/2019 16:28:41
	Initializing decrypt action...	28/10/2019 16:28:42
	Initializing decrypt action... Completed	28/10/2019 16:28:42
	Creating new directory... "/volume2/test/volume1/Manyfiles"	28/10/2019 16:28:42
	Creating new directory... "/volume2/test/volume1/Manyfiles/#recycle"	28/10/2019 16:28:42
	Downloading... "/volume2/test/volume1/Manyfiles/#recycle/desktop.ini" (Total 74 bytes)	28/10/2019 16:28:42
	Creating new directory... "/volume2/test/volume1/Manyfiles/1000x100K1"	28/10/2019 16:28:42
	Downloading... "/volume2/test/volume1/Manyfiles/1000x100K1/100KB_1" (Total 100k bytes)	28/10/2019 16:28:42
	Downloading... "/volume2/test/volume1/Manyfiles/1000x100K1/100KB_10" (Total 100k bytes)	28/10/2019 16:28:43
	Downloading... "/volume2/test/volume1/Manyfiles/1000x100K1/100KB_100" (Total 100k bytes)	28/10/2019 16:28:46
	Downloading... "/volume2/test/volume1/Manyfiles/1000x100K1/100KB_1000" (Total 100k bytes)	28/10/2019 16:28:46
	Downloading... "/volume2/test/volume1/Manyfiles/1000x100K1/100KB_101" (Total 100k bytes)	28/10/2019 16:28:46
	Downloading... "/volume2/test/volume1/Manyfiles/1000x100K1/100KB_102" (Total 100k bytes)	28/10/2019 16:28:46
	Downloading... "/volume2/test/volume1/Manyfiles/1000x100K1/100KB_103" (Total 100k bytes)	28/10/2019 16:28:46
	Downloading... "/volume2/test/volume1/Manyfiles/1000x100K1/100KB_104" (Total 100k bytes)	28/10/2019 16:28:46
	Downloading... "/volume2/test/volume1/Manyfiles/1000x100K1/100KB_105" (Total 100k bytes)	28/10/2019 16:28:46
	Downloading... "/volume2/test/volume1/Manyfiles/1000x100K1/100KB_106" (Total 100k bytes)	28/10/2019 16:28:46
	Downloading... "/volume2/test/volume1/Manyfiles/1000x100K1/100KB_107" (Total 100k bytes)	28/10/2019 16:28:46
	Downloading... "/volume2/test/volume1/Manyfiles/1000x100K1/100KB_108" (Total 100k bytes)	28/10/2019 16:28:47
	Downloading... "/volume2/test/volume1/Manyfiles/1000x100K1/100KB_109" (Total 100k bytes)	28/10/2019 16:28:47
	Downloading... "/volume2/test/volume1/Manyfiles/1000x100K1/100KB_11" (Total 100k bytes)	28/10/2019 16:28:47

- In the Restore window, click **Close** to close the Restore window.
- To exit AhsayOBM, click the "x" on the top right corner. A message will appear to ask for your confirmation. Click **Yes** to close the application. If you wish to use AhsayOBM again, you will have to launch it again.

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

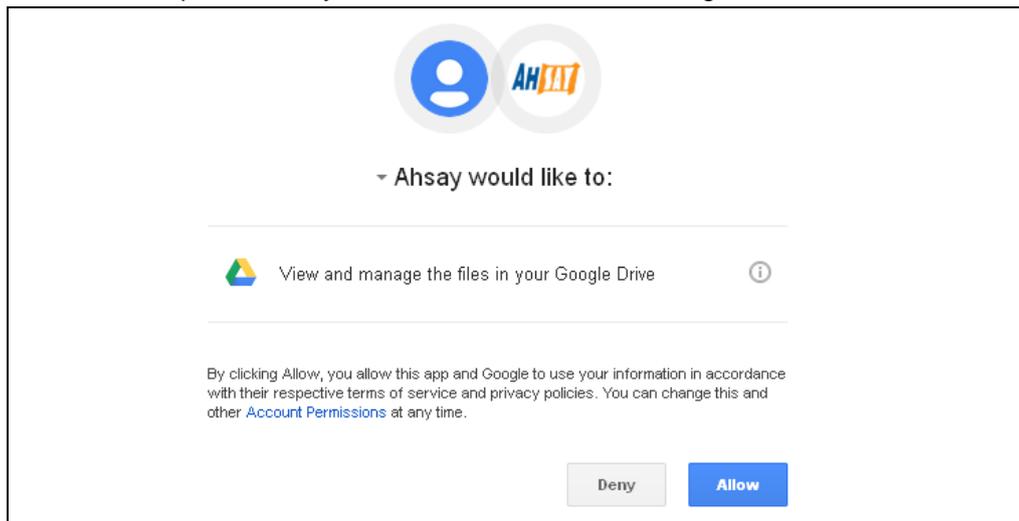
Appendix A: Cloud Storage as Backup Destination

