Ahsay Backup

Ahsay Online Backup Manager v8

Quick Start Guide for QNAP NAS

Ahsay Systems Corporation Limited

30 April 2021

Copyright Notice

Trademarks

Disclaimer

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

Revision History

Date	Descriptions	Type of modification
3 January 2020	Modified the diagram for the Overview on the Backup Process and added a diagram for the Detailed Process of Periodic Data Integrity Check in Ch. 8	New / Modification
6 February 2020	Modified the Data Integrity Check in Ch. 6 and added the TCP port requirement in Ch. 2	New / Modification
30 July 2020	Modified system architecture in Ch.1.2; Modified requirements in Ch. 2; Added periodic backup schedule and DIC diagram in Ch. 6; Updated PDIC diagram in Ch. 8	New / Modifications
23 September 2020	Updated PDIC diagram in Ch. 8	Modification
7 April 2021	Updated Ch. 8; added sub-chapters for the detailed process diagrams in Ch. 8.1, 8.2, 8.2.1, 8.2.2 and 8.3	Modifications
30 April 2021	Updated description of Data Integrity Check in Ch. 6.10.1; Updated description of Delete Backup Data in Ch. 6.10.2; Added notes for Periodic Data Integrity Check (PDIC) in Ch. 8.1	New / Modifications

Table of Contents

1 Overview

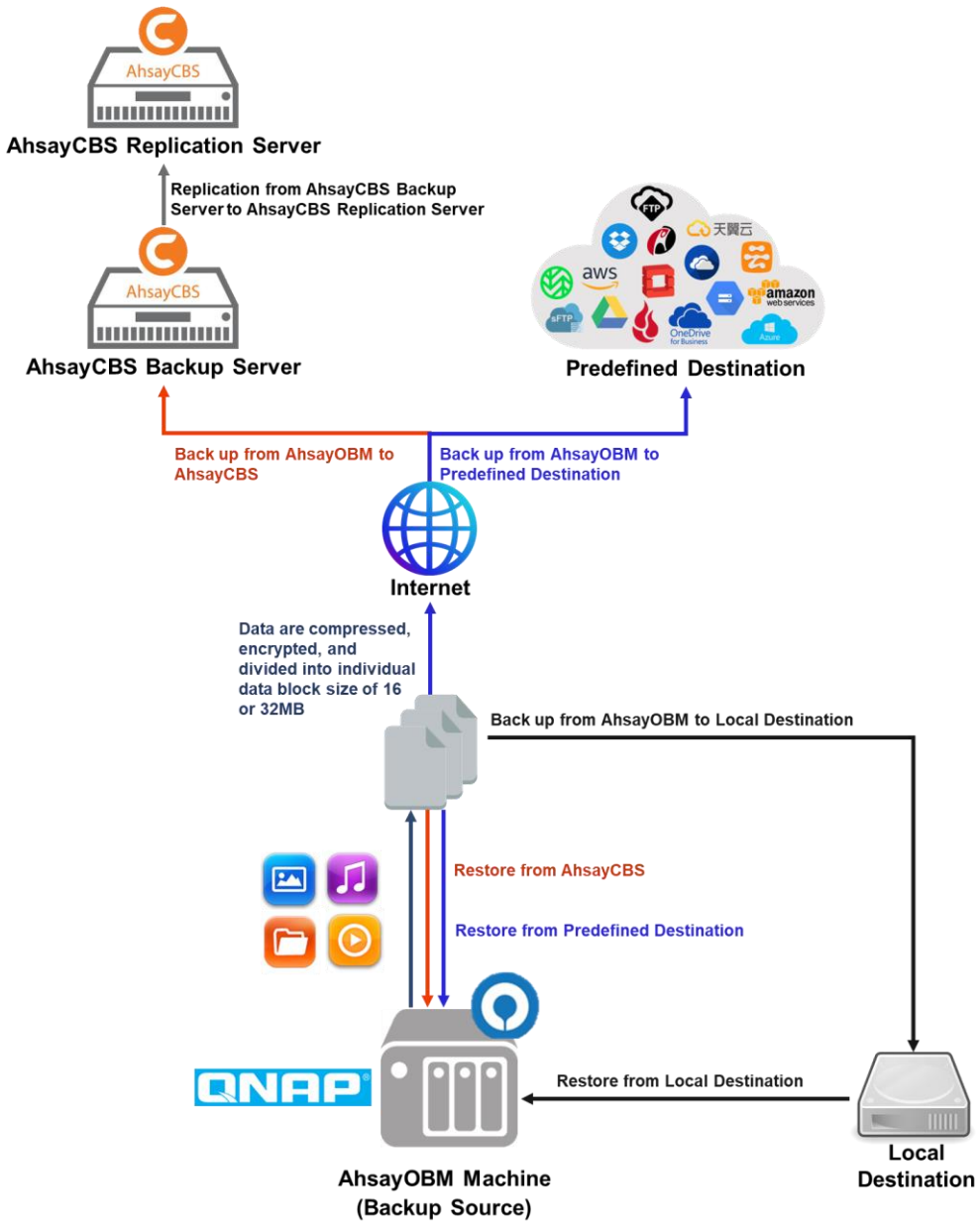
1.1 What is this software?

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

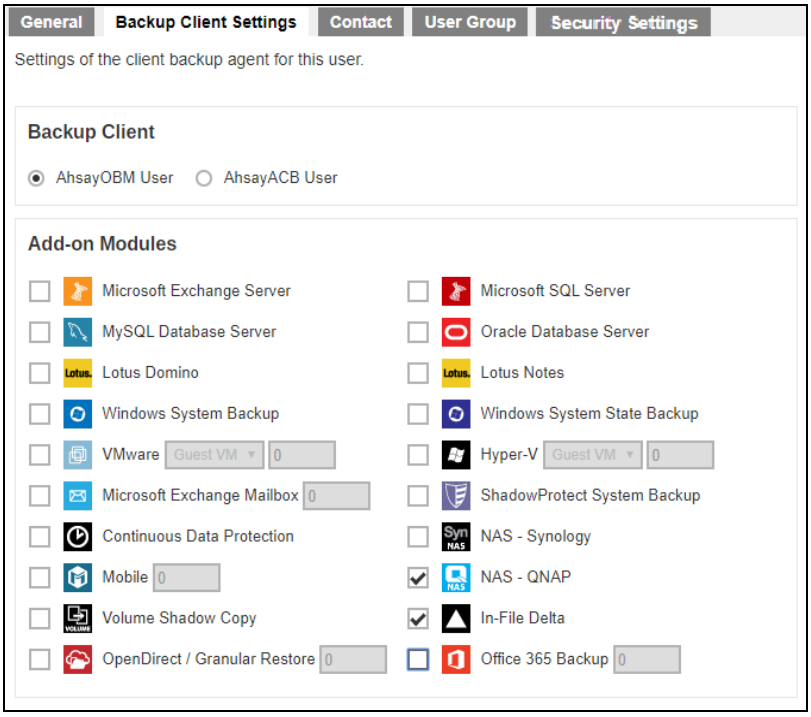
The latest version of AhsayOBM must be installed on the QNAP NAS.

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.



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 v8 the Oracle Java JDK files are already included and deployed as part of the AhsayOBM installation.

2.7 Memory Requirement

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

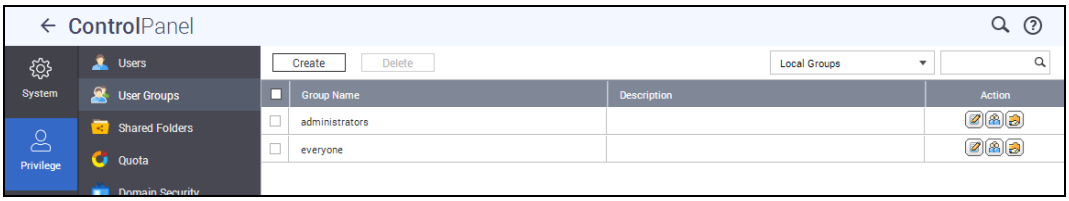
2.8 TCP Port Requirement

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.

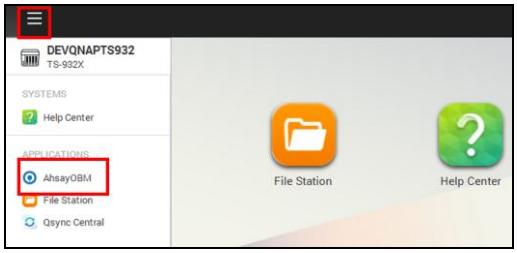
2.9 QNAP NAS User Account Permission

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 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**

