

Online-Backup.dk v9

Guide for QNAP NAS

Ahsay Systems Corporation Limited

11 February 2022

Copyright Notice

© 2022 Ahsay Systems Corporation Limited. All rights reserved.

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

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

Trademarks

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

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

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

Dropbox is a registered trademark of Dropbox Inc.

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

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

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

MariaDB is a registered trademark of MariaDB Corporation AB.

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

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

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

OpenJDK is a registered trademark of Oracle America, Inc.

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

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

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

Ubuntu is a registered trademark of Canonical Ltd.

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

Rocky is a registered trademark of Rocky Brands.

ShadowProtect is a registered trademark of StorageCraft Technology Corporation.

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

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

Disclaimer

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

Revision History

Date	Descriptions	Version
25 January 2022	▪ Ch 6.6 – added Deduplication	9.1.0.0

Table of Contents

1	Overview	1
1.1	What is this software?	1
1.2	System Architecture	1
2	Requirements for AhsayOBM on QNAP NAS	2
2.1	Hardware Requirements.....	2
2.2	Software Requirements	2
2.3	AhsayOBM Installation	2
2.4	NAS-QNAP Add-on Module.....	2
2.5	Backup Quota Storage	3
2.6	Java Requirement	3
2.7	Memory Requirement	3
2.8	TCP Port Requirement	3
2.9	QNAP NAS User Account Permission	3
2.10	Network Bandwidth.....	4
2.11	Limitations	4
2.12	Supported Features from AhsayCBS Web Console.....	4
3	Get started with AhsayOBM	5
4	Download and Install AhsayOBM	6
4.1	Download AhsayOBM	6
4.2	Install AhsayOBM using QPKG online installer	7
4.3	AhsayOBM Scheduler Service Check.....	10
4.4	RunLevel Symlink Check.....	11
5	Start AhsayOBM	12
6	AhsayOBM Overview	17
6.1	Profile	18
6.2	Online Help.....	23
6.3	Language	24
6.4	Information	24
6.5	Backup	25
6.6	Backup Sets	26
6.7	Report	41
	6.7.1 Backup	41
	6.7.2 Restore.....	47
6.8	Restore.....	48

6.9	Settings	49
	6.9.1 Scheduler	49
	6.9.2 Proxy	50
6.10	Utilities.....	51
	6.10.1 Data Integrity Check	51
	6.10.2 Delete Backup Data.....	64
7	Create a Backup Set	68
8	Overview on the Backup Process	76
8.1	Periodic Data Integrity Check (PDIC) Process.....	77
8.2	Backup Set Index Handling Process.....	79
	8.2.1 Start Backup Job.....	79
	8.2.2 Completed Backup Job	80
8.3	Data Validation Check Process	81
9	Run Backup Jobs	82
	Start a Manual Backup.....	82
10	Restore Data.....	86
10.1	Login to AhsayOBM.....	86
10.2	Restore Data	86
11	Contact Ahsay.....	94
11.1	Technical Assistance.....	94
11.2	Documentation	94
Appendix	95
	Appendix A: Cloud Storage as Backup Destination	95
	Appendix B: Uninstall AhsayOBM	97
	Appendix C: Scheduler Scenarios.....	99
	Appendix D: Create Free Trial Account in AhsayOBM.....	103

1 Overview

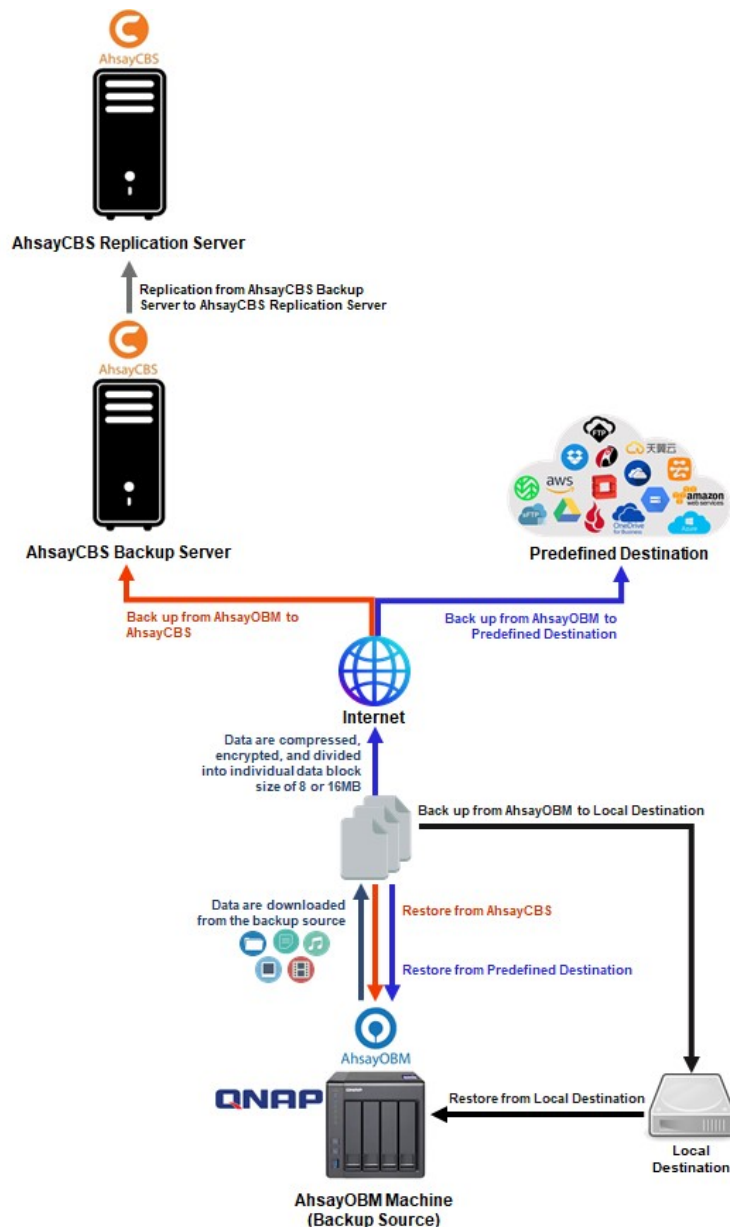
1.1 What is this software?

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 QNAP NAS

2.1 Hardware Requirements

Refer to the following article for the list of supported QNAP NAS modes:

[FAQ: Ahsay Hardware Compatibility List \(HRL\) for AhsayOBM on QNAP NAS](#)

WARNING

QNAP NAS models with less than 1GB RAM are not supported. As 1GB RAM or above is required to ensure application stability and optimal backup/restore performance. To back up data on unsupported QNAP NAS models, share the folder(s) then backup the data as network shared folder from a Windows machine.

For more details on how to create a shared folder(s), please refer to this link [Creating a Shared Folder](#).

2.2 Software Requirements

Refer to the following article on supported QTS versions for QNAP NAS

[FAQ: Ahsay Hardware Compatibility List \(HRL\) for AhsayOBM on QNAP NAS](#)

2.3 AhsayOBM Installation

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

2.4 NAS-QNAP Add-on Module

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

NOTE

The NAS-QNAP add-on module allows for the backup of unlimited number of QNAP NAS devices. However, each new AhsayOBM installation on a QNAP 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 profile. The 'Add-on Modules' section contains the following items:

Module Name	Checked
Microsoft Exchange Server	<input type="checkbox"/>
MySQL Database Server	<input type="checkbox"/>
Lotus Domino	<input type="checkbox"/>
Windows System Backup	<input type="checkbox"/>
VMware	<input type="checkbox"/>
Microsoft Exchange Mailbox	<input type="checkbox"/>
NAS - QNAP	<input checked="" type="checkbox"/>
Mobile (max. 10)	<input type="checkbox"/>
Volume Shadow Copy	<input type="checkbox"/>
OpenDirect / Granular Restore	<input type="checkbox"/>
MariaDB Database Server	<input type="checkbox"/>
Microsoft SQL Server	<input type="checkbox"/>
Oracle Database Server	<input type="checkbox"/>
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 type="checkbox"/>
Continuous Data Protection	<input type="checkbox"/>
In-File DeltaOnly apply to v8 or before	<input type="checkbox"/>
Office 365 Backup	<input type="checkbox"/>
Deduplication	<input checked="" 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 QNAP NAS device.

Please contact your backup service provider for more details.

2.6 Java Requirement

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

2.7 Memory Requirement

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

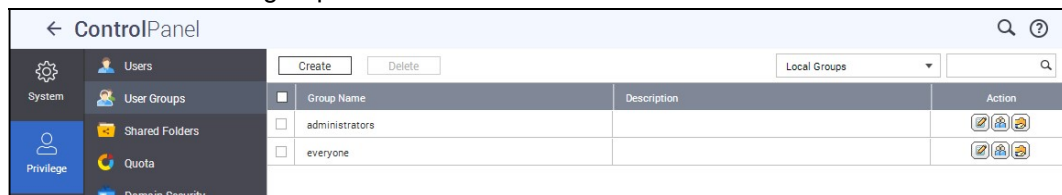
2.8 TCP Port Requirement

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

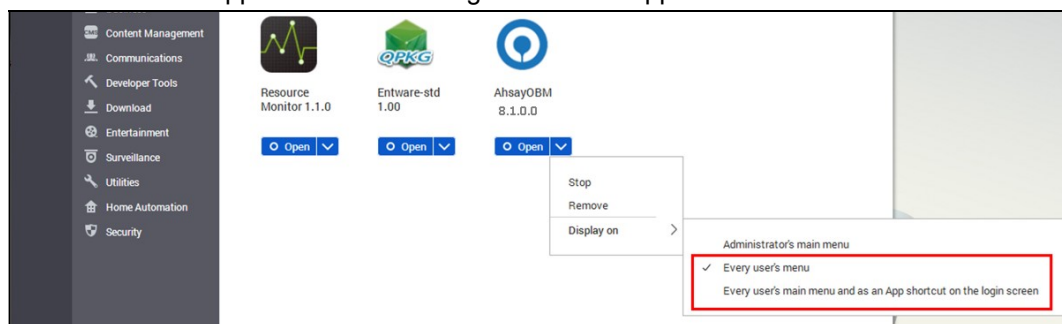
TCP port 32168 must be free on the machine. Otherwise, the AhsayOBM client will not start and its backup and/or restore functions will not work.

2.9 QNAP NAS User Account Permission

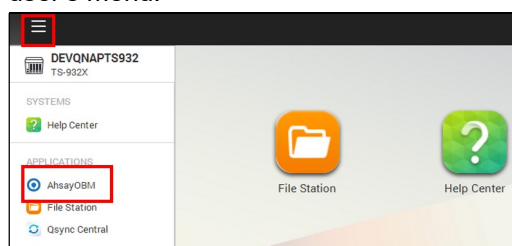
The QNAP NAS user account used for the AhsayOBM installation must be a member of “**administrator**” user group.



The QNAP NAS user account belongs to “**everyone**” user group can apply AhsayOBM after administrator assigning AhsayOBM to Display on “Every user’s menu” or “Every user’s main menu and as an App shortcut on the login screen” in App Center.



After login with user account belongs to “everyone” user group, you can find the App in the user’s menu.



2.10 Network Bandwidth

10 Mbps or above connection speed.

2.11 Limitations

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

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

2.12 Supported Features from AhsayCBS Web Console

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

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

3 Get started with AhsayOBM

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

Download and Install

Download and install AhsayOBM on your QNAP 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 **QNAP** section under the **AhsayOBM** tab of the download page, download the AhsayOBM **QPKG online installer**.

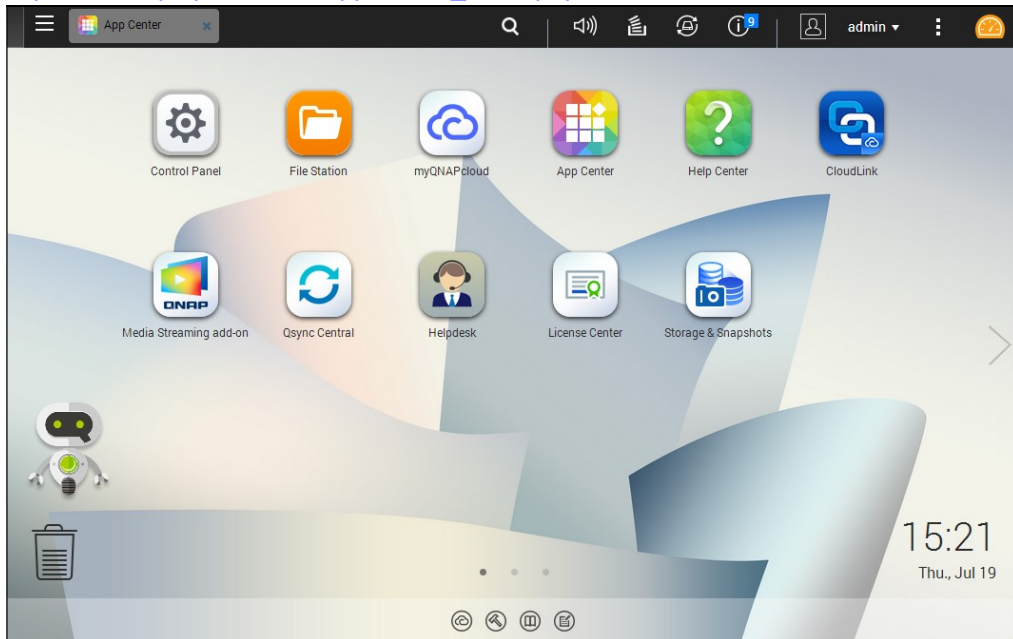


4.2 Install AhsayOBM using QPKG online installer

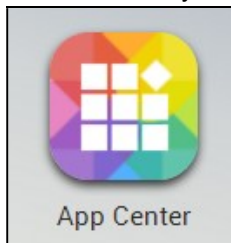
1. Log in to QNAP QTS with the admin account. In a web browser, enter the QNAP NAS device IP address and use the login credentials to login.

Note: Refer to the following user manual for information on how to login to QTS:

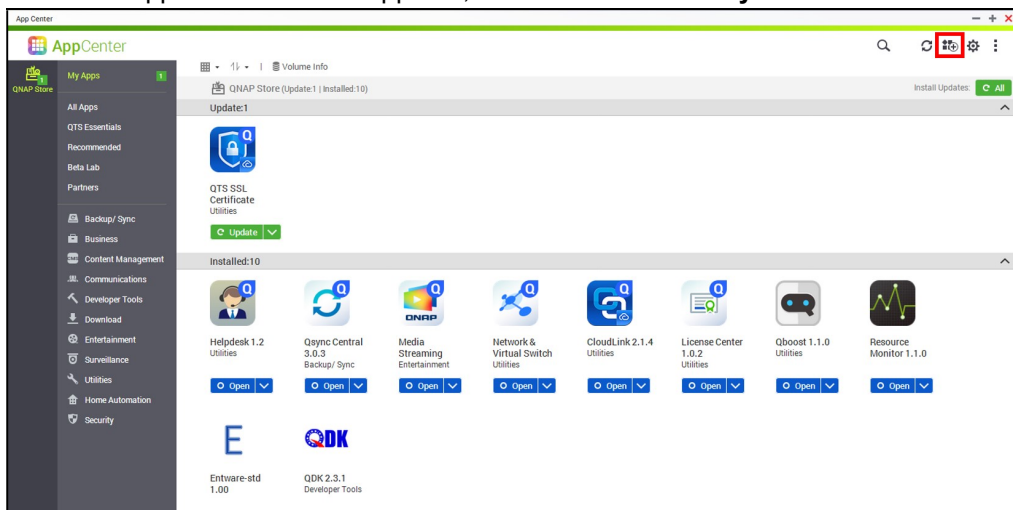
https://www.qnap.com/en/support/con_show.php?cid=11



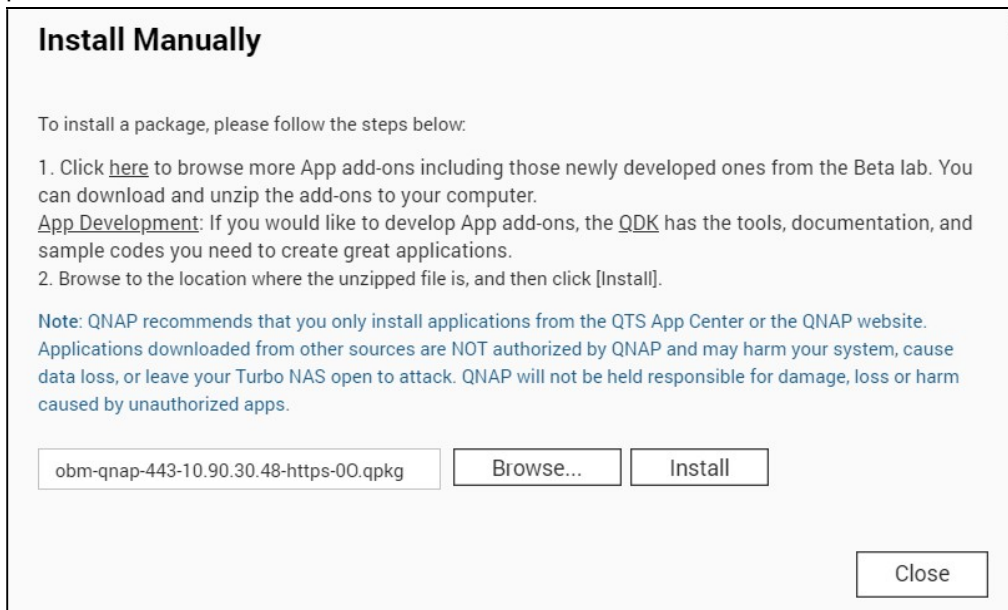
2. To install AhsayOBM on QNAP NAS, click the **App Center** icon from the desktop.



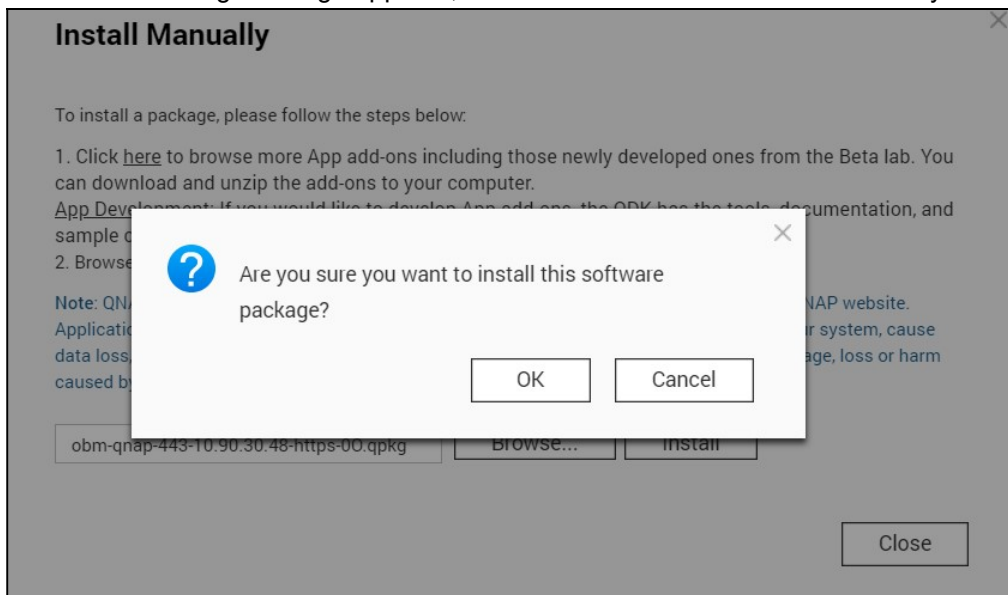
3. When the App Center window appears, select **Install Manually**.

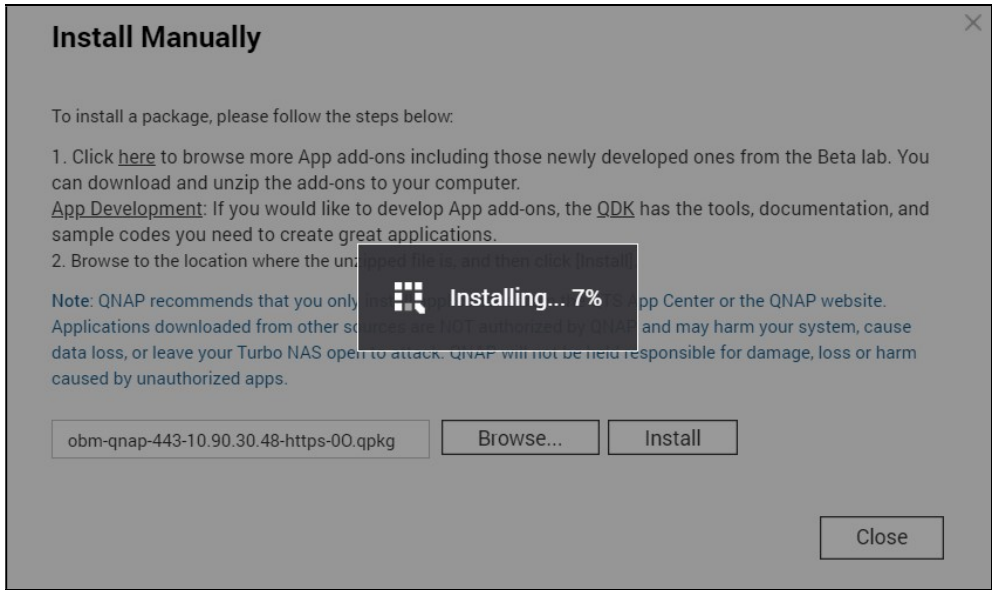


- When the Install Manually window appears, click **Browse** to select the AhsayOBM QPKG file which you have downloaded (e.g., obm-qnap-443-10.90.30.48-https-00). Then, click **Install** to proceed.

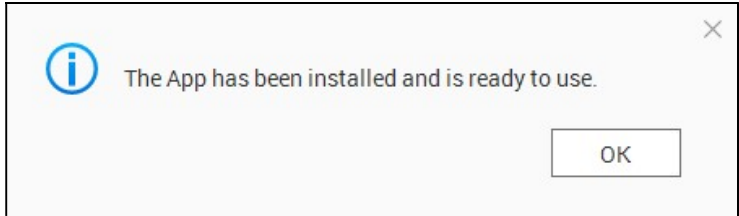


- When the following message appears, click **OK** to start the installation of AhsayOBM.

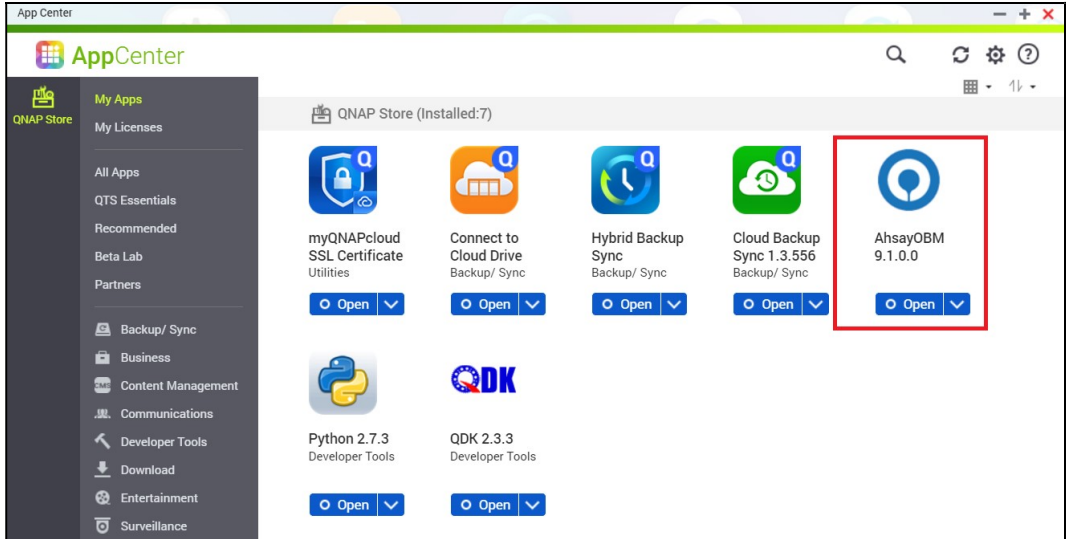


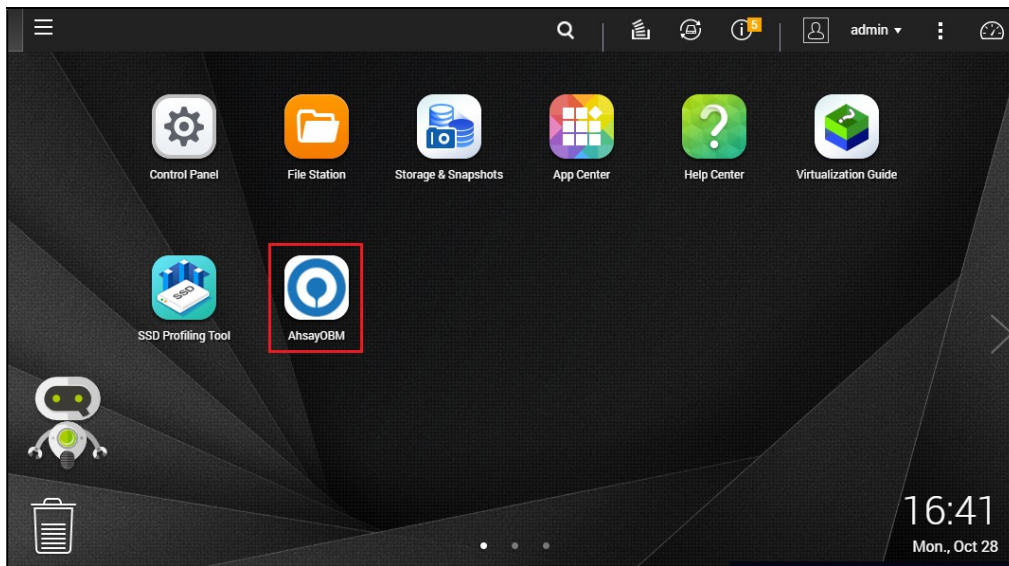


6. When the installation is completed, the following message will be displayed. Click **OK** to finish the installation.



7. After the installation, AhsayOBM will be listed in App Center and desktop.





4.3 AhsayOBM Scheduler Service Check

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

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

Scheduler service is running, highlighted in **red**.

```
login as: admin
admin@10.3.0.122's password:
[~] # ps -ef|grep java
3562 admin 640772 S
/share/CACHEDEV1_DATA/.qpkg/AhsayOBM/obm/jvm/bin/java
-Xrs -Xms64m -Xmx1024m -Dsun.nio.PageAlignDirectMemory=true -
Djava.library.path= . -cp ../cb.jar WuiService
/share/CACHEDEV1_DATA/.qpkg/AhsayOBM/obm /share/CACH
EDEV1_DATA/.qpkg/AhsayOBM/.obm --port=32168
11017 admin 956 S grep java
20327 admin 157000 S /share/CACHEDEV1_DATA/.qpkg/AhsayOBM/obm/jvm/bin/java
-Xms64m -Xmx256m -Dsun.nio.PageAlignDirectMemory=true -Djava.library.path=.
-cp ../cbs.jar cbs /share/CACHEDEV1_DATA/.qpkg/AhsayOBM/obm
```

To manually **stop** the scheduler service,

- First get the system volume path, use the **getcfg SHARE_DEF defVoIMP -f /etc/config/def_share.info** script
- Then use the **touch /%system volume path%/.qpkg/AhsayOBM/obm/ipc/Scheduler/stop** script
- Last, use the **ps** command to check if the scheduler is still running.

For example

```
[~] # getcfg SHARE_DEF defVolMP -f /etc/config/def_share.info
/share/CACHEDEV1_DATA
[~] # touch /share/CACHEDEV1_DATA/.qpkg/AhsayOBM/obm/ipc/Scheduler/stop
[~] # ps -ef|grep java
 3562 admin 640772 S
/share/CACHEDEV1_DATA/.qpkg/AhsayOBM/obm/jvm/bin/java -Xrs -Xms64m -
Xmx1024m -Dsun.nio.PageAlignDirectMemory=true -Djava.library.path=
. -cp ../cb.jar WuiService /share/CACHEDEV1_DATA/.qpkg/AhsayOBM/obm
/share/CACHEDEV1_DATA/.qpkg/AhsayOBM/.obm --port=32168
12542 admin 1000 S grep java
```

To manually **start** the scheduler service, use the

/%system volume path%/.qpkg/AhsayOBM/obm/bin/Scheduler.sh script and use the **ps** command again to check.

In our example, the scheduler service is running highlighted in **red**.

```
[~] # /share/CACHEDEV1_DATA/.qpkg/AhsayOBM/obm/bin/Scheduler.sh
[~] # ps -ef|grep java
 3562 admin 640772 S /share/CACHEDEV1_DATA/.qpkg/AhsayOBM/obm/jvm/bin/java
-Xrs -Xms64m -Xmx1024m -Dsun.nio.PageAlignDirectMemory=true -
Djava.library.path=. -cp ../cb.jar WuiService
/share/CACHEDEV1_DATA/.qpkg/AhsayOBM/obm
/share/CACHEDEV1_DATA/.qpkg/AhsayOBM/.obm --port=32168
17562 admin 86536 S /share/CACHEDEV1_DATA/.qpkg/AhsayOBM/obm/jvm/bin/java
-Xms64m -Xmx256m -Dsun.nio.PageAlignDirectMemory=true -
Djava.library.path=. -cp ../cbs.jar cbs
/share/CACHEDEV1_DATA/.qpkg/AhsayOBM/obm
18004 admin 944 R grep java
```

4.4 RunLevel Symlink Check

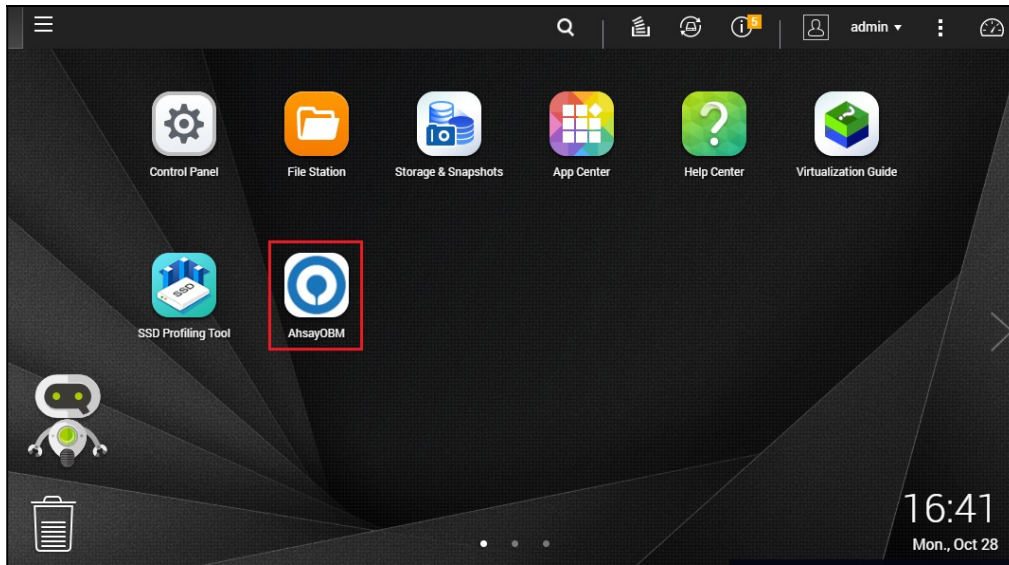
During installation, the following symlinks to the scheduler startup script **/%system volume path%/.qpkg/AhsayOBM/AhsayOBM.sh** will be created that allows the AhsayOBM Scheduler Service to automatically start each time the machine is rebooted or restarted.

To verify if the symlinks have been created correctly, use the **ls** command. You will see the symlink, highlighted in **red**.

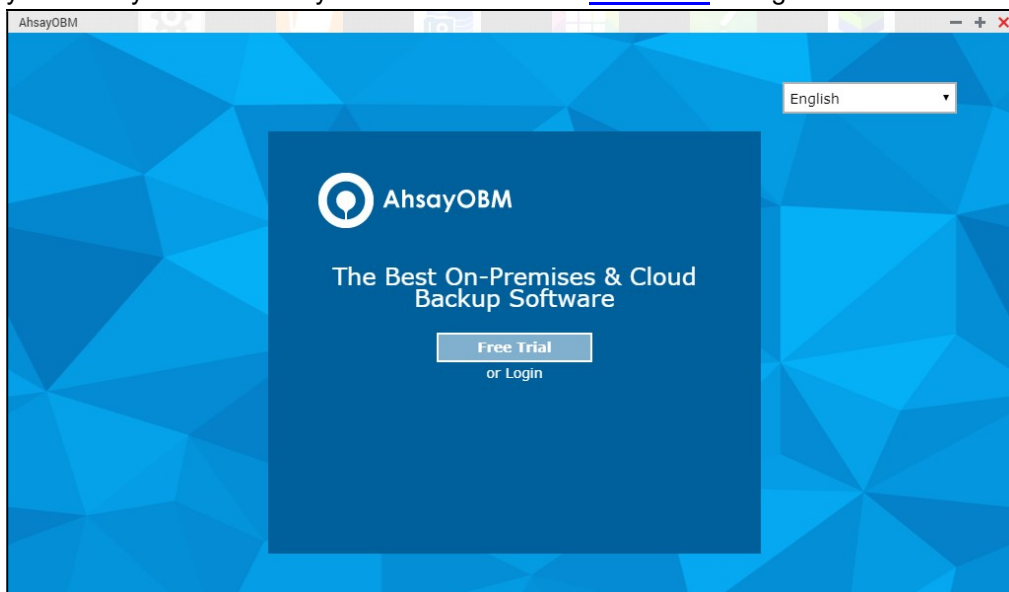
```
[~] # ls -la /etc/init.d/Ahsay*
lrwxrwxrwx 1 admin administrators 48 2019-05-23 12:55 /etc/init.d/AhsayOBM
.sh -> /share/CACHEDEV1_DATA/.qpkg/AhsayOBM/AhsayOBM.sh*
[~] #
```


5 Start AhsayOBM

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



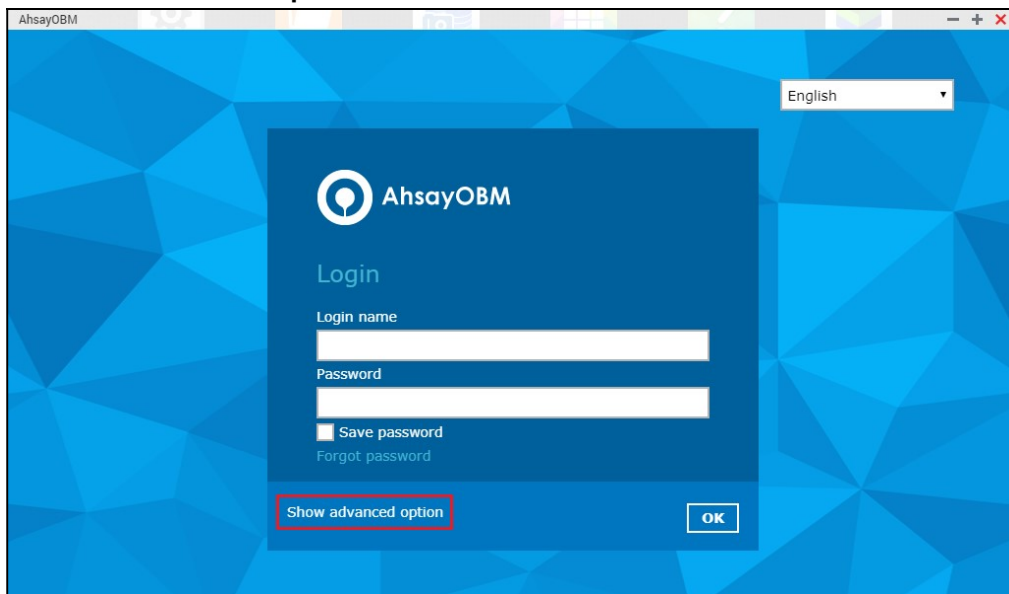
2. The Free Trial Registration menu may display when you login for the first time. Click **Login** if you already have an AhsayOBM account or click [Free Trial](#) to register for a trial backup account.



NOTE

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

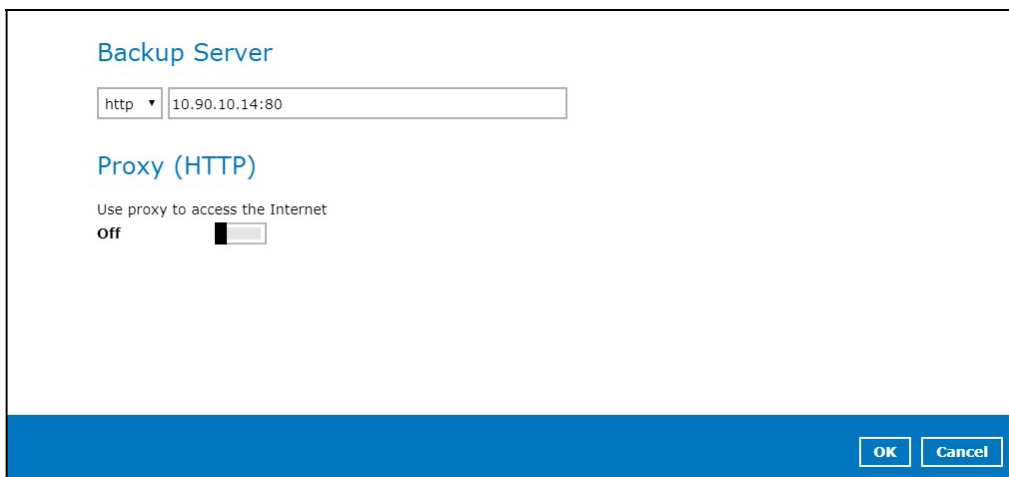
- In case you want to enter the backup server setting provided by your backup service provider, click **Show advanced option**.



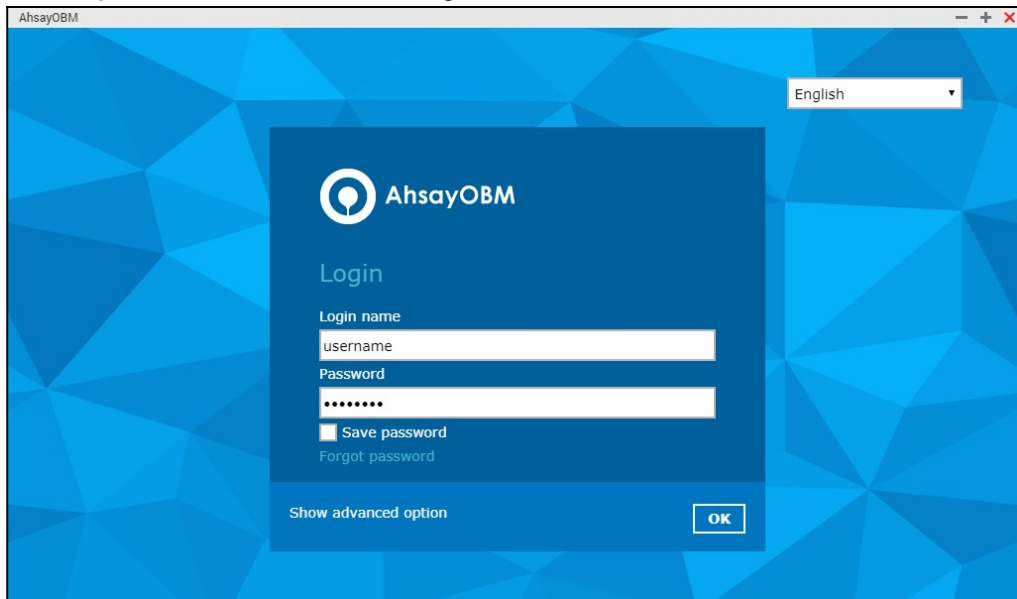
NOTE

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

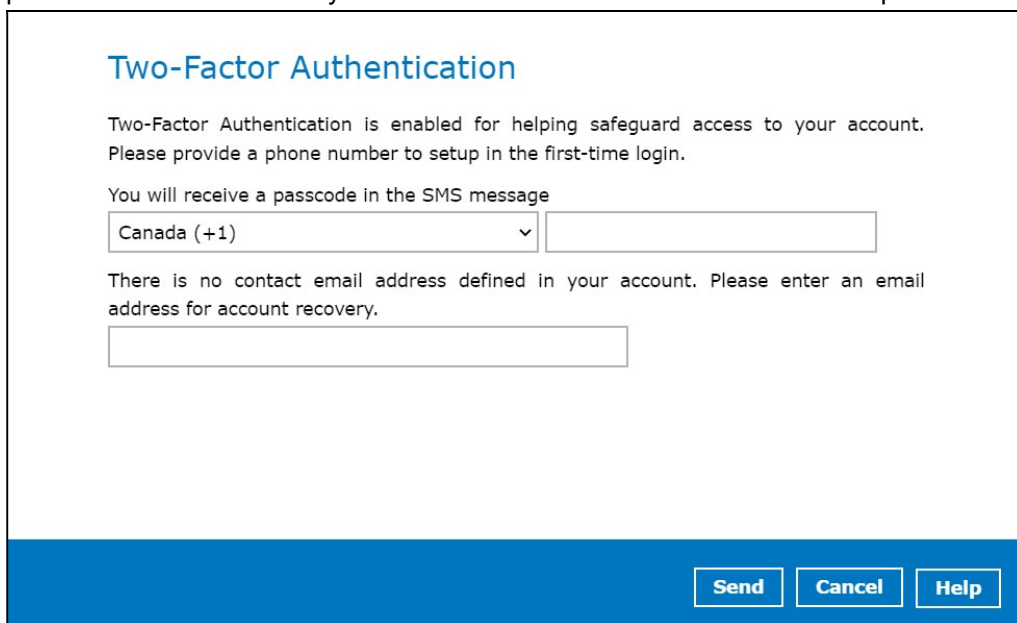
- Click **OK** after typing in the backup server information. You can turn on the Proxy feature if needed.