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

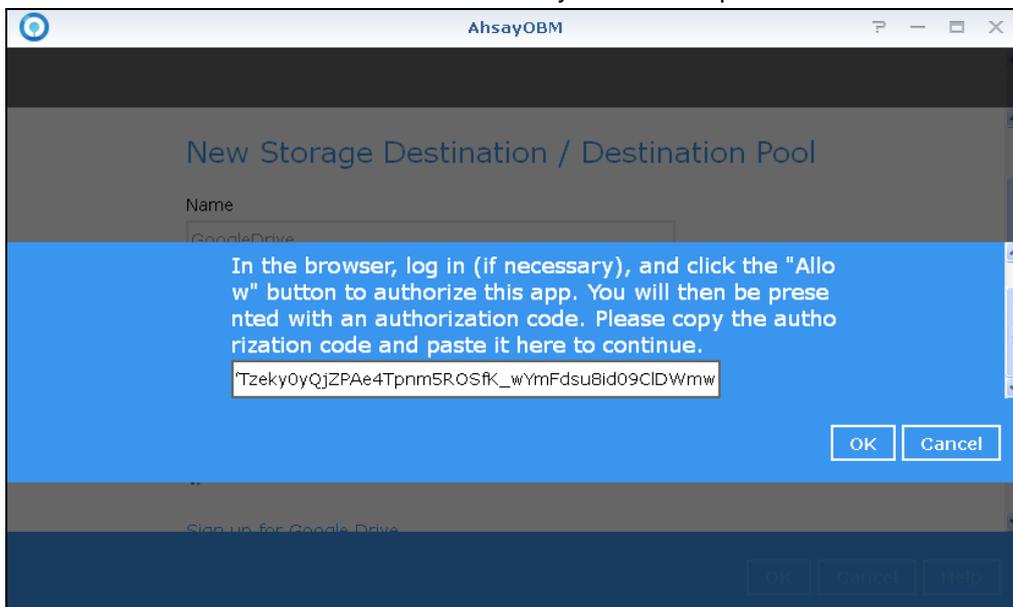
Important

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

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



5. 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:
http://wiki.ahsay.com/doku.php?id=public:8002_faq:faq_on_backup_destination

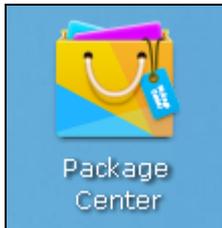
Appendix B: Uninstall AhsayOBM

Refer to the following steps to uninstall AhsayOBM.

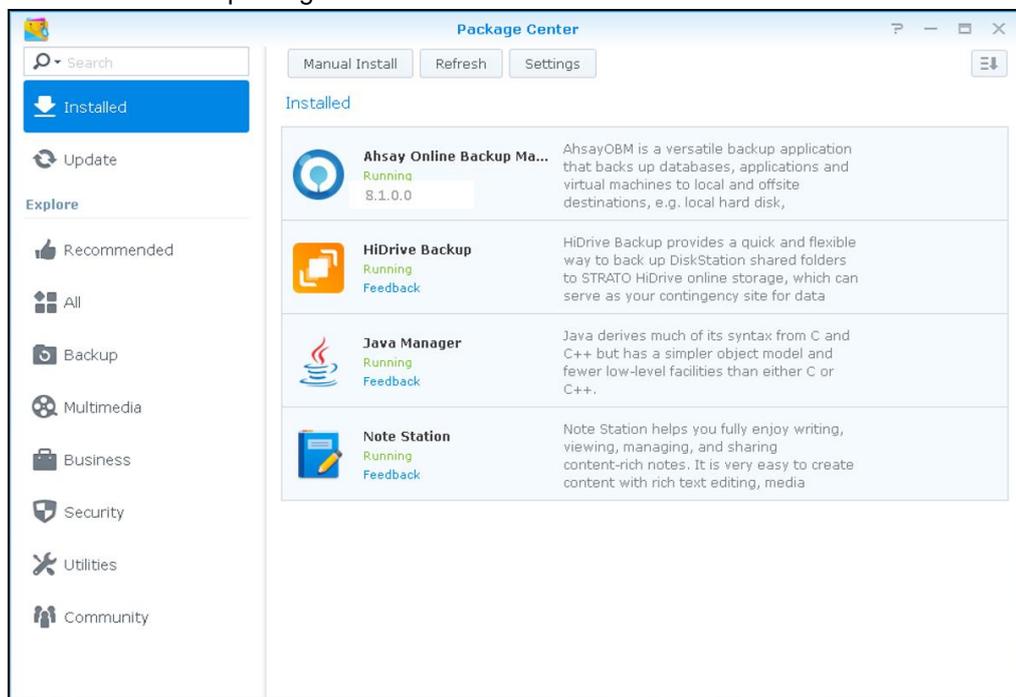
1. Sign into DiskStation Manager (DSM) with the admin account. In a web browser, enter the Synology NAS device IP address, followed by 5000
https://nas_hostname:5000

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

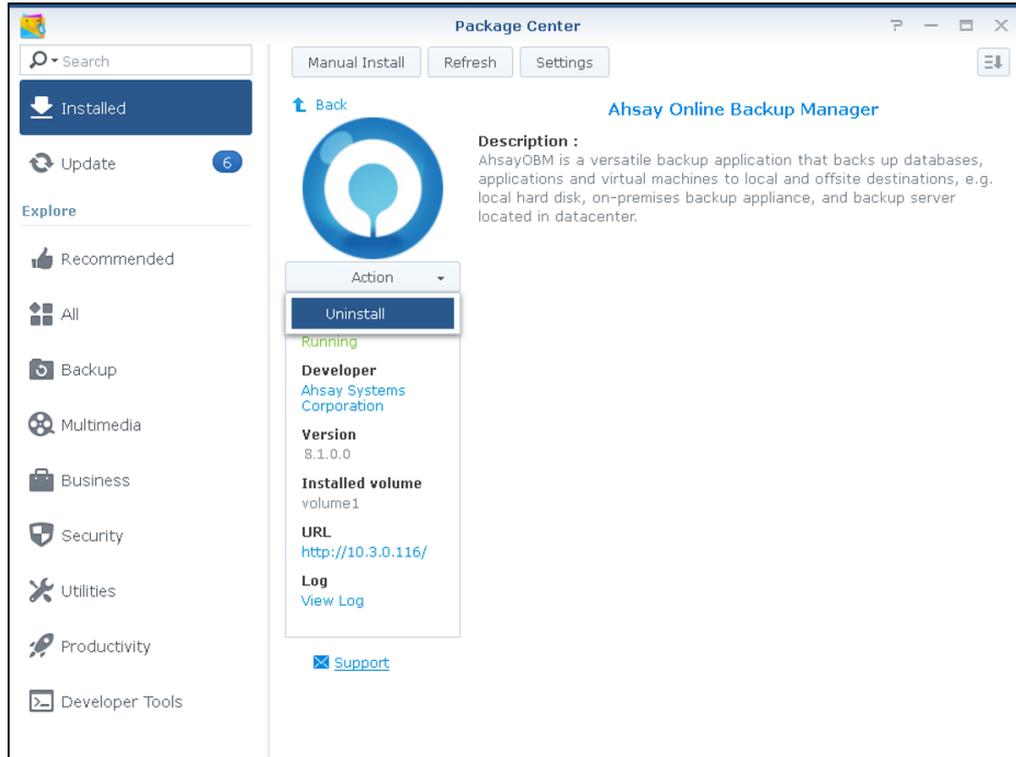
2. Double-click the Package Center icon on the desktop.