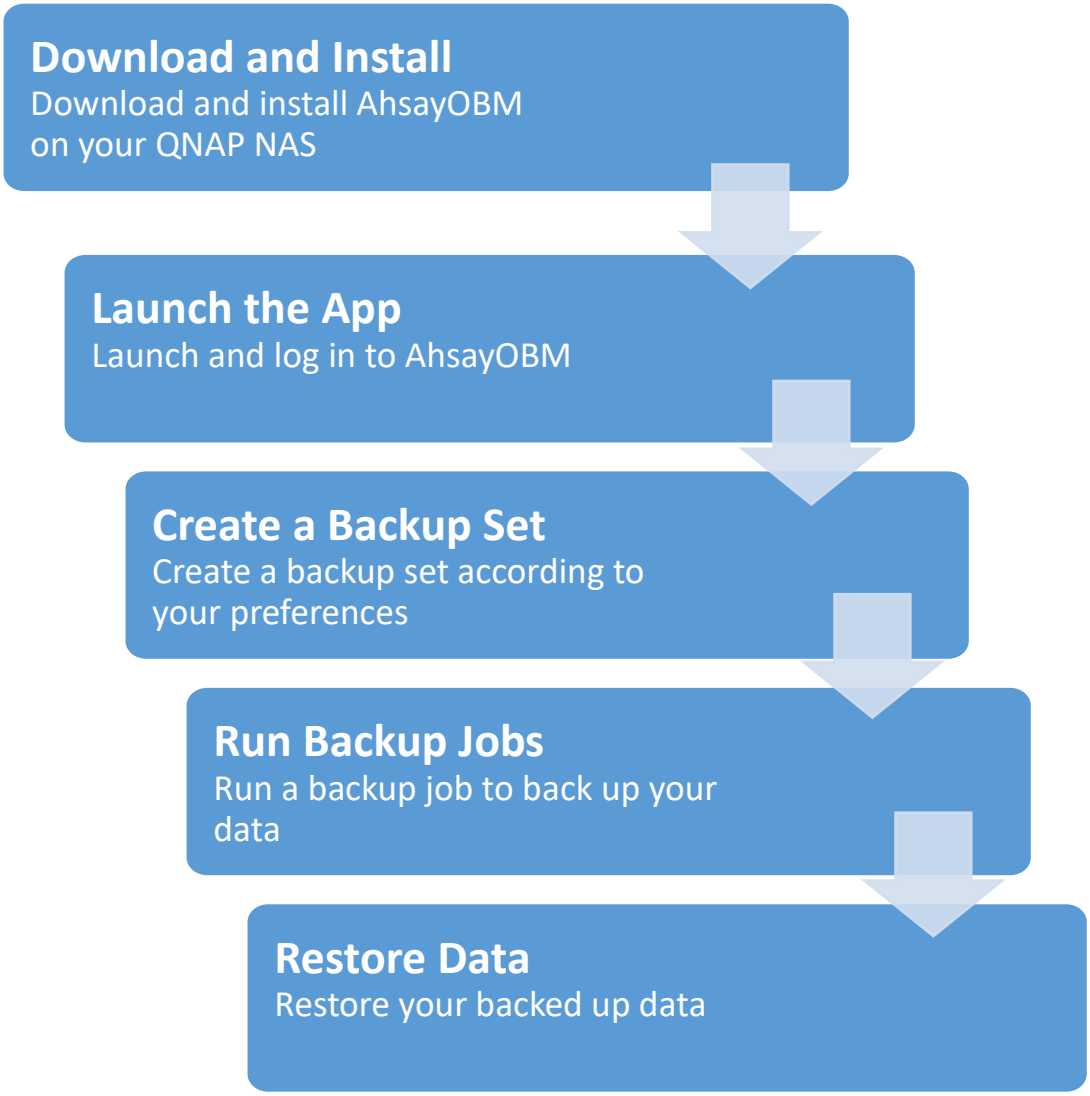
2.11 Supported Features from AhsayCBS Web Console

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 Statics Report**

3 Get started with AhsayOBM

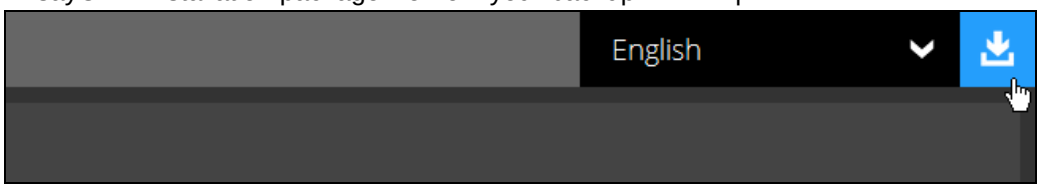
This quick start guide will walk you through the following 5 major parts to get you started with using AhsayOBM.



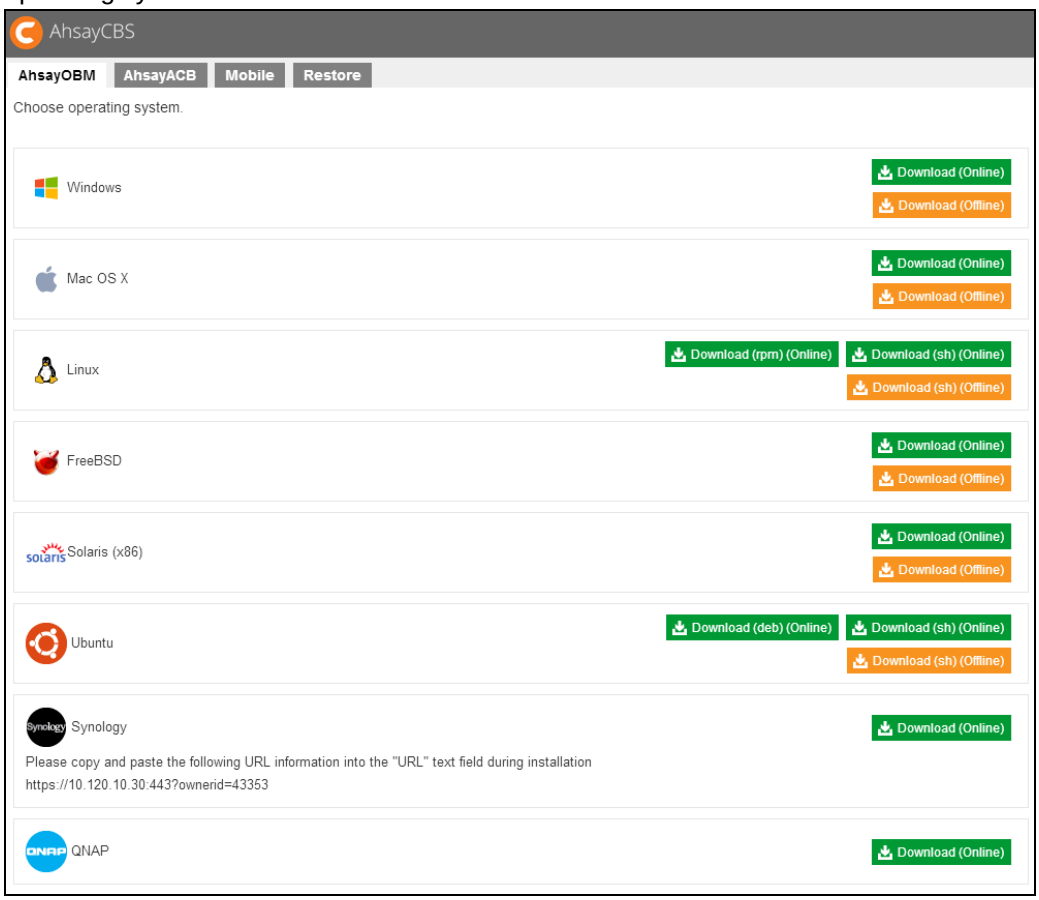
4 Download and Install AhsayOBM

4.1 Download AhsayOBM

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



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

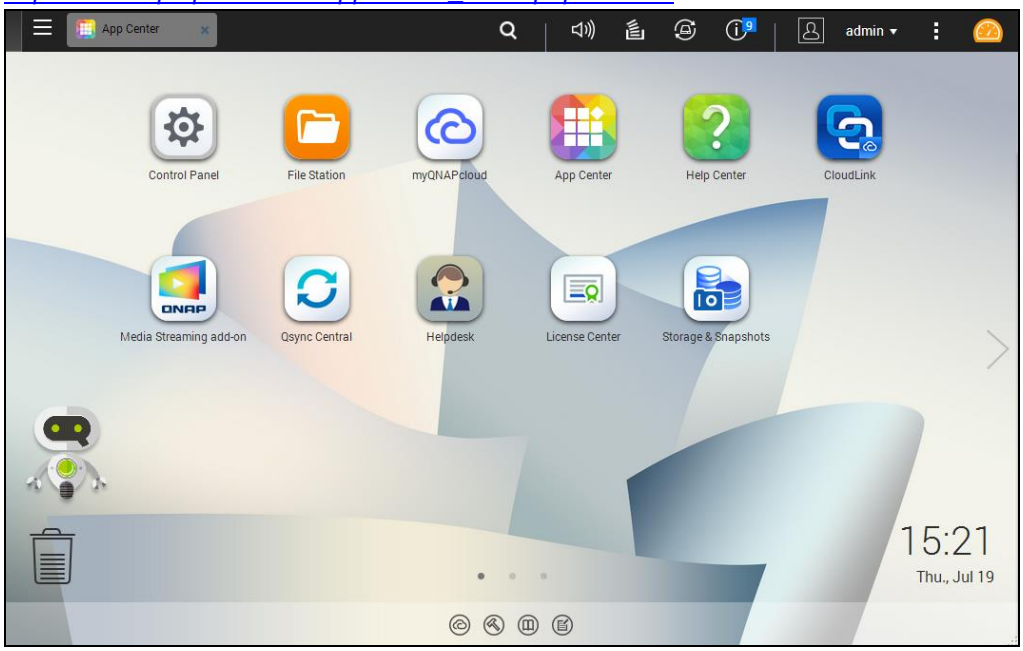


3. In the QNAP section, click the **Download (Online)** icon to download the AhsayOBM installation package.

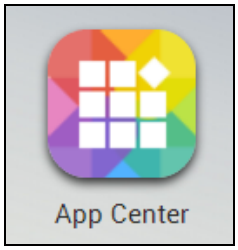
4.2 Install AhsayOBM

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.