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



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






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

Two-Factor Authentication

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

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

-  **Philippines (+63) - *****36123**
-  **Austria (+43) - ****5814**
-  **Georgia (+995) - ****3685**

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

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

Two-Factor Authentication

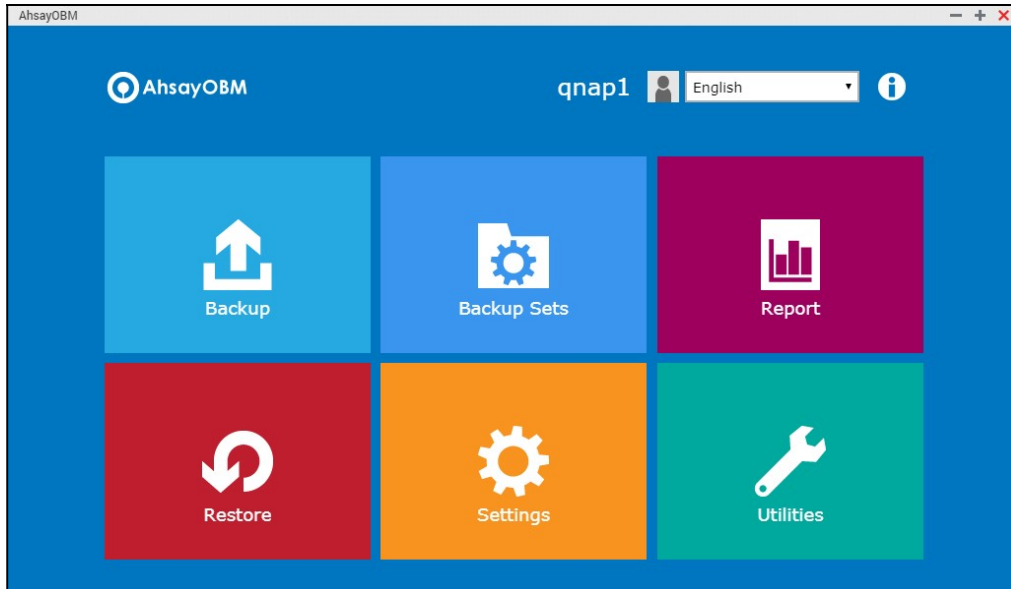
SMS message with a passcode was already sent to the phone number (+63) - *****36123 Please enter the passcode to continue login.

KKFZ - (00:04:52)

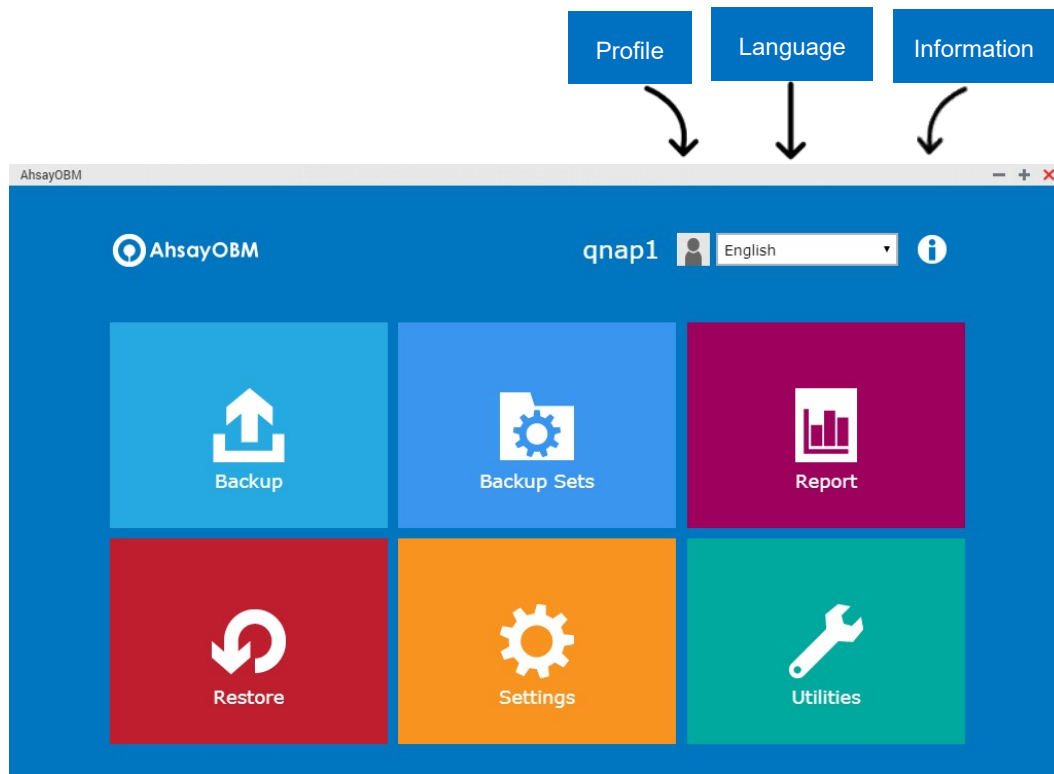
[Resend passcode](#)

[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.



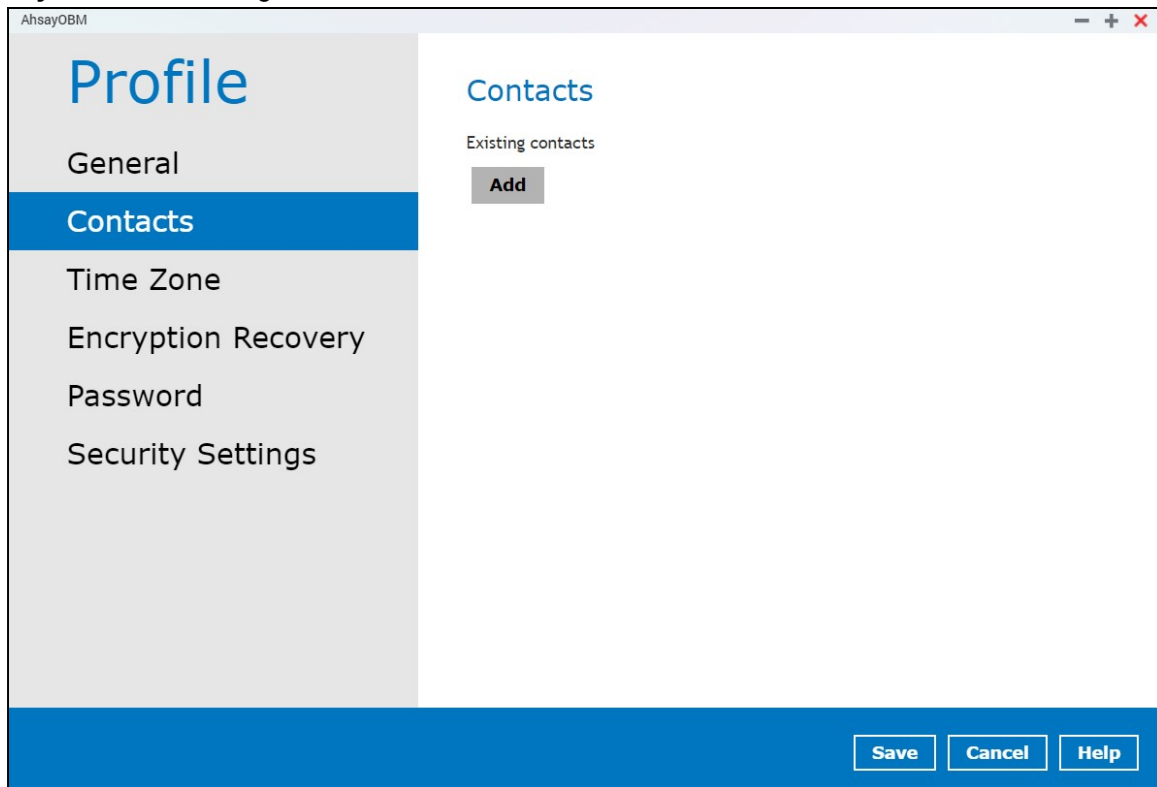
Profile has six (6) features:

- [General](#)
- [Contacts](#)
- [Time Zone](#)
- [Encryption Recovery](#)
- [Password](#)
- [Security Settings](#)

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

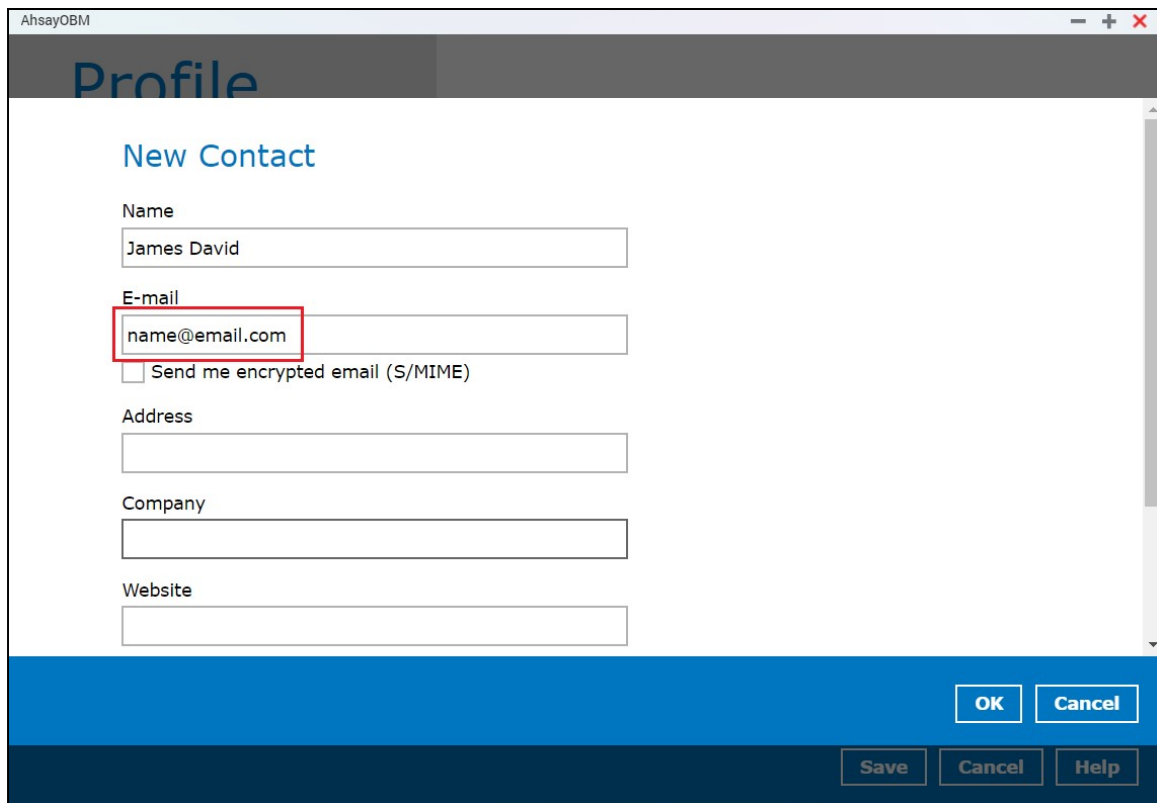
- The **Login name** is the name of your backup account.
- The **Display name** is the display name of your backup account as you log on to the AhsayCBS management console.
- The **Time** is the date and time the user last logged in.
- The **IP address** used to login.
- The **Phone number (MFA)** is where the sms authentication will be sent when 2FA is enabled.
- The **Browser / App** used to login to AhsayCBS User Web Console or AhsayOBM.

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.

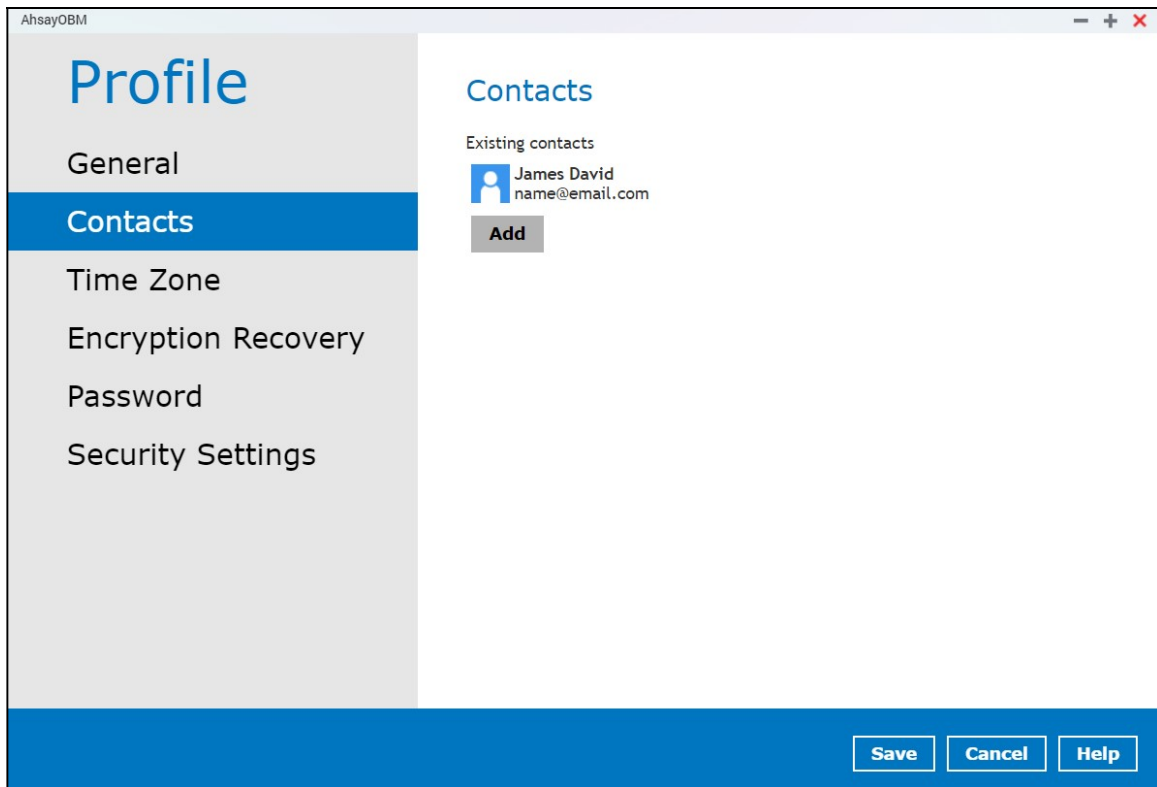


The screenshot shows the AhsayOBM Profile page. On the left is a navigation menu with options: General, Contacts (highlighted in blue), Time Zone, Encryption Recovery, Password, and Security Settings. The main content area is titled 'Contacts' and shows 'Existing contacts' with an 'Add' button. At the bottom right, there are 'Save', 'Cancel', and 'Help' buttons.

E-mail cannot be left blank.



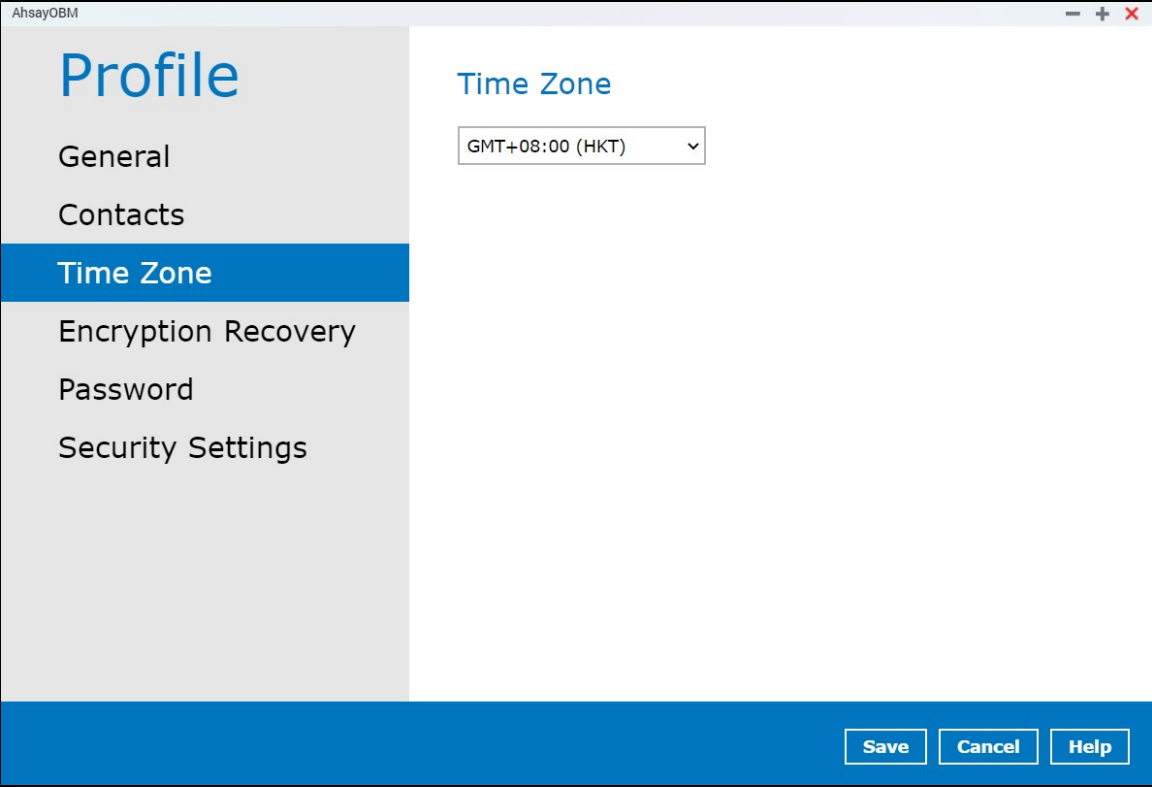
The screenshot shows the 'New Contact' form in the AhsayOBM Profile page. The form fields are: Name (filled with 'James David'), E-mail (filled with 'name@email.com' and highlighted with a red box), Address, Company, and Website. There is a checkbox for 'Send me encrypted email (S/MIME)'. At the bottom right, there are 'OK', 'Cancel', 'Save', and 'Help' buttons.



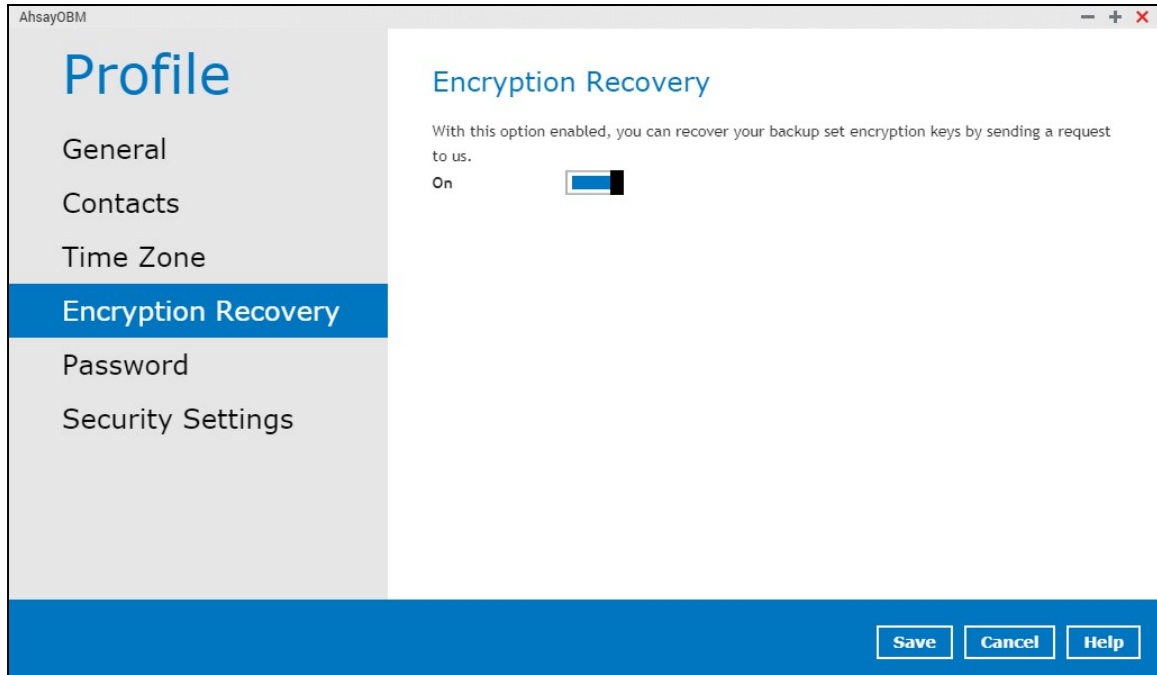
NOTE

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.



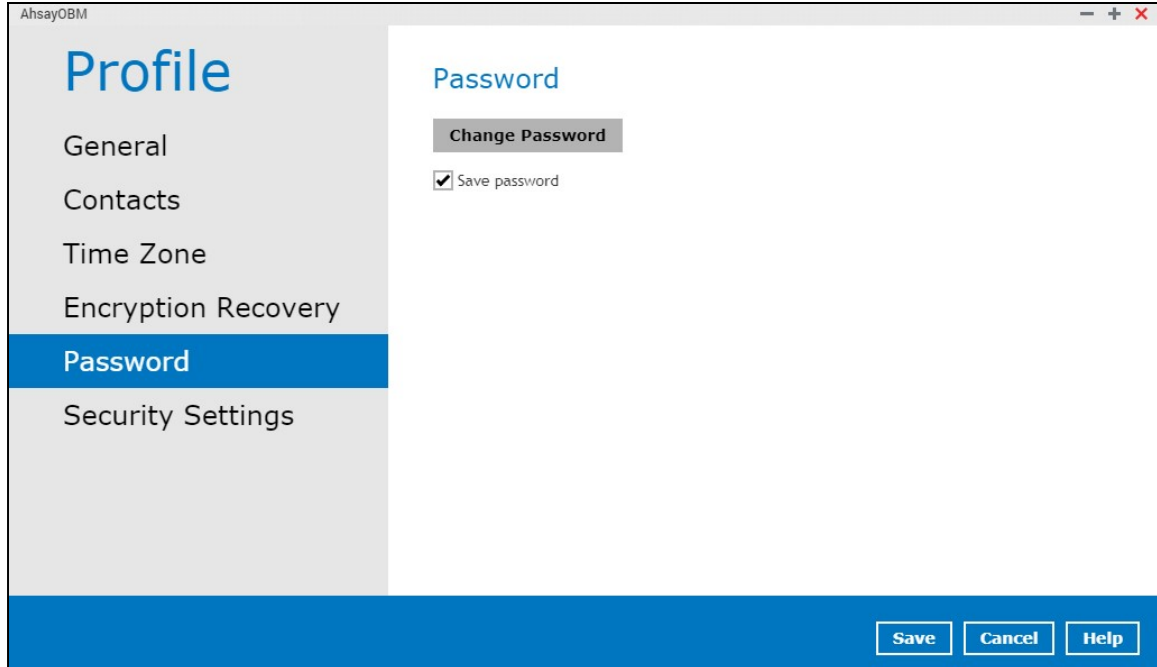
Backup set encryption key can be recovered by turning this feature on.



NOTE

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

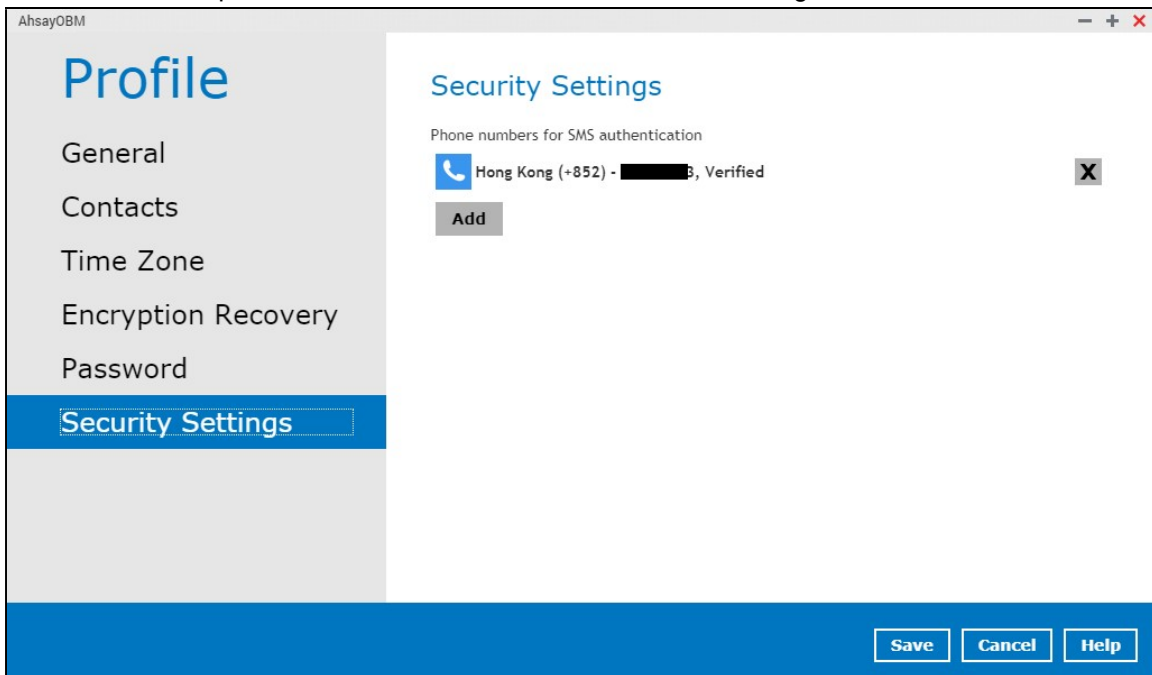
Login password can be modified anytime. You can also check the **Save password** box to bypass the password entry when opening the AhsayOBM interface.



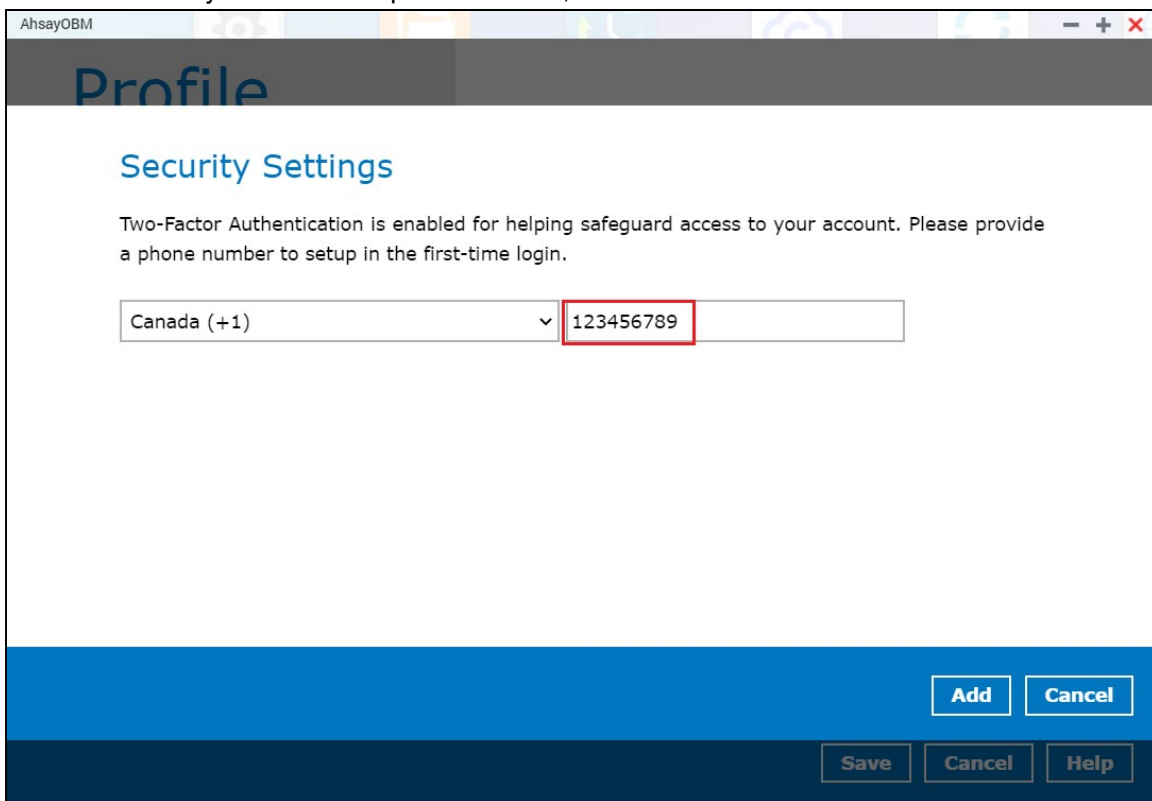
NOTE

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

Security Settings will only be visible if two-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.

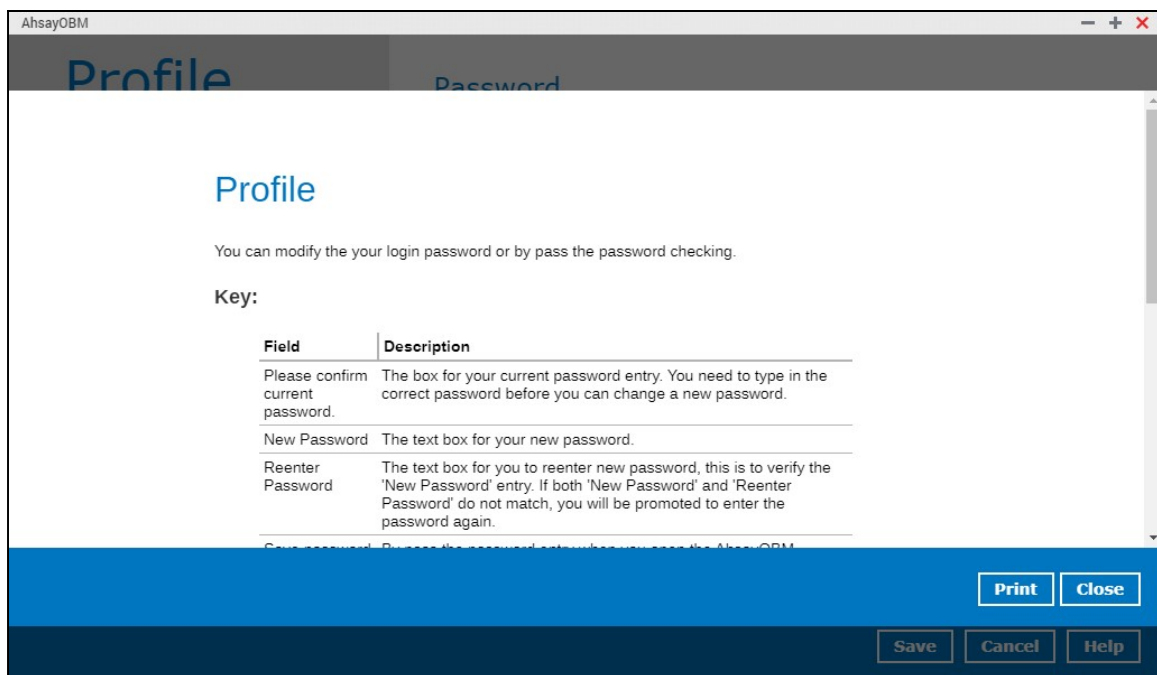
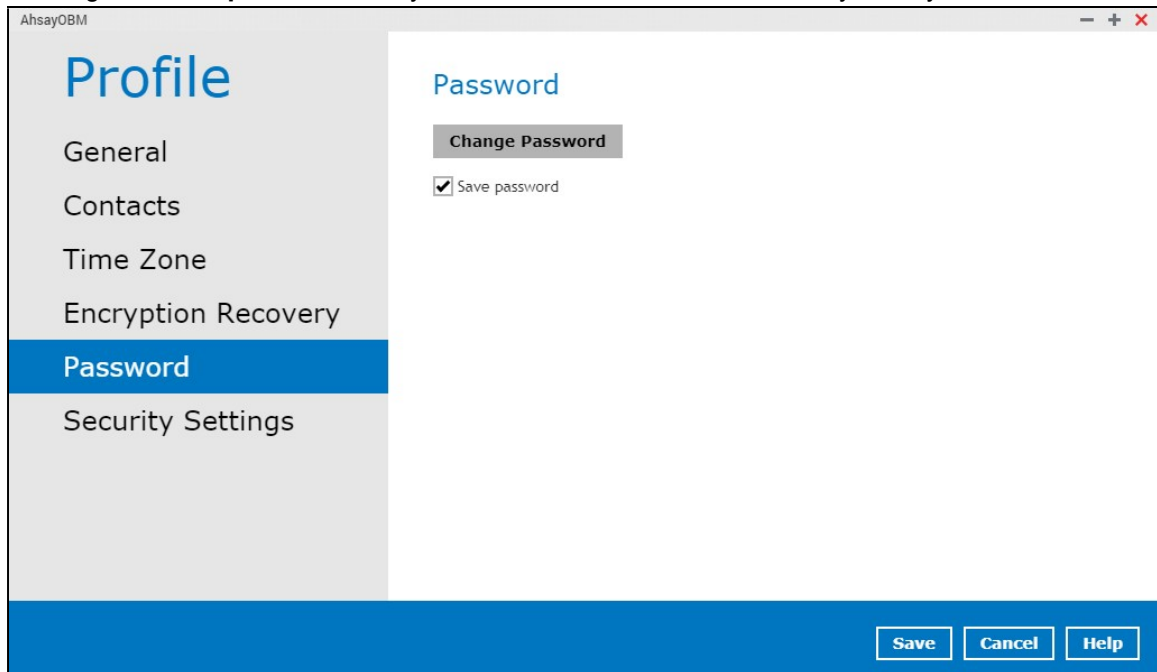


Select the country and enter the phone number, then click **Add**.



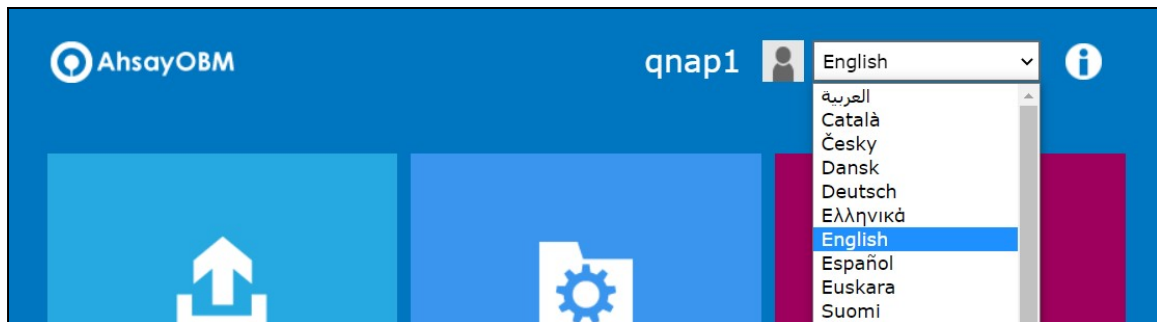
6.2 Online Help

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



6.3 Language

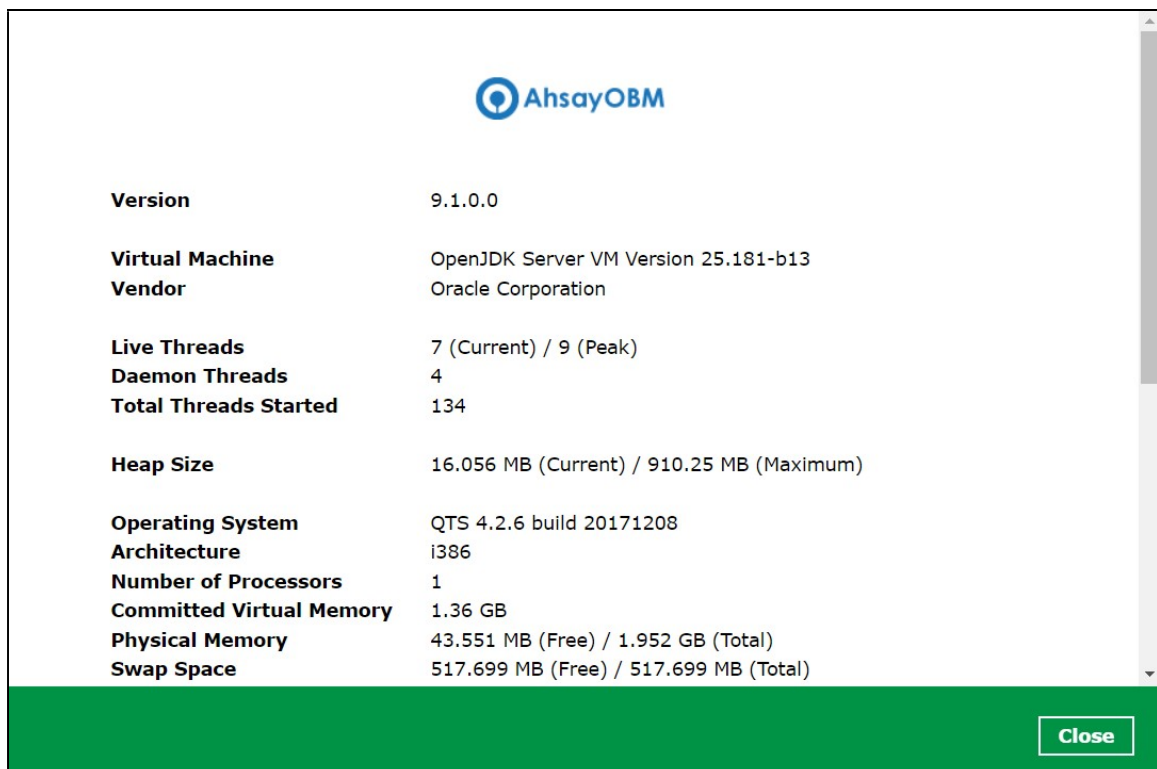
This option is used to change the language of the user interface. The list of available languages depends on the backup service provider.



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.