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**.

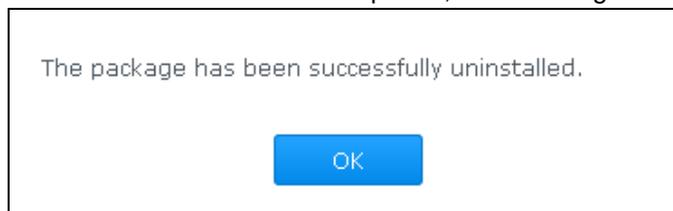


5. Click **Yes** to uninstall AhsayOBM.



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.



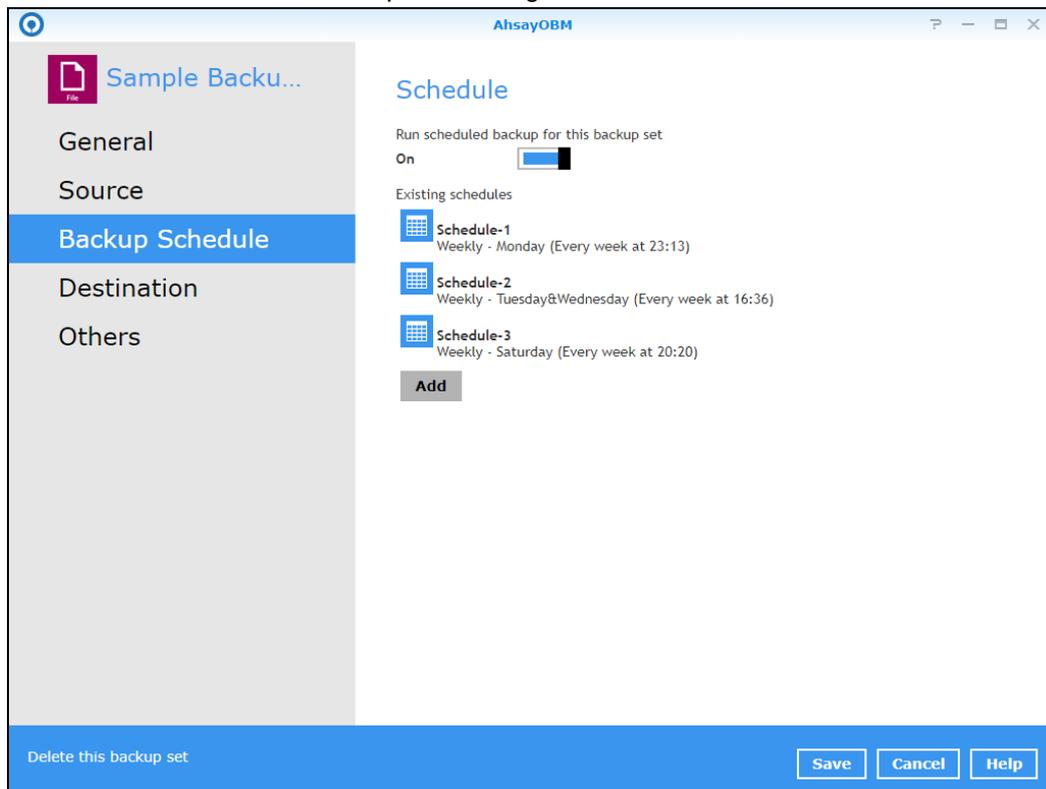
Note: Ahsay Online Backup Manager will no longer appear in the list of Installed packages. The uninstaller will also remove the .obm folder and all binary files from the following paths respectively:

/volume1/@appstore/AhsayOBM/.obm
/volume1/@appstore/AhsayOBM/

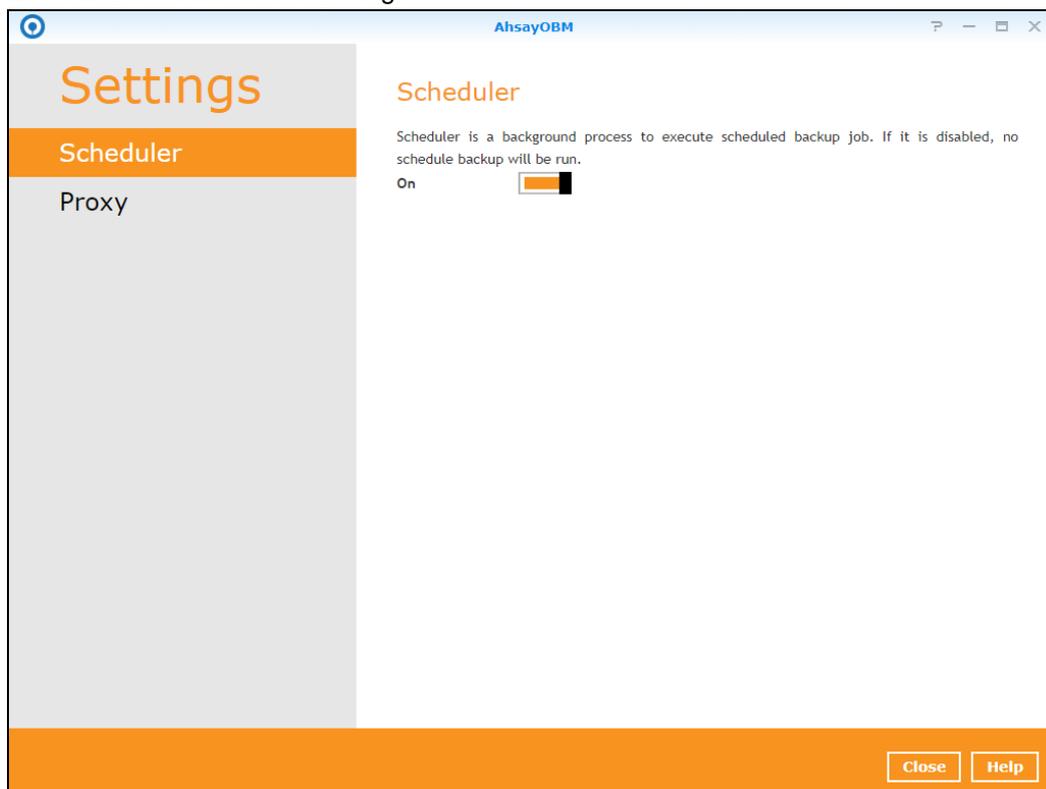
Appendix C: Scheduler Scenarios

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

Level 1: Scheduler under Backup Set Settings

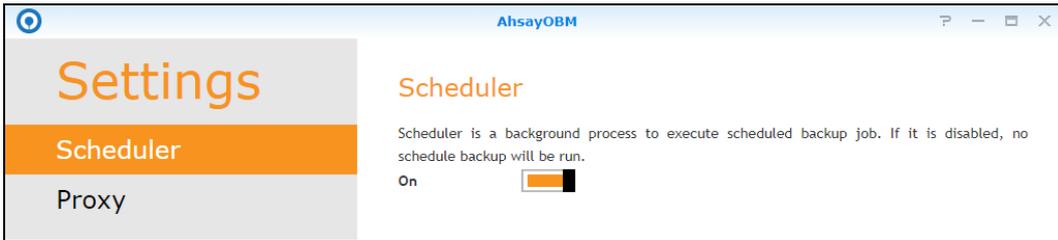


Level 2: Scheduler under Settings

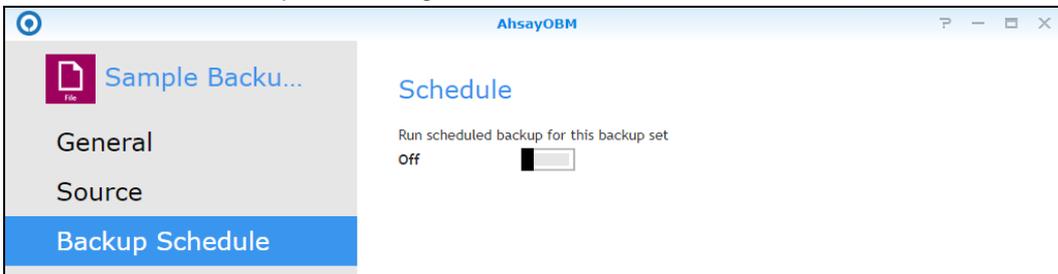


Scenario no. 1: Scheduler under Setting is ON and Scheduler under Backup Set Settings is OFF

Scheduler under Setting



Scheduler under Backup Set Settings



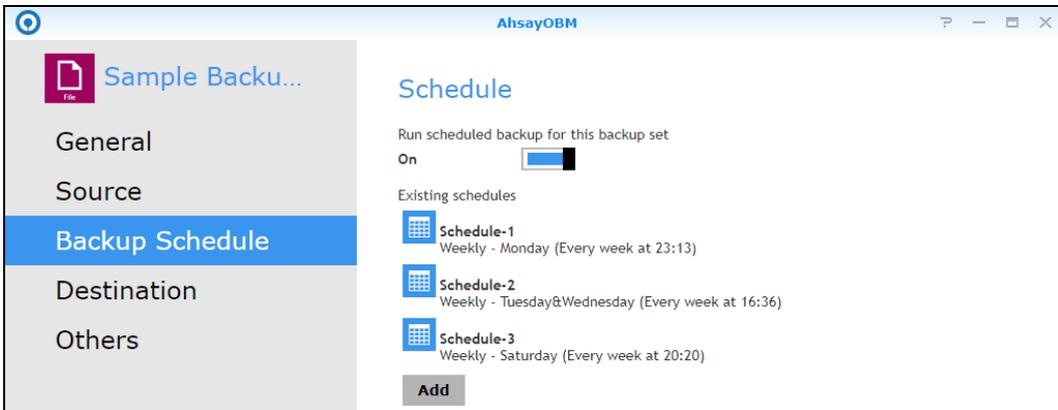
Result: There is no scheduled backup job will be run for the backup set.