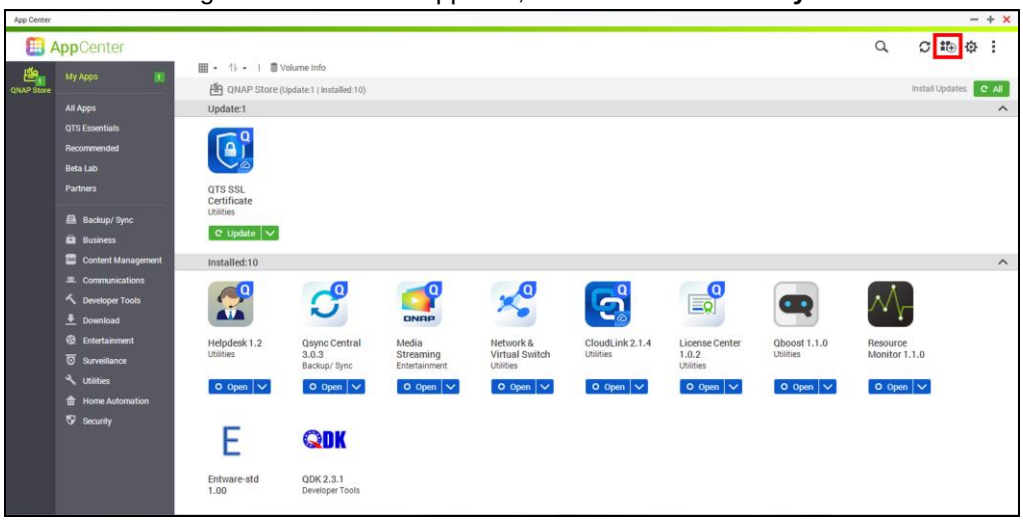
   Note: *Refer to the following user manual for information on how to login to QTS:* *https://www.qnap.com/en/support/con_show.php?cid=11*



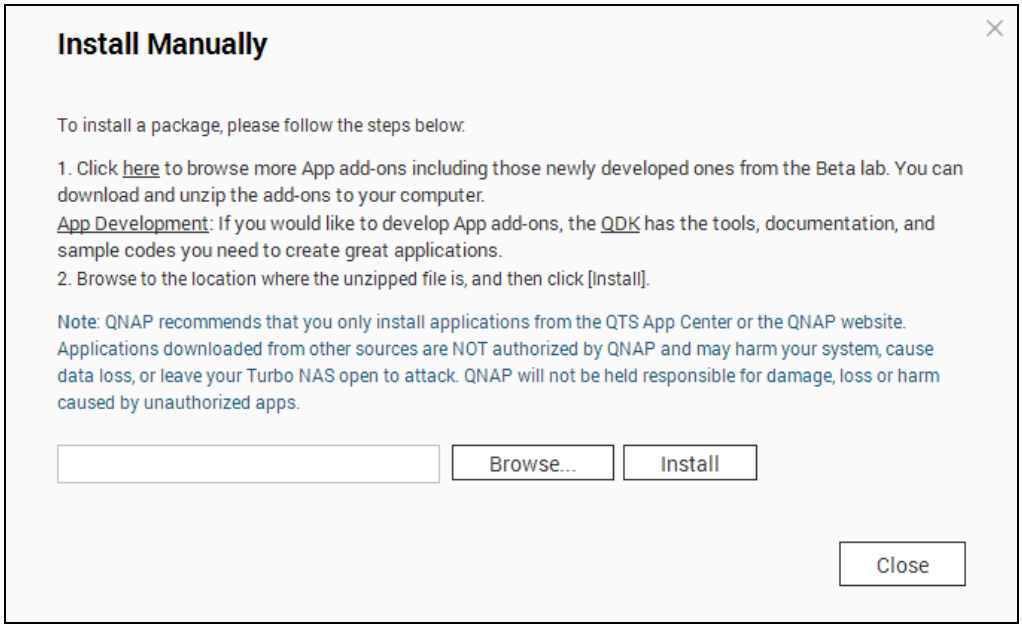
2. To install AhsayOBM on QNAP NAS, click the **App Center** icon from the desktop.



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



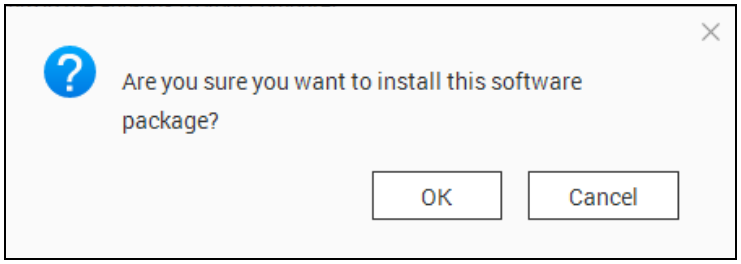
4. When the Install Manually window appears, click **Browse** to select the AhsayOBM package file which you have downloaded (e.g. **obm-qnap-port number-Backup Service Provider Web Console IP Address-https-0O.qpkg**).



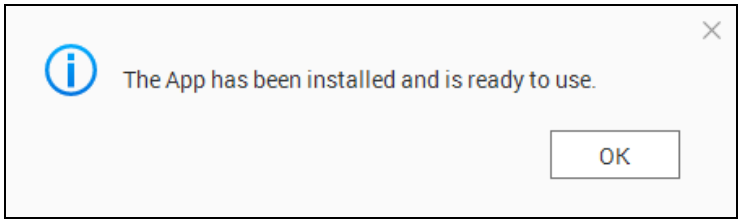
After selecting the AhsayOBM package file, obm-qnap-443-10.120.10.30-https-0O.qpkg, click **Open** to proceed.

5. Click **Install** to proceed with the installation.

6. Click **OK** to start the installation of AhsayOBM when the window prompt.

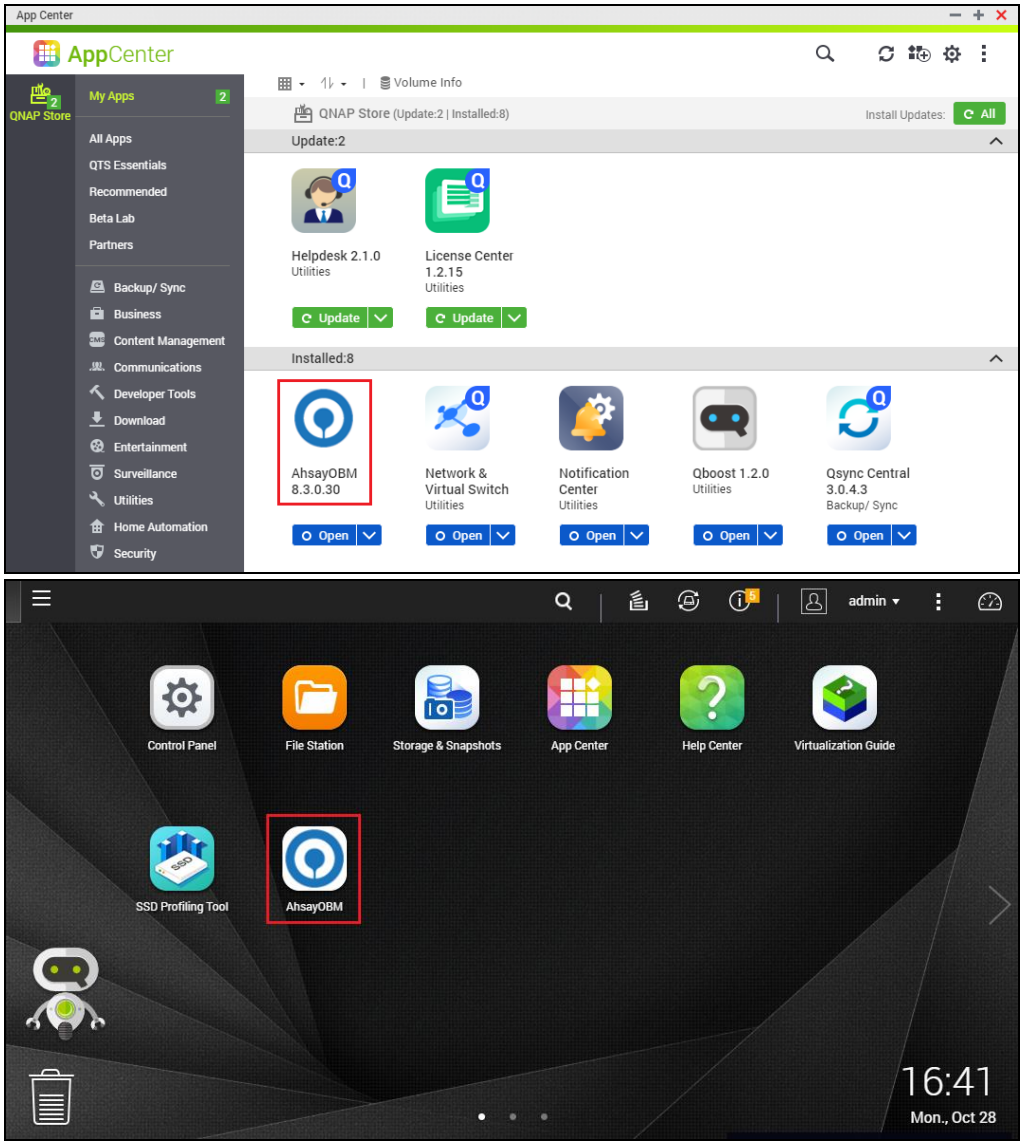


7. Upon successful installation, the following message will be prompted.



Click **OK** to finish the installation.