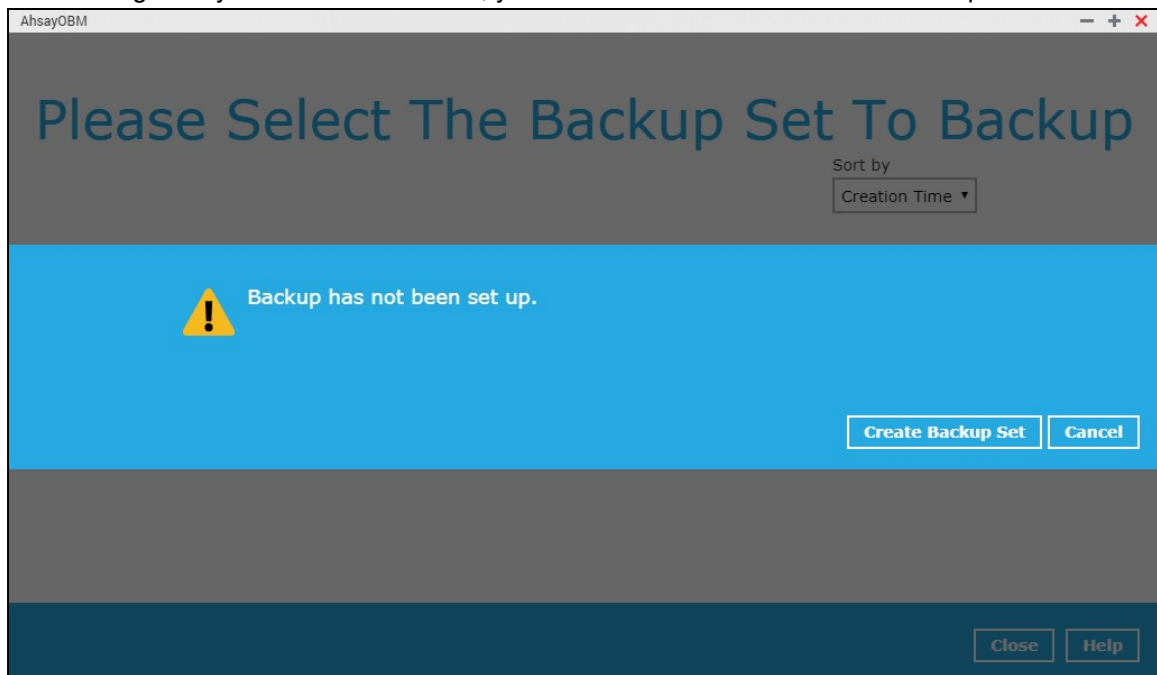


6.5 Backup

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.



For instructions on how to start a backup, refer to [Chapter 9 Run Backup Jobs](#).

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](#).

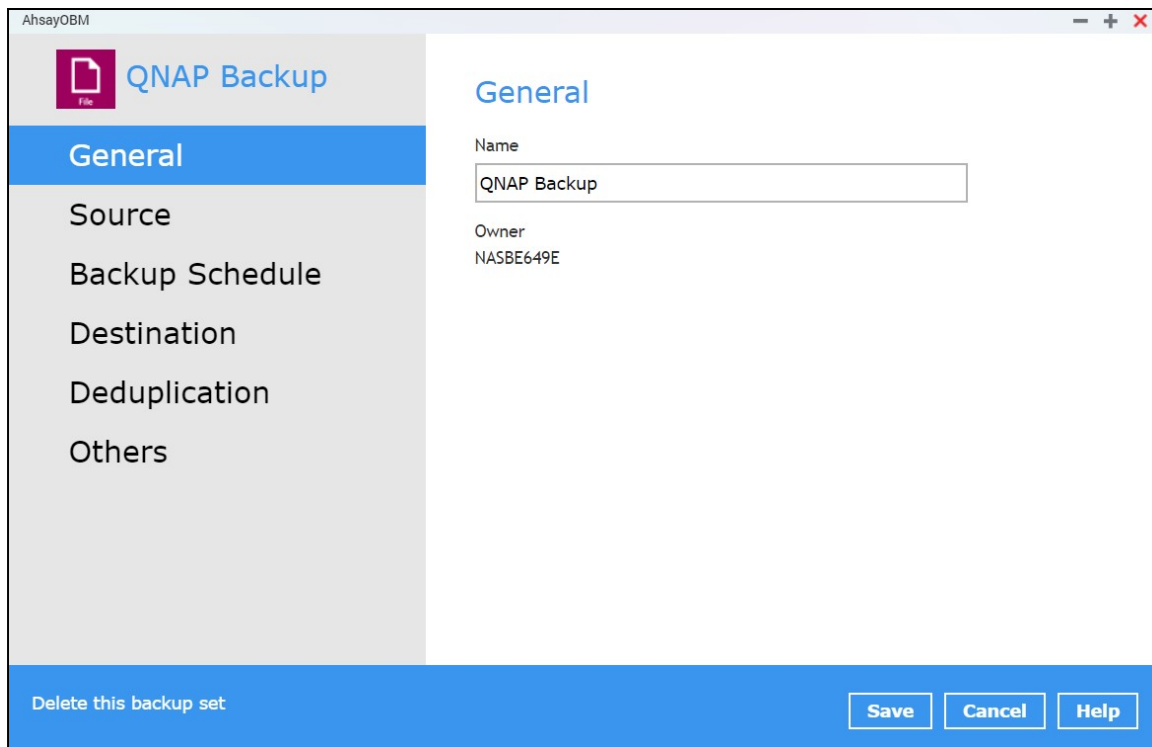
Backup Set Settings

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

- [General](#)
- [Source](#)
- [Backup Schedule](#)
- [Destination](#)
- [Deduplication](#)
- [Others](#)

General

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

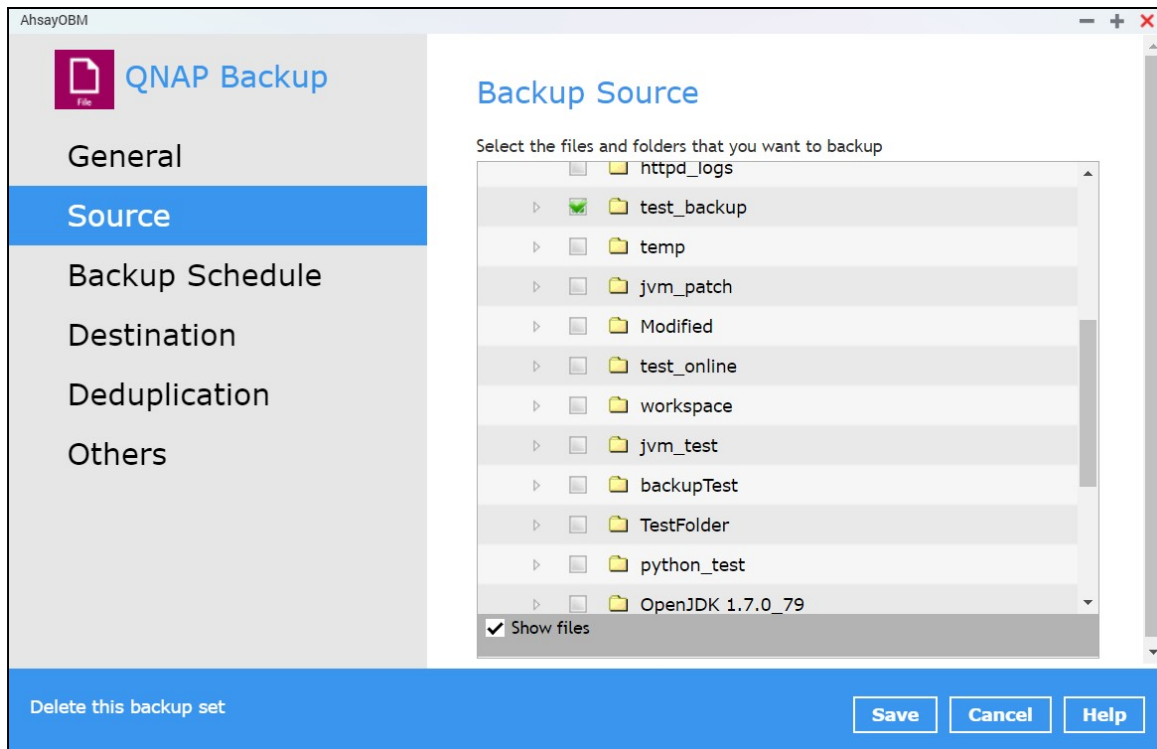


To modify the backup set name, follow the instructions below:

1. Select **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.

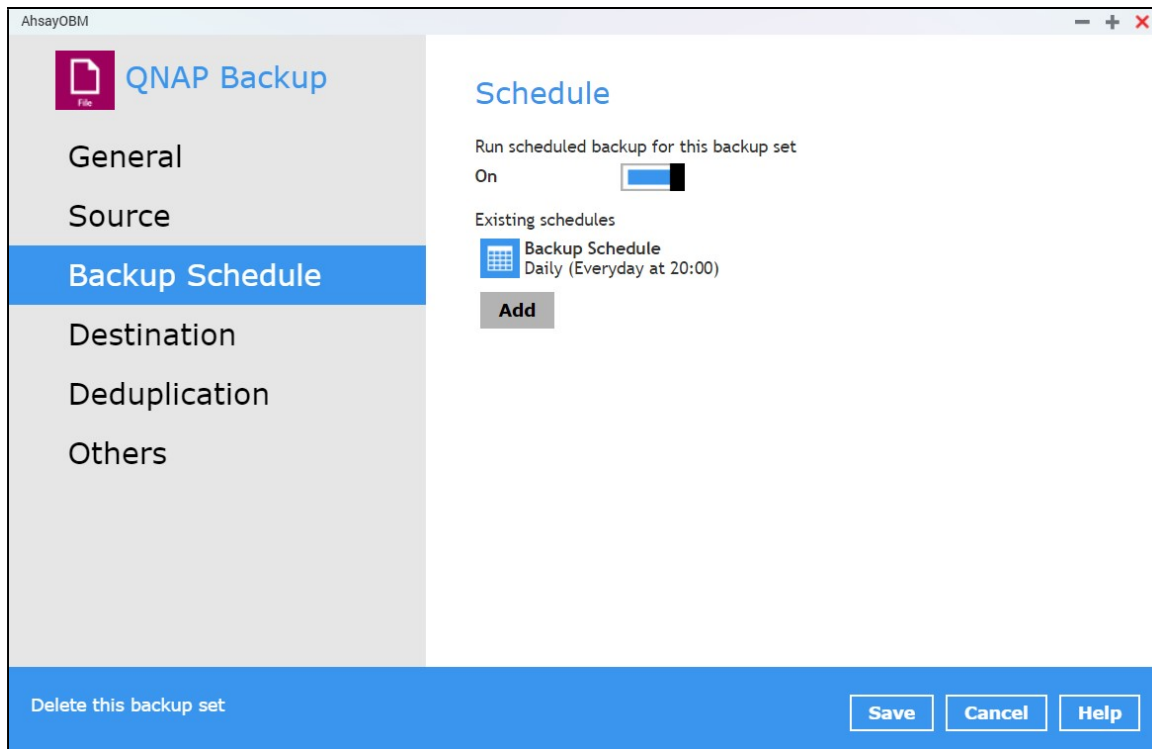


To add backup source, follow the instructions below:

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.

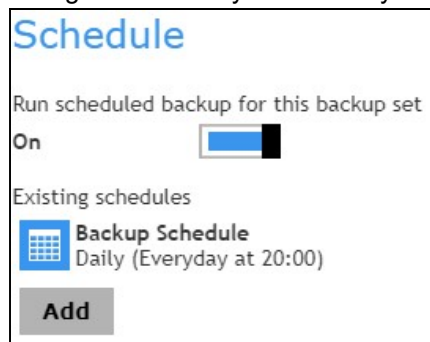
Backup Schedule

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

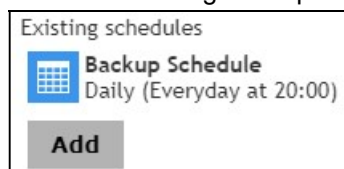


To configure a backup schedule, follow the steps below:

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.

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

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

New Backup Schedule

Name

Type

Backup on the following day every month
 Day
 Last

Start backup at
 : on the selected days

Stop

Run Retention Policy after backup

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

New 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.
- ⦿ **every** – this option will start a backup job in intervals of minutes or hours.

<p>Start backup <input type="button" value="every"/></p> <p>Stop <input type="button" value="until full backup completed"/></p> <p><input type="checkbox"/> Run Retention Policy after backup</p>	<p>1 minute 1 minute 2 minutes 3 minutes 4 minutes 5 minutes 6 minutes 10 minutes 12 minutes 15 minutes</p>	<p>Start backup <input type="button" value="every"/></p> <p>Stop <input type="button" value="until full backup completed"/></p> <p><input type="checkbox"/> Run Retention Policy after backup</p>	<p>1 minute 20 minutes 30 minutes 1 hour 2 hours 3 hours 4 hours 6 hours 8 hours 12 hours</p>
---	---	---	---

Here is an example of a backup set that has a periodic and normal backup schedule.

Figure 1.1

Figure 1.2

Figure 1.1 – Periodic backup schedule runs every 4 hours from Monday – Friday during business hours

Figure 1.2 – Normal backup schedule runs at 21:00 or 9:00 PM on Saturday and Sunday on weekend non-business hours

- **Stop** – the stop **time** of the backup job. This only applies to schedules with start backup “at” and is not supported for periodic backup schedule (start backup “every”)
- **until full backup completed** – this option will stop a backup job once it is complete. This is the configured stop time of the backup job by default.
- **after (defined no. of hrs.)** – this option will stop a backup job after a certain number of hours regardless of whether the backup job has completed or not. This can range from 1 to 24 hrs.

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

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

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

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

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

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





6. Multiple backup schedules can be created.

Schedule

Run scheduled backup for this backup set

On

Existing schedules

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

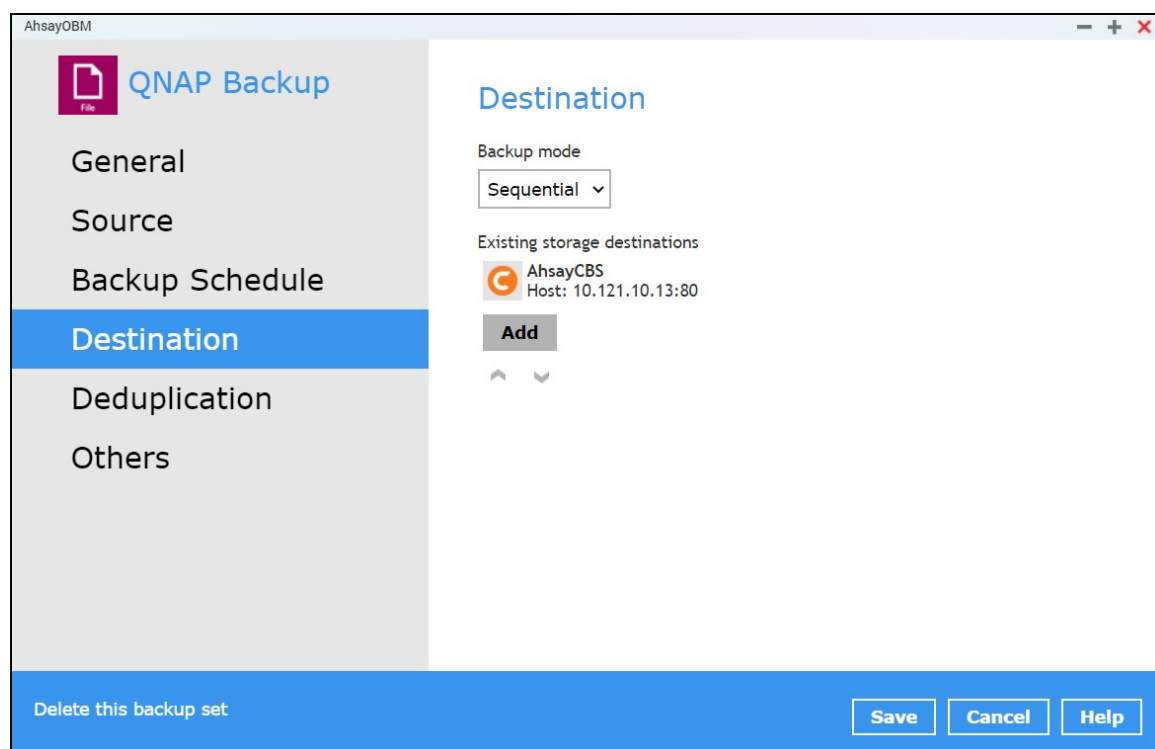
Add

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 storage destination(s). It also allows the user to add more storage destinations.



To add a destination, follow the instructions below:

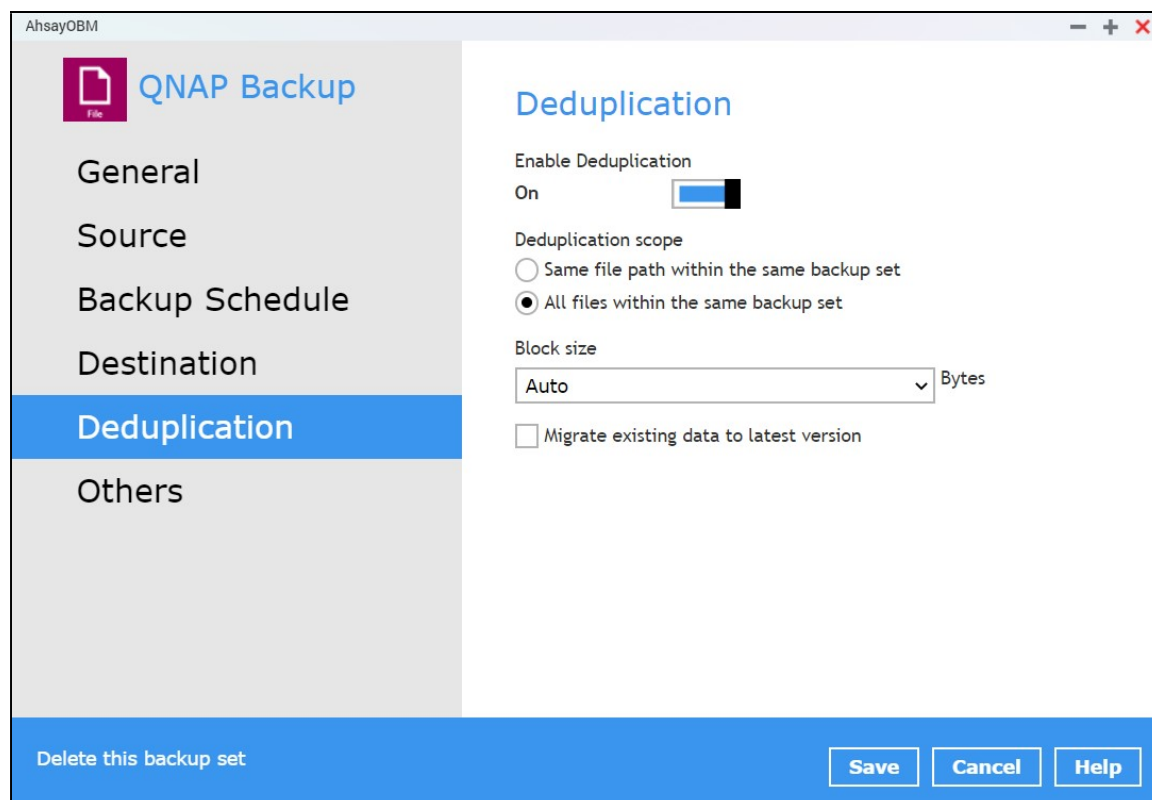
1. Select **Destination**.
2. Click the **Add** button.
3. Complete the following fields:
 - a. Name
 - b. Destination Storage
4. Click the **OK** button to add the new schedule.
5. Click the **Save** button to save the changes made.

Deduplication

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

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

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



There are two types of deduplication scope:

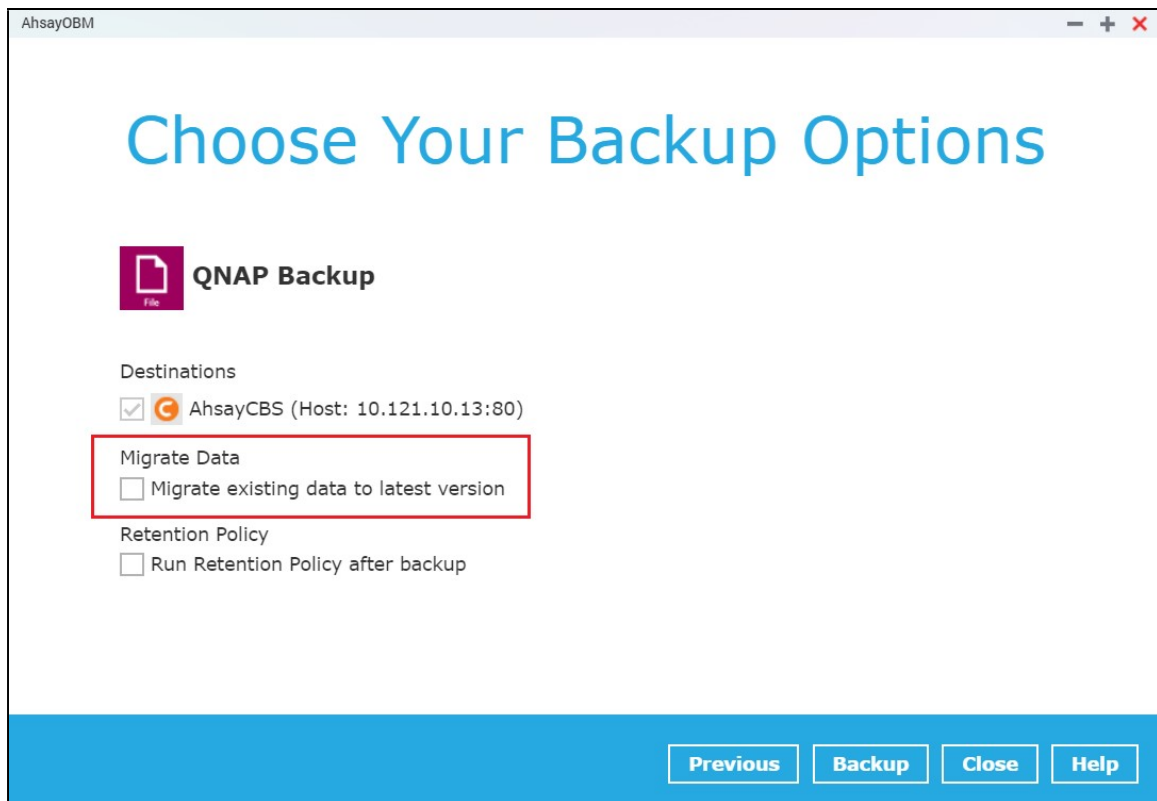
- ▶ Same file path within the same backup set – deduplication will be applied to the contents within a file during the current backup job.
- ▶ All files within the same backup set – deduplication will be applied across the different files in the backup set.

NOTE

For more details about the **Deduplication** feature, refer to the [AhsayCBS v9 New Features Supplemental document](#).

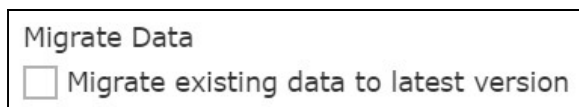
When the Deduplication feature is enabled for the backup set, a **Migrate Data** option will be available in the advanced backup options which can be configured before starting a backup job.

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



Migrate Data

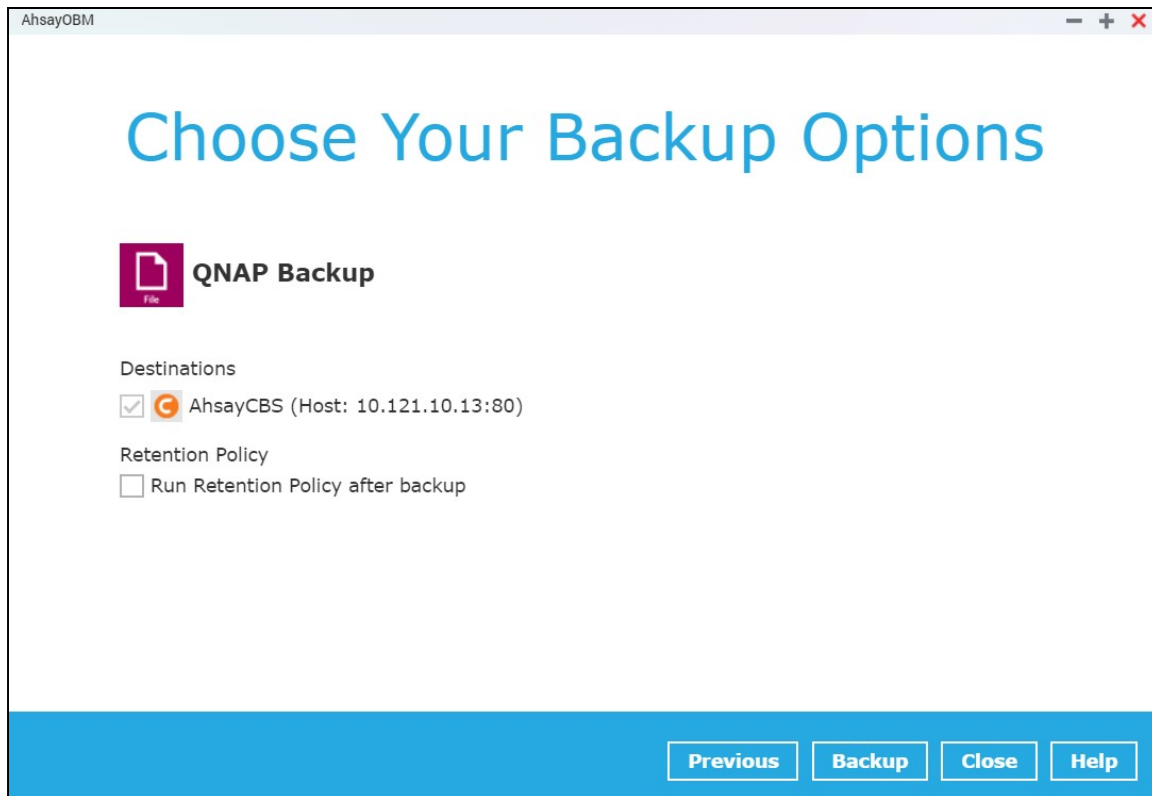
When this option is enabled, the existing data will be migrated to the latest version during a backup job. This option is disabled by default.



NOTE

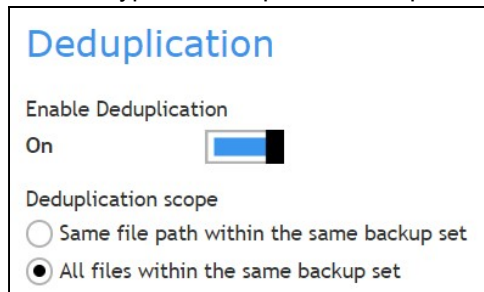
In case the Deduplication setting is **Off (disabled)** for the backup set, the Migrate Data option will not be displayed.

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

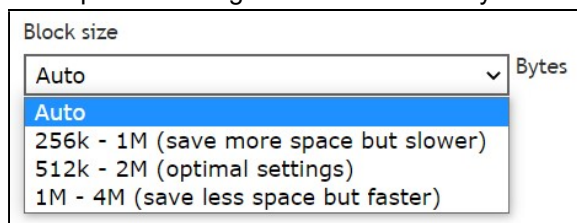


To configure the Deduplication settings, follow the steps below:

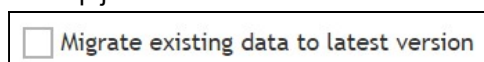
1. Select a type of Deduplication scope.



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



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

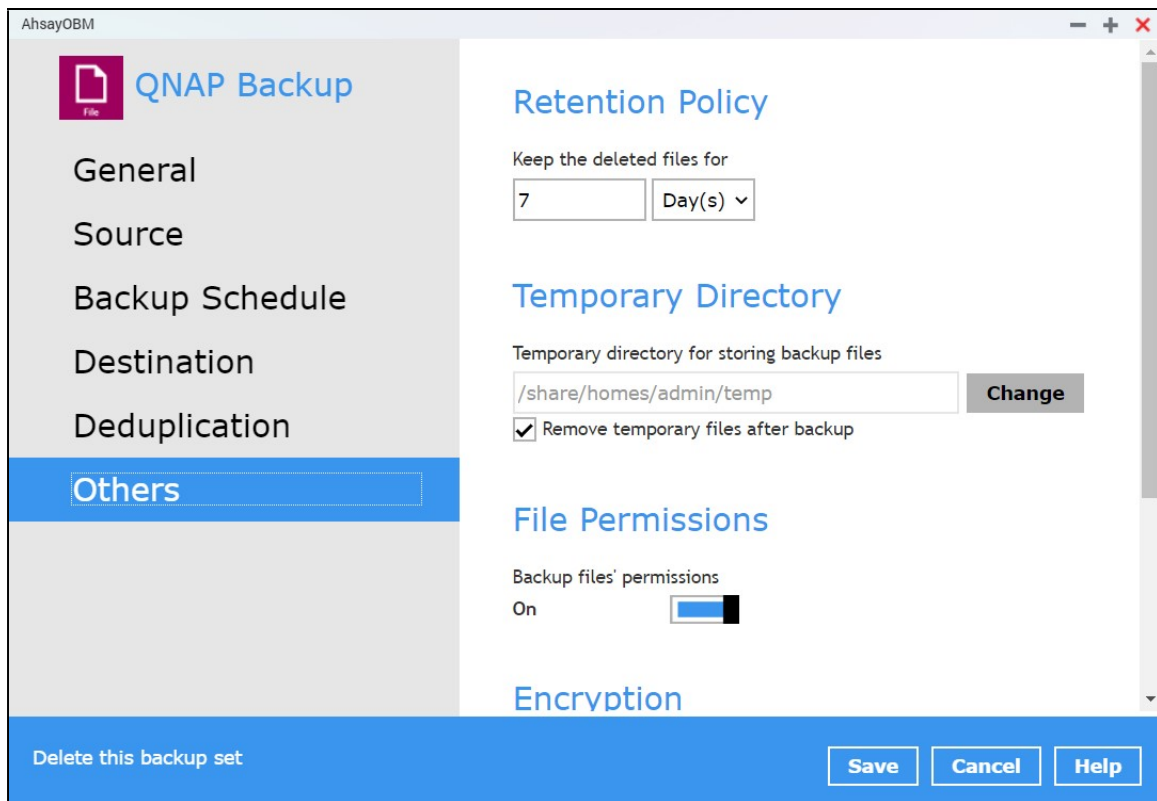


4. Click the **Save** button to store the modified Deduplication settings.

Others

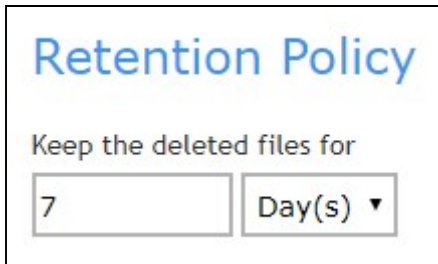
These are the list of other backup set settings that can be configured.

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



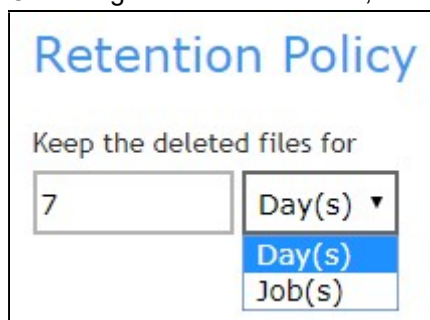
Retention Policy

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:

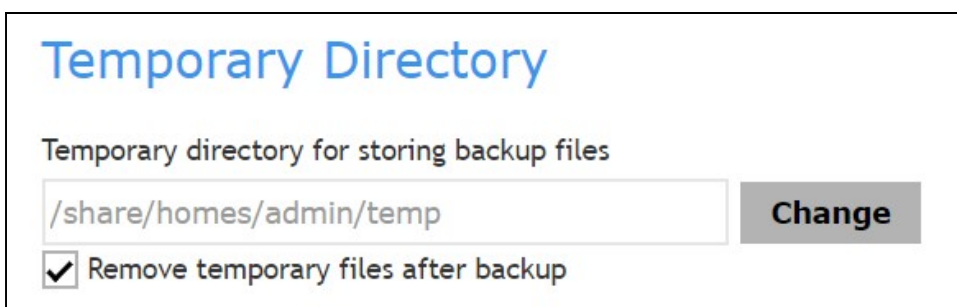
1. Select **Others**.
2. On the right side of the screen, select from the two (2) options: Day(s) or Job(s).



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.

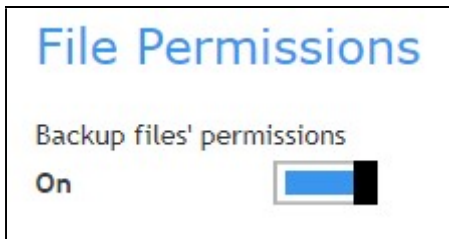


To configure the temporary directory, follow the instructions below:

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) functions that are 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:

- Date Range
- Backup set
- Destination
- Status

The screenshot shows the AhsayOBM interface. On the left is a sidebar with a "Report" header and two menu items: "Backup" (highlighted in purple) and "Restore". The main content area is titled "Backup Report" and features a date range filter set to "From 10 Jan 2022 To 17 Jan 2022" with a "Go" button. Below the filter is a table with columns for "Backup set", "Destination", "Completion", and "Status".

Backup set	Destination	Completion	Status
Q NAP Backup	AhsayCBS	Today 09:40	Completed
Backup Set 1	AhsayCBS	Today 09:11	Interrupted
Backup Set 1	AhsayCBS	Today 08:51	Interrupted
Q NAP Backup	AhsayCBS	Today 08:23	Completed

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

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

Backup Report

From 10 Jan 2022 To 17 Jan 2022 **Go**

Backup set	Destination	Completion	Status
QNAP Backup	AhsayCBS	Today 09:40	Completed
Backup Set 1	AhsayCBS	Today 09:11	Interrupted
Backup Set 1	AhsayCBS	Today 08:51	Interrupted
QNAP Backup	AhsayCBS	Today 08:23	Completed

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

Backup Report

From 10 Jan 2022 To 17 Jan 2022 **Go**

Backup set Destination Completion Status

Backup Set 1	AhsayCBS	Today 09:11	Interrupted
Backup Set 1	AhsayCBS	Today 08:51	Interrupted
QNAP Backup	AhsayCBS	Today 09:40	Completed
QNAP Backup	AhsayCBS	Today 08:23	Completed

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

Backup Report

From To

Backup set	Destination	Completion	Status
Backup Set 1	AhsayCBS	Today 09:11	Interrupted
Backup Set 1	AhsayCBS	Today 08:51	Interrupted
QNAP Backup	AhsayCBS	Today 09:40	Completed
QNAP Backup	AhsayCBS	Today 08:23	Completed

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

Backup Report

From To

Backup set	Destination	Completion	Status
QNAP Backup	AhsayCBS	Today 09:40	Completed
QNAP Backup	AhsayCBS	Today 08:23	Completed
Backup Set 1	AhsayCBS	Today 09:11	Interrupted
Backup Set 1	AhsayCBS	Today 08:51	Interrupted

To view a backup report in detail, choose a specific backup set.

The screenshot shows the AhsayOBM Backup Report interface. On the left, there is a navigation menu with 'Report', 'Backup', and 'Restore' options. The main area is titled 'Backup Report' and features a date range selector (From: 10 Jan 2022, To: 17 Jan 2022) and a 'Go' button. Below this is a table listing backup sets with columns for Backup set, Destination, Completion, and Status.

Backup set	Destination	Completion	Status
Q NAP Backup	AhsayCBS	Today 09:40	Completed
Backup Set 1	AhsayCBS	Today 09:11	Interrupted
Backup Set 1	AhsayCBS	Today 08:51	Interrupted
Q NAP Backup	AhsayCBS	Today 08:23	Completed

At the bottom right, there are 'Close' and 'Help' buttons.

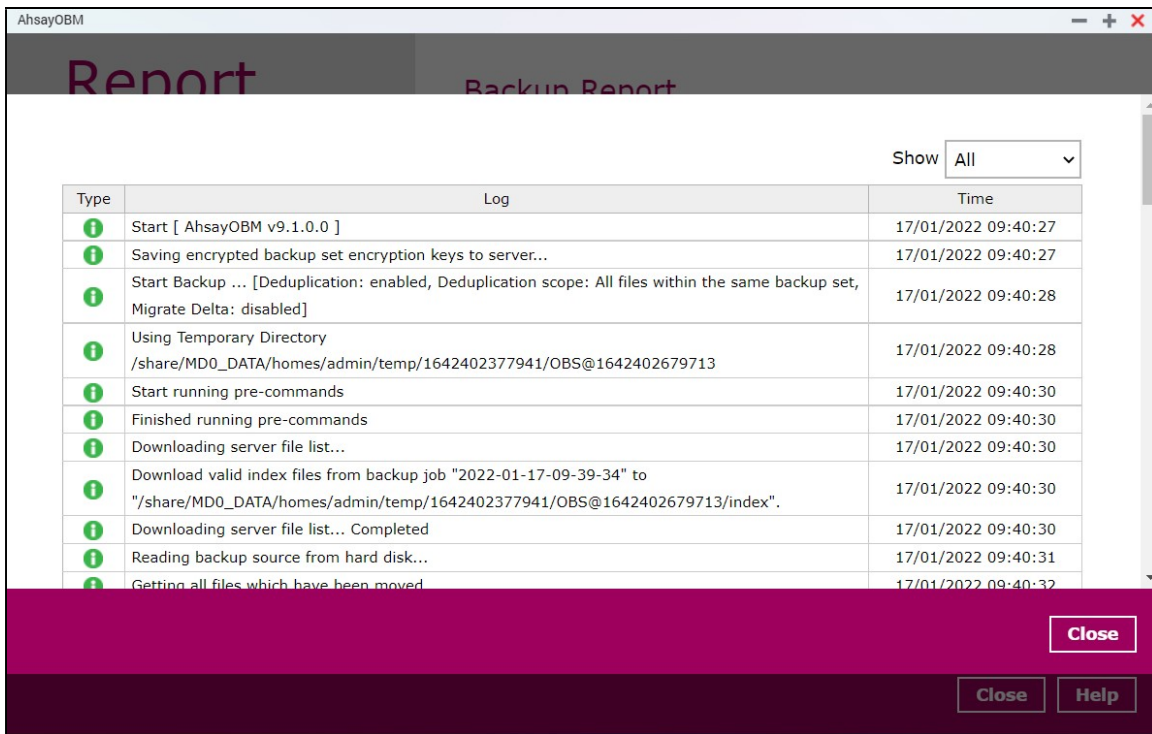
Click **View log** to show the event log during a backup.