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

Scheduler under Setting



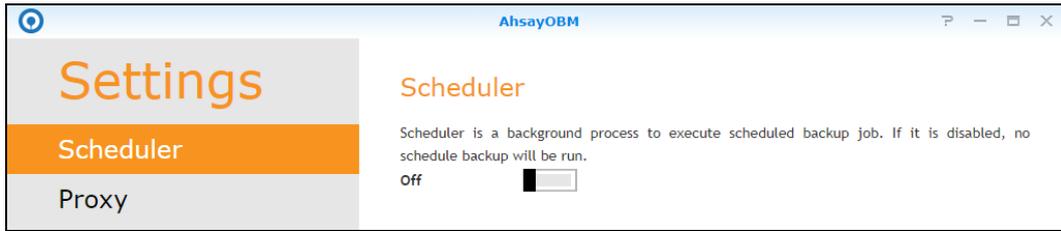
Scheduler under Backup Set Settings



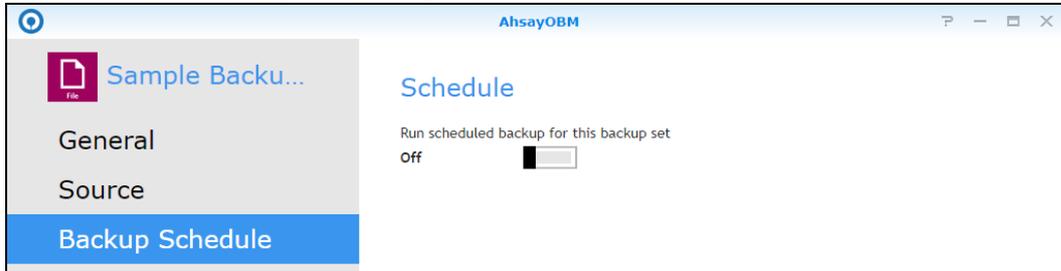
Result: Scheduled backup jobs which are Schedule-1, Schedule-2, and Schedule-3 for the backup set will run.

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

Scheduler under Setting



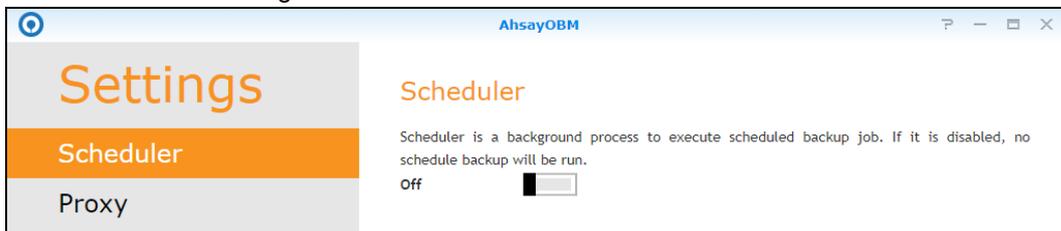
Scheduler under Backup Set Settings



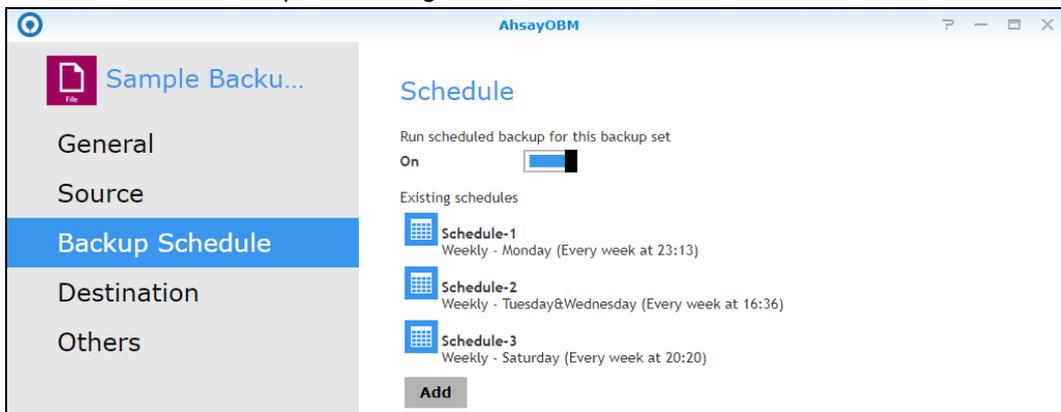
Result: There is no scheduled backup job will be run for the backup set.