8. 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, use the

touch /share/CACHEDEV1_DATA/.qpkg/AhsayOBM/obm/ipc/Scheduler/stop script and use the **ps** command.

```
[~] # 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

/share/CACHEDEV1_DATA/.qpkg/AhsayOBM/obm/bin/Scheduler.sh script and use the **ps** command again.

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

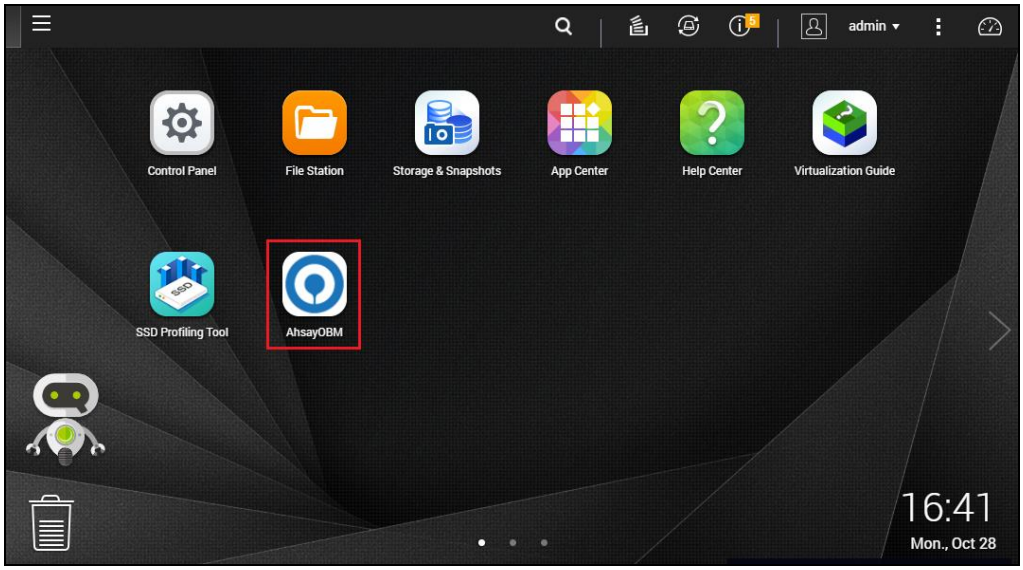
During installation, the following symlinks to the scheduler startup script **/share/CACHEDEV1_DATA/.qpkg/AhsayOBM/AhsayOBM.sh** will be created that allows the AhsayOBM Scheduler Service to start automatically each time the machine is rebooted or restarted.

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

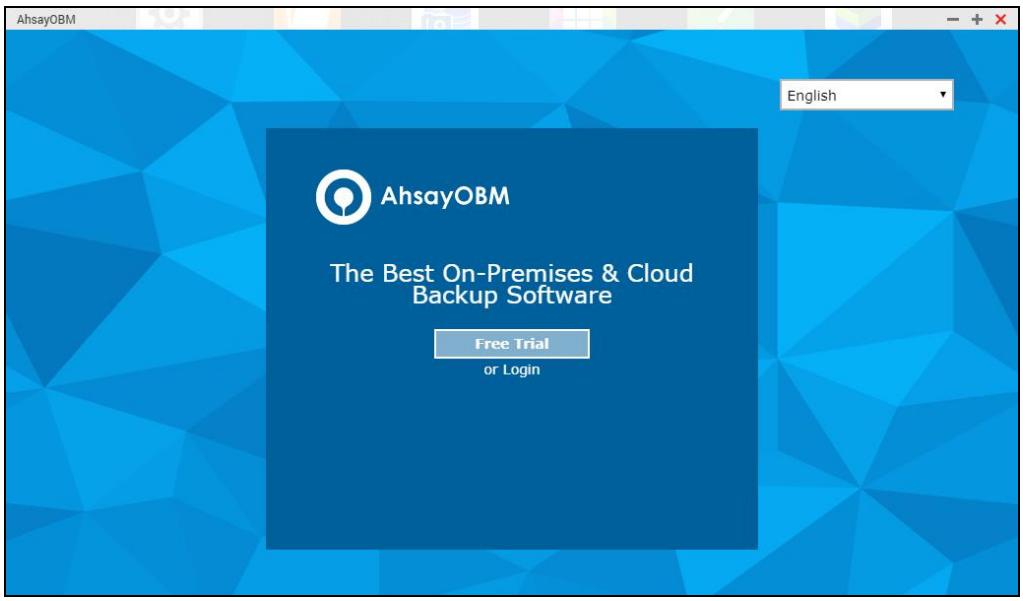
```
[~] # ls -la /etc/init.d/Ahsay*
lrwxrwxrwx 1 admin administrators 48 2019-05-23 12:55 /etc/init.d/AhsayOBM