The screenshot shows the AhsayOBM Backup Report interface with detailed information for a specific backup set. The left navigation menu is the same. The main area is titled 'Backup Report' and displays the following details for the 'Q NAP Backup' set:

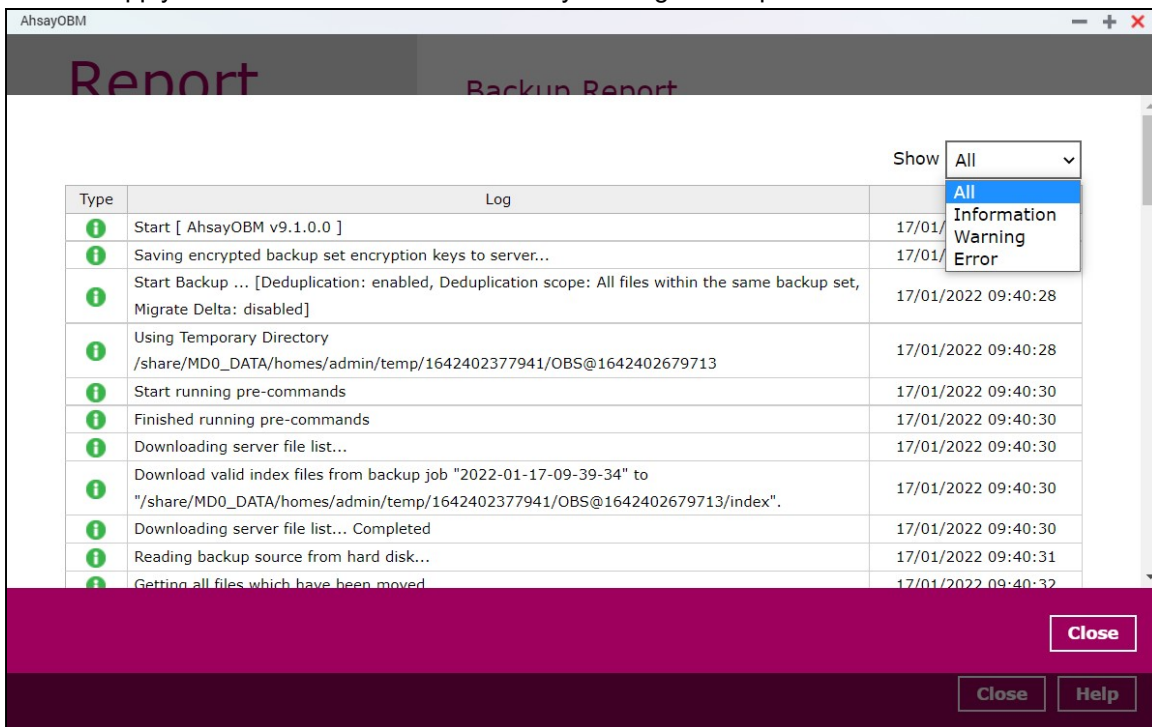
- Backup set: Q NAP Backup
- Destination: AhsayCBS
- Job: 17/01/2022 09:40
- Time: Today 09:40 - 09:40 (GMT)
- Status: ✓ Completed successfully
- New files *: 12 [38.9 MB / 38.9 MB (0%)]
- Updated files *: 0
- Updated access permissions *: 0
- Moved files *: 0
- Deleted files *: 0

A note at the bottom states: * Unit = No of files [Total zipped size / Total unzipped size (compression ratio)]

At the bottom, there are 'View log' and 'Close' buttons. At the bottom right of the window, there are 'Close' and 'Help' buttons.



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



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

The screenshot shows a web application window titled "AhsayOBM" displaying a "Backup Report". The report is a table with the following data:

File Name	Percentage	Timestamp
[New File]... 20% of "/share/MD0_DATA/test_backup/volume1/photo/(Google DRA Restore copy) Copy of IMG_8304.JPG"	20%	17/01/2022 09:40:33
[New File]... 10% of "/share/MD0_DATA/test_backup/volume1/photo/(Google Dest Pool Restore copy) Copy of IMG_8304.JPG"	10%	17/01/2022 09:40:33
[New File]... 30% of "/share/MD0_DATA/test_backup/volume1/photo/(Google DRA Restore copy) Copy of IMG_8304.JPG"	30%	17/01/2022 09:40:33
[New File]... 20% of "/share/MD0_DATA/test_backup/volume1/photo/(Google Dest Pool Restore copy) Copy of IMG_8304.JPG"	20%	17/01/2022 09:40:33
[New File]... 40% of "/share/MD0_DATA/test_backup/volume1/photo/(Google DRA Restore copy) Copy of IMG_8304.JPG"	40%	17/01/2022 09:40:33
[New File]... 30% of "/share/MD0_DATA/test_backup/volume1/photo/(Google Dest Pool Restore copy) Copy of IMG_8304.JPG"	30%	17/01/2022 09:40:33
[New File]... 50% of "/share/MD0_DATA/test_backup/volume1/photo/(Google DRA Restore copy) Copy of IMG_8304.JPG"	50%	17/01/2022 09:40:33
[New File]... 40% of "/share/MD0_DATA/test_backup/volume1/photo/(Google Dest Pool Restore copy) Copy of IMG_8304.JPG"	40%	17/01/2022 09:40:33

Below the table, there is a "Logs per page" dropdown menu with the following options: 50, 100, 200, 500, 1000. The "50" option is currently selected. To the right of the dropdown are navigation buttons: "Previous", "1", "2", "3", and "Next". At the bottom right of the window, there are "Close" and "Help" buttons.

6.7.2 Restore

This feature is used for viewing restore report(s). You can also apply filter on **Date Range**, **Backup set**, **Destination** and **Status** here.

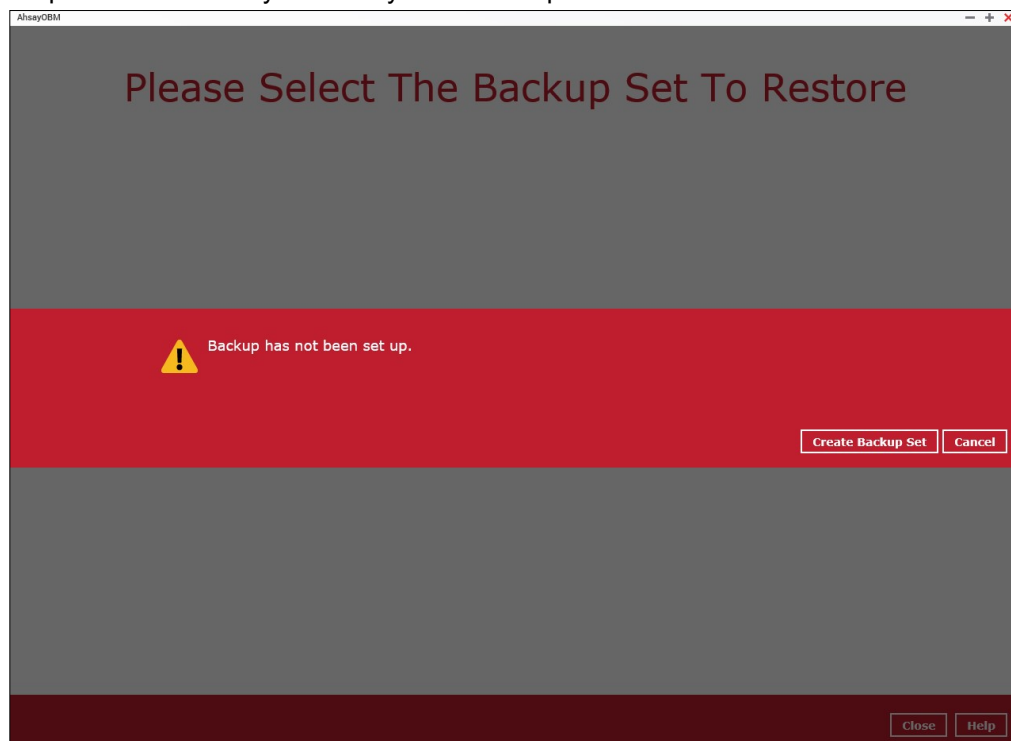
Backup set	Destination	Job	Status
QNAP Backup	AhsayCBS	Today 08:46	Completed
QNAP Backup	AhsayCBS	Today 08:45	Failed

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.



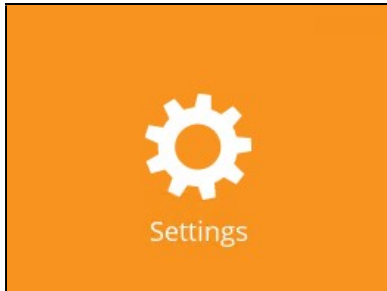
If using AhsayOBM for the first time, you will be asked to create a backup set first. A restore cannot be performed unless you already run a backup.



For instructions on how to perform a restore, refer to [Chapter 10 Restore Data](#).

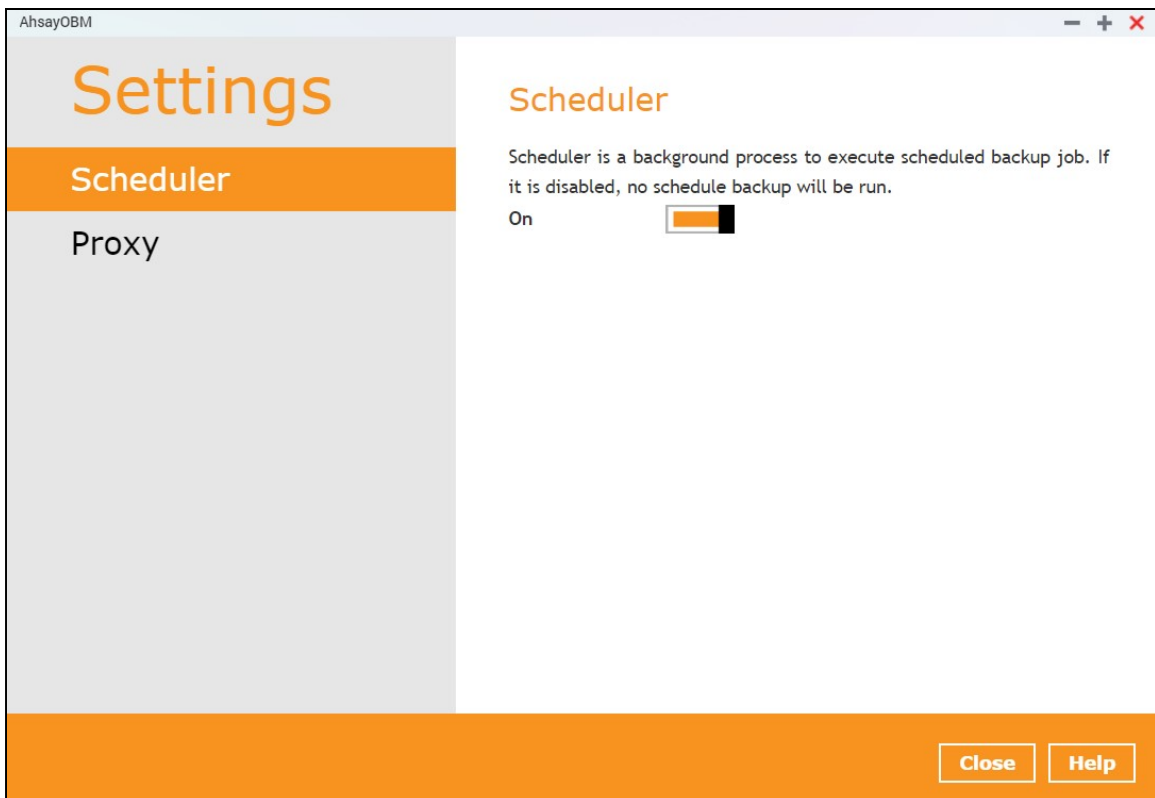
6.9 Settings

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



6.9.1 Scheduler

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

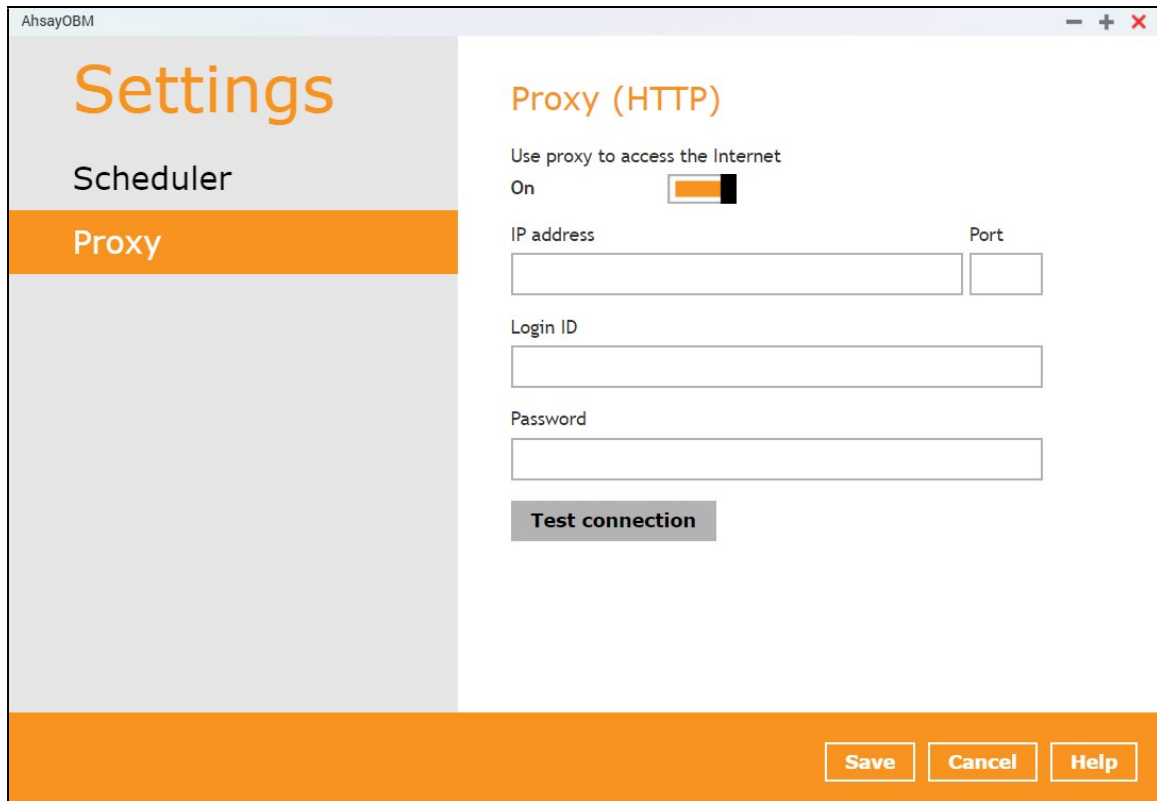


NOTE

For more details on the scenario for the Scheduler 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 AhsayOBM Settings window with the 'Proxy (HTTP)' section selected. The window title is 'AhsayOBM'. The left sidebar contains 'Settings', 'Scheduler', and 'Proxy' (highlighted in orange). The main content area is titled 'Proxy (HTTP)' and includes a toggle for 'Use proxy to access the Internet' (set to 'On'), input fields for 'IP address' and 'Port', 'Login ID', and 'Password', and a 'Test connection' button. At the bottom right, there are 'Save', 'Cancel', and 'Help' buttons.

AhsayOBM

Settings

Scheduler

Proxy

Proxy (HTTP)

Use proxy to access the Internet
On

IP address Port

Login ID

Password

Test connection

Save Cancel 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).

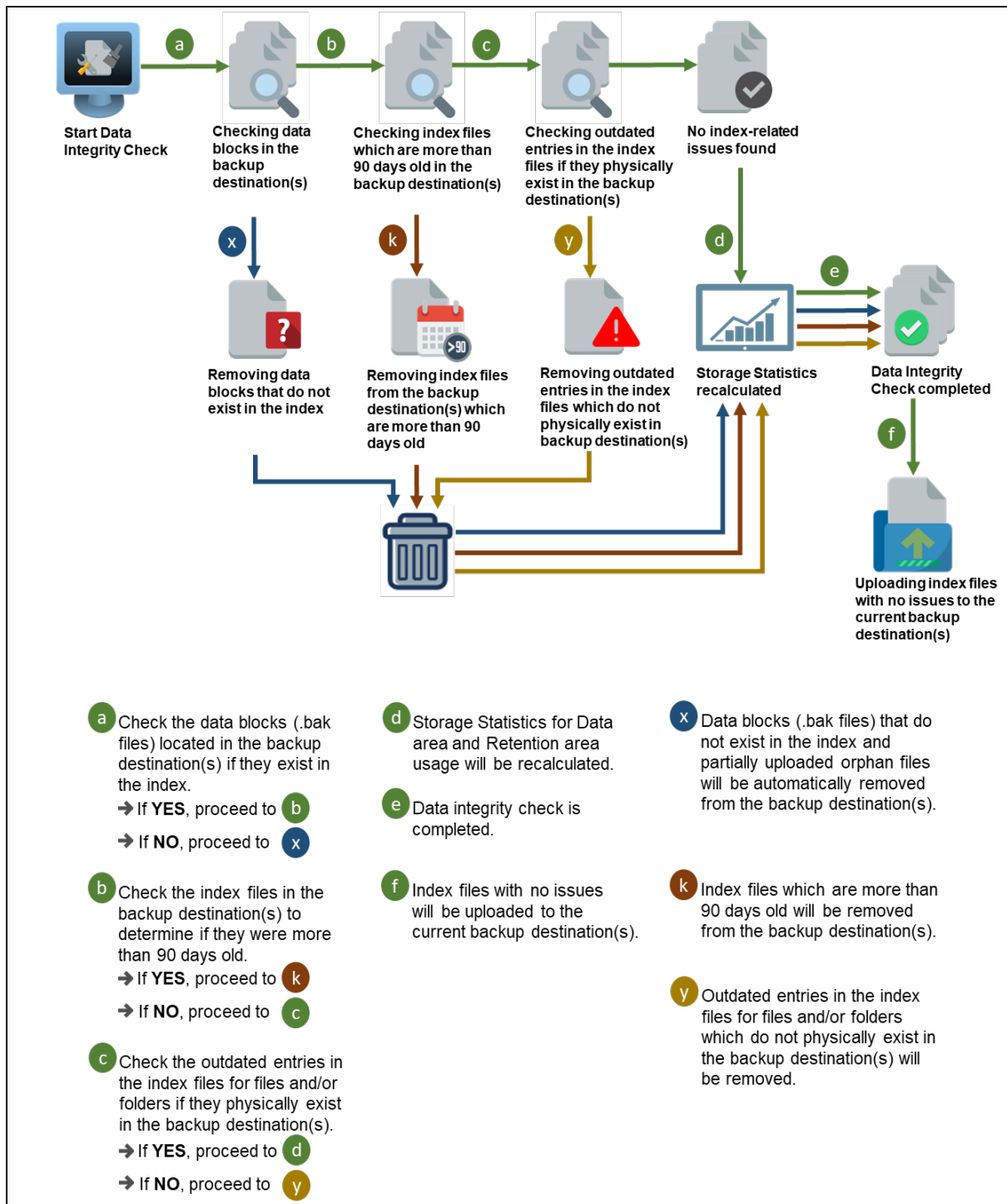
There are two (2) options in performing the Data Integrity Check:

<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.

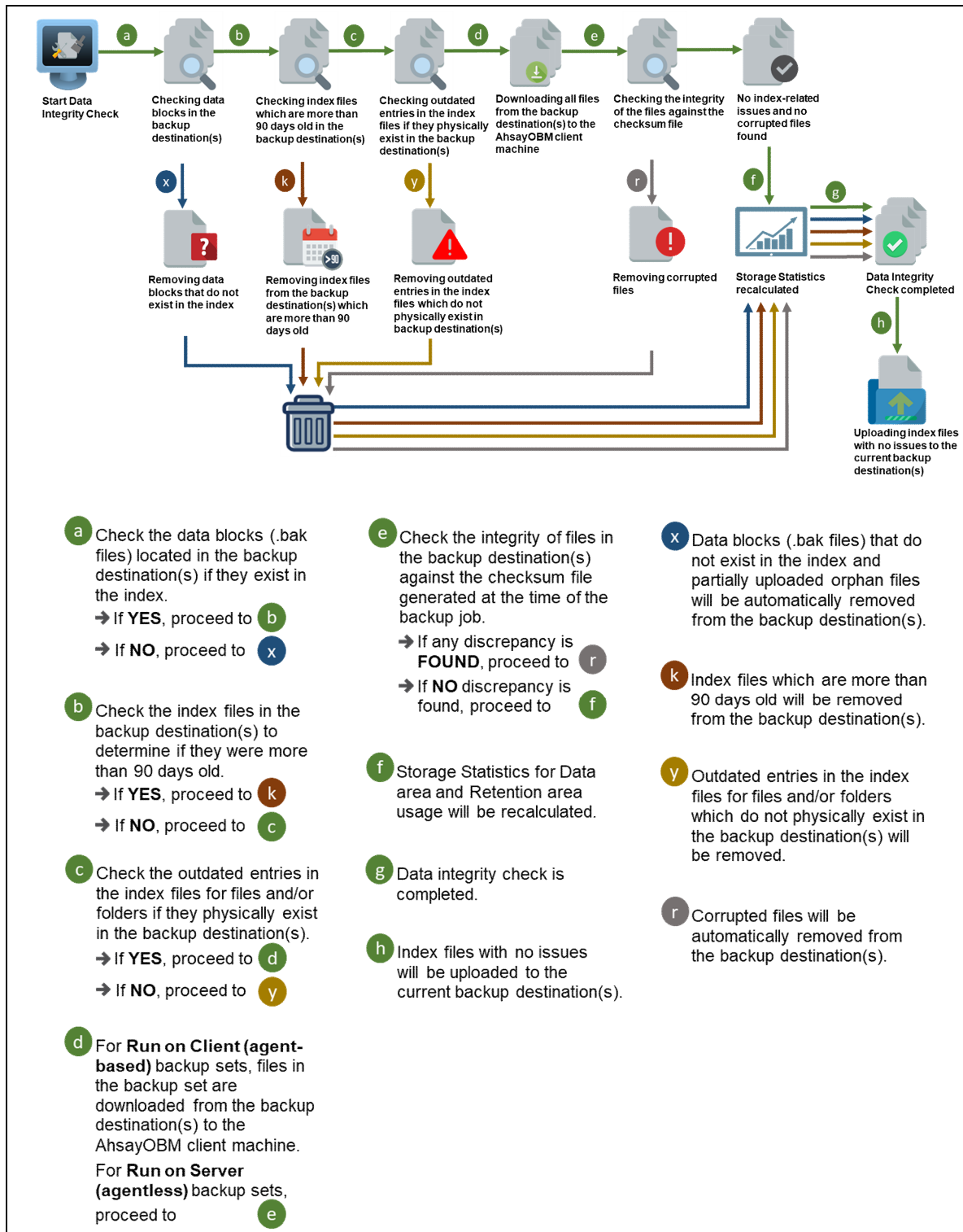
The following diagrams show the detailed process of the Data Integrity Check (DIC) in two (2) modes:

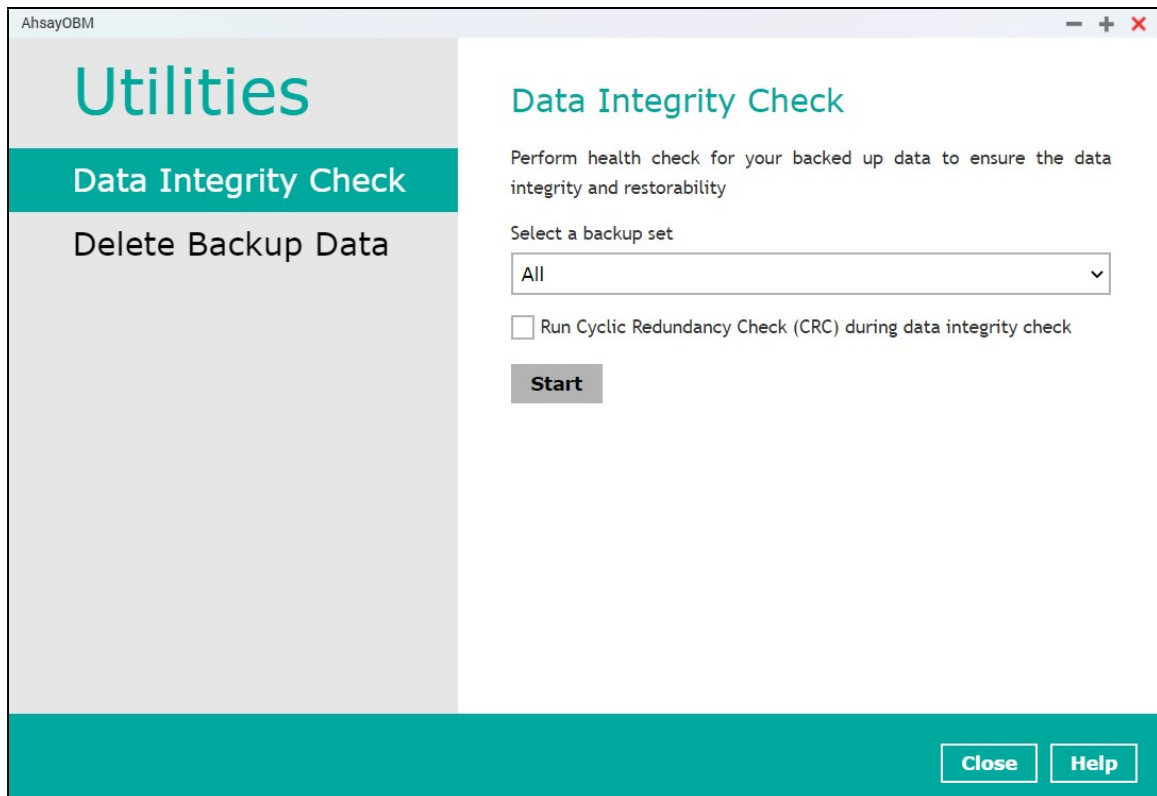
- **Option 1**
Disabled Run Cyclic Redundancy Check (CRC) - (**Default mode**)
- **Option 2**
Enabled Run Cyclic Redundancy Check (CRC)

**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

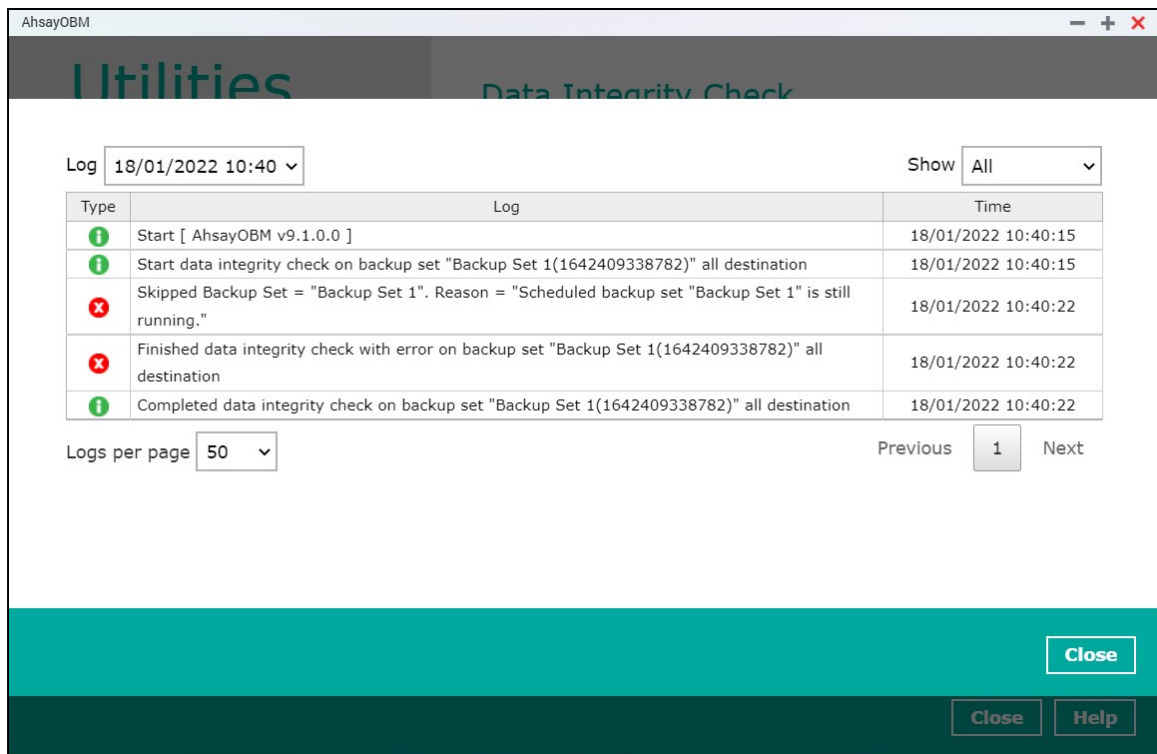
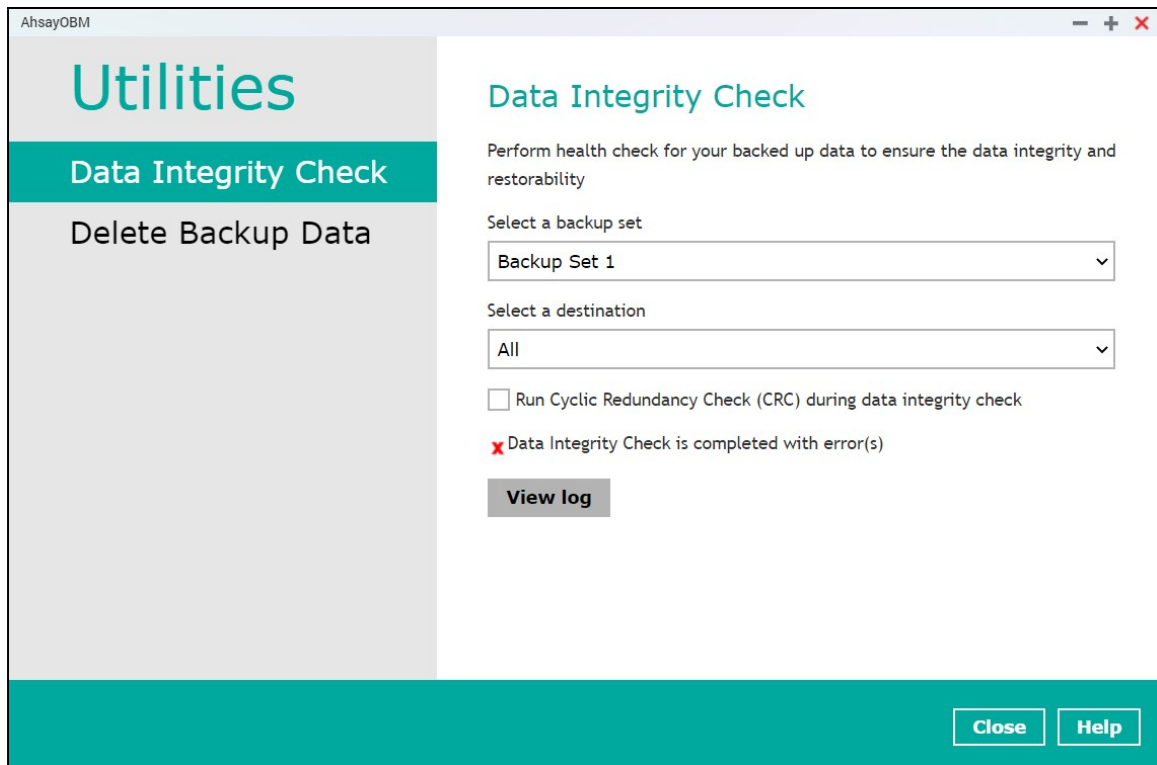




NOTES

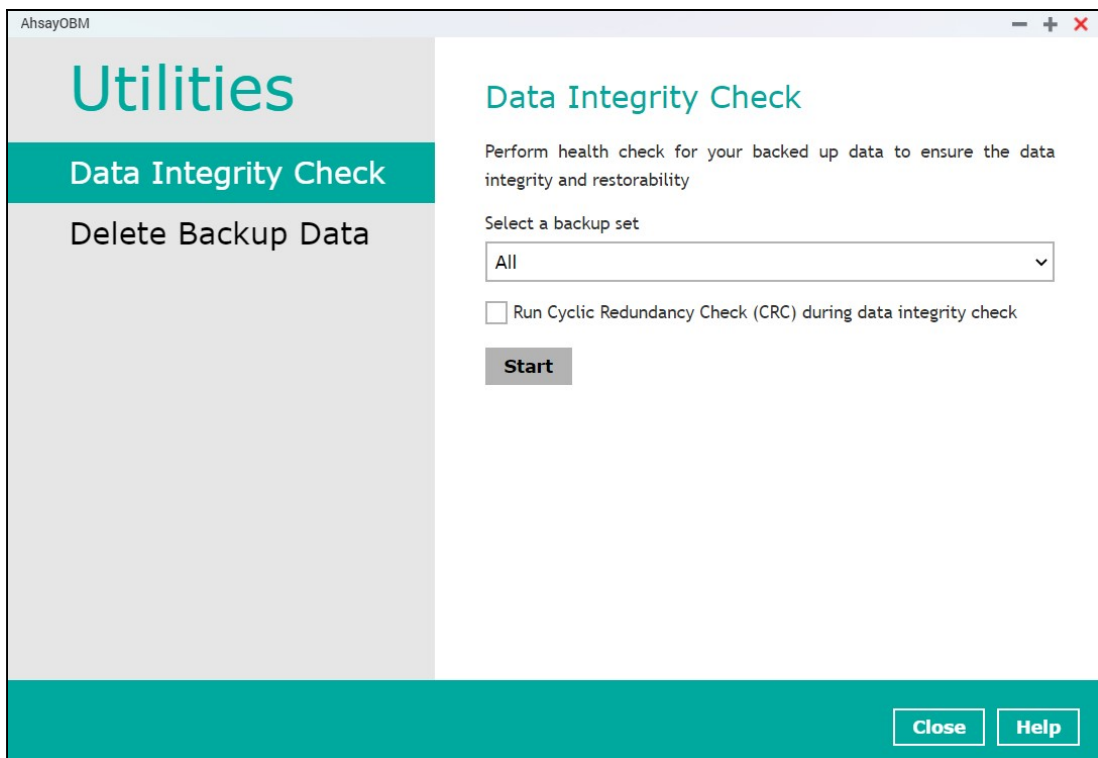
1. Data Integrity Check CANNOT fix or repair files that are already corrupted.
2. Data Integrity Check can only be started if there is NO active backup or restore job(s) running on the backup set selected for the DIC job. As the **backup**, **restore** and **data integrity check** are using the same 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).

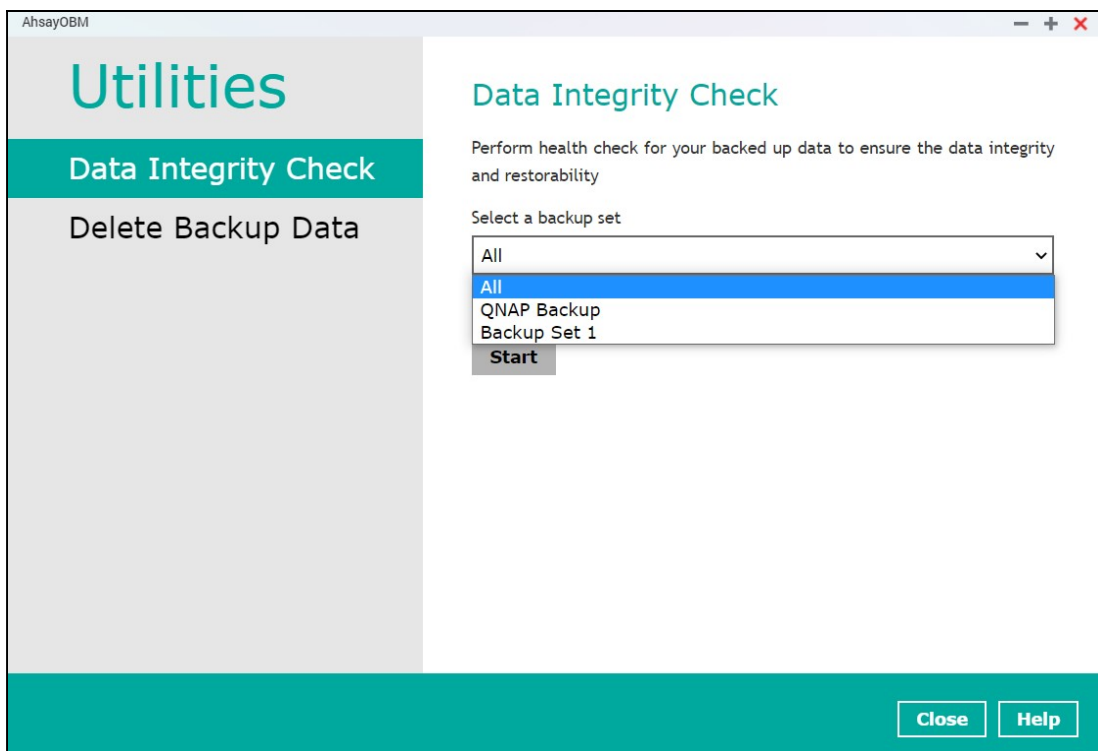


To perform a Data Integrity Check, follow the instructions below:

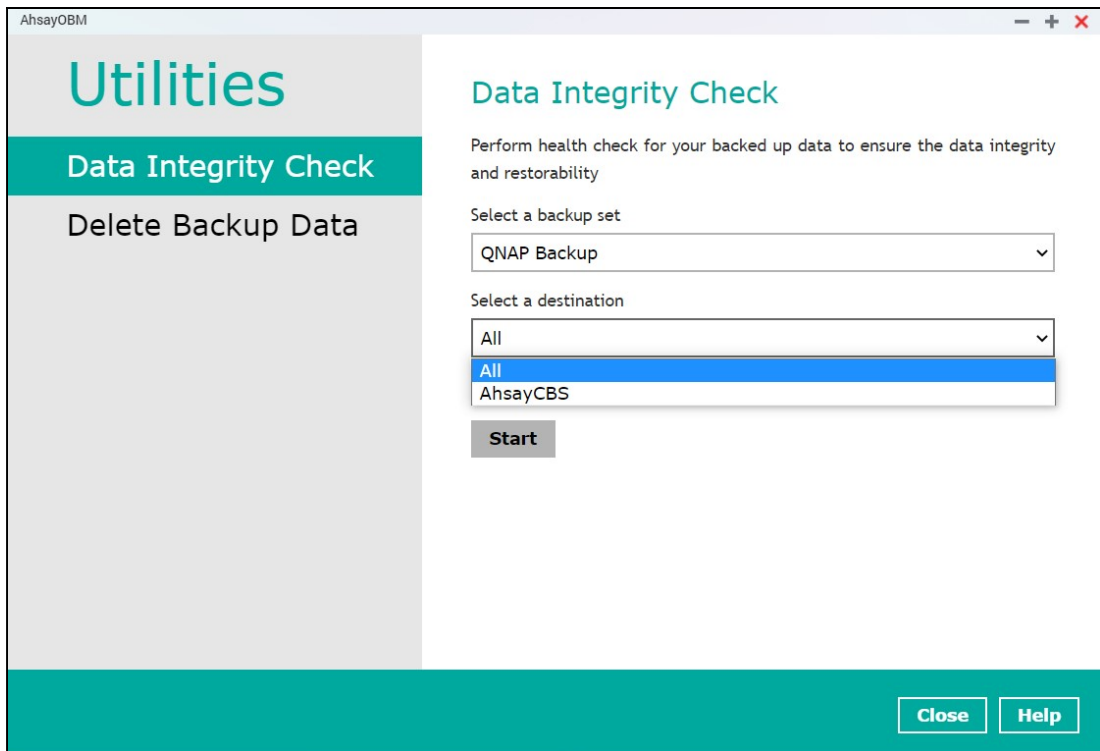
1. Go to the Data Integrity Check tab in the Utilities menu.



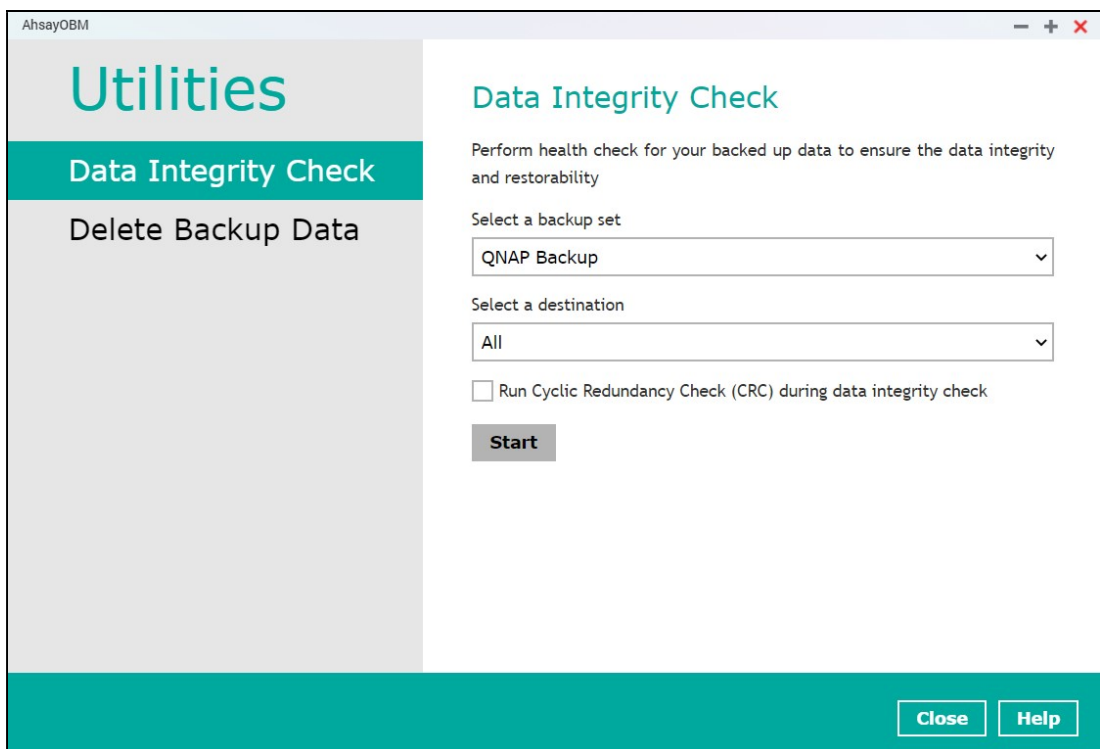
2. Click the drop-down button to select a backup set.