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

Scheduler under Setting



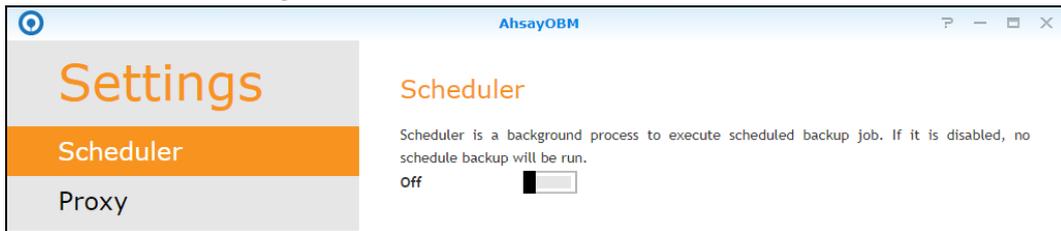
Scheduler under Backup Set Settings



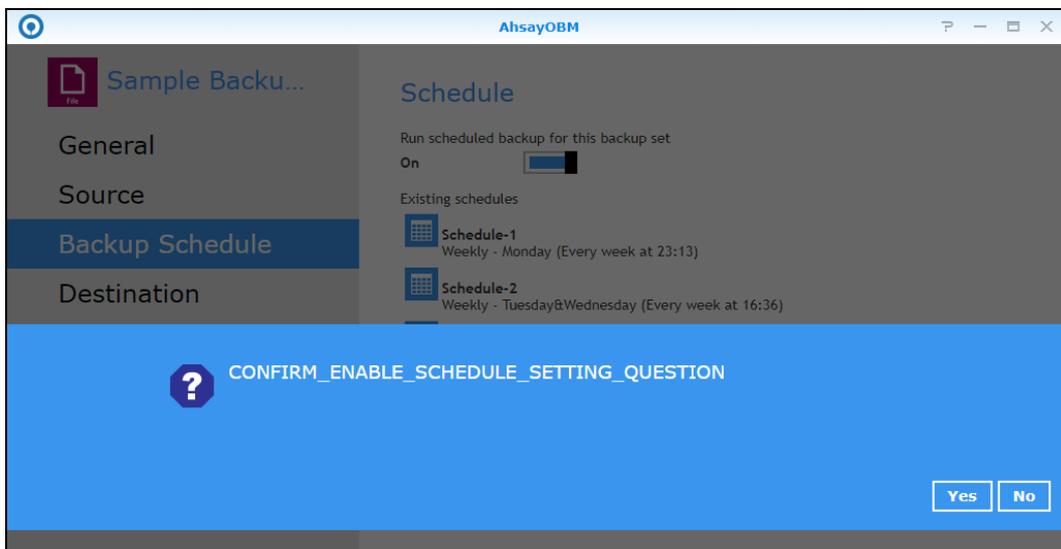
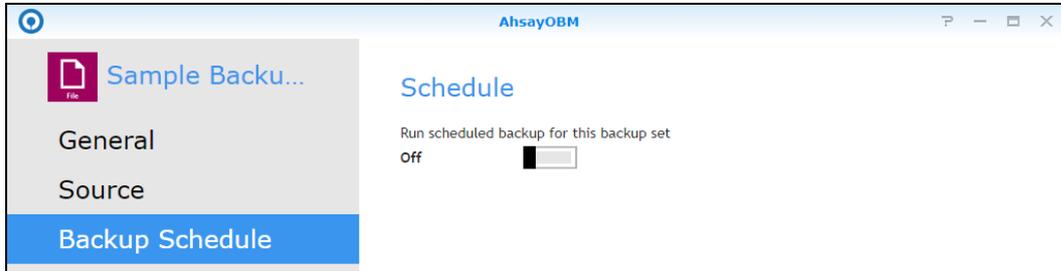
Result: There is no scheduled backup job will be run for the backup set.

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

Scheduler under Setting



Scheduler under Backup Set Settings



Result: There is an alert message that will be displayed confirming to set the Scheduler under Setting 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 turned OFF.

Appendix D: Create Free Trial Account in AhsayOBM

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

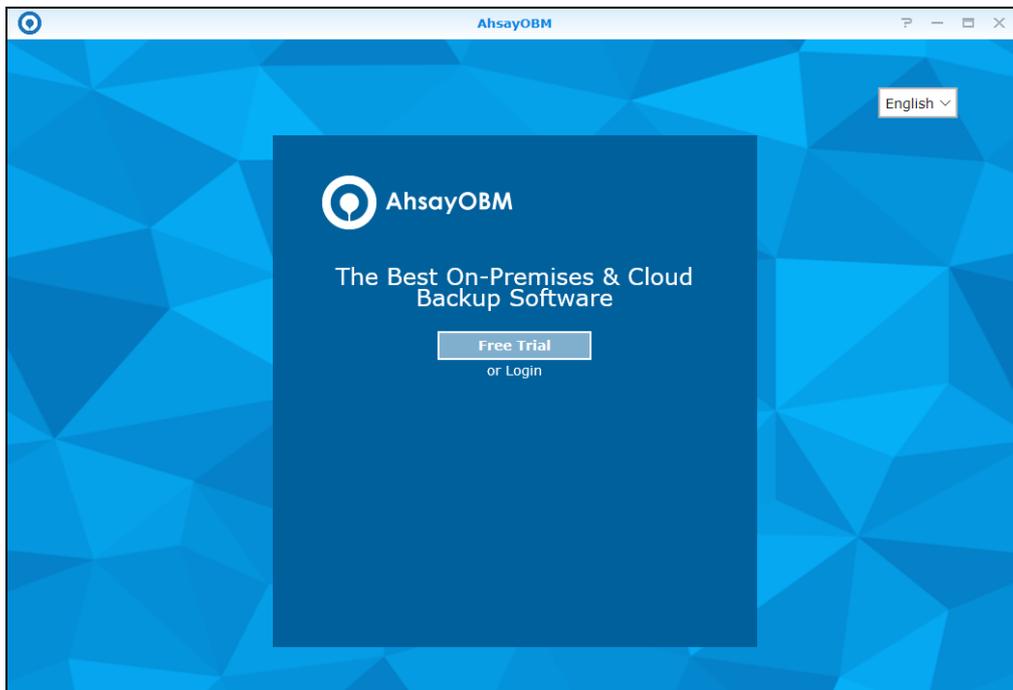
- A valid email address which will be used for receiving notices. A welcome message will also be sent upon creation of the account which specifies the User Setting and Quota set for backup in AhsayCBS.