.sh -> /share/CACHEDEV1_DATA/.qpkg/AhsayOBM/AhsayOBM.sh*
[~] #
```

5 Start AhsayOBM

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

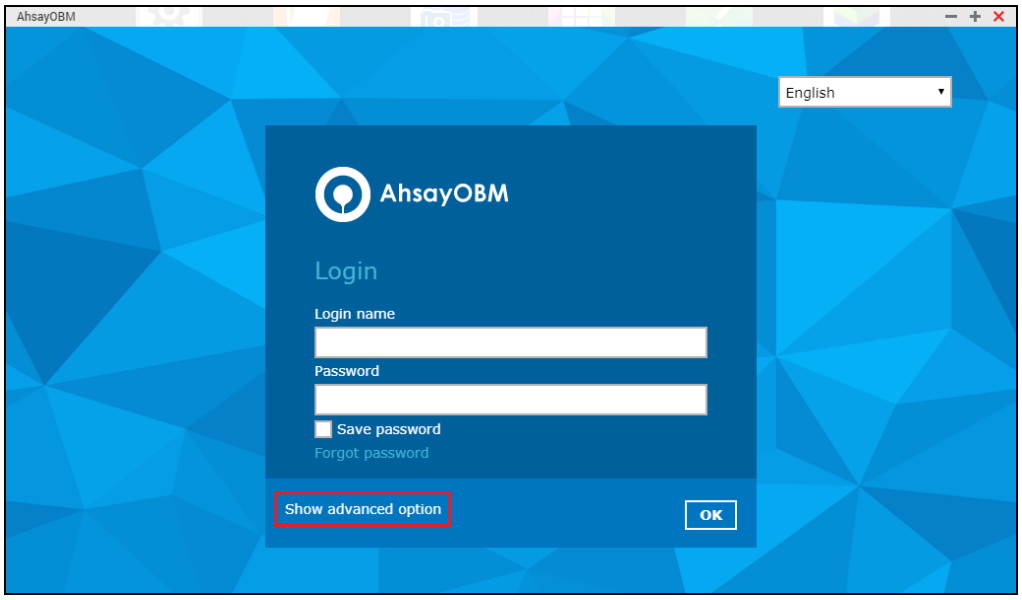


2. The Free Trial Registration menu may display when you login for the first time. Click **Login** if you already have an AhsayOBM account, or click **Free Trial** to register for a trial backup account.

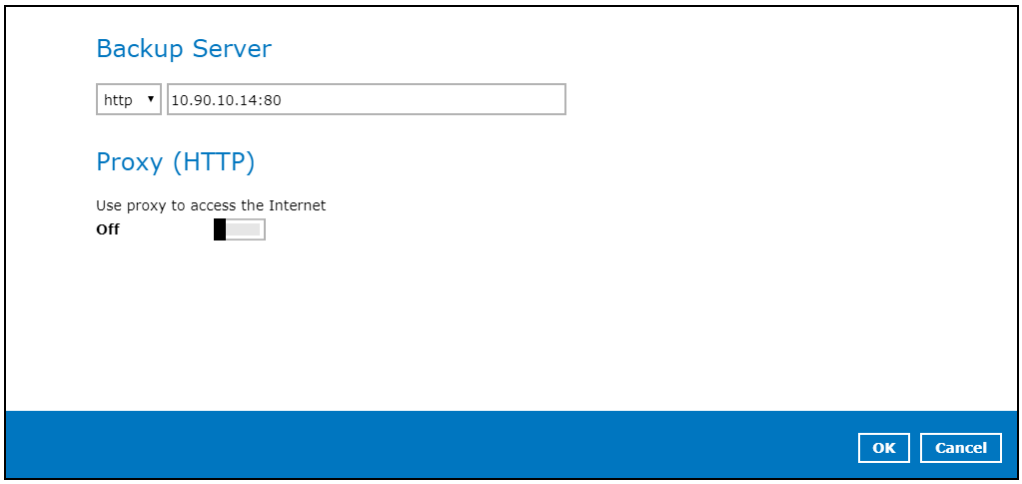


Note: *The free trial registration menu will only be displayed if your service provider has enabled free trial registration on the backup server.*

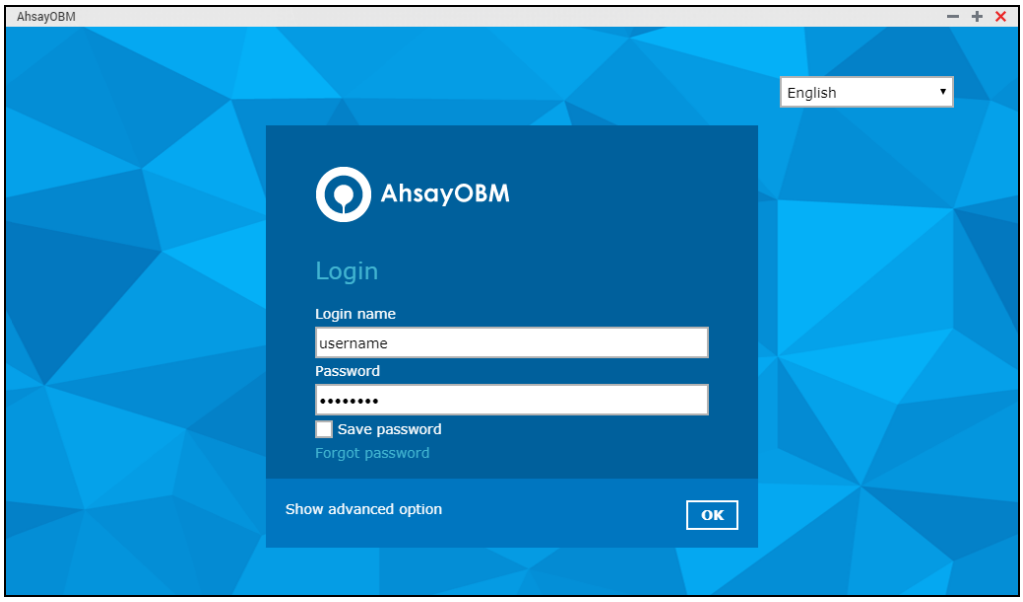
3. In case you want to enter the backup server setting provided by your backup service provider, click **Show advanced option**.



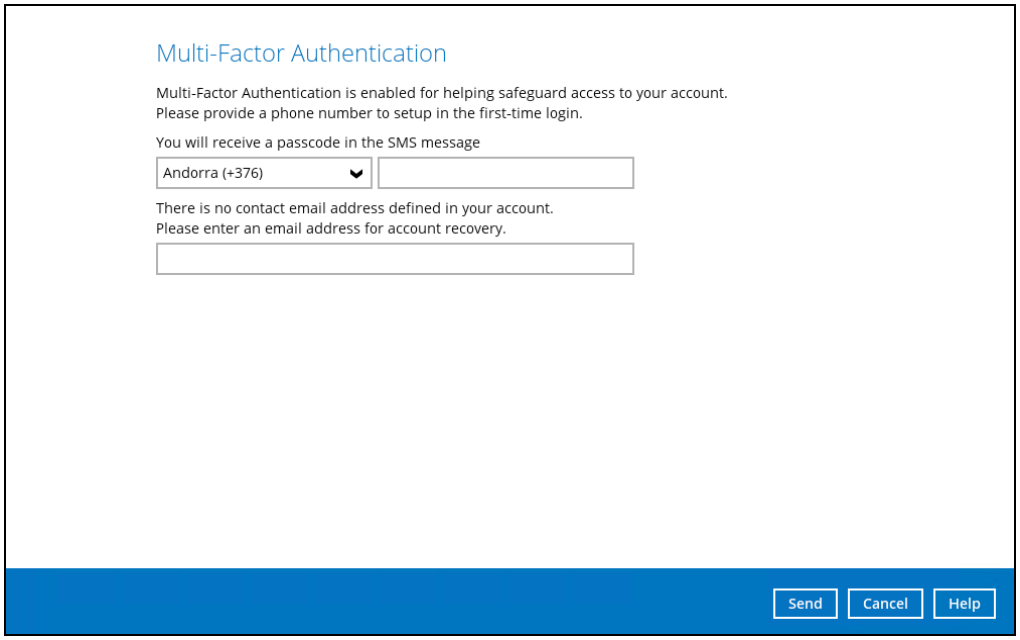