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.

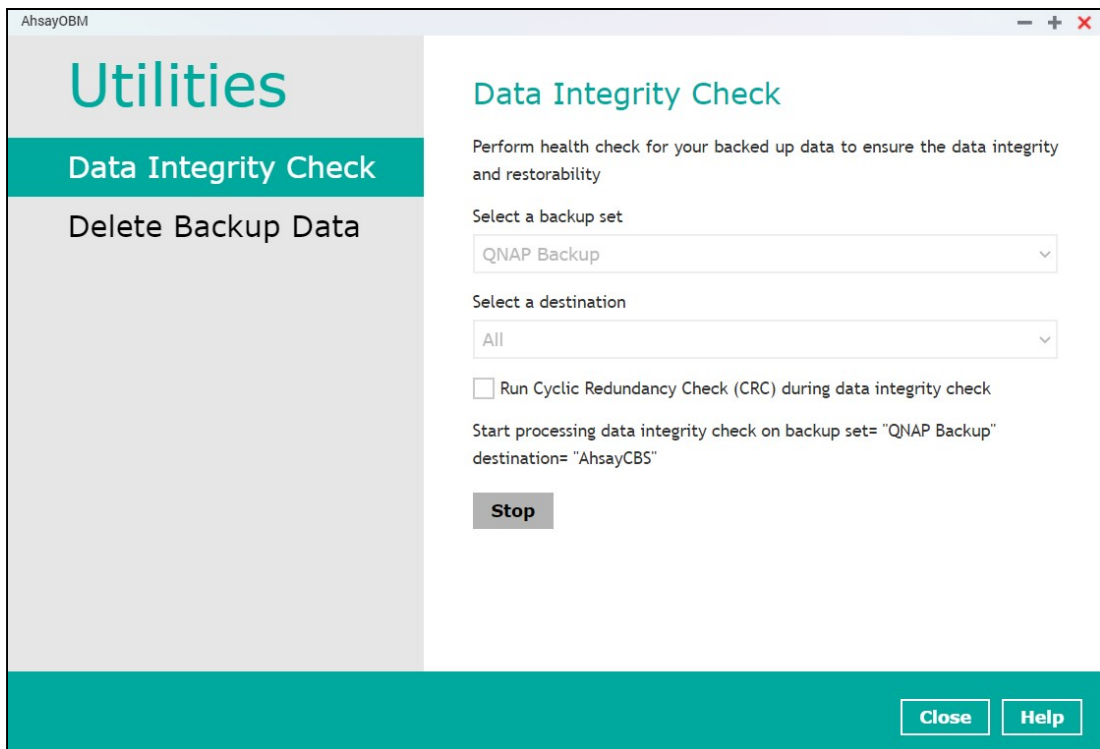
The time required to complete a data integrity check depends on the number of factors such as:

- 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

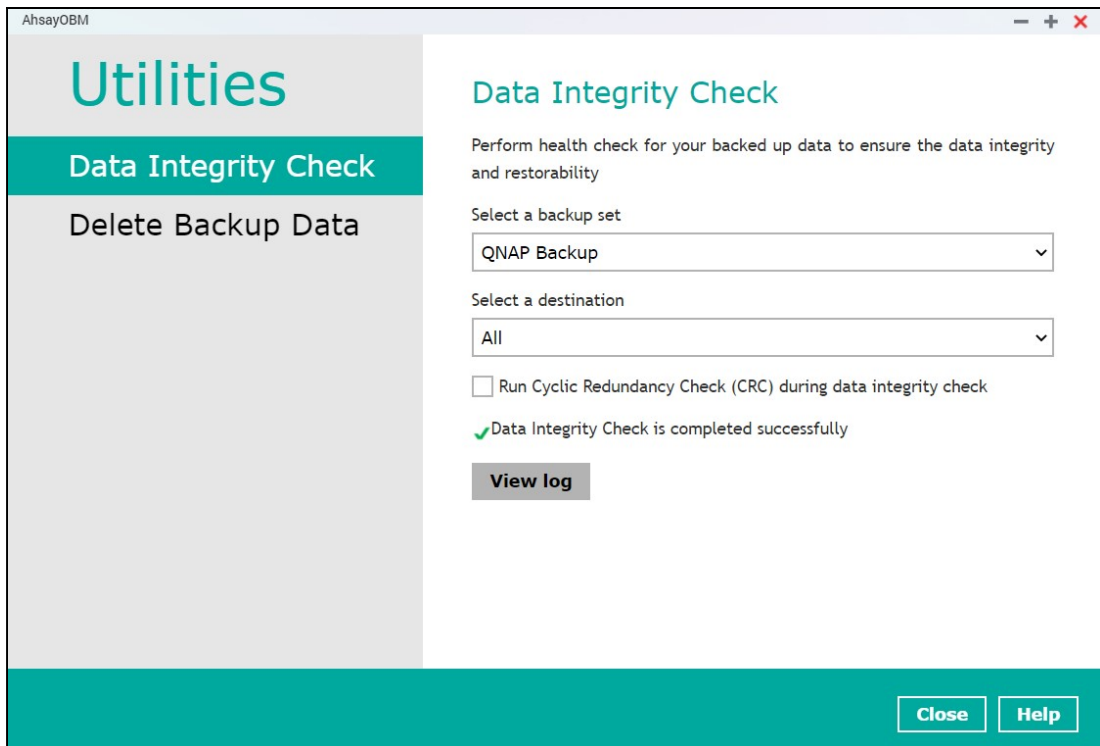
NOTE

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.

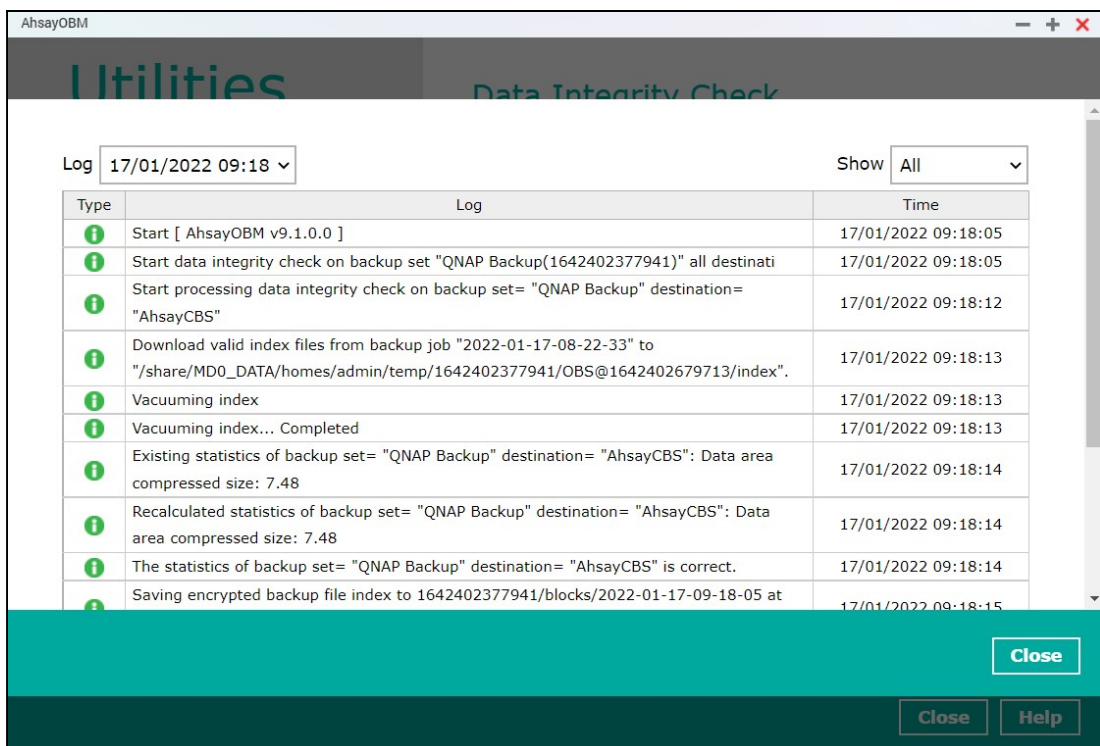
5. Click the **Start** button to begin the Data Integrity Check.
6. Data Integrity Check will start running on the selected backup set(s) and backup destination(s).



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

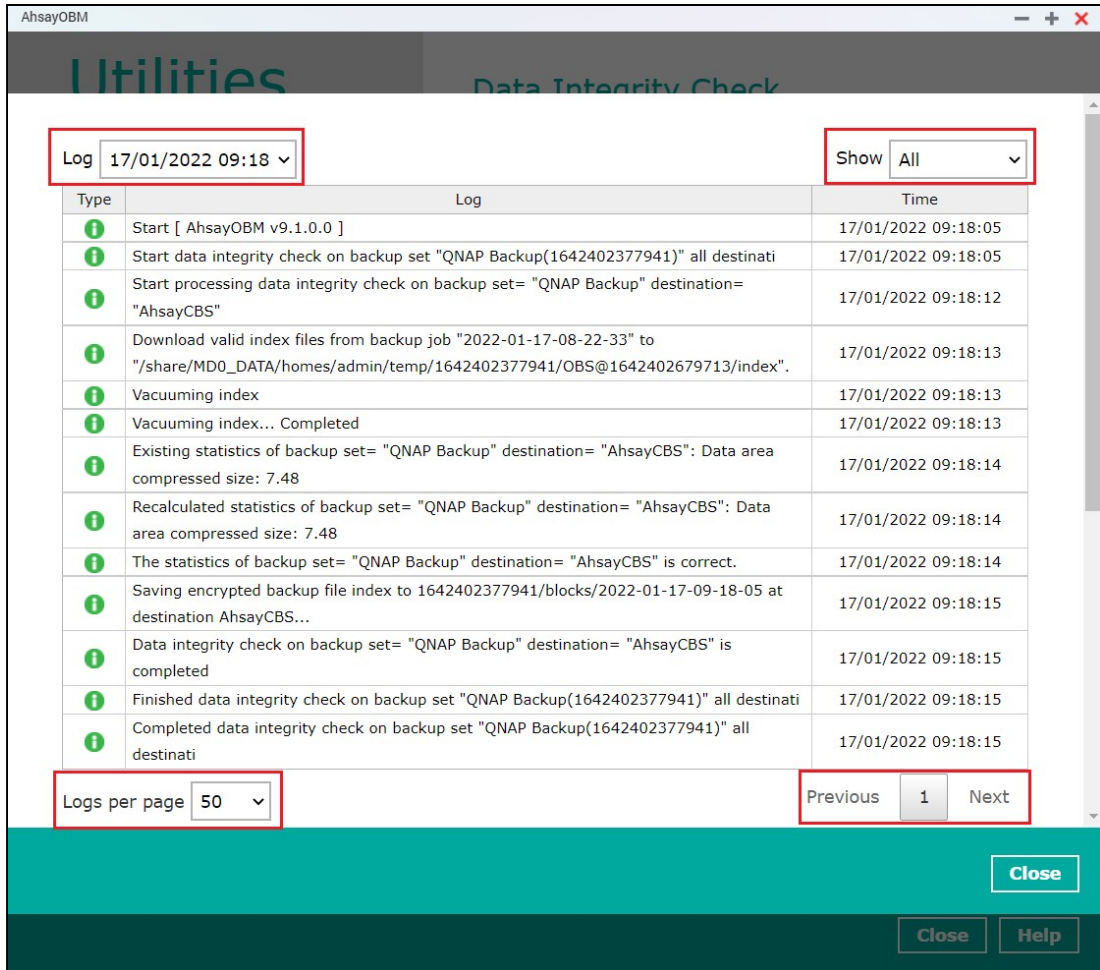


- The detailed log of data integrity check process will be displayed.

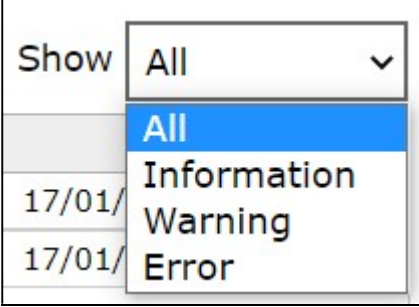
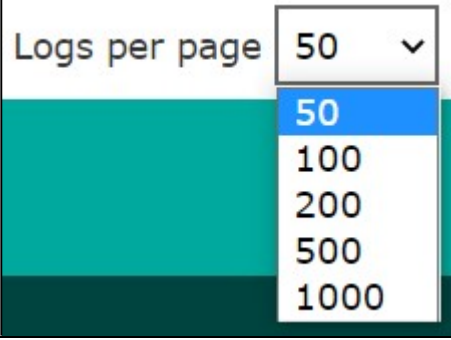



The following options can be used for further viewing of the detailed DIC log:

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



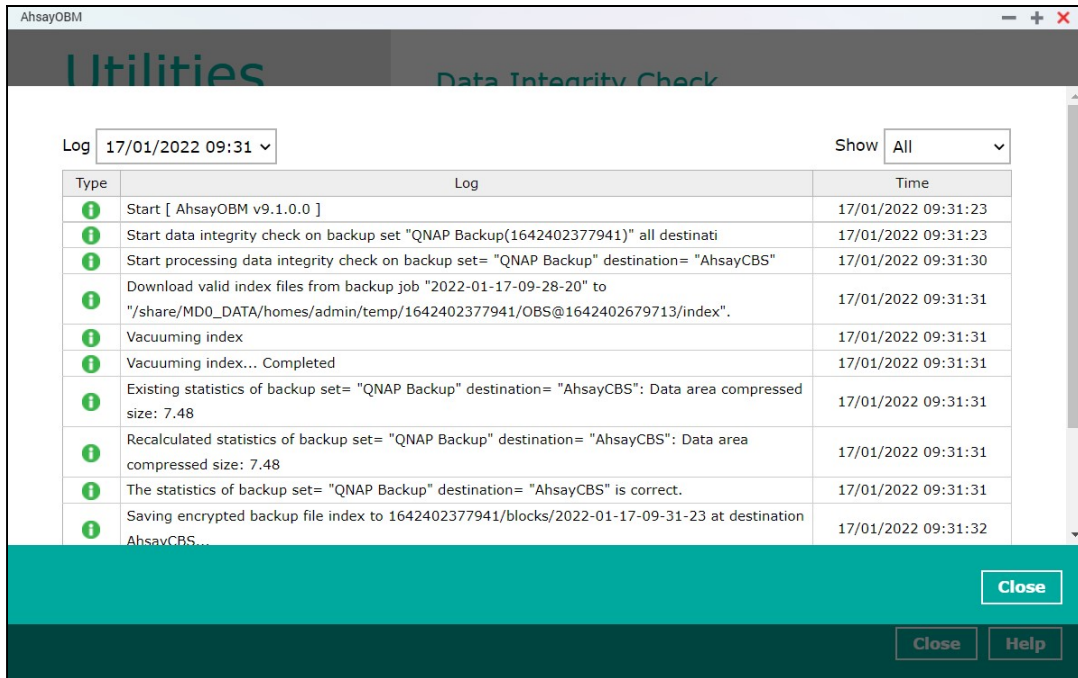
Control	Screenshot	Description
Log filter		This option can be used to display logs of the previous data integrity check jobs.

<p>Show filter</p>		<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>
<p>Logs per page</p>		<p>This option allows user to control the displayed number of logs per page.</p>
<p>Page</p>		<p>This option allows user to navigate the logs to the next page(s).</p>

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 and deleted

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



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



NOTE

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

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

The (TEST MODE) confirmation screen is not supported on QNAP 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 QNAP NAS, the DIC logs are located in the following directory:

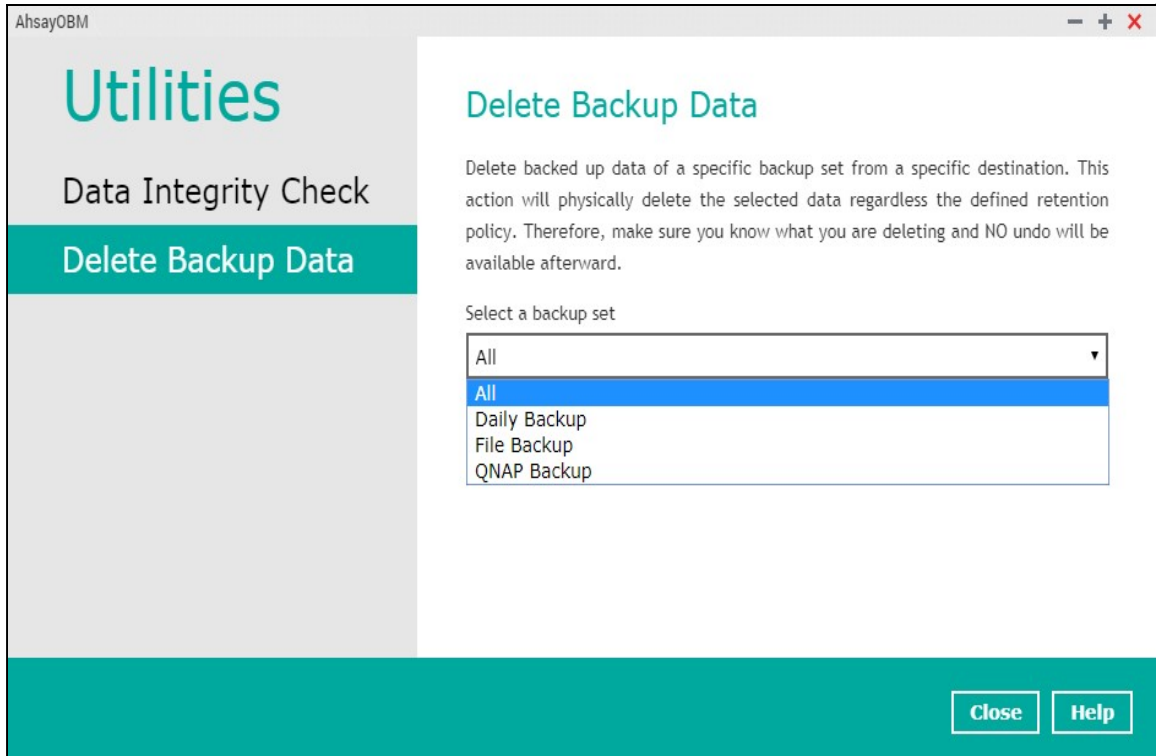
`${system_volume_path}/homes/admin/.obm/system/IntegrityCheck`

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:

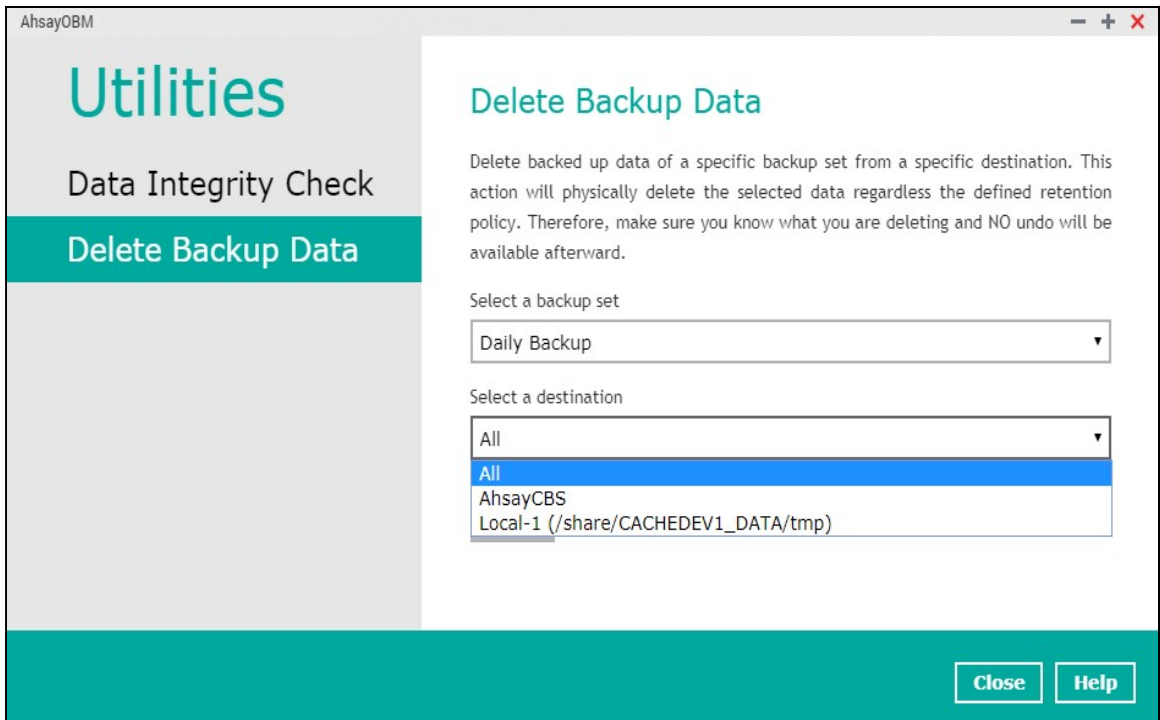
1. Select a backup set from the drop-down list.



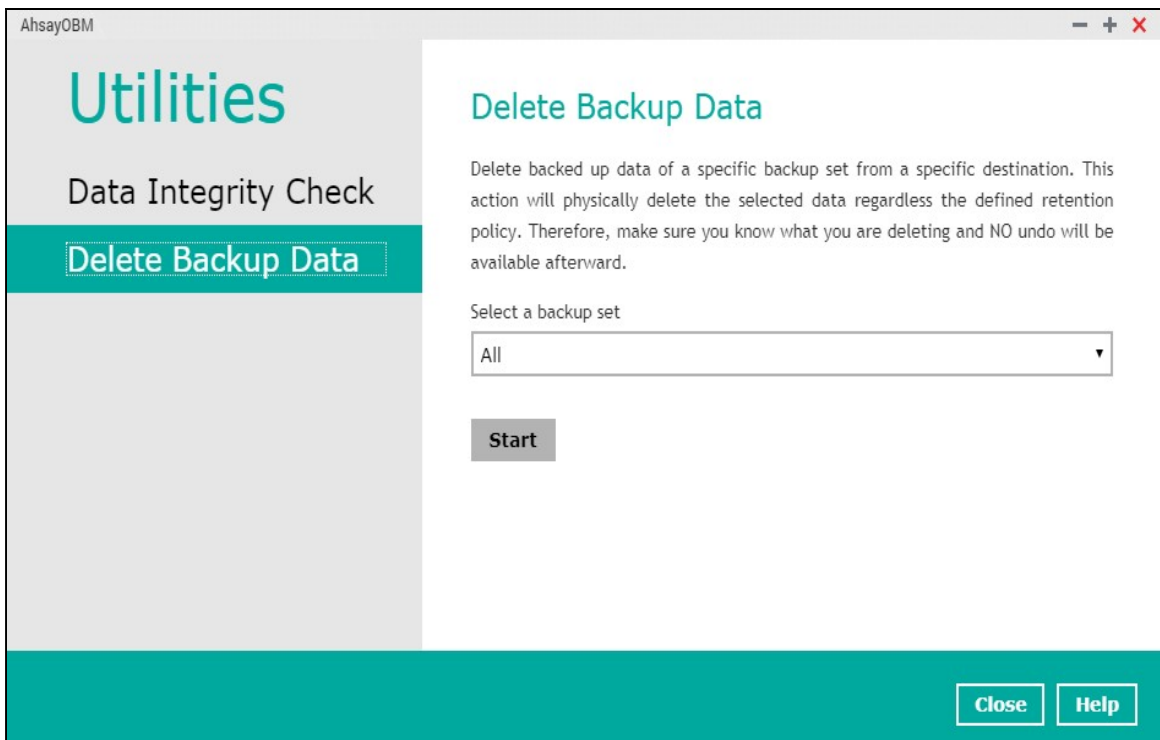
NOTE

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

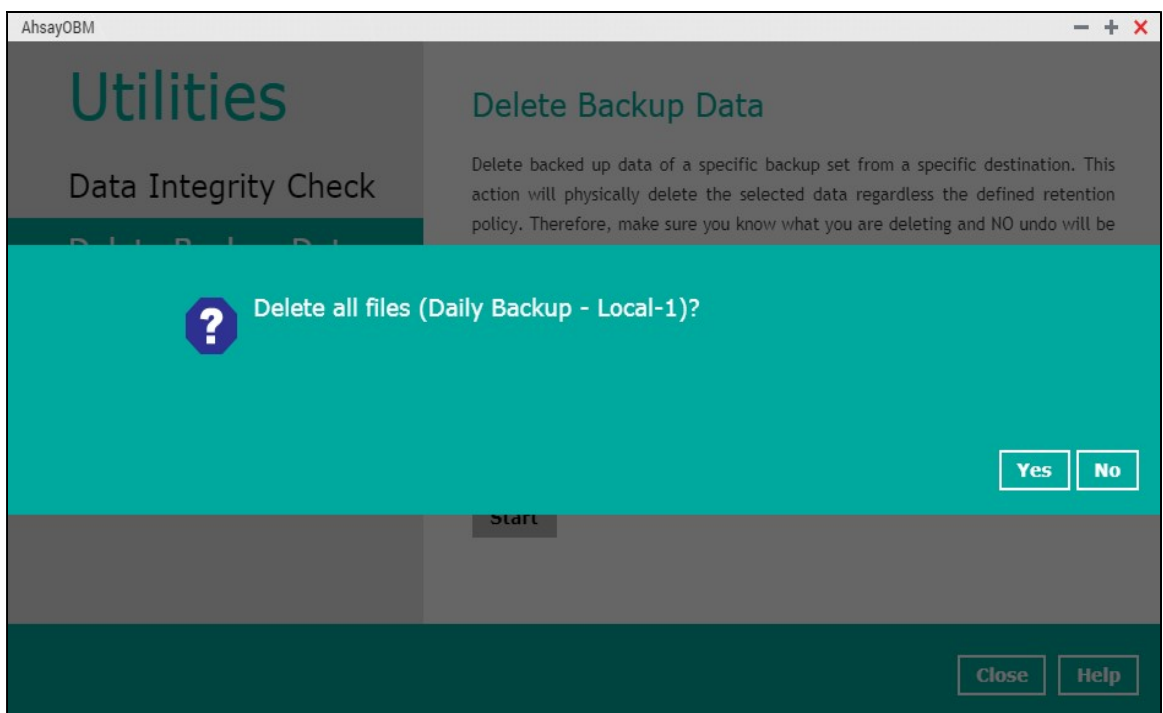
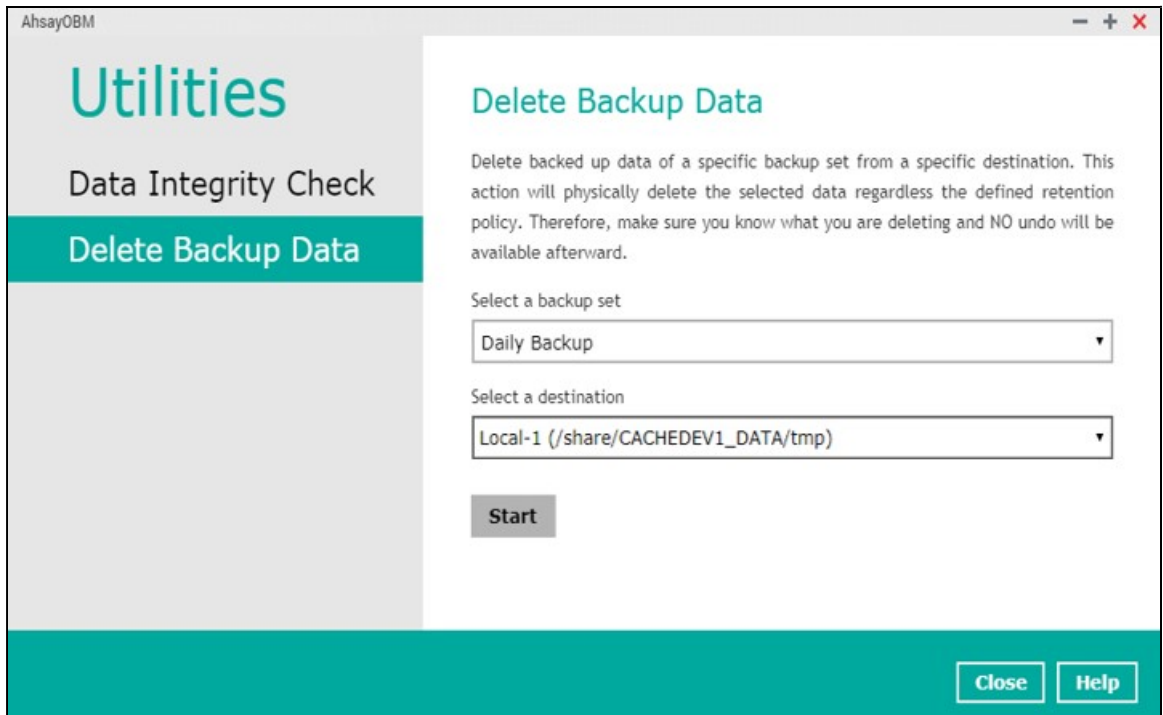
If you select a specific backup set, then you will also have to select a specific destination or all destinations.



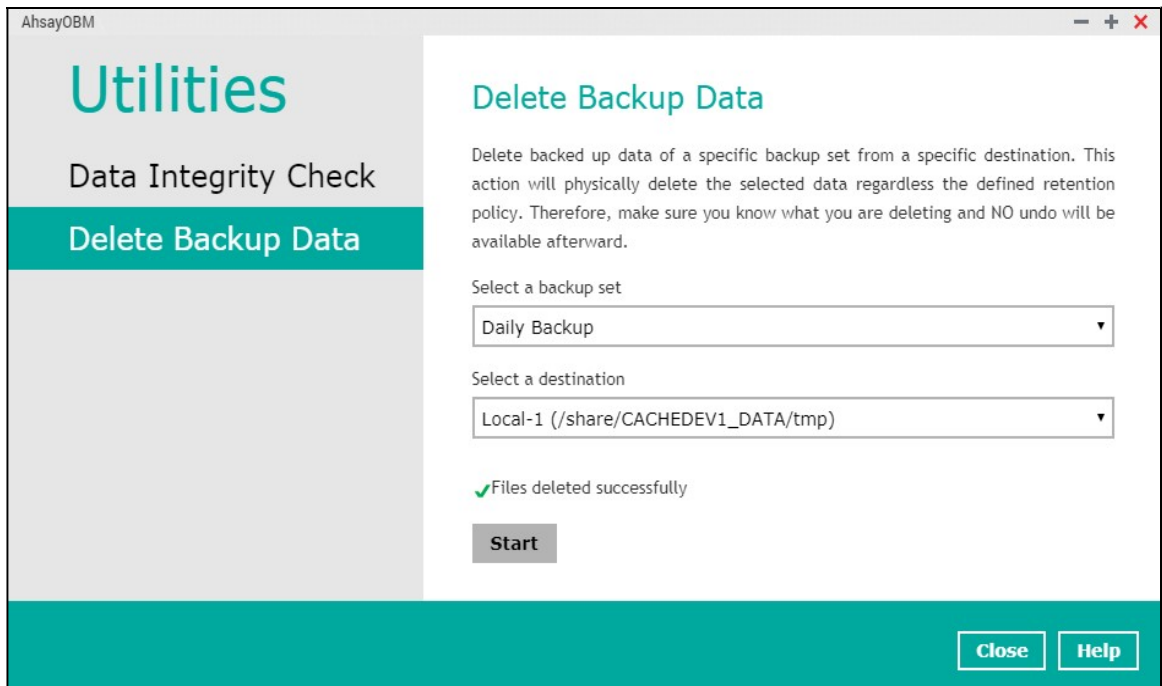
If you select **All** backup sets, then there is no need to select a destination.



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.

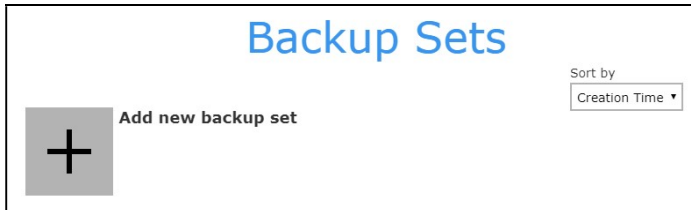


7 Create a Backup Set

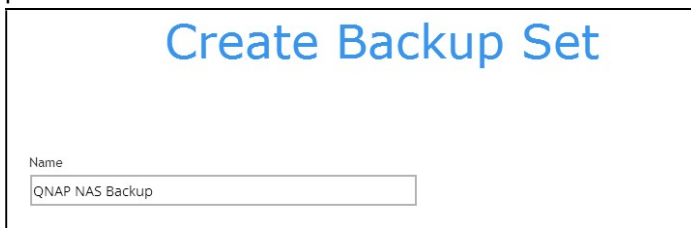
1. Click the **Backup Sets** icon on the main interface of AhsayOBM.



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.

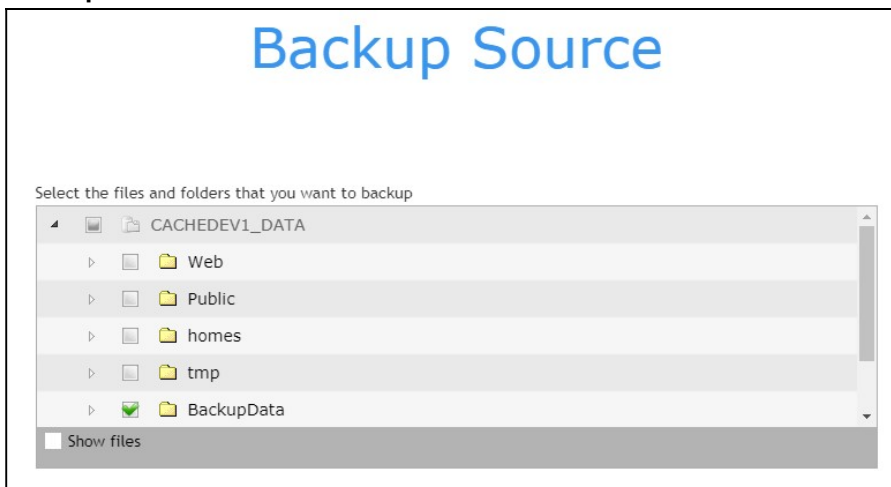


4. In the Backup Source window, select the files and folders that you would like to back up.

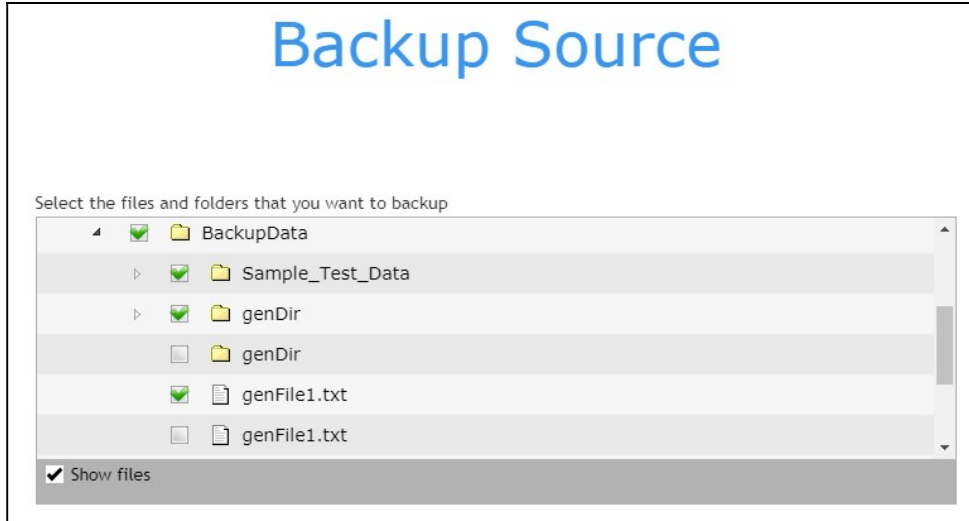
NOTE

AhsayOBM supports backup of files and/or folders from an external USB drive attached to the QNAP NAS machine where the AhsayOBM is installed.

Backup Source on the QNAP NAS



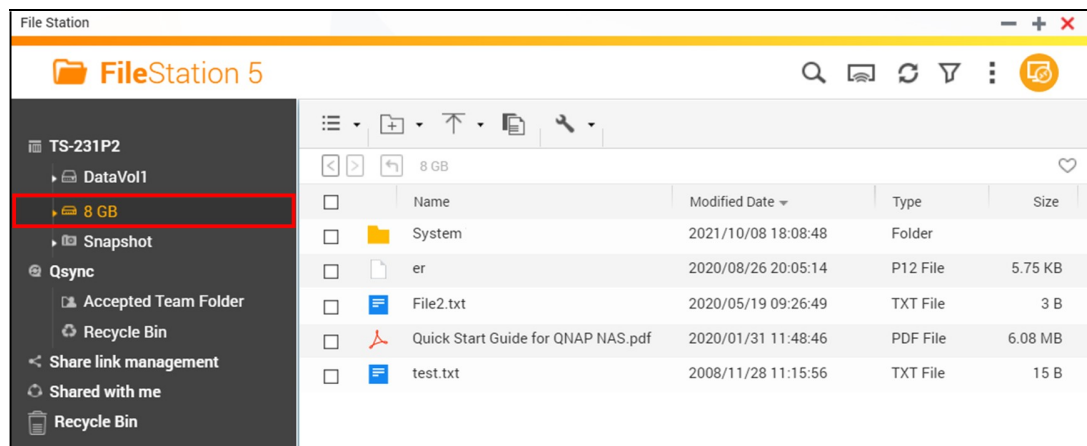
You may click the **Show files** checkbox if you want to select individual file(s) for backup.



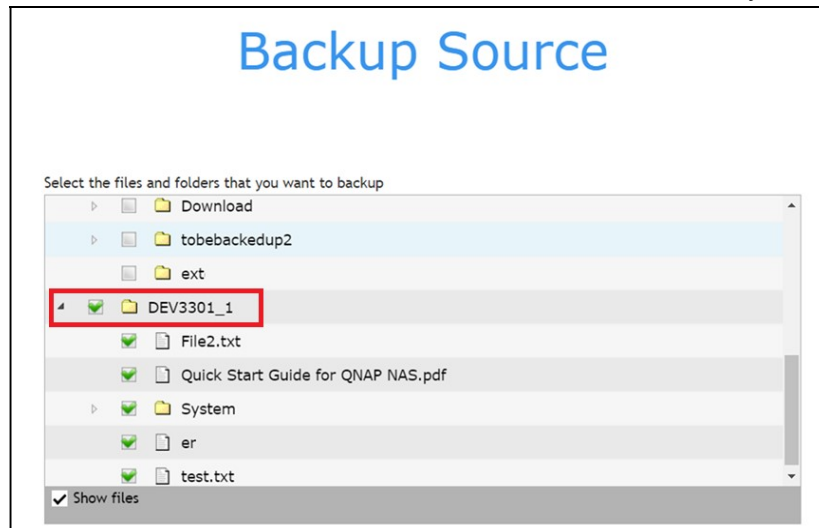
Backup Source on the External USB Drive

To select a backup source from an external USB drive, follow the instructions below:

- i. Ensure that your AhsayOBM is updated to v9.1.0.0 (or above).
- ii. Attach your external USB drive, then verify if the attached external USB drive is visible on the File Station.