While here are the limitations of a trial account:

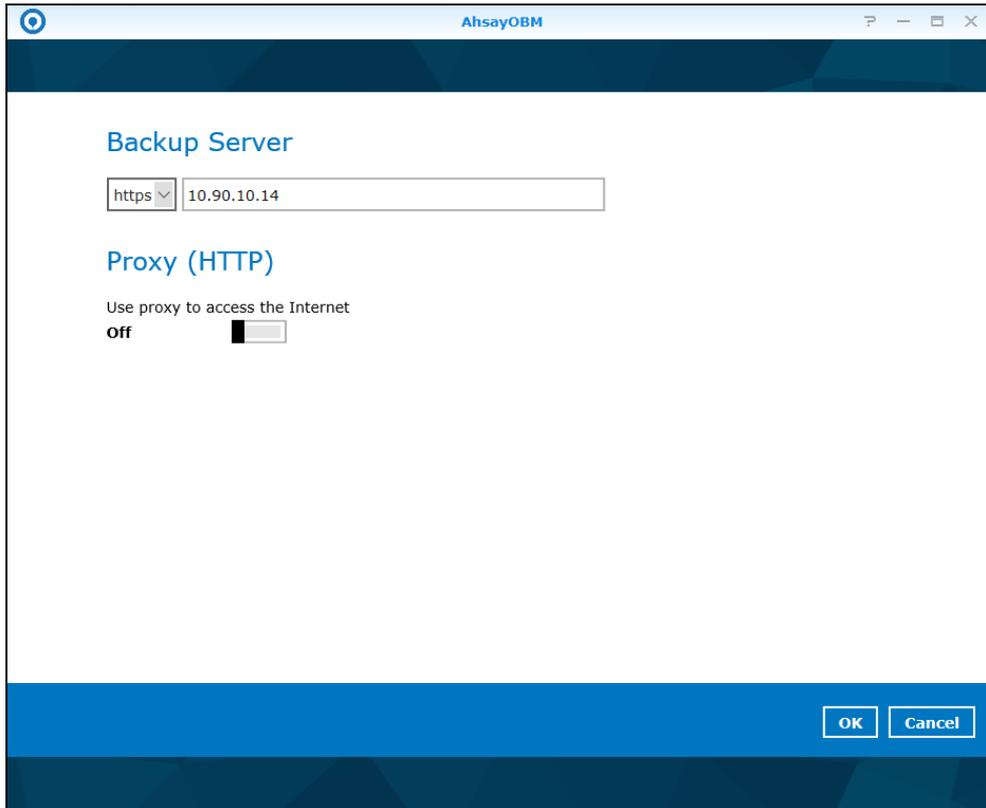
- The Free Trial button will only be displayed once, when the user login for the first time. If you cannot create a free trial account kindly contact your backup service provider.
- Only alphanumeric characters and selected special characters, A to Z, 0 to 9, @, - and _ , are allowed to be used for the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