4. Click **OK** after typing in the backup server information. You can turn on the Proxy feature if needed.



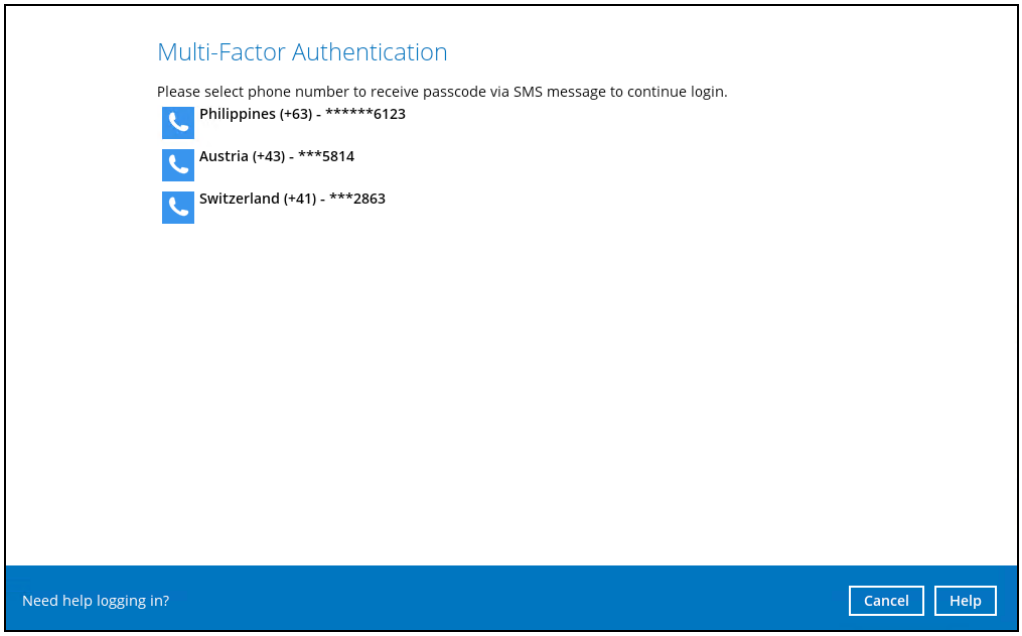
5. Enter the Login name and Password of your AhsayOBM account provided by your backup service provider. Then, click **OK** to login.



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

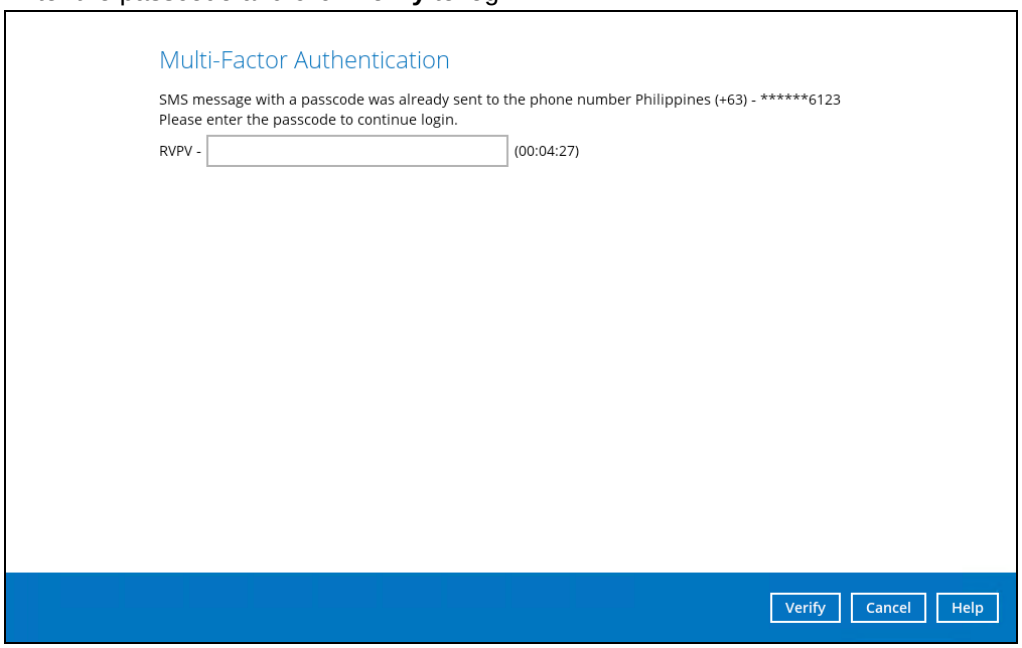


For succeeding login this will be the screen displayed. Select your phone number.

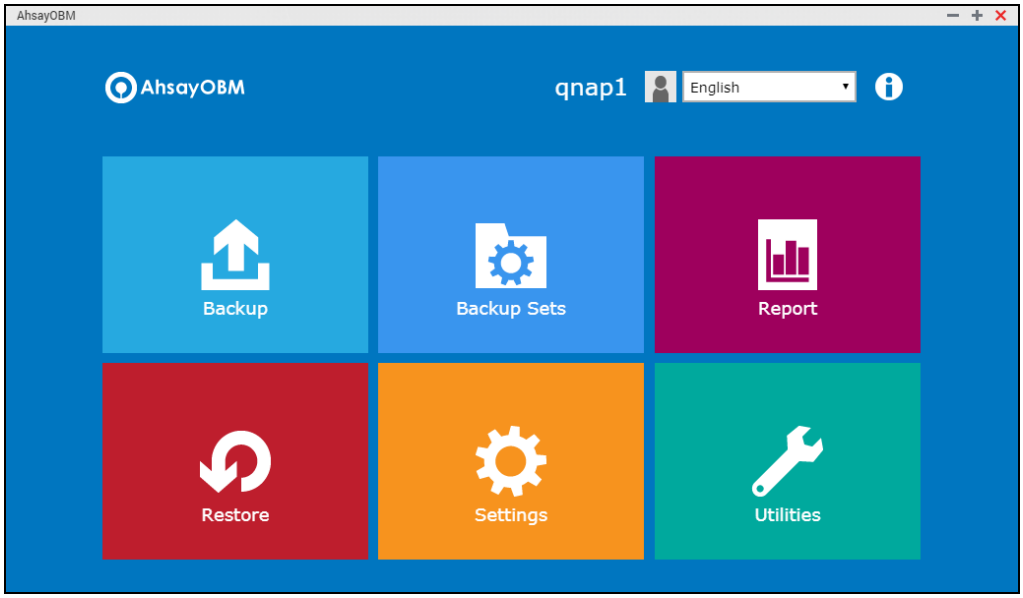


Note: If **Need help logging in?** is clicked, enter the email address where login instructions will be sent.

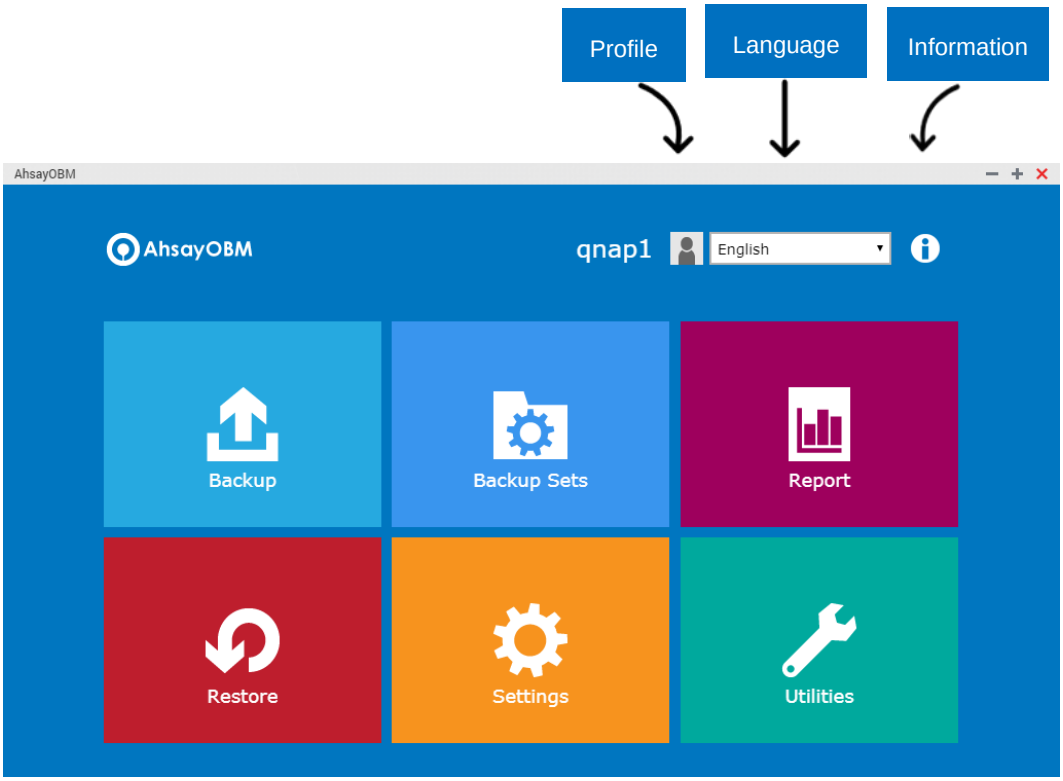
7. Enter the passcode and click **Verify** to login.



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**

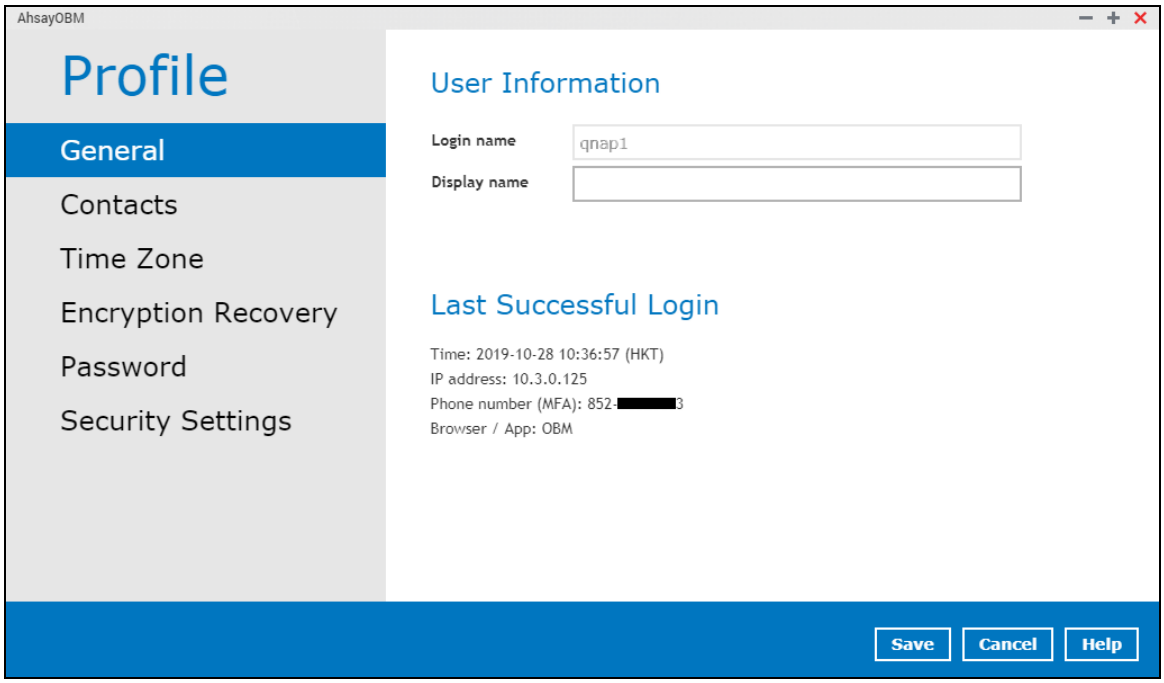
6.1 Profile

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

Profile has six (6) features:

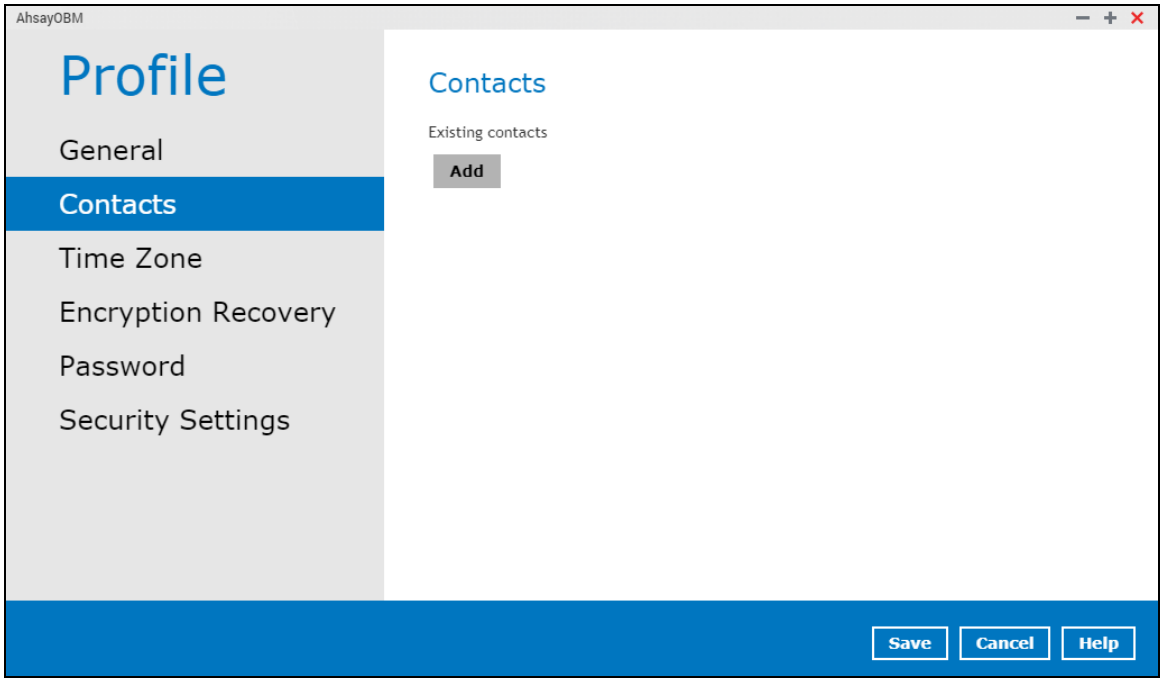
- **General**
- **Contacts**
- **Time Zone**
- **Encryption Recovery**
- **Password**
- **Security Settings**

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

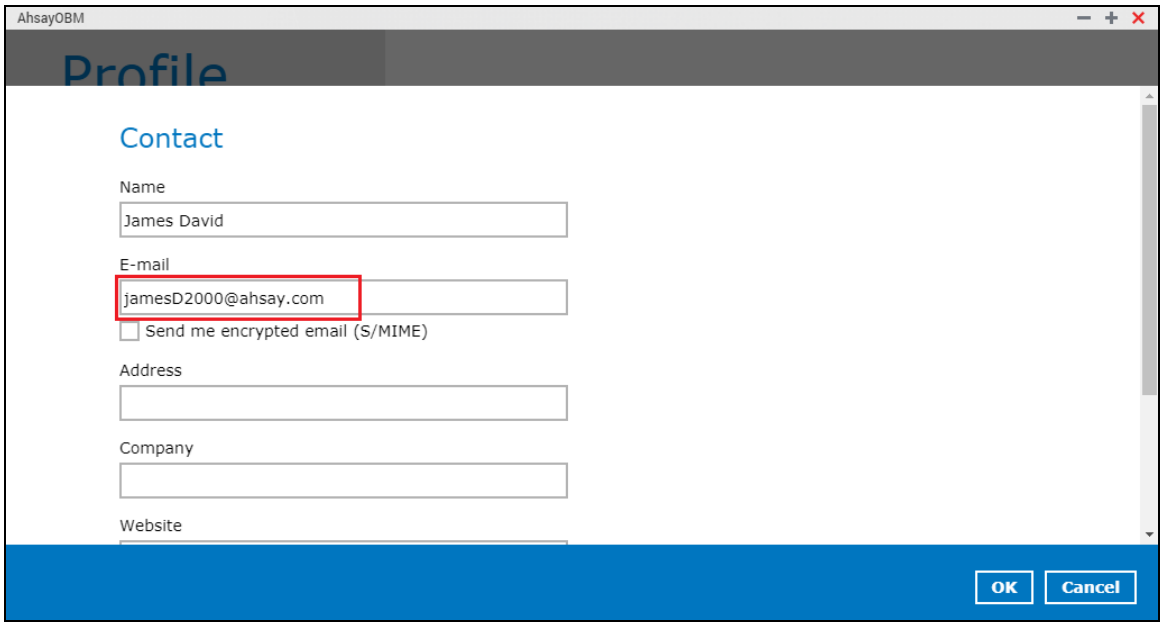


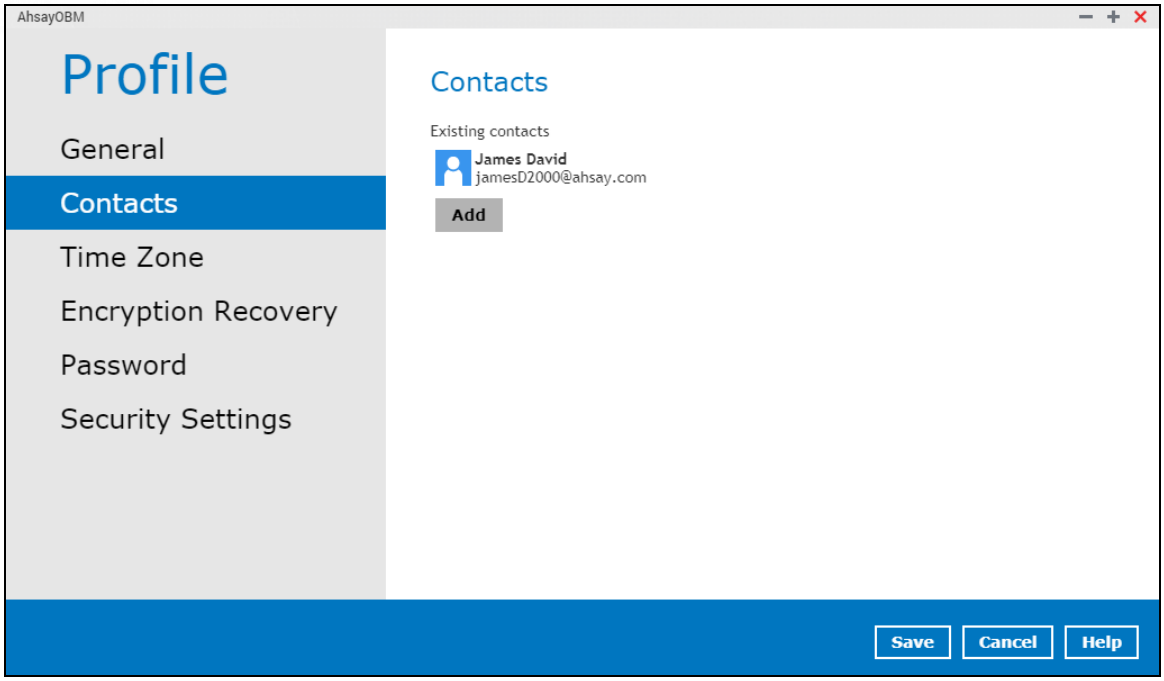
- The **login name** is the name of your backup account.
- The **display name** is the display name of your backup account as you log on to the AhsayCBS management console.
- The **time** is the date and time the user last logged in.
- The **IP address** used to login.
- The **phone number (MFA)** is where the sms authentication will be sent when MFA 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.



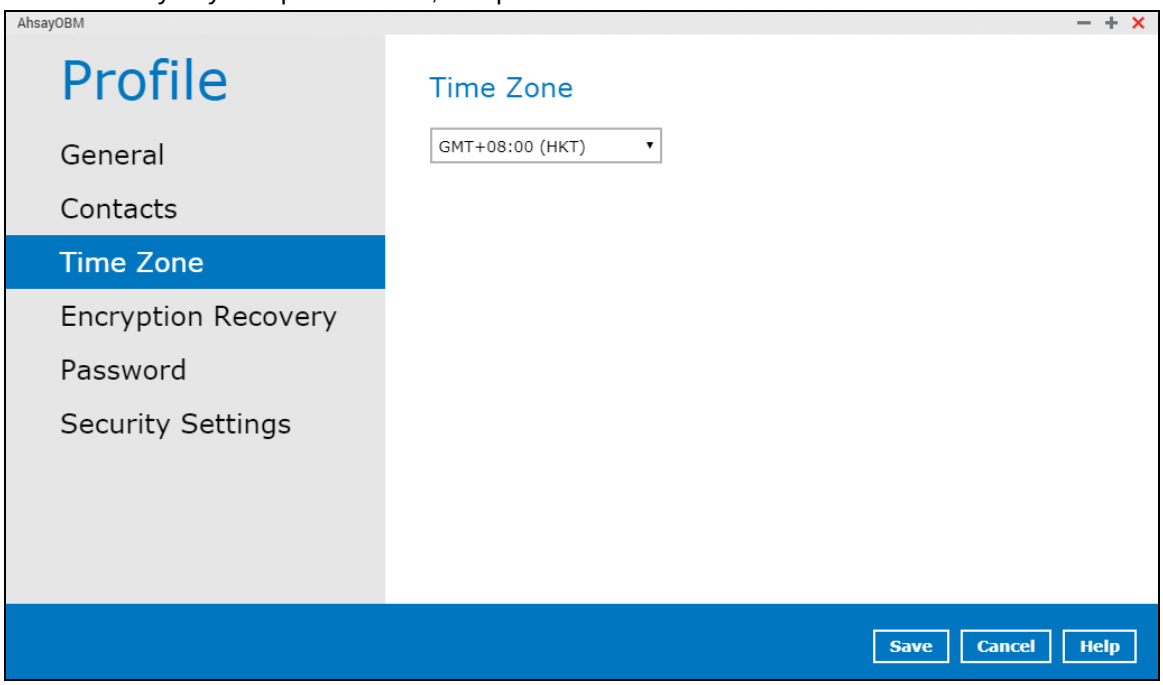
E-mail cannot be left blank.



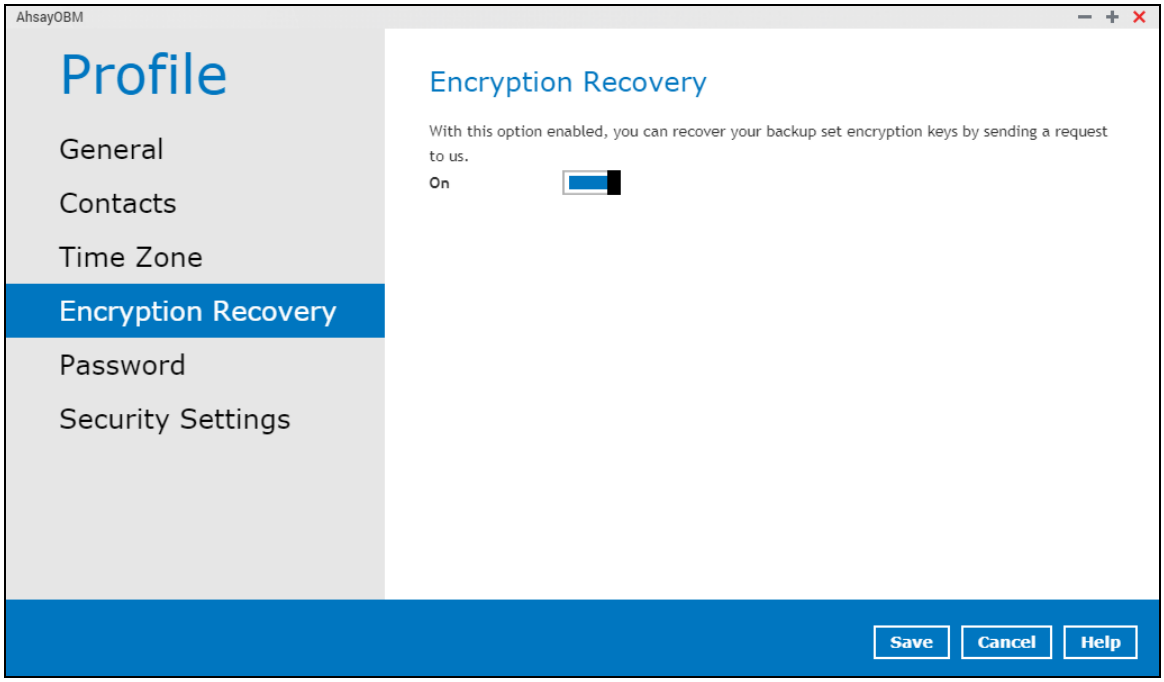


Note: You can add multiple contacts here.