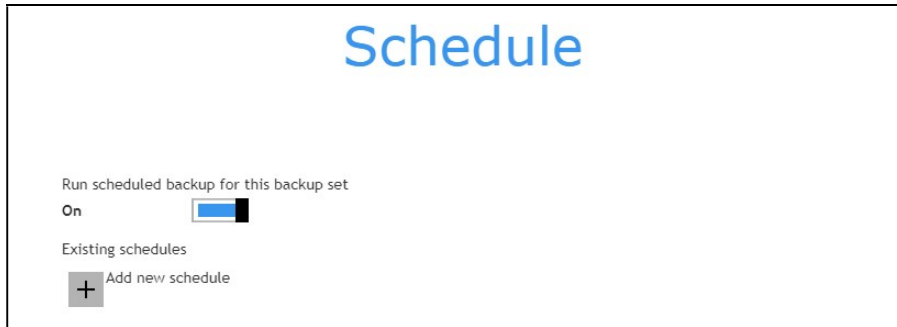
- iii. Select the files and/or folders from the external USB drive that you would like to back up.



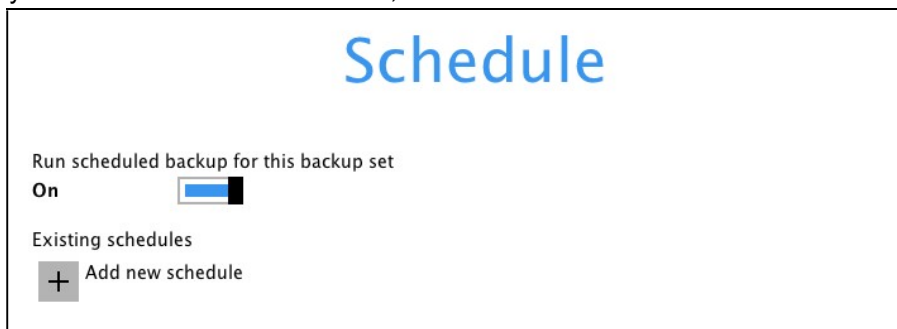
After selecting the backup source, click **Next** to proceed.

5. 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 **On** by default.

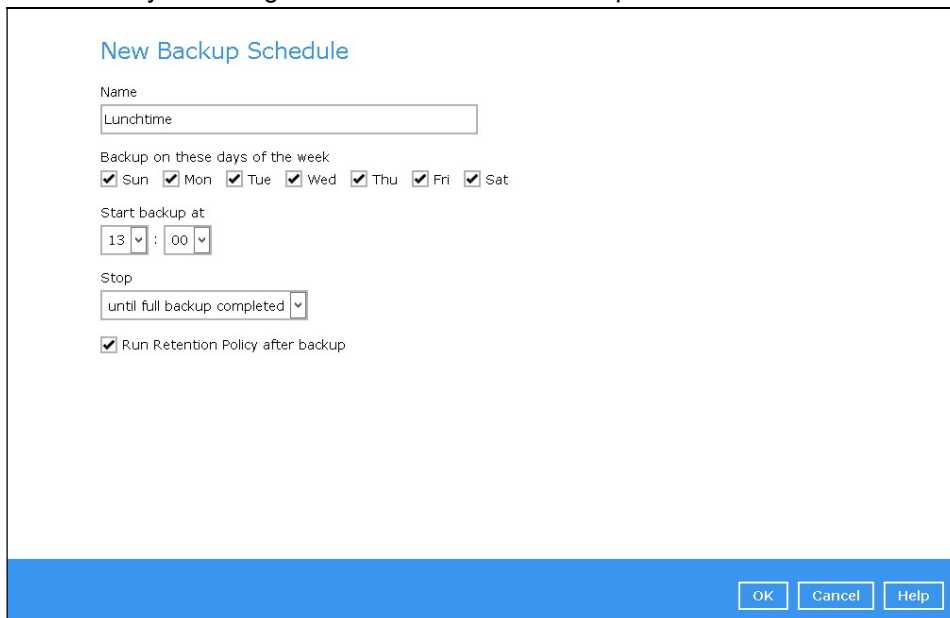
- You can leave it as is or you can turn it **Off** if you do not want to add a schedule again.



- If you want to add a schedule now, click “+” next to Add New schedule.



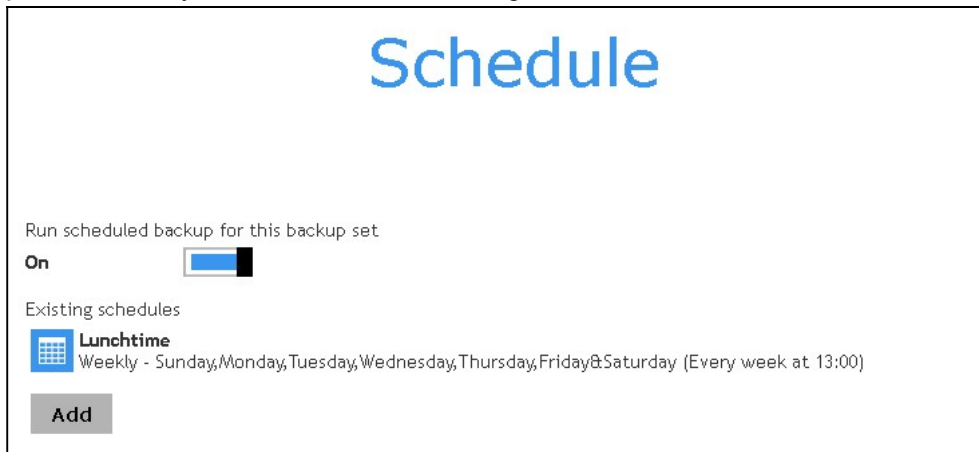
When the **New Backup Schedule** window appears, specify your backup schedule. Then, click **OK** to save your changes and close the New Backup Schedule window.



NOTE

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

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




Schedule

Run scheduled backup for this backup set

On

Existing schedules

 **Lunchtime**
Weekly - Sunday,Monday,Tuesday,Wednesday,Thursday,Friday&Saturday (Every week at 13:00)

Add

7. The Destination window will appear.



Destination

Backup mode

Sequential

Existing storage destinations

 Add new storage destination / destination pool

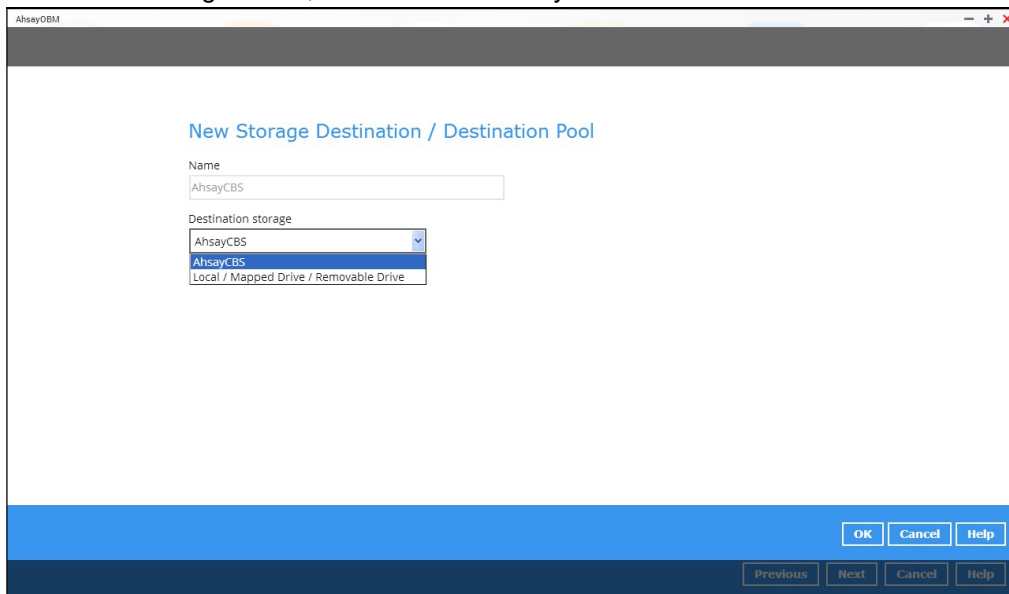
 

Select the appropriate option from the **Backup mode** drop down menu.

- ⦿ **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**.

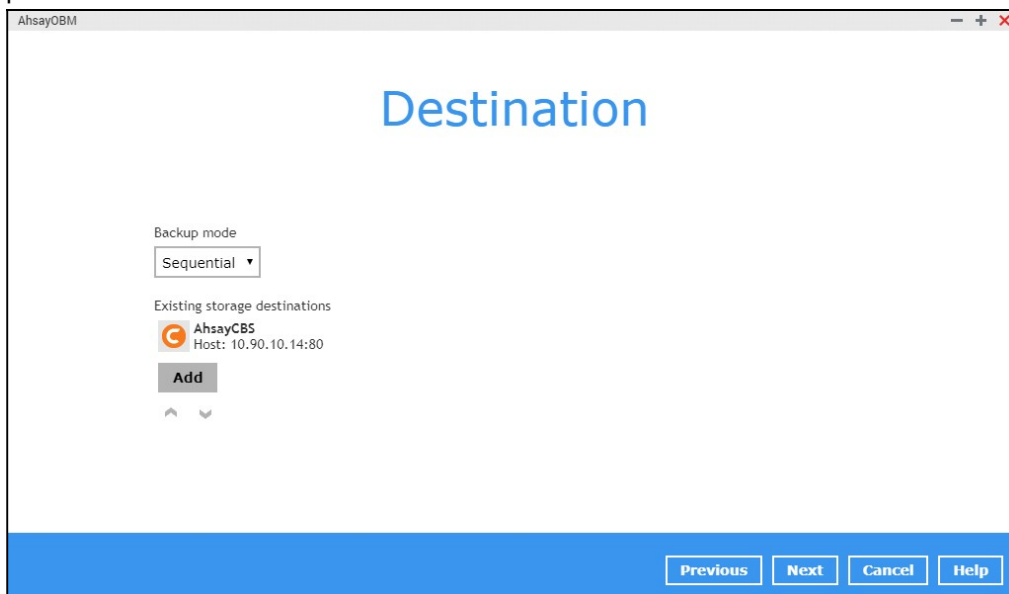
8. In the New Storage Destination / Destination Pool window, select the destination type and destination storage. Then, click **OK** to confirm your selection.



NOTE

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

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

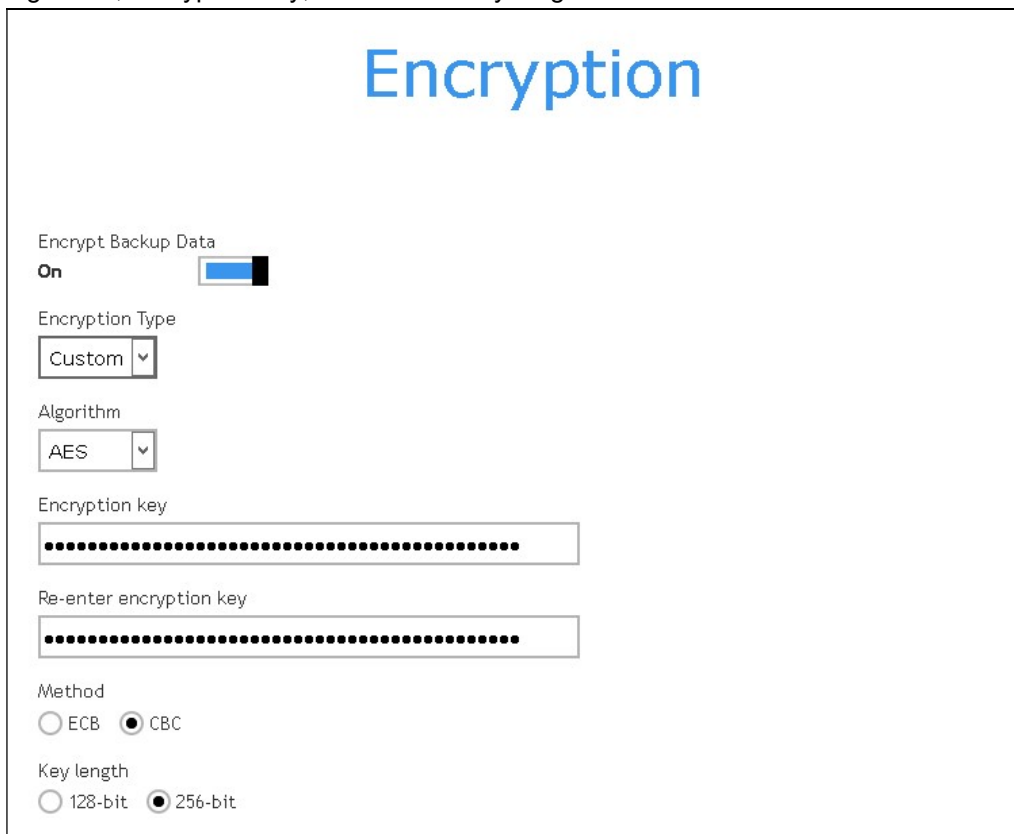


10. In the Encryption window, the default **Encrypt Backup Data** option is enabled with an encryption key preset by the system which provides the most secure protection.



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

- **Default** – an encryption key with 44 alpha numeric characters will be randomly generated by the system.
- **User password** – the encryption key will be the same as the login password of your AhsayOBM at the time when this backup is created. Please be reminded that if you change the AhsayOBM login password later, the encryption keys of the backup sets previously created with this encryption type will remain unchanged.
- **Custom** – you can customize your encryption key, where you can set your own algorithm, encryption key, method and key length.



NOTE

For best practice on managing your encryption key, refer to the following Wiki article. [FAQ: Best practices for managing encryption key on AhsayOBM or AhsayACB?](#)

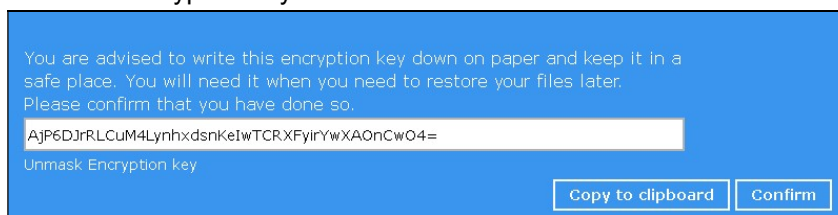
Click **Save** when you are done with the settings.

11. 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.



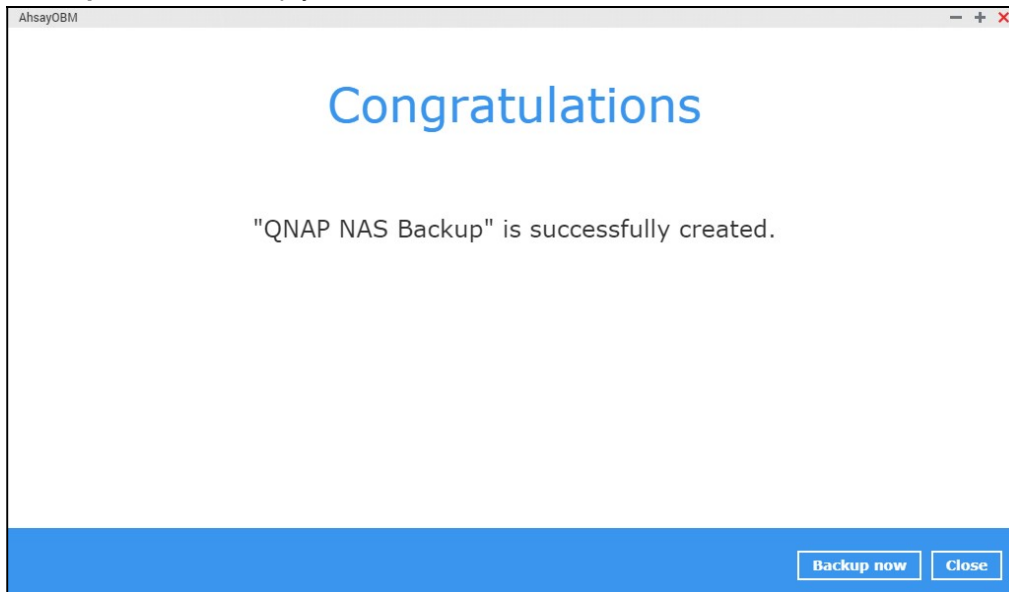
The pop-up window has the following three options to choose from:

- **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.

12. 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.



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 \(Step 4\)](#)
 - [Completed Backup Job \(Step 11\)](#)
- [Data Validation Check Process \(Step 9\)](#)



8.1 Periodic Data Integrity Check (PDIC) Process

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

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

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

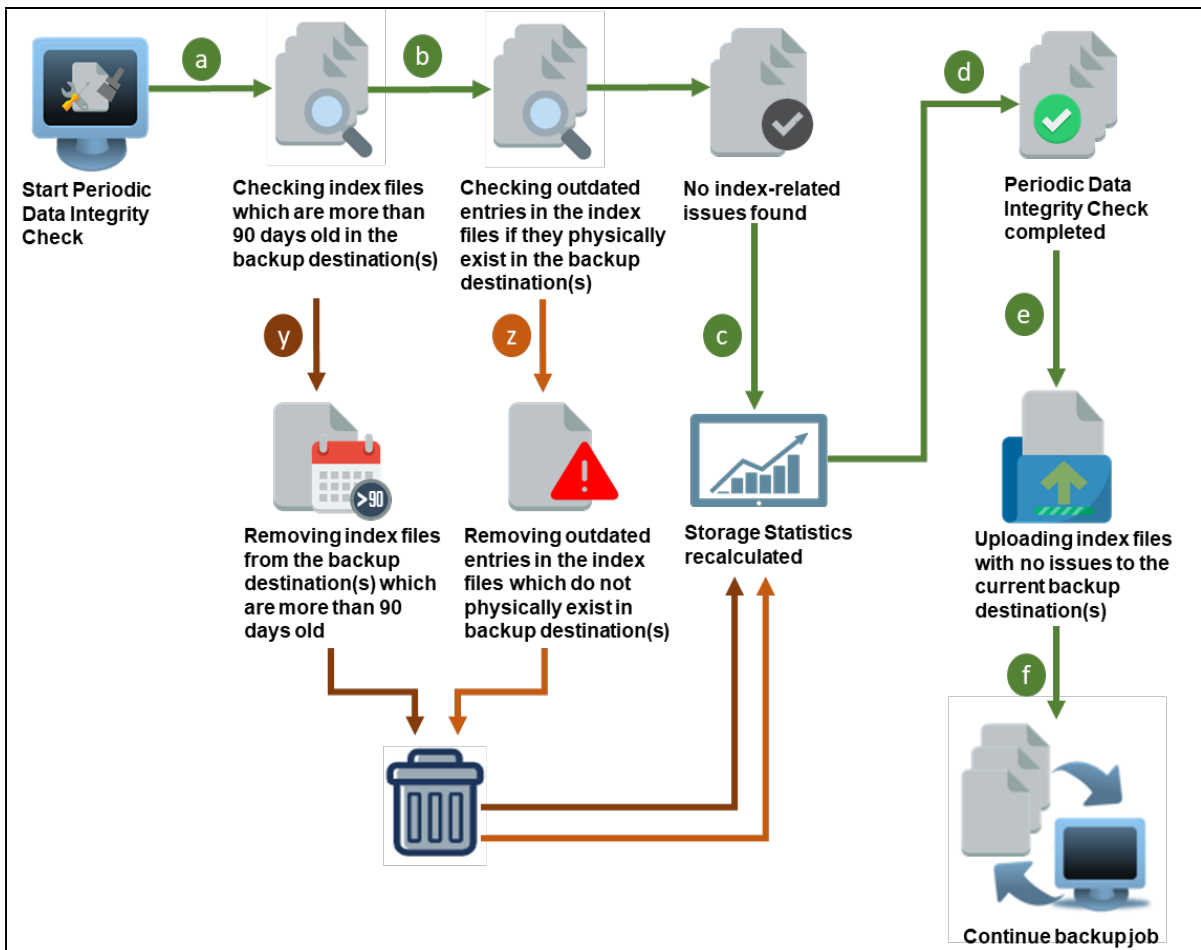
- the PDIC will run on the first backup job that falls on Wednesday; or
- if there is no active backup job(s) running from Monday to Friday, then the PDIC will run on the next available backup job.

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



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

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

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

d Periodic Data Integrity check is completed.

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

f The backup job process will continue.

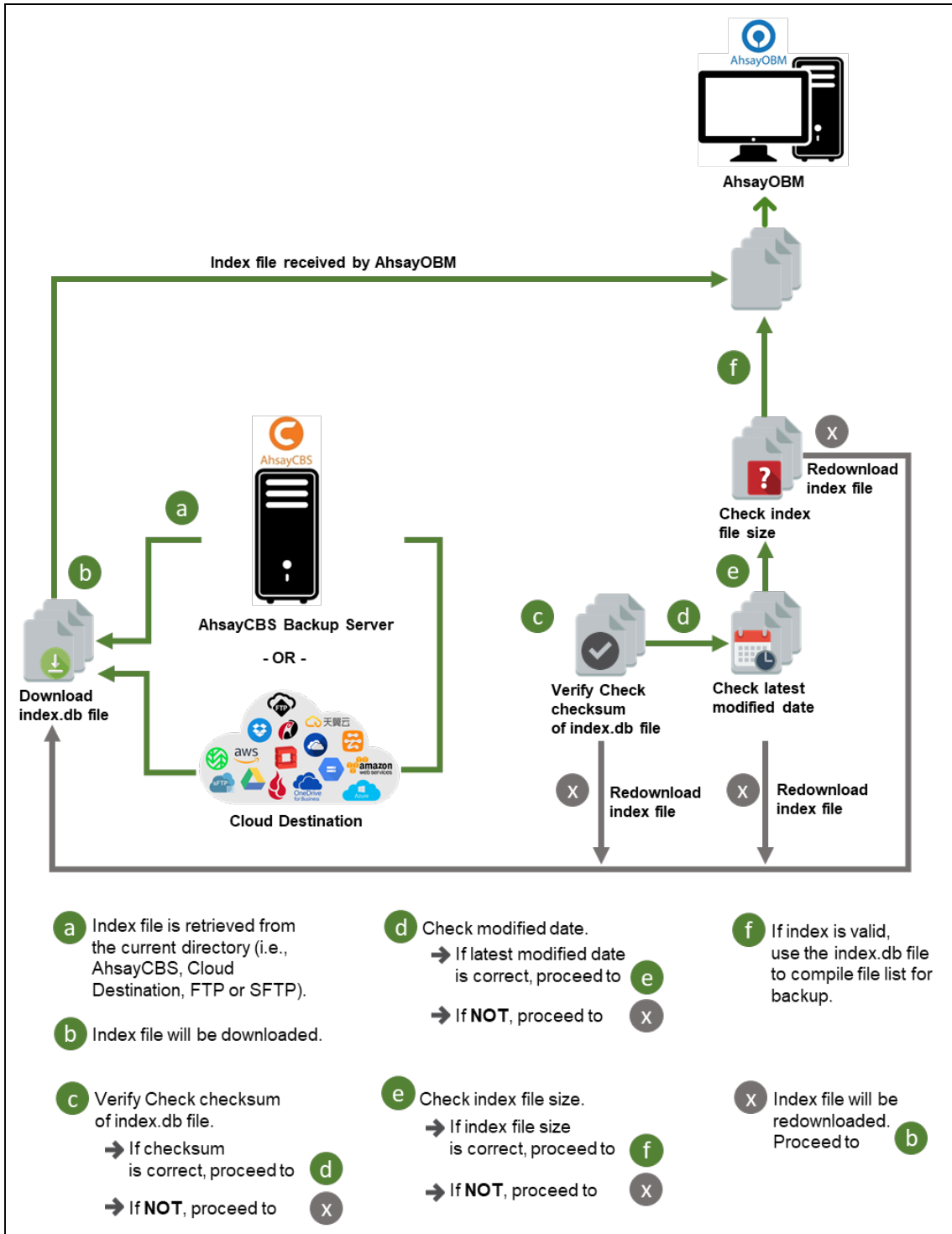
y Index files which are more than 90 days old will be removed from the backup destination(s).

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

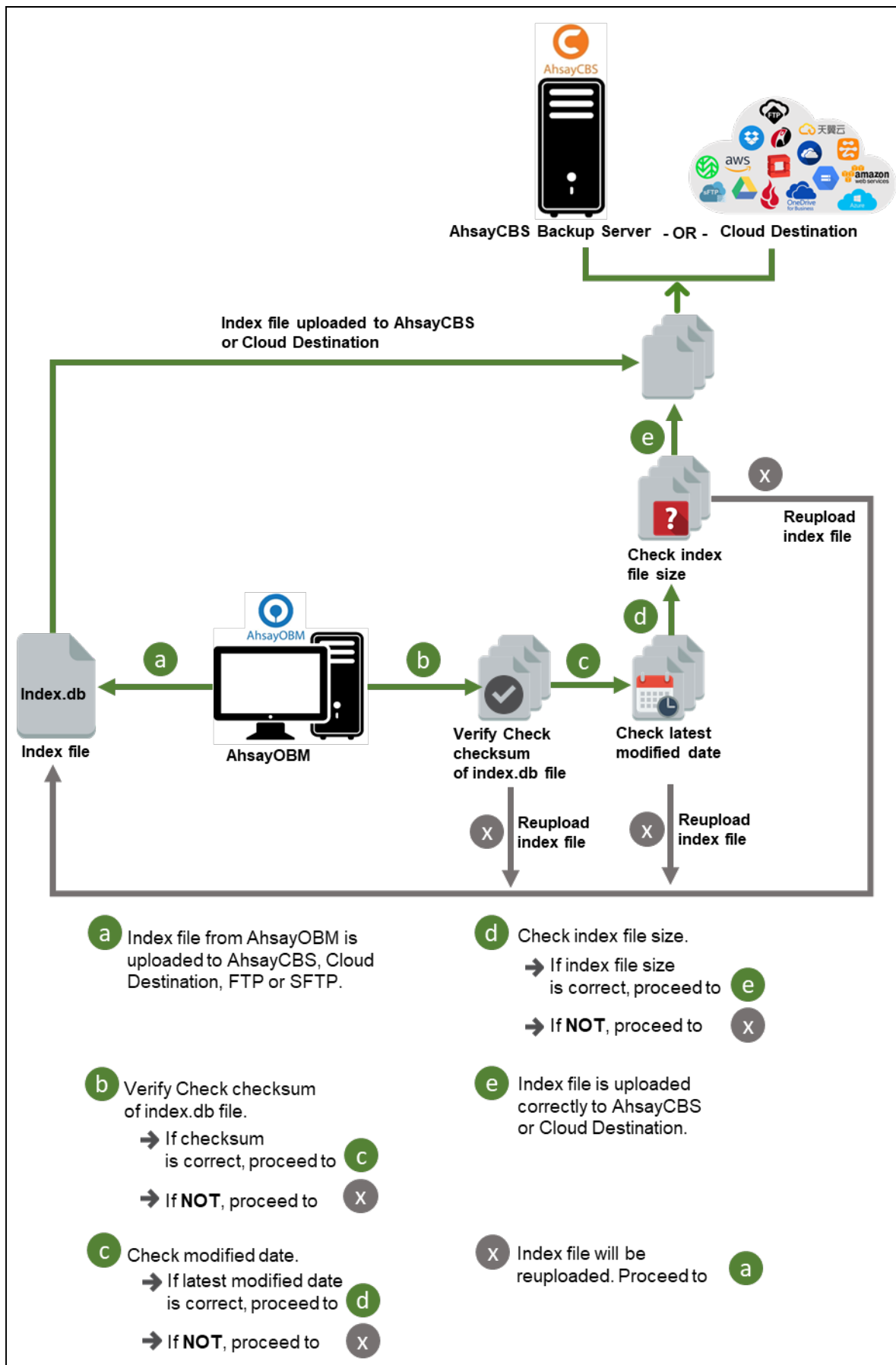
8.2 Backup Set Index Handling Process

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

8.2.1 Start Backup Job

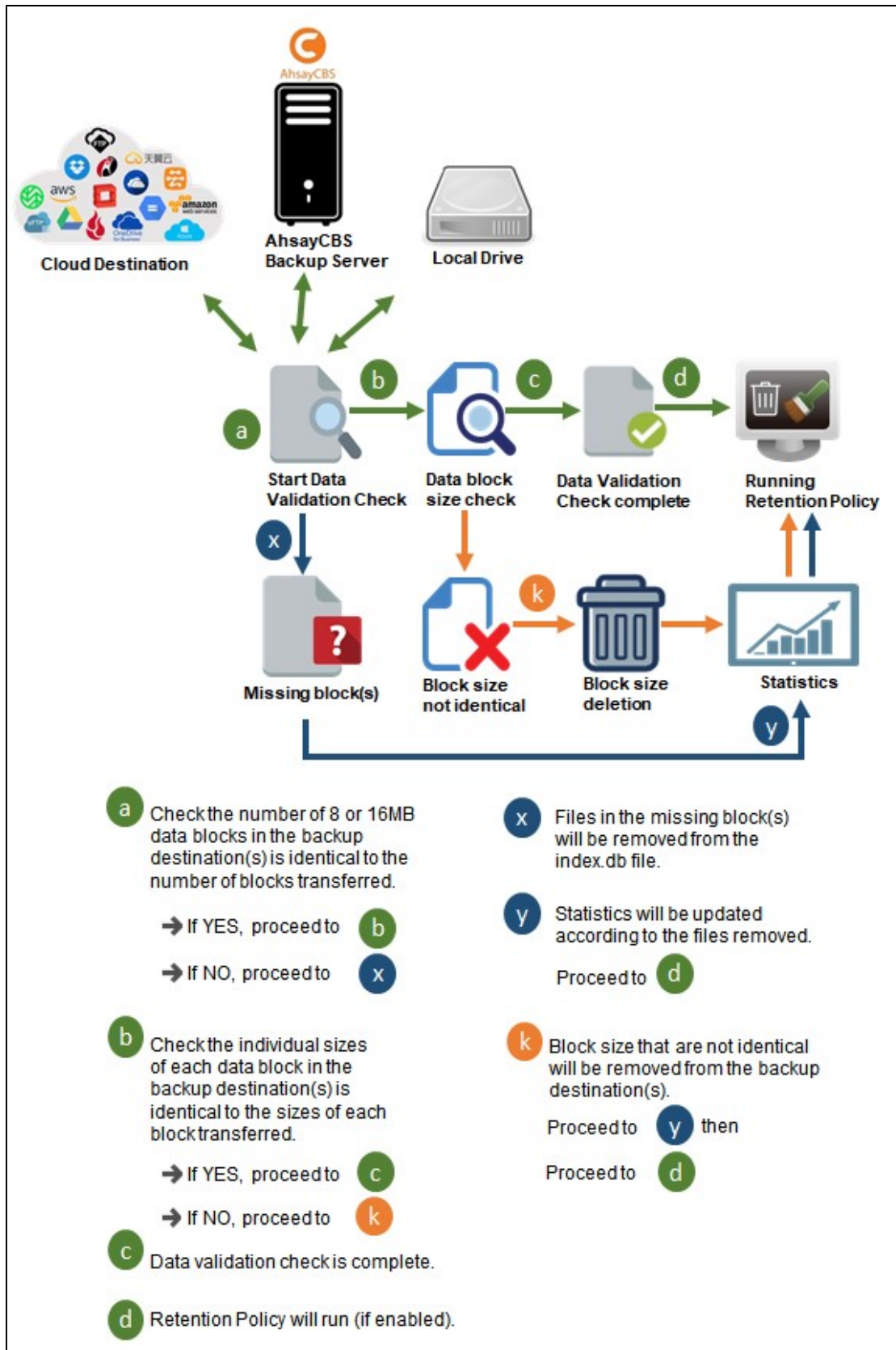


8.2.2 Completed Backup Job



8.3 Data Validation Check Process

As an additional measure to ensure that all files transferred to the backup destination(s) are received and saved correctly, both the number of 8 or 16 MB data block files and the size of each block file are checked again after the files are transferred.



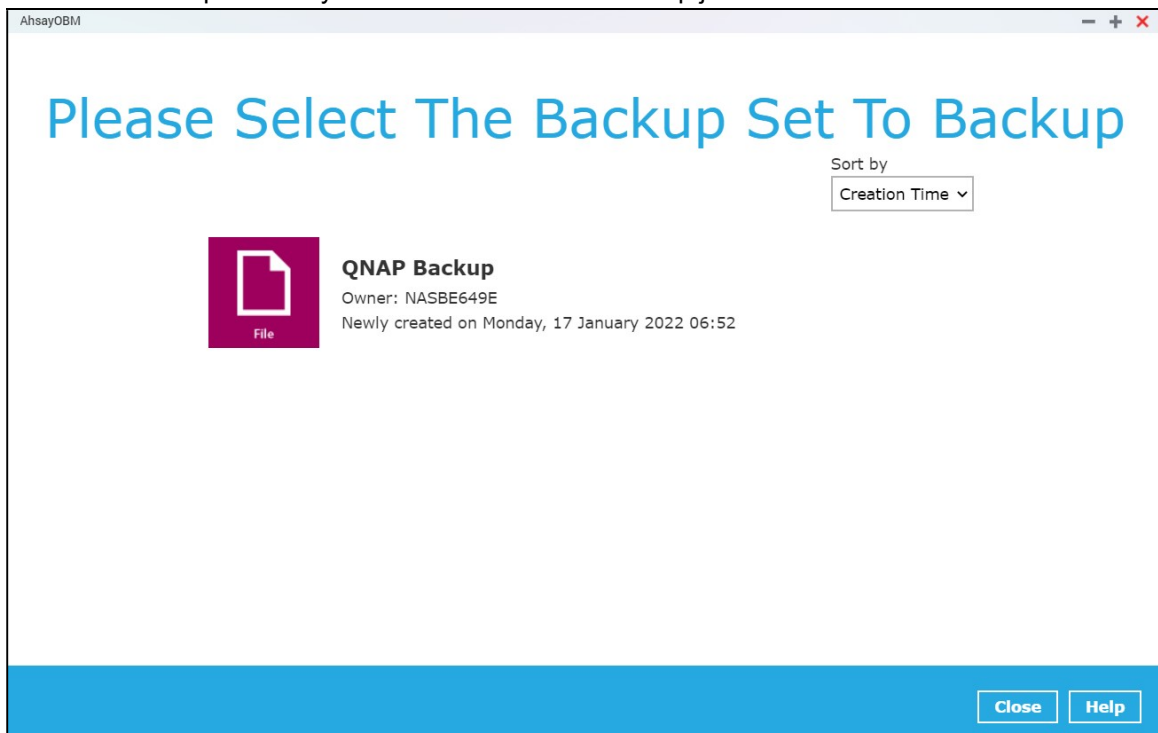
9 Run Backup Jobs

Start a Manual Backup

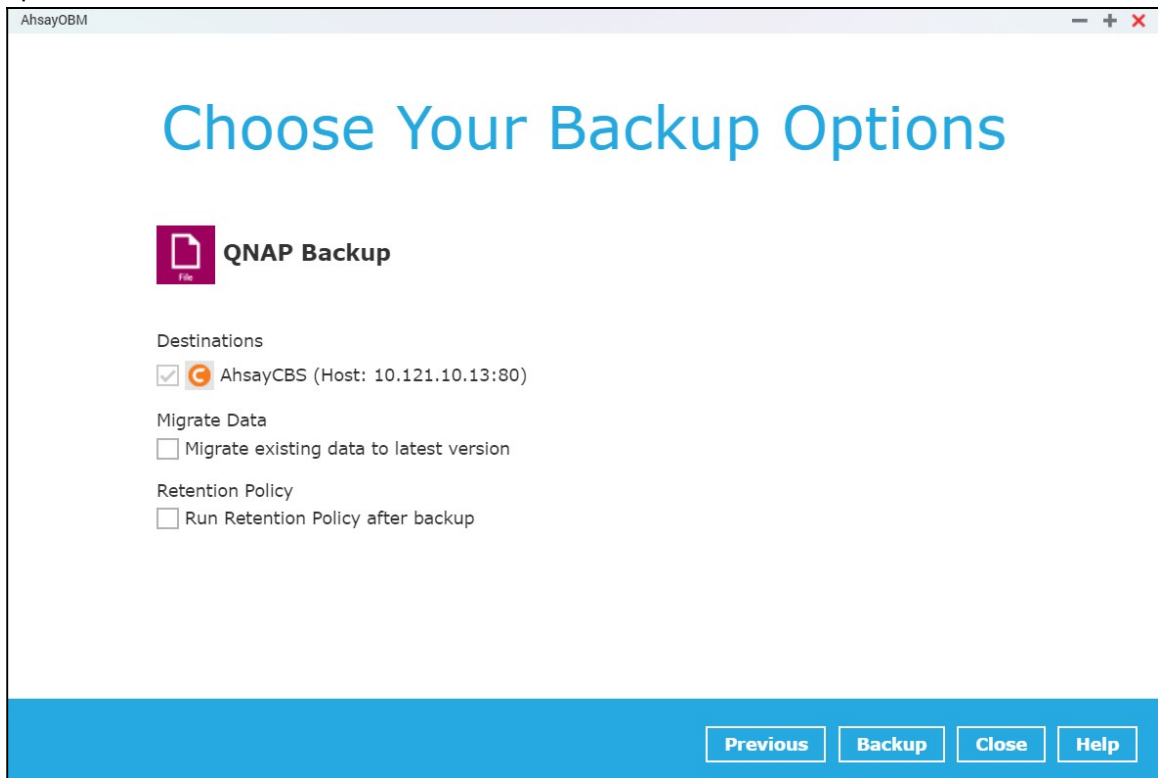
1. Login to the AhsayOBM application with the instructions provided in [Login to AhsayOBM](#).
2. Click **Backup** on the main interface of AhsayOBM.