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

1. Click on **Free Trial**.

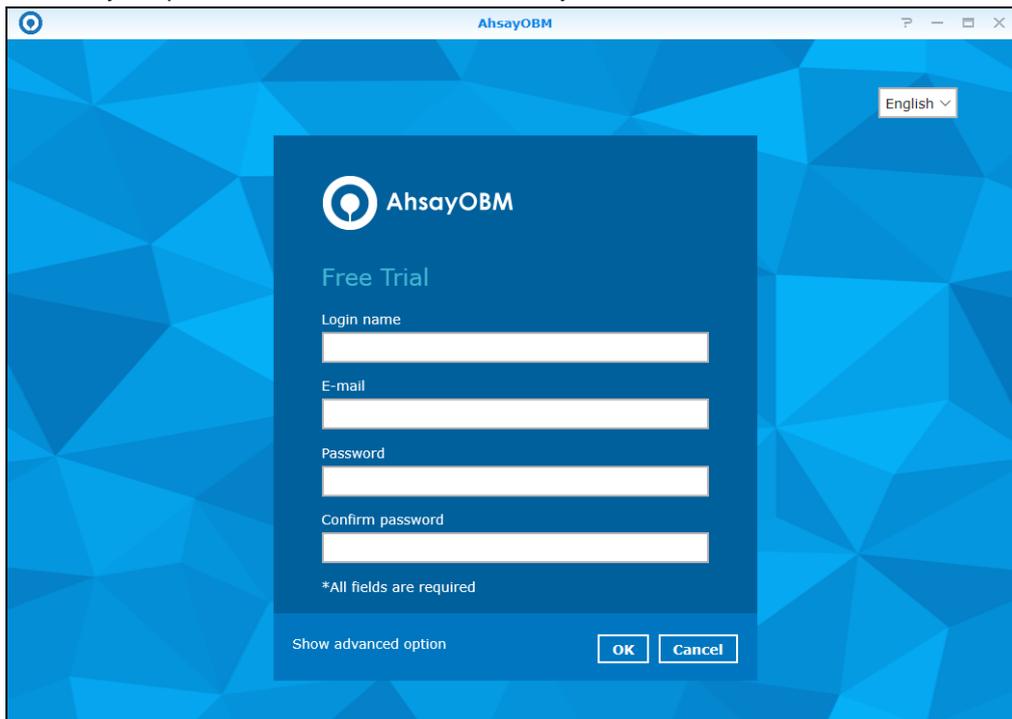


2. Configure your Backup Server settings.



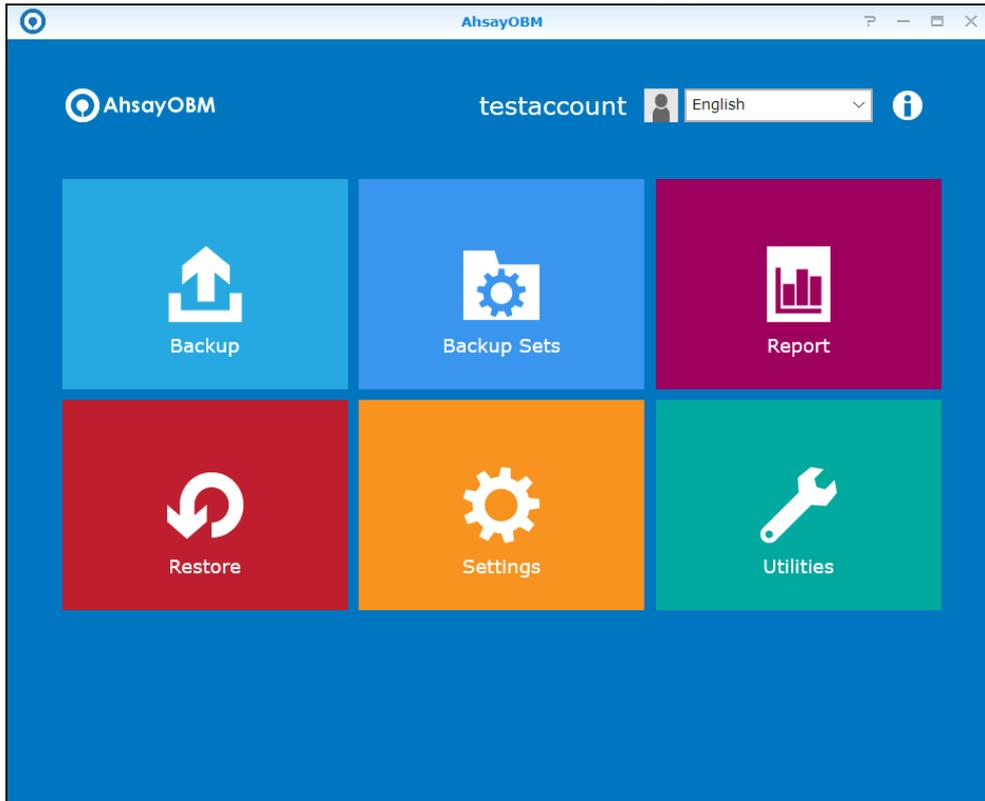
The screenshot shows the 'Backup Server' configuration window in AhsayOBM. The window title is 'AhsayOBM'. The main heading is 'Backup Server'. Below the heading, there is a dropdown menu set to 'https' and a text input field containing '10.90.10.14'. Underneath, the heading is 'Proxy (HTTP)'. Below this heading, there is a label 'Use proxy to access the Internet' and a toggle switch labeled 'off' which is currently turned off. At the bottom right of the window, there are two buttons: 'OK' and 'Cancel'.

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



The screenshot shows the 'Free Trial' registration window in AhsayOBM. The window title is 'AhsayOBM'. The background is a blue geometric pattern. In the top right corner, there is a language dropdown menu set to 'English'. The main heading is 'Free Trial'. Below the heading, there is the AhsayOBM logo and the text 'Free Trial'. There are four text input fields labeled 'Login name', 'E-mail', 'Password', and 'Confirm password'. Below the input fields, there is a note '*All fields are required'. At the bottom left, there is a link 'Show advanced option'. At the bottom right, there are two buttons: 'OK' and 'Cancel'.

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



5. After your trial account has been created, you need to check several things:
- The expiry date of the trial account, which determines when it will be suspended.
 - The Language which will be used for sending reports.
 - And the Time zone, this is to ensure that your backup schedule will run at the correct time.

You can check this by logging in to AhsayCBS, go to **Backup / Restore > User > User Profile > General**. For more information please refer to the [AhsayCBS User's Guide](#).

User Profile	General	Backup Client Settings	Contact	User Group	Security Settings
Backup Set	Suspend At 30-Oct-2019				
Settings	Status <input checked="" type="radio"/> Enable <input type="radio"/> Suspended <input type="radio"/> Locked				
Report	Upload Encryption Key <input type="checkbox"/> Upload encryption key after running backup for recovery				
Statistics	Language English				
Effective Policy	Timezone GMT+08:00 (CST)				

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

Settings of the client backup agent for this user.

Backup Client

AhsayOBM User AhsayACB User

Add-on Modules

<input checked="" type="checkbox"/> Microsoft Exchange Server	<input checked="" type="checkbox"/> Microsoft SQL Server
<input checked="" type="checkbox"/> MySQL Database Server	<input checked="" type="checkbox"/> Oracle Database Server
<input checked="" type="checkbox"/> Lotus Domino	<input checked="" type="checkbox"/> Lotus Notes
<input checked="" type="checkbox"/> Windows System Backup	<input checked="" type="checkbox"/> Windows System State Backup
<input checked="" type="checkbox"/> VMware <input type="text" value="Guest VM"/> <input type="text" value="10"/>	<input checked="" type="checkbox"/> Hyper-V <input type="text" value="Guest VM"/> <input type="text" value="10"/>
<input checked="" type="checkbox"/> Microsoft Exchange Mailbox <input type="text" value="10"/>	<input checked="" type="checkbox"/> ShadowProtect System Backup
<input checked="" type="checkbox"/> Continuous Data Protection	<input checked="" type="checkbox"/> NAS - Synology
<input checked="" type="checkbox"/> Mobile <input type="text" value="10"/>	<input checked="" type="checkbox"/> NAS - QNAP
<input checked="" type="checkbox"/> Volume Shadow Copy	<input checked="" type="checkbox"/> In-File Delta
<input checked="" type="checkbox"/> OpenDirect / Granular Restore <input type="text" value="10"/>	<input checked="" type="checkbox"/> Office 365 Backup <input type="text" value="10"/>

Quota

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

Destination	Quota
<input checked="" type="checkbox"/> AhsayCBS	<input type="text" value="50.0"/> <input type="text" value="Gbytes"/>

(If preempted mode is enabled in policy settings, the quota settings are disabled)

7. Lastly, you need to verify if your contact details are correct by going to the **Contact** tab. If you want to add more contact information, you can add it here.

Contact information for this user.

Manage Contact Information

Name	Email	Encrypt Email
<input checked="" type="checkbox"/> trial	trial@email.com	No