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.

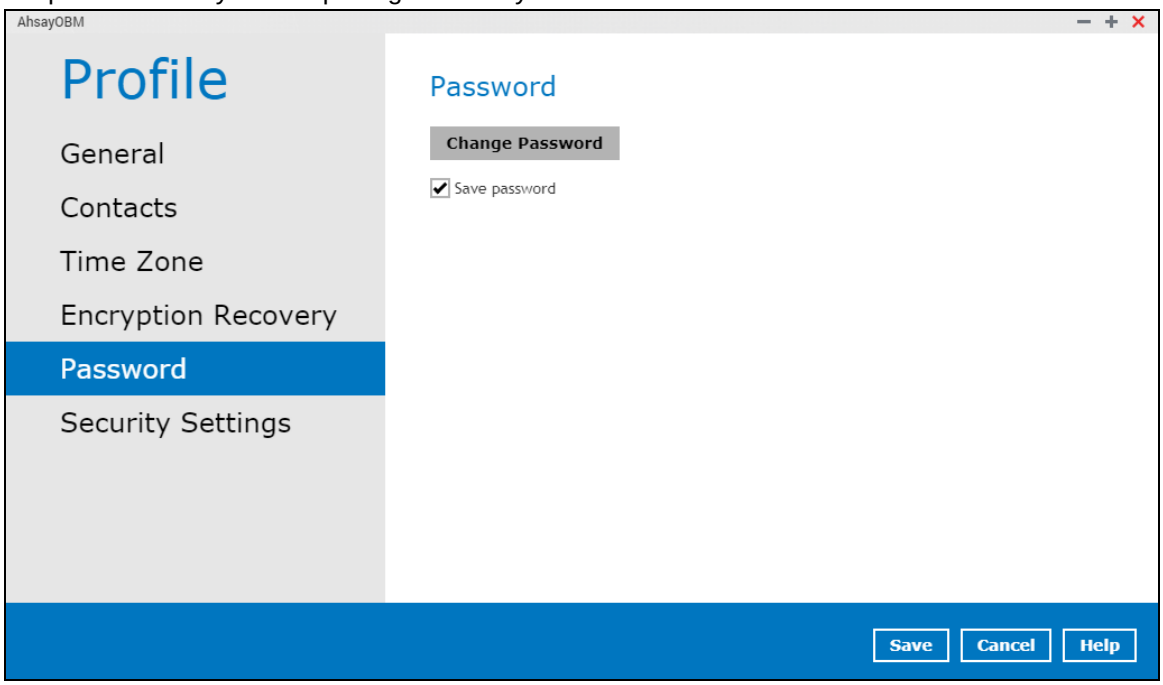


Backup set encryption key can be recovered by turning this feature on.

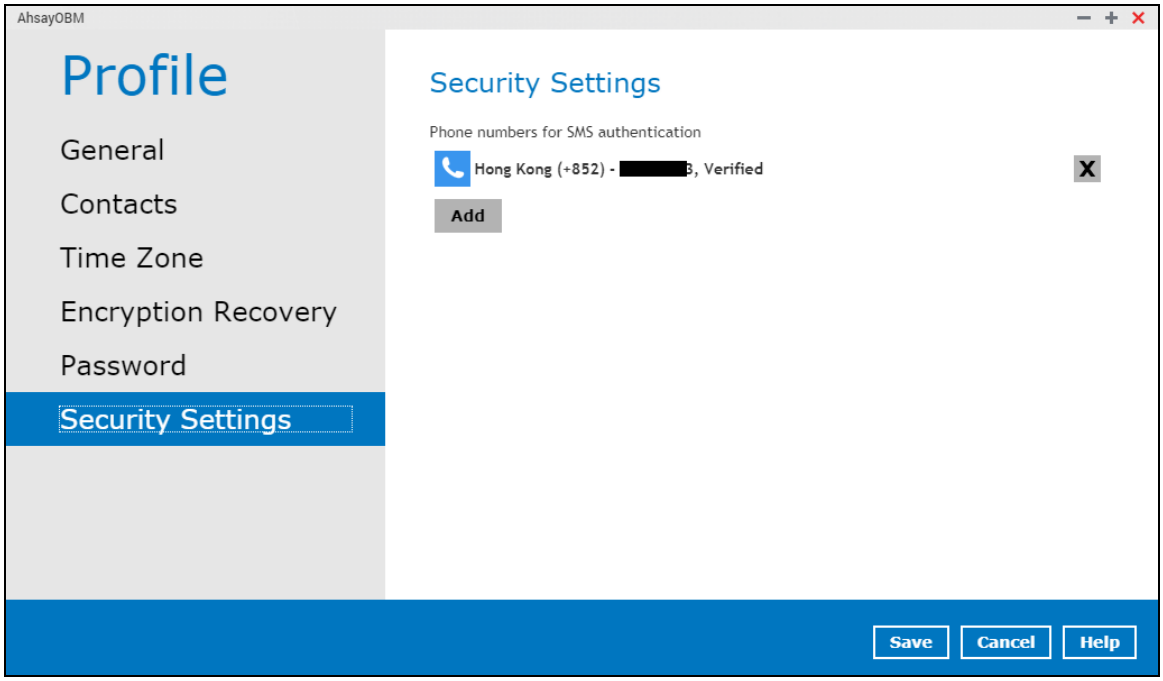


Note: This option may not be available. Please contact your backup service provider for details.

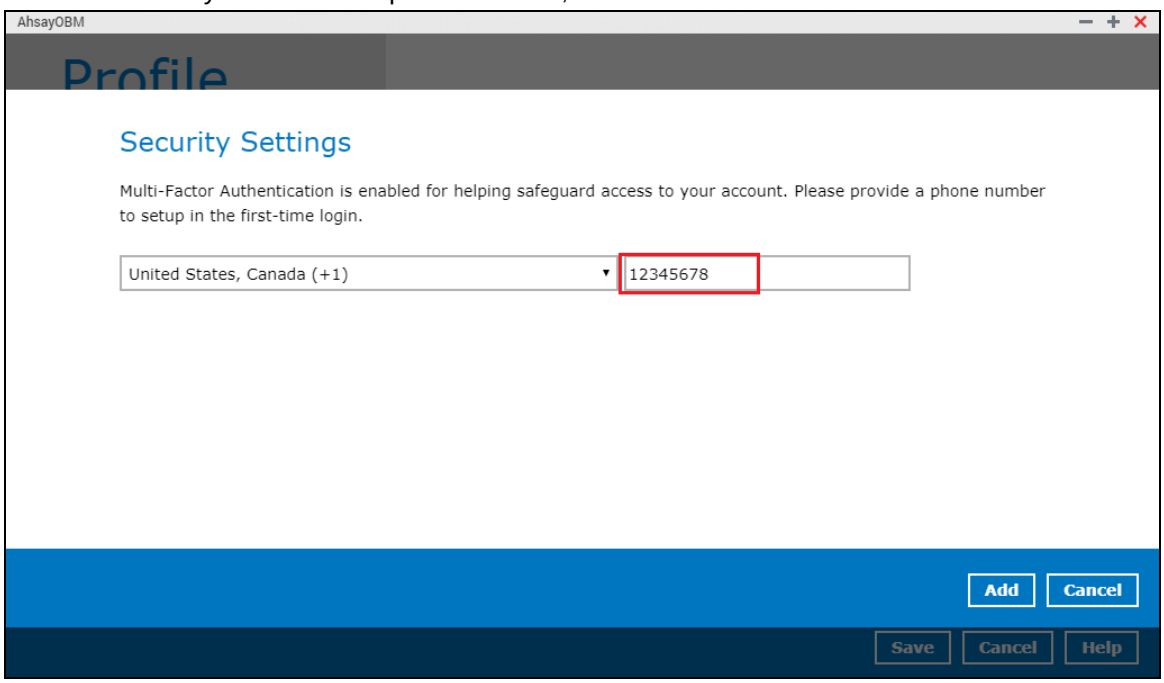
Login password can be modified anytime. You can also check the **save password** box to bypass the password entry when opening the AhsayOBM interface.



Security Settings will only be visible if multi-factor authentication is enabled. Phone numbers that will be used for sending sms authentication will be listed here and will show the status if it is verified or not. You can also add phone numbers here that can be used for sending the sms authentication.

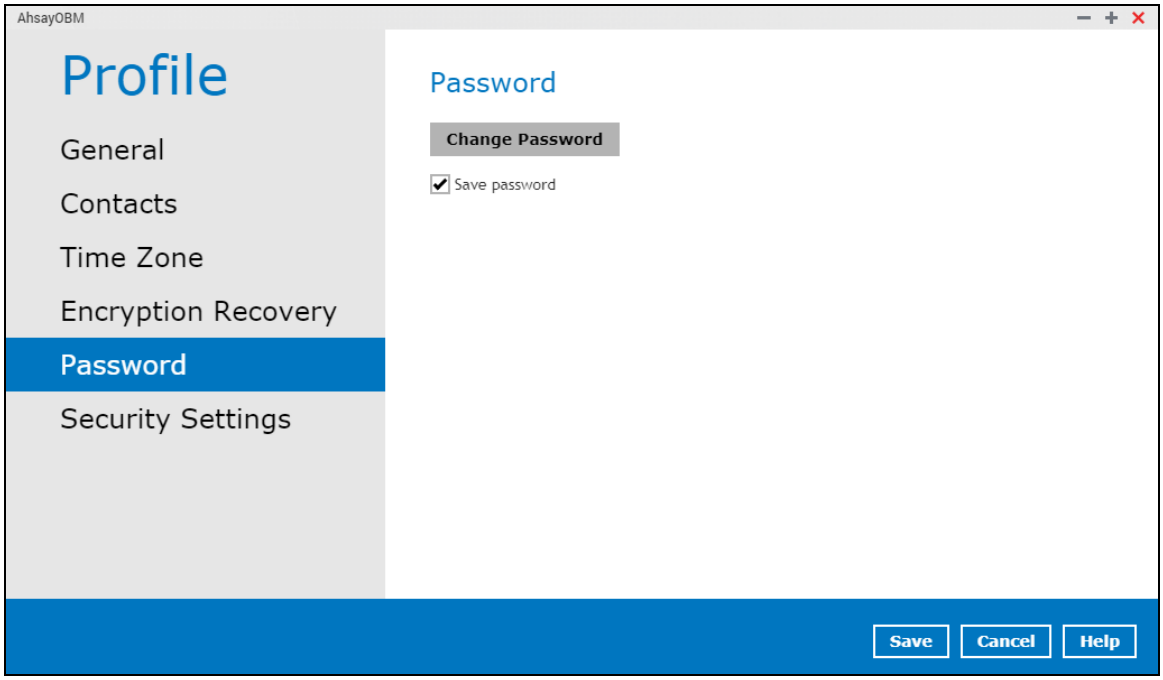