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




4. 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:




AhsayOBM

Choose Your Backup Options

 **QNAP Backup**

Destinations

 AhsayCBS (Host: 10.121.10.13:80)

Migrate Data

Migrate existing data to latest version

Retention Policy

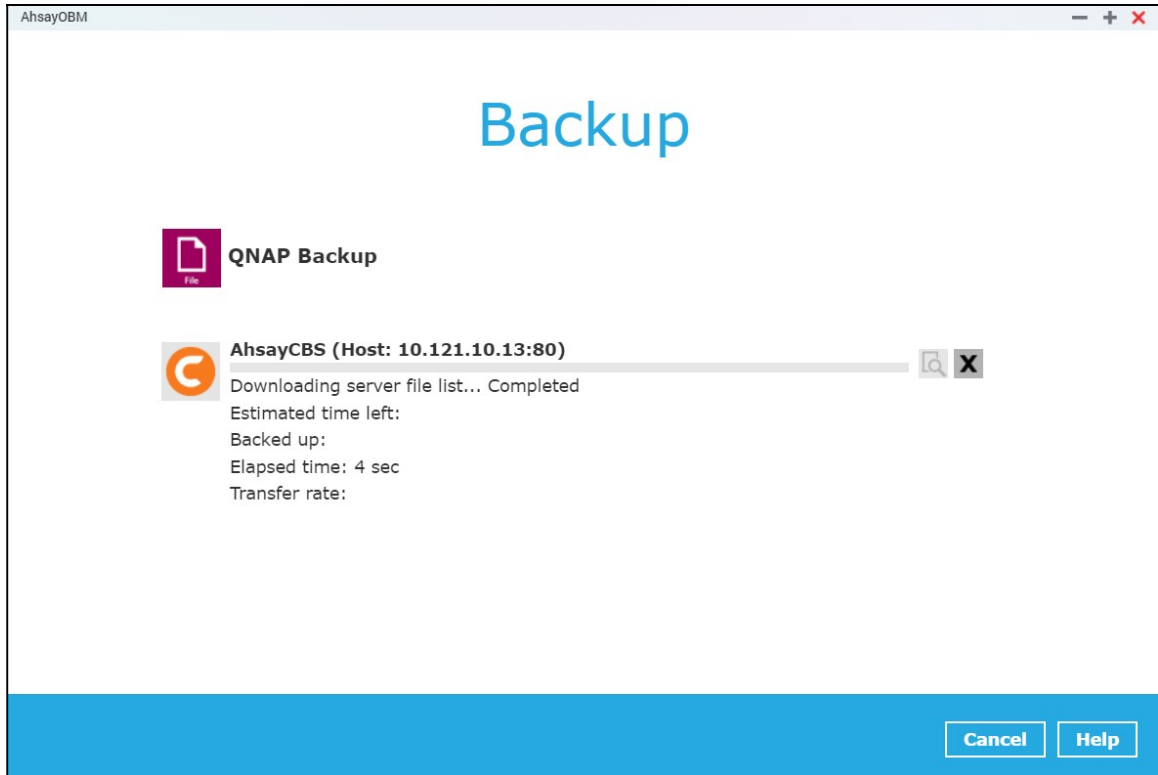
Run Retention Policy after backup

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

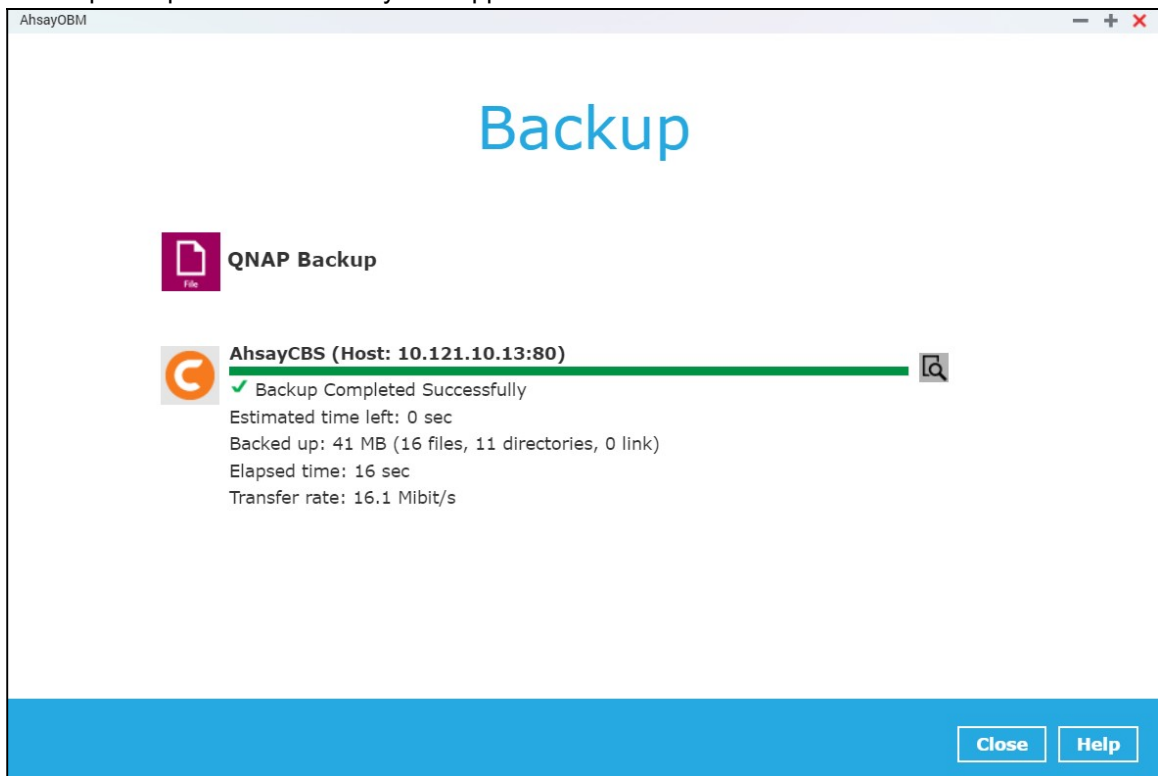
NOTE


When the **Migrate Data** option is enabled, the existing data will be migrated to the latest version during a backup job. This option is disabled by default. Backup job(s) for backup sets with Migrate Data enabled may take longer to finish. For more information about this feature, refer to [AhsayCBS v9 New Features Supplemental document](#).

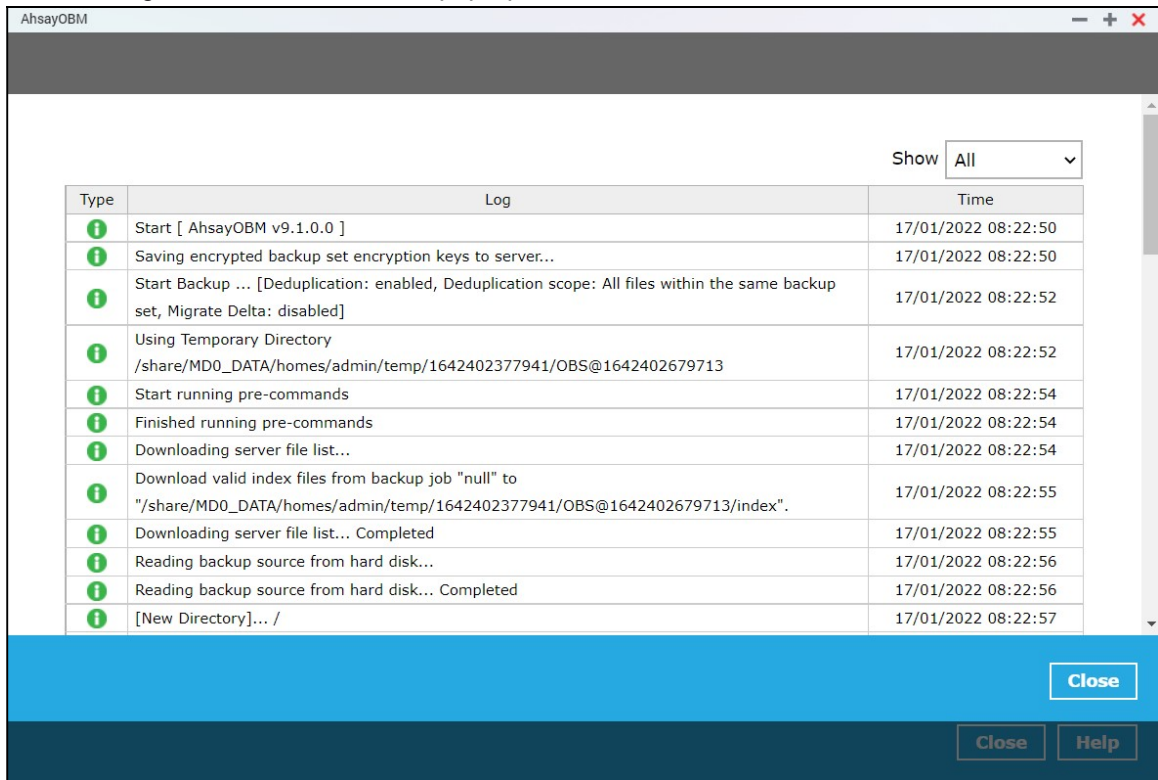
5. Click **Backup** to start the backup job. The status will be shown.















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



- 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 v9.1.0.0]	17/01/2022 08:22:50
	Saving encrypted backup set encryption keys to server..	17/01/2022 08:22:50
	Start Backup ... [Deduplication: enabled, Deduplication scope: All files within the same backup set, Migrate Delta: disabled]	17/01/2022 08:22:52
	Using Temporary Directory /share/MD0_DATA/homes/admin/temp/1642402377941/OBS@1642402679713	17/01/2022 08:22:52
	Start running pre-commands	17/01/2022 08:22:54
	Finished running pre-commands	17/01/2022 08:22:54
	Downloading server file list...	17/01/2022 08:22:54
	Download valid index files from backup job "null" to "/share/MD0_DATA/homes/admin/temp/1642402377941/OBS@1642402679713/index".	17/01/2022 08:22:55
	Downloading server file list... Completed	17/01/2022 08:22:55
	Reading backup source from hard disk...	17/01/2022 08:22:56
	Reading backup source from hard disk... Completed	17/01/2022 08:22:56
	[New Directory]... /	17/01/2022 08:22:57

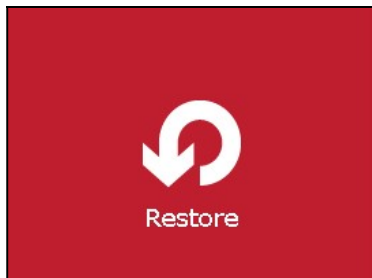
10 Restore Data

10.1 Login to AhsayOBM

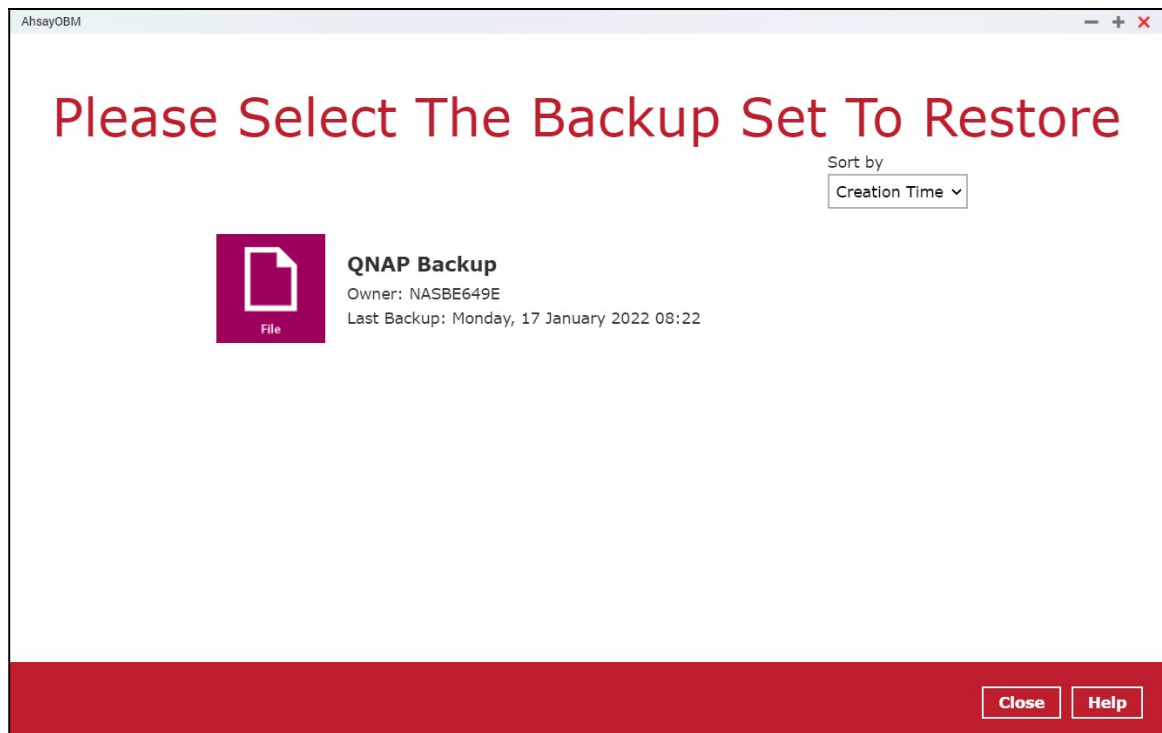
Login to the AhsayOBM application with the instructions provided in [Login to AhsayOBM](#).

10.2 Restore Data

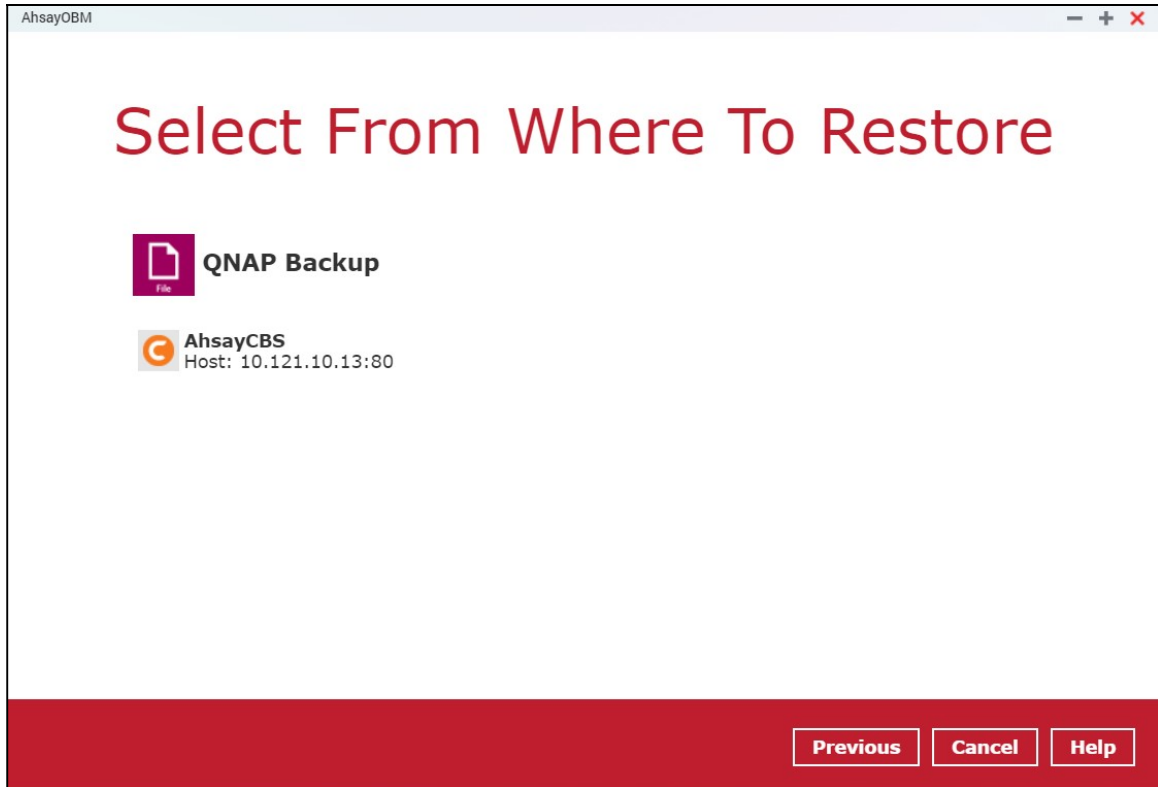
1. Click the **Restore** icon on the main interface of AhsayOBM.



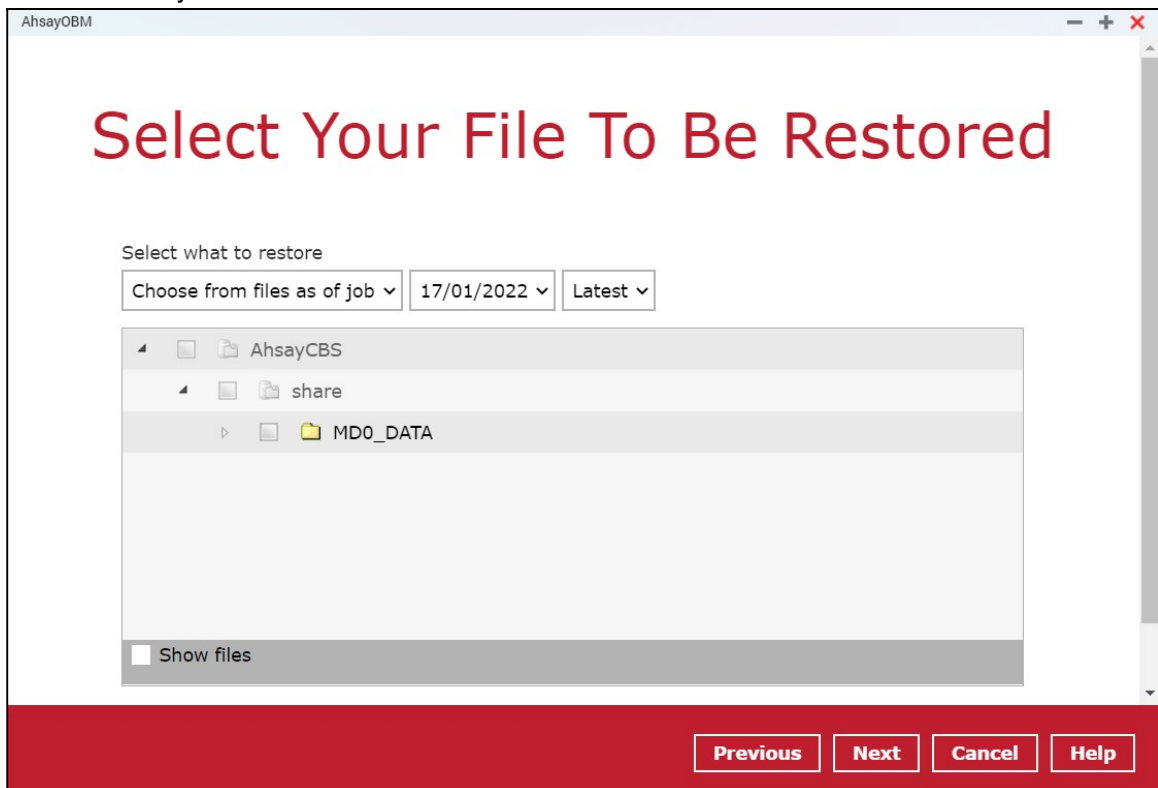
2. All the available backup sets for restore will be listed. Select the backup set that you would like to restore the data from.



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:

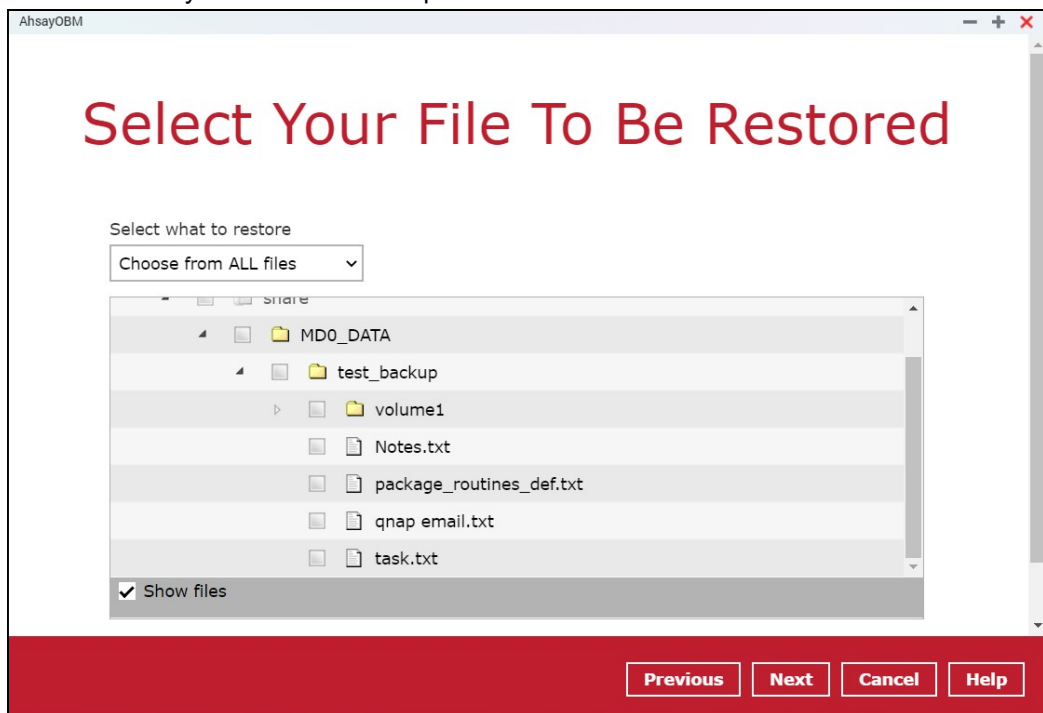
- **Choose from files as of job** – This option allows you to select a backup version from a specific date and time to restore.



Select what to restore

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

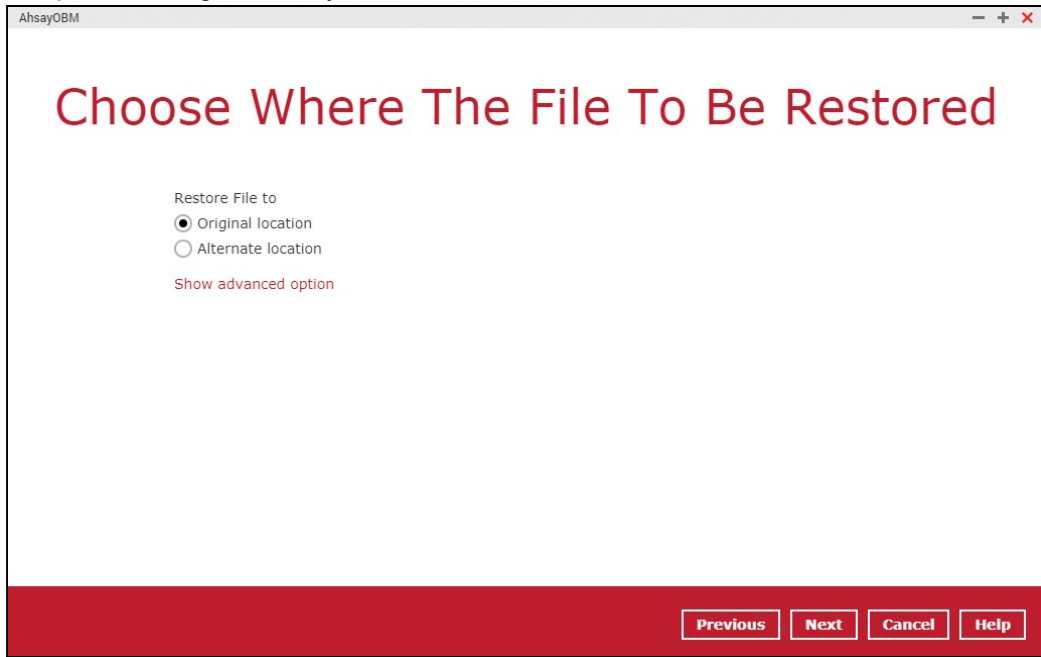
- **Choose from ALL files** – This option allows you to restore all the available backup files and folders for this backup set. Among all the available backup files and folders, you can even select only some of the backup files or folders to restore.



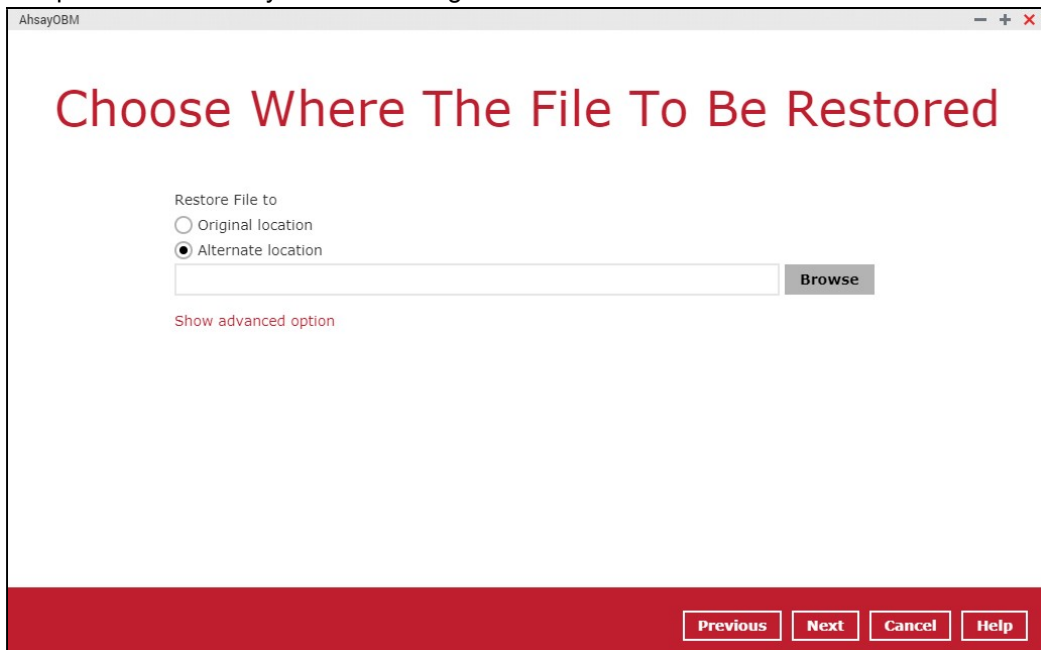
Click the **Show files** checkbox to select individual files for restoration. Click **Next** to proceed when you are done with the selections.

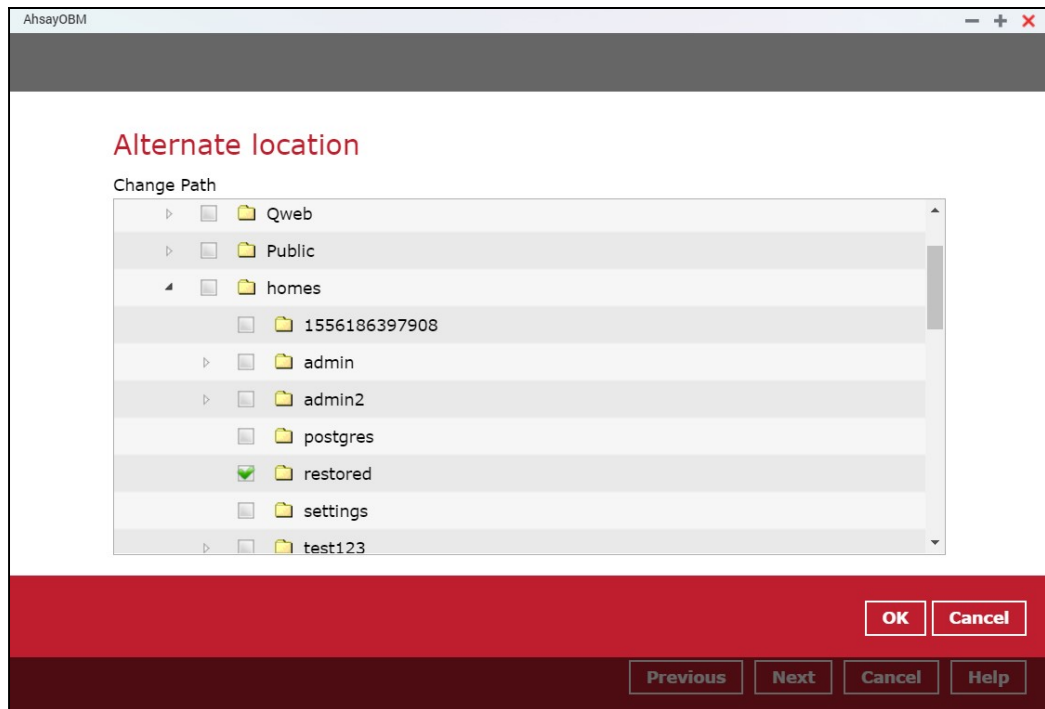
5. Select to restore the files to their **Original location**, or to an **Alternate location**. Then click **Next** to proceed.

- **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.

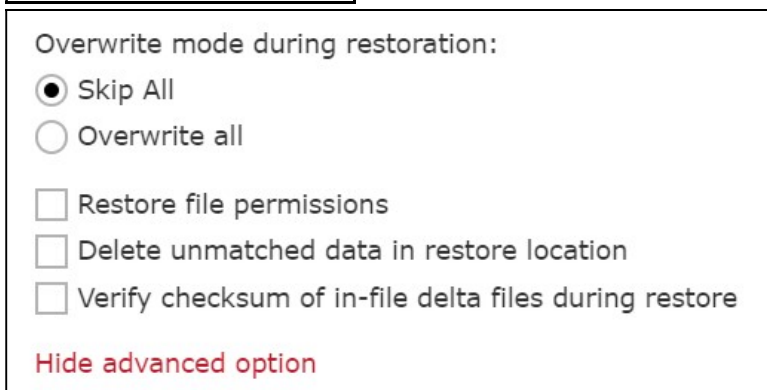
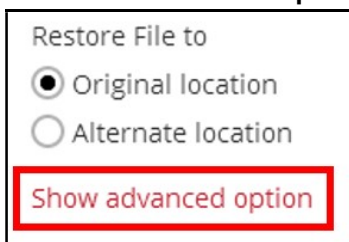


- **Alternate location** – you can choose to restore the data to a location of your choice on the computer where AhsayOBM is running.





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



Overwrite mode during restoration

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

Restore file permissions

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

Delete unmatched data in restore location

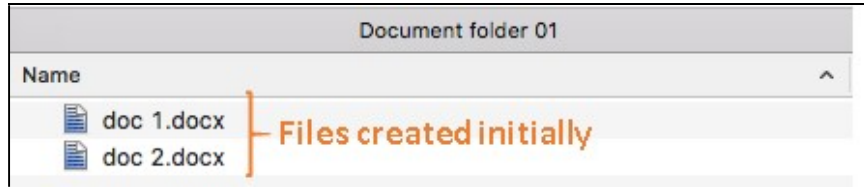
Synchronize the selected restore source with the restore destination.

By enabling this option, the restore process will attempt to synchronize the selected restore

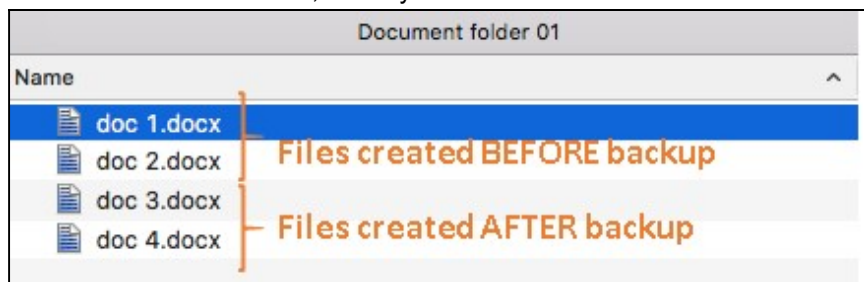
source with the restore destination, making sure the data in the restore destination is exactly the same as the restore source. Any data created after backup will be treated as “unmatched data” and will be deleted from the restore source if this feature is enabled.

Example:

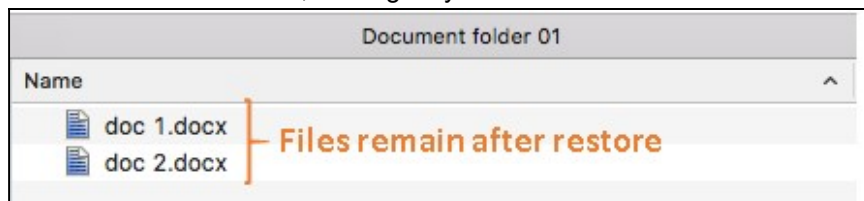
- Two files are created under the Document folder 01, namely doc 1 & doc 2.



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



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



WARNING

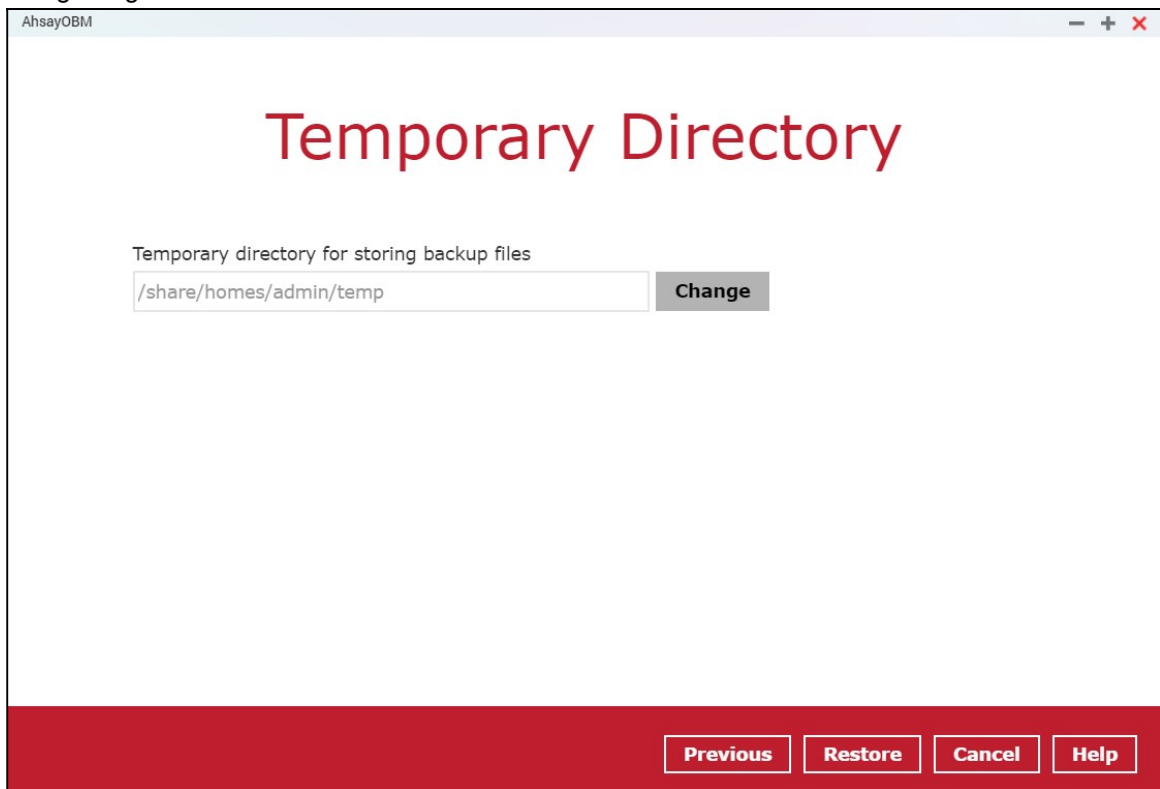
Please exercise extra caution when enabling this feature. Consider what data in the restore source has not been backed up and what impact it would cause if those data were deleted.

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

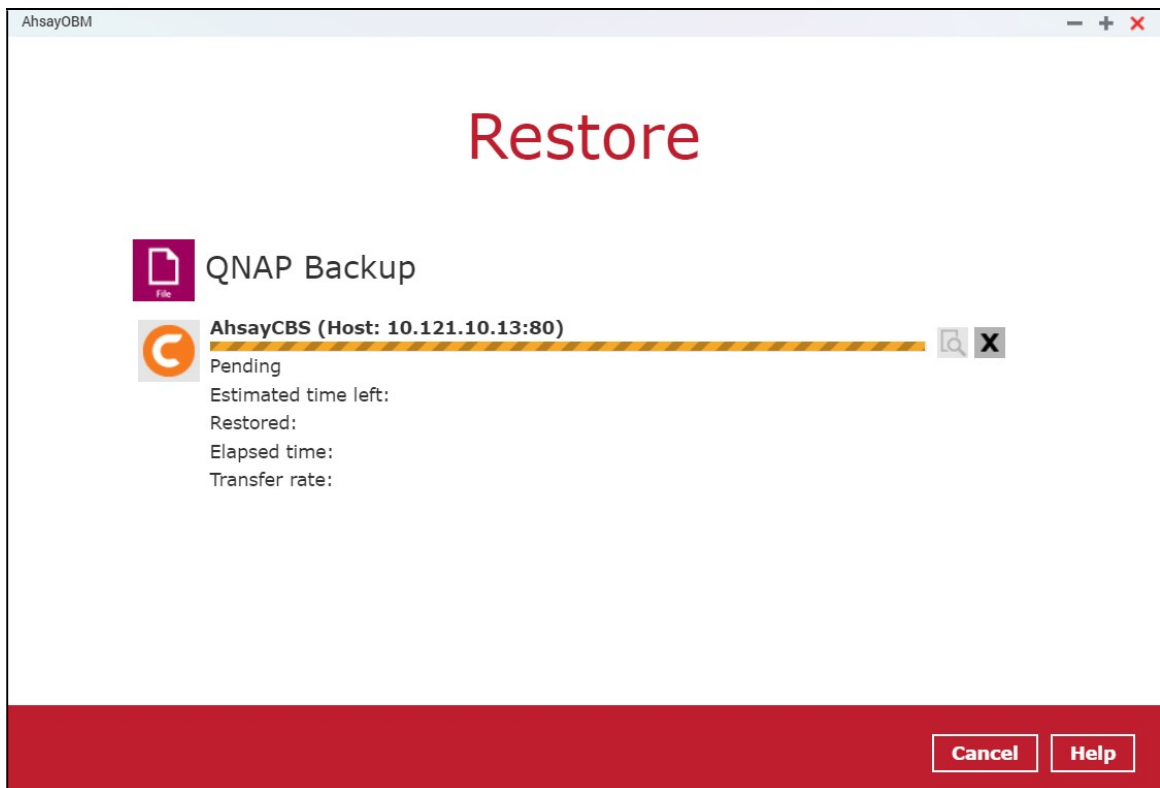
- **Verify checksum of in-file delta files during restore**
Verify checksum of in-file delta files during restore is disabled by default. You can enable the feature by ticking the checkbox so that the checksum of in-file delta files will be verified. As the feature will make the restore process time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

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

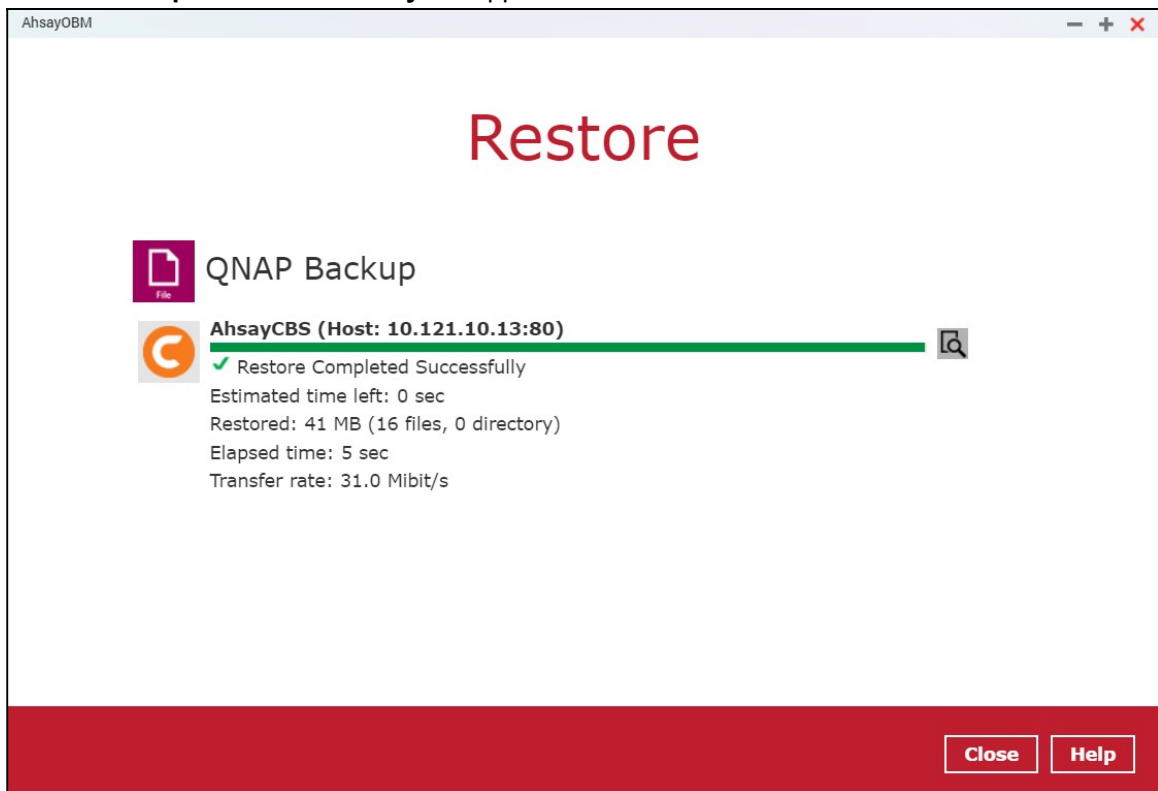
7. Select the temporary directory for storing temporary files, such as delta files when they are being merged.




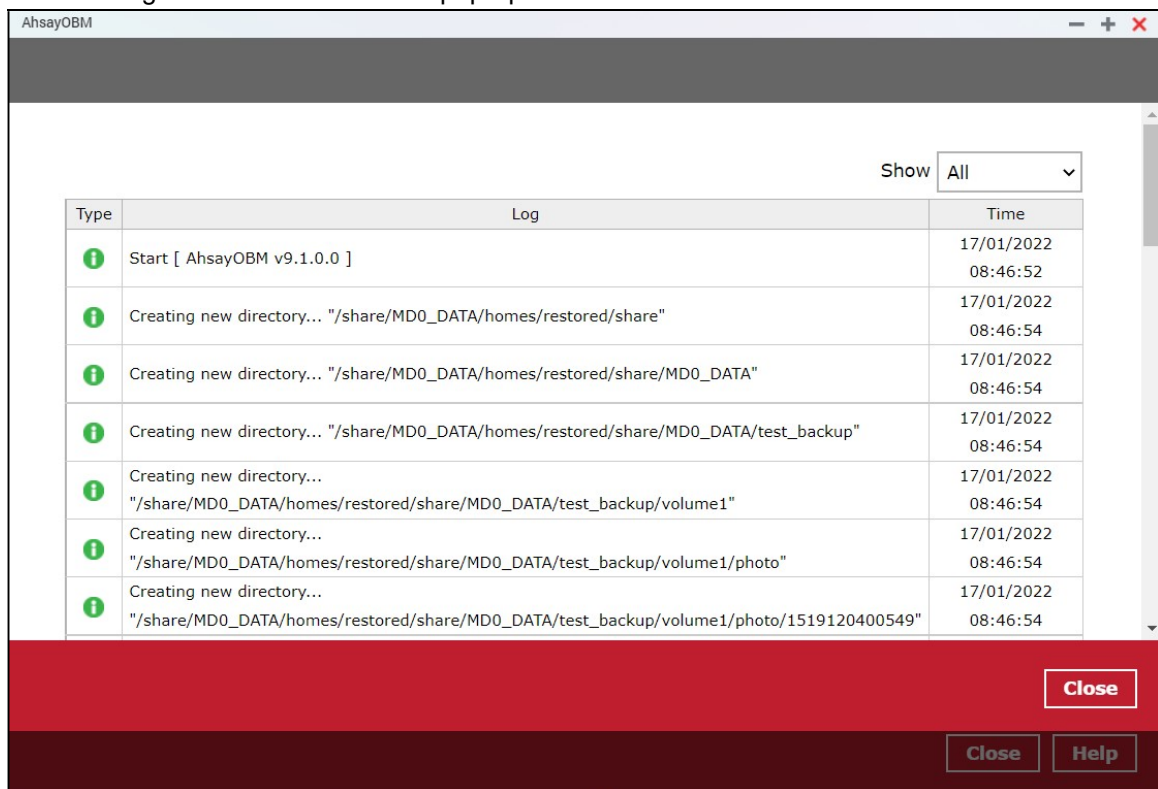
8. Click **Restore** to start the restore. The status will be shown.



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



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.



- In the Restore window, click **Close** to close the Restore window.

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:

<https://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

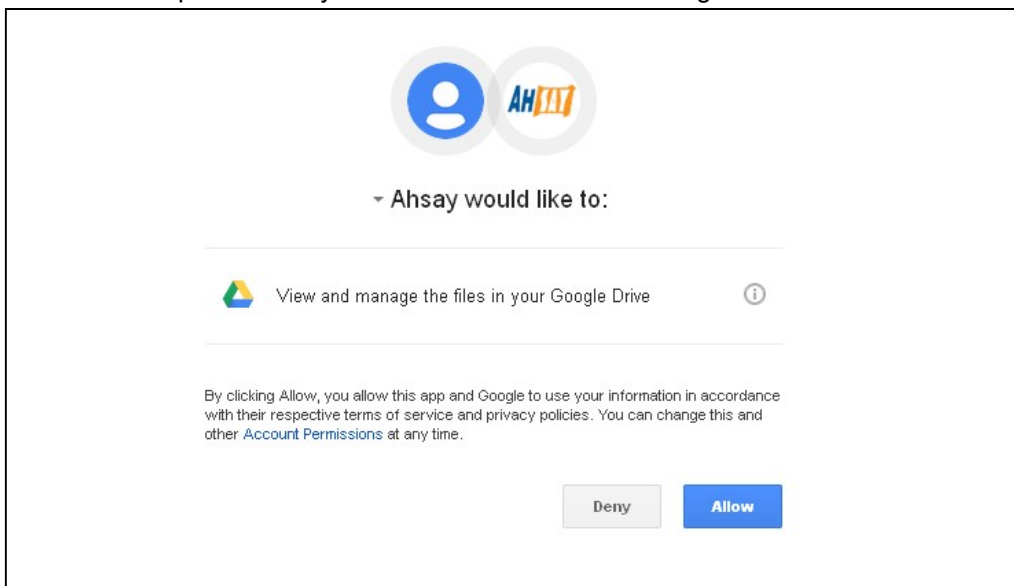
Appendix A: Cloud Storage as Backup Destination

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.

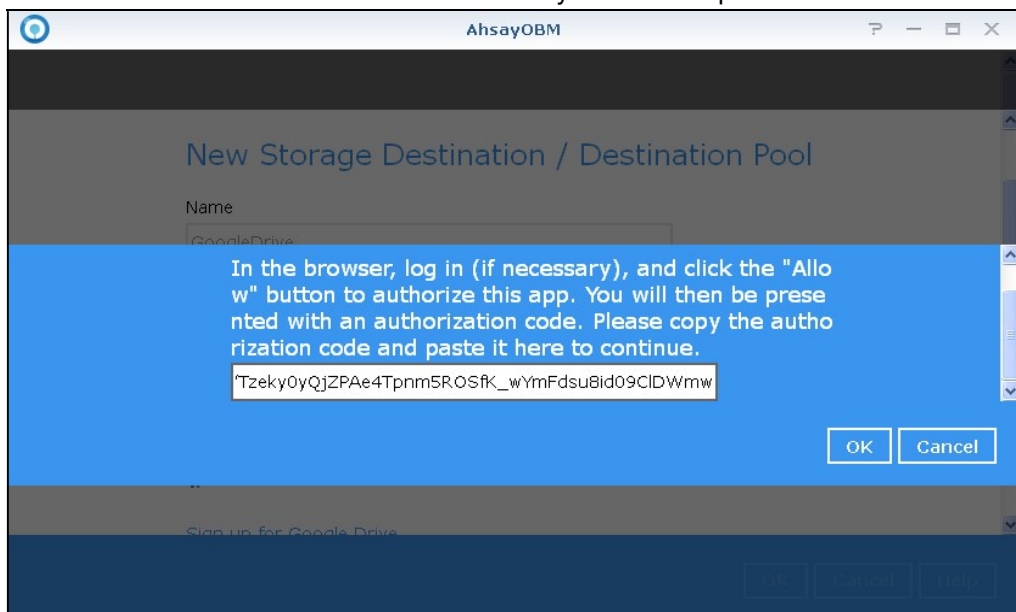
IMPORTANT

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

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



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



NOTE

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

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

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

[FAQ: Frequently Asked Questions on Backup Destination](#)

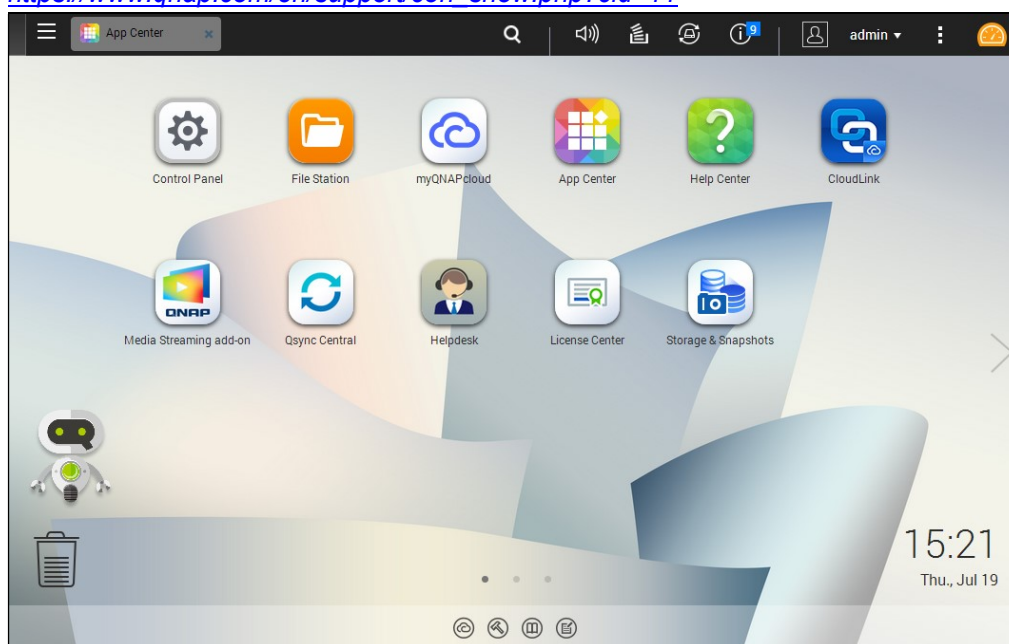
Appendix B: Uninstall AhsayOBM

Refer to the following steps to uninstall AhsayOBM.

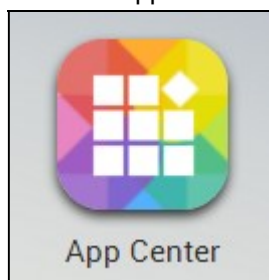
1. Login to QNAP QTS with the admin account. In a web browser, enter the QNAP NAS device IP address and use the login credentials to login.

Note: Refer to the following user manual for information on how to login to QTS:

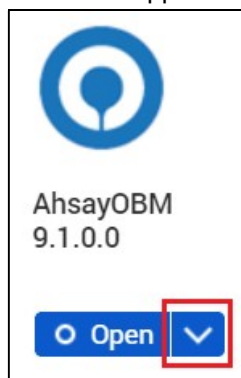
https://www.qnap.com/en/support/con_show.php?cid=11



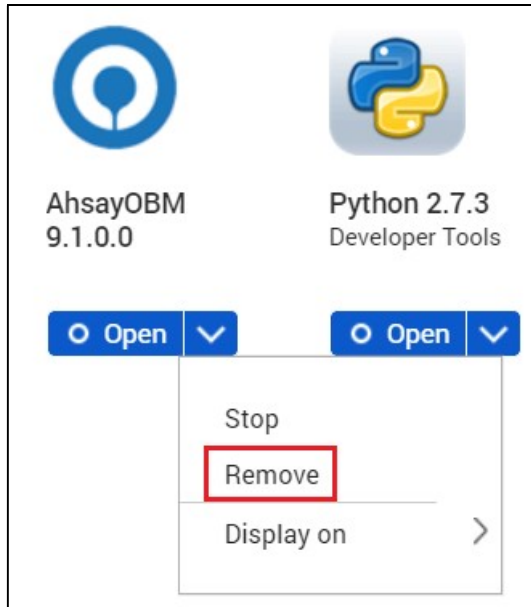
2. Click the App Center icon on the desktop.



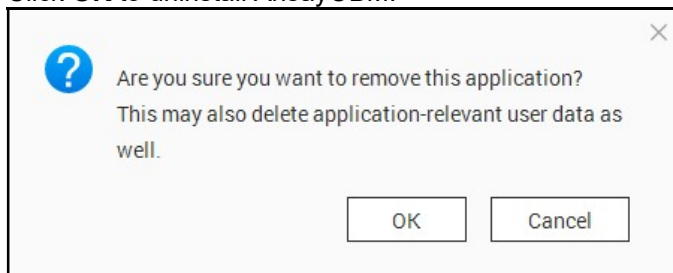
3. When the App Center window appears, click the arrow icon of AhsayOBM.



4. Select **Remove** to uninstall the AhsayOBM.



5. Click **OK** to uninstall AhsayOBM.



NOTE

If you select **OK**, AhsayOBM program files, user settings and AhsayOBM-relevant user data will be removed from the NAS drive.

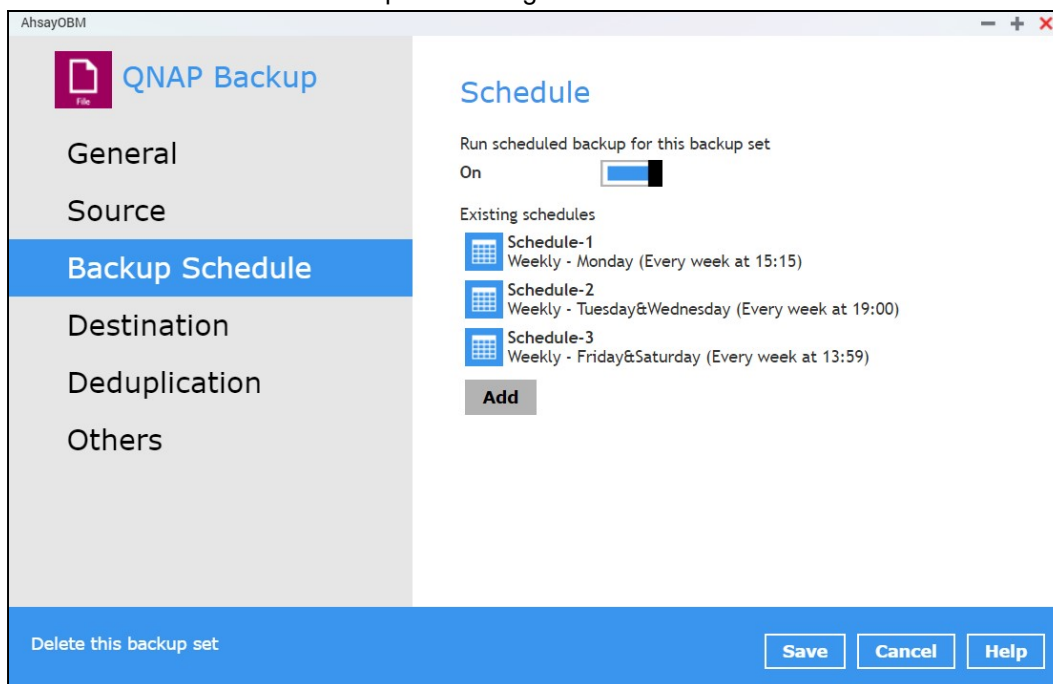
6. When the uninstallation is completed, the following message will appear.



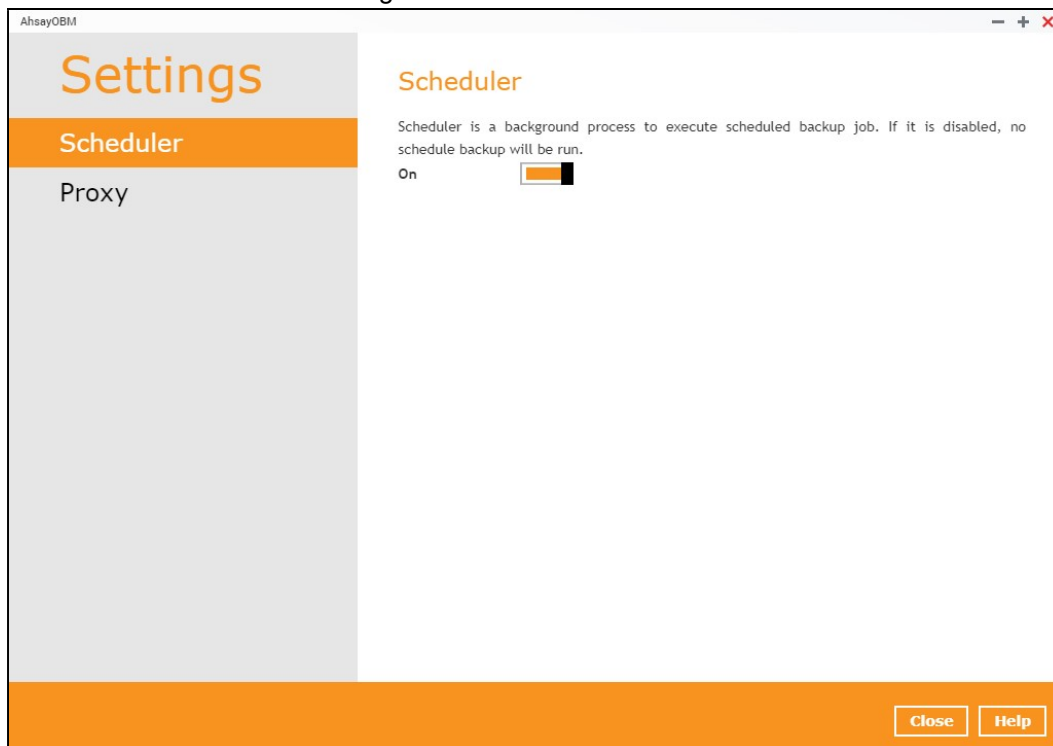
Appendix C: Scheduler Scenarios

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

Level 1: Scheduler under Backup Set Settings

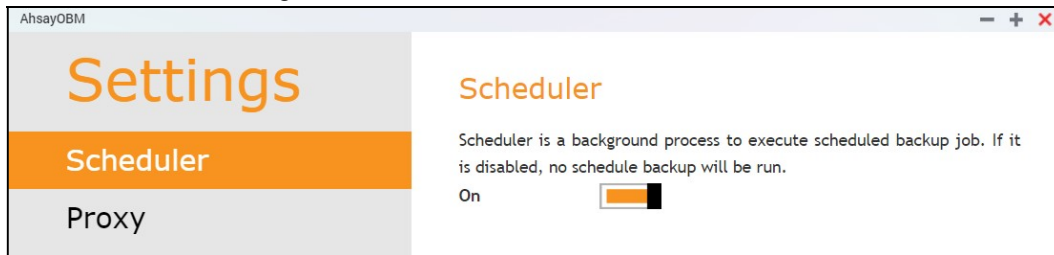


Level 2: Scheduler under Settings

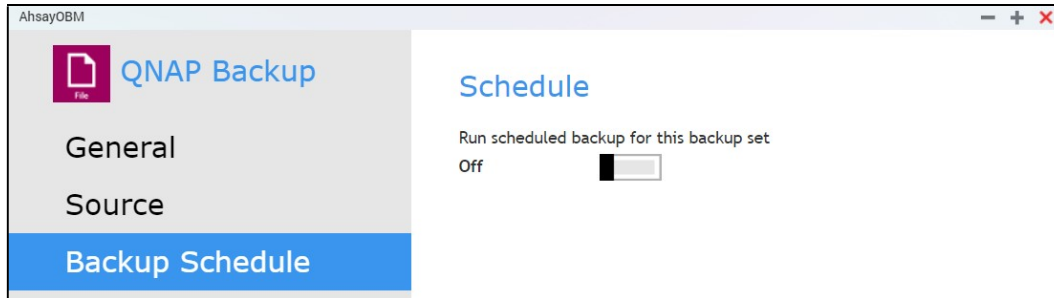


Scenario no. 1: Scheduler under Setting is ON, and Scheduler under Backup Set Settings is OFF

Scheduler under Setting



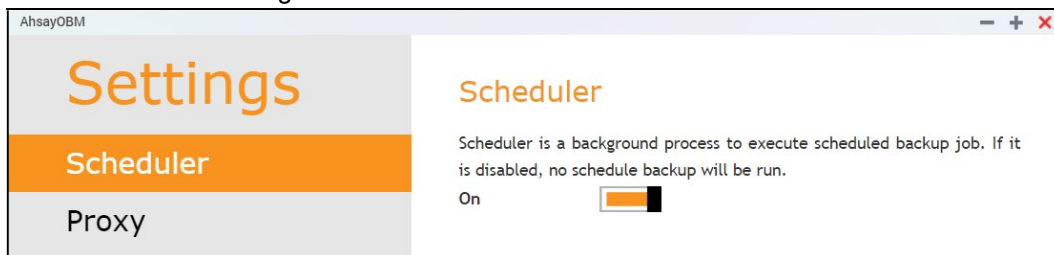
Scheduler under Backup Set Settings



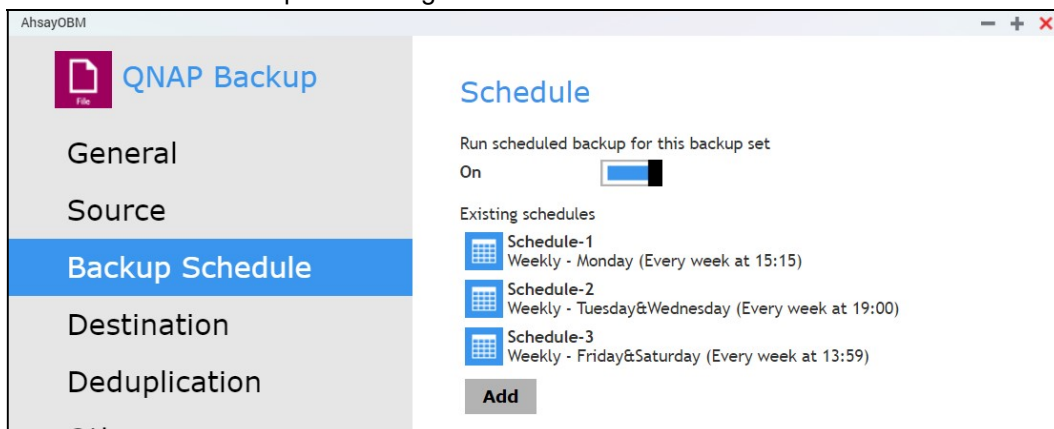
Result: There is no scheduled backup job will be run for the backup set.

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

Scheduler under Setting



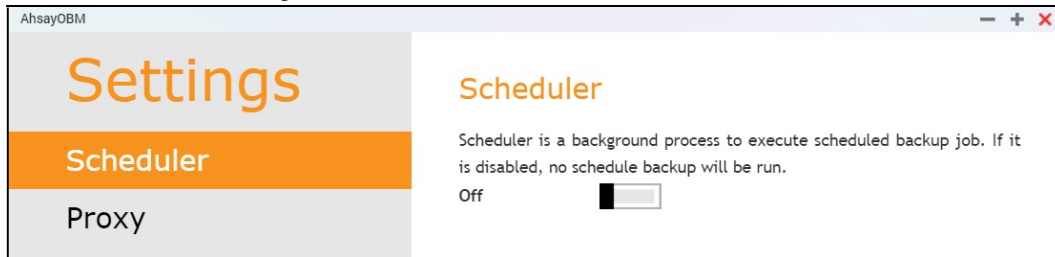
Scheduler under Backup Set Settings



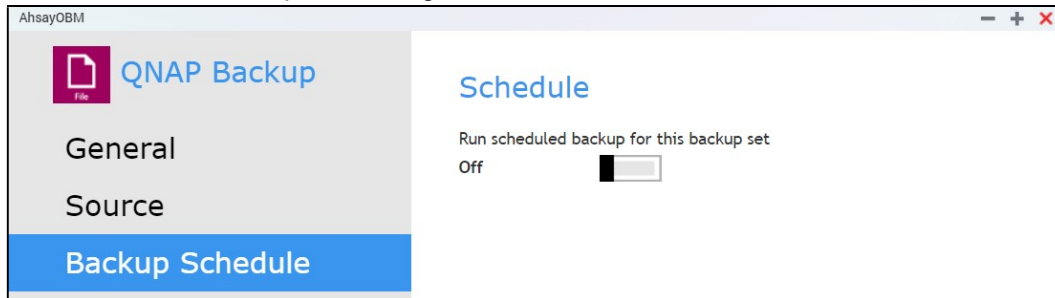
Result: Scheduled backup jobs which are Schedule-1, Schedule-2, and Schedule-3 for the backup set will run.

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

Scheduler under Setting



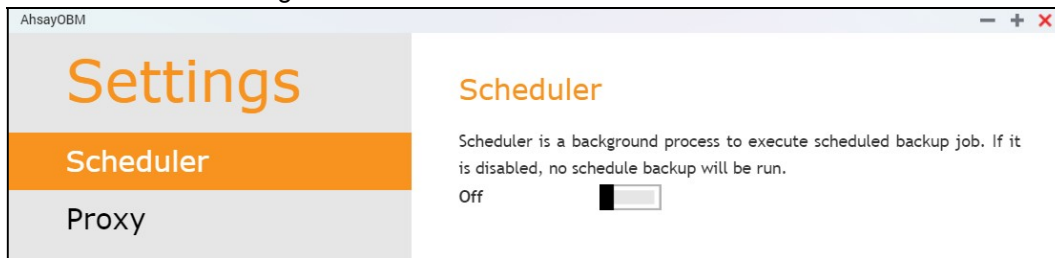
Scheduler under Backup Set Settings



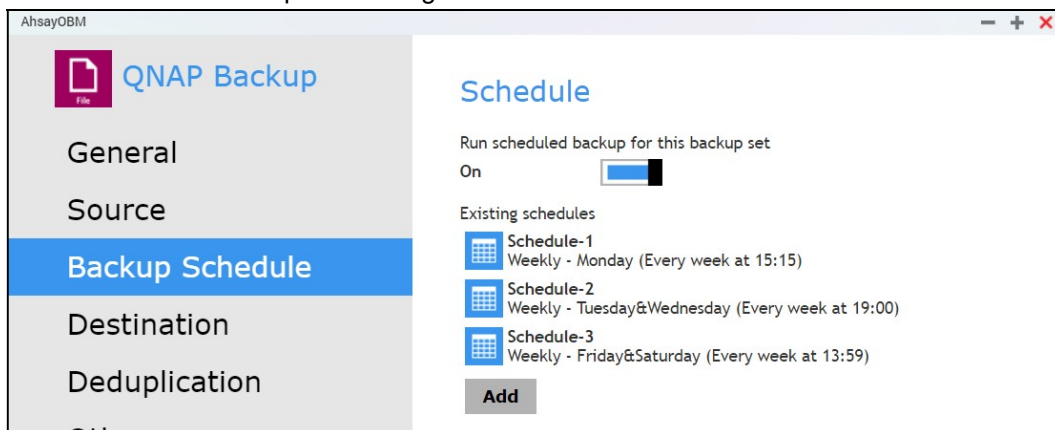
Result: There is no scheduled backup job will be run for the backup set.

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

Scheduler under Setting



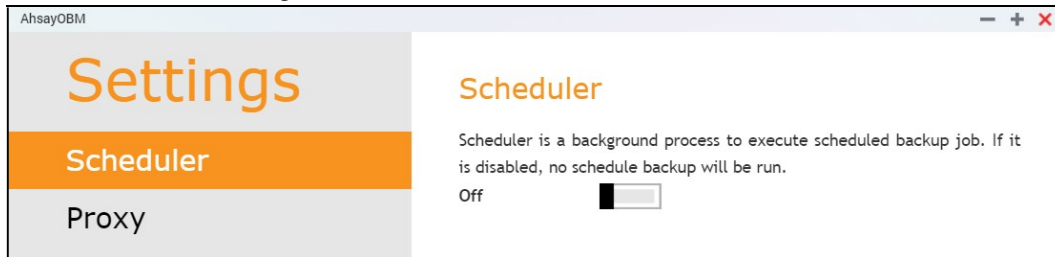
Scheduler under Backup Set Settings



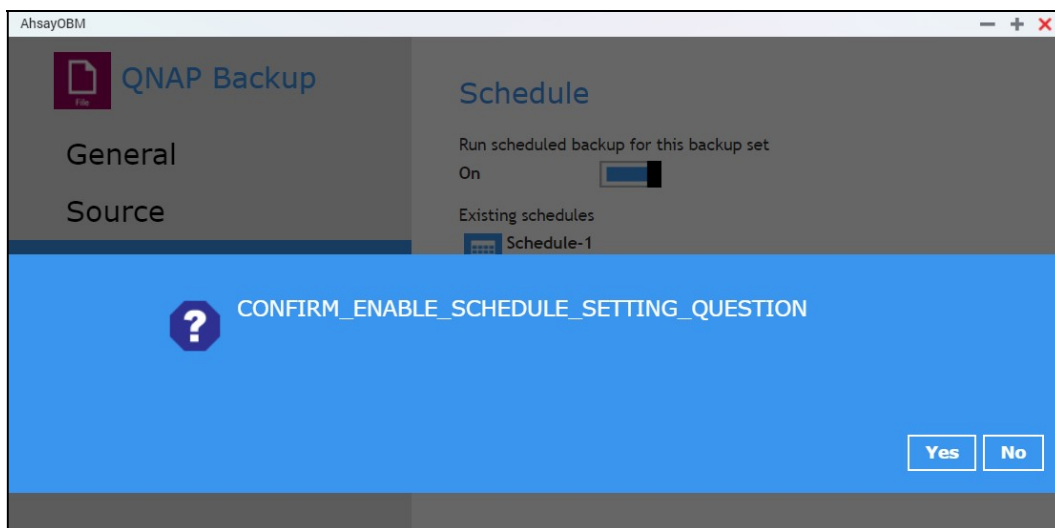
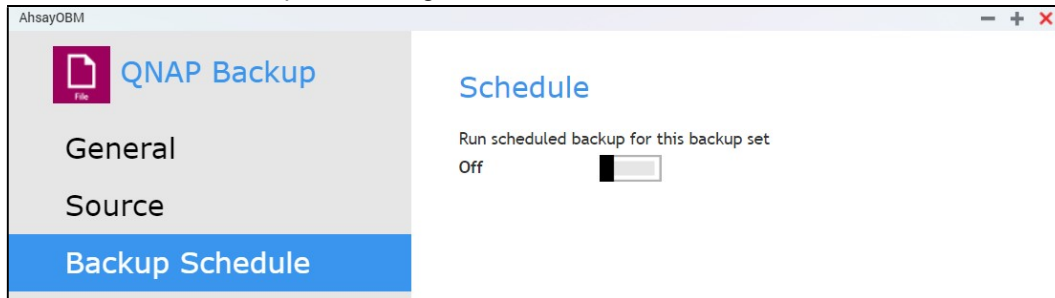
Result: There is no scheduled backup job will be run for the backup set.

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:

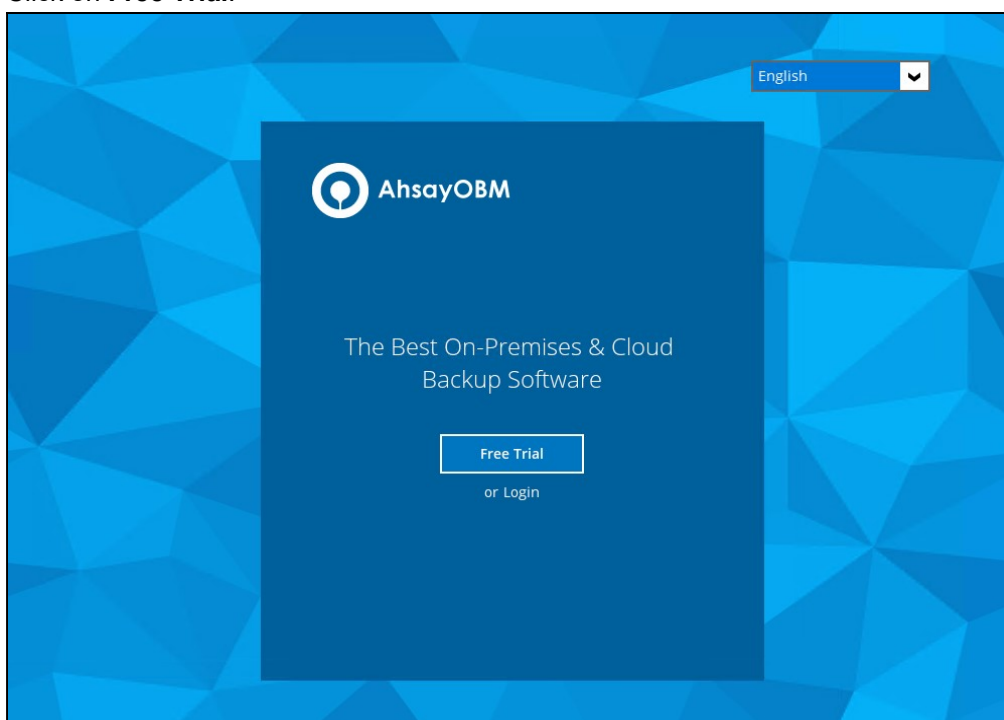
- A valid email address which will be used for receiving notices. A welcome message will also be sent upon creation of the account which specifies the User Setting and Quota set for backup in AhsayCBS.

While here are the limitations of a trial account:

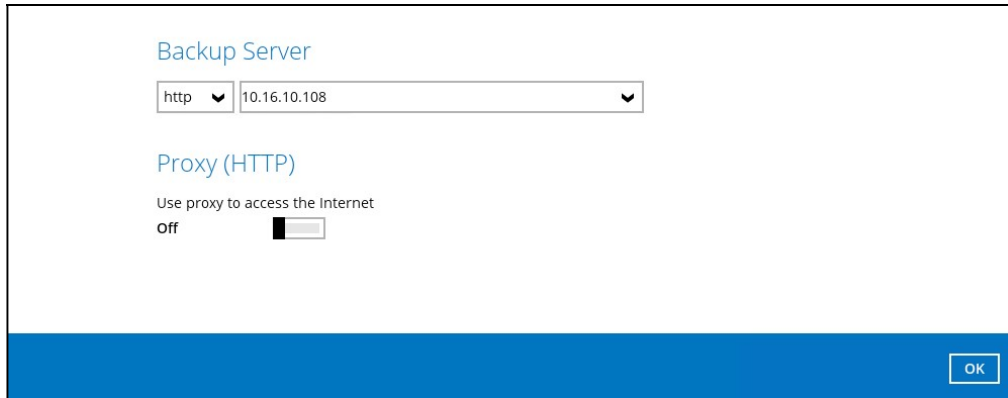
- The Free Trial button will only be displayed once when the user login for the first time. If you cannot create a free trial account kindly contact your backup service provider.
- Only alphanumeric characters and selected special characters, A to Z, 0 to 9, @, - and _ , are allowed to be used for the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

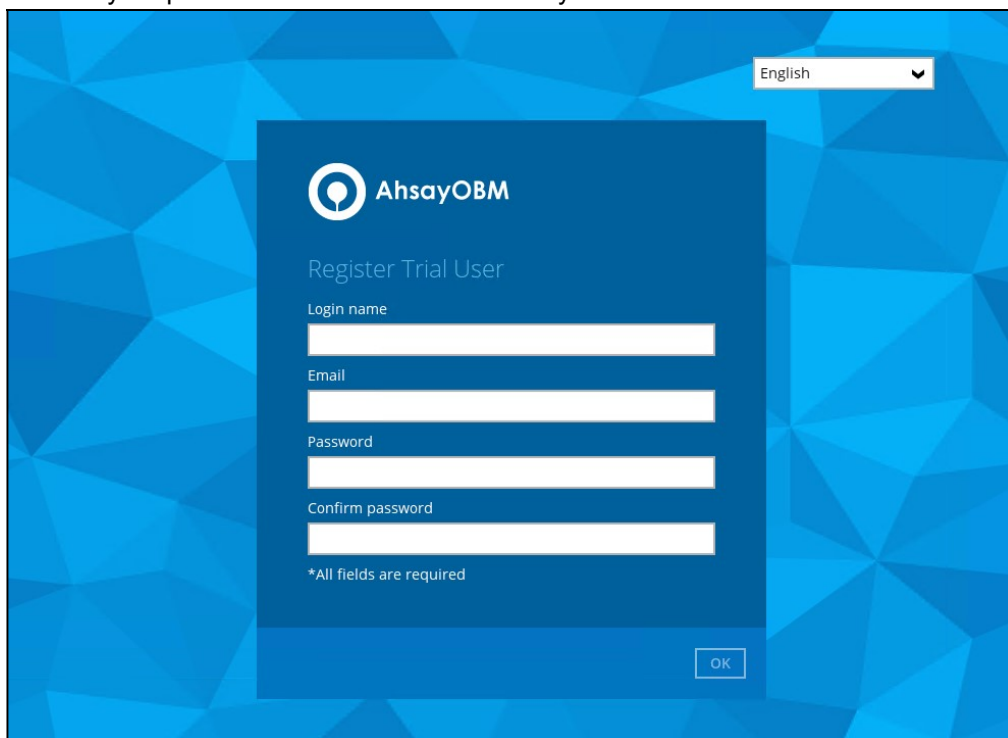


2. Configure your Backup Server settings.



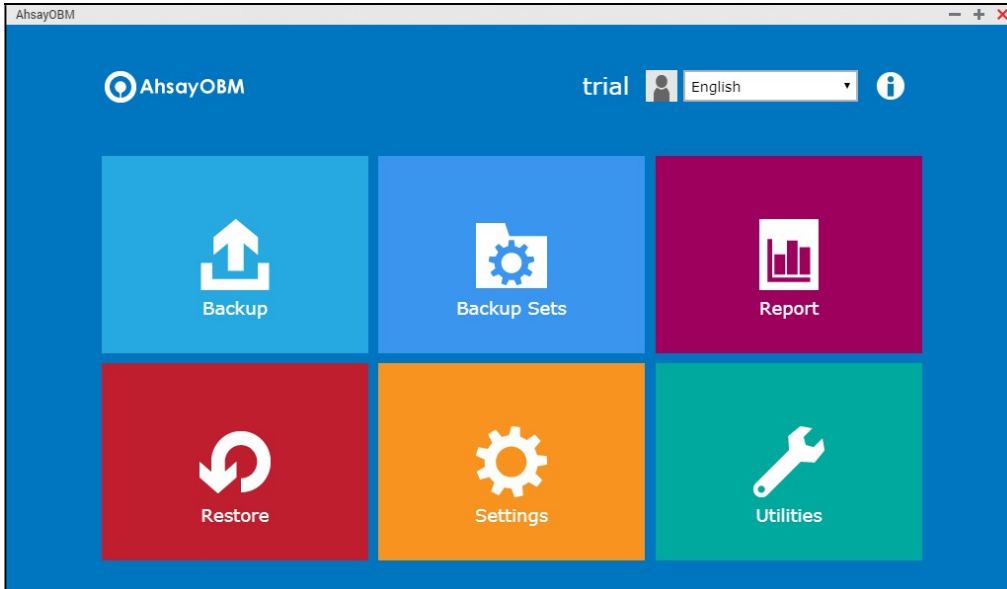
The screenshot shows a configuration window titled "Backup Server". It contains two dropdown menus: the first is set to "http" and the second is set to "10.16.10.108". Below these is a section titled "Proxy (HTTP)" with the text "Use proxy to access the Internet" and a toggle switch labeled "off". An "OK" button is located in the bottom right corner of the window.

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 "AhsayOBM Register Trial User" form. The background is a blue geometric pattern. In the top right corner, there is a language dropdown menu set to "English". The form itself is a dark blue box with the AhsayOBM logo and the title "Register Trial User". It contains four input fields: "Login name", "Email", "Password", and "Confirm password". Below the fields is the text "*All fields are required". An "OK" button is located in the bottom right corner of the form.

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



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

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

User Profile	General	Backup Client Settings	Contact	User Group	Authentication	Mobile Backup
Backup Set	Suspend At <input type="text" value="17-02-2022"/> (dd-mm-yyyy)					
Settings	Status <input checked="" type="radio"/> Enable <input type="radio"/> Suspended <input type="radio"/> Locked					
Report	Upload Encryption Key <input checked="" type="checkbox"/> Upload encryption key after running backup for recovery					
Statistics	Language <input type="text" value="English"/>					
Effective Policy	Timezone <input type="text" value="GMT+08:00 (CST)"/>					

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

The screenshot shows the 'Backup Client Settings' tab for a user profile. The left sidebar contains 'User Profile', 'Backup Set', 'Settings', 'Report', 'Statistics', and 'Effective Policy'. The main content area has tabs for 'General', 'Backup Client Settings', 'Contact', 'User Group', 'Authentication', and 'Mobile Backup'. Under 'Backup Client Settings', there are radio buttons for 'AhsayOBM User' (selected) and 'AhsayACB User'. Below is the 'Add-on Modules' section with a grid of 20 items, each with a checked checkbox and a numerical input field:

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

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.

The screenshot shows the 'Contact' tab for a user profile. The left sidebar is the same as in the previous screenshot. The main content area has tabs for 'General', 'Backup Client Settings', 'Contact', 'User Group', 'Authentication', and 'Mobile Backup'. Under 'Contact', there is a 'Manage Contact Information' section with a plus icon to add and a trash icon to delete. Below is a table with one contact entry:

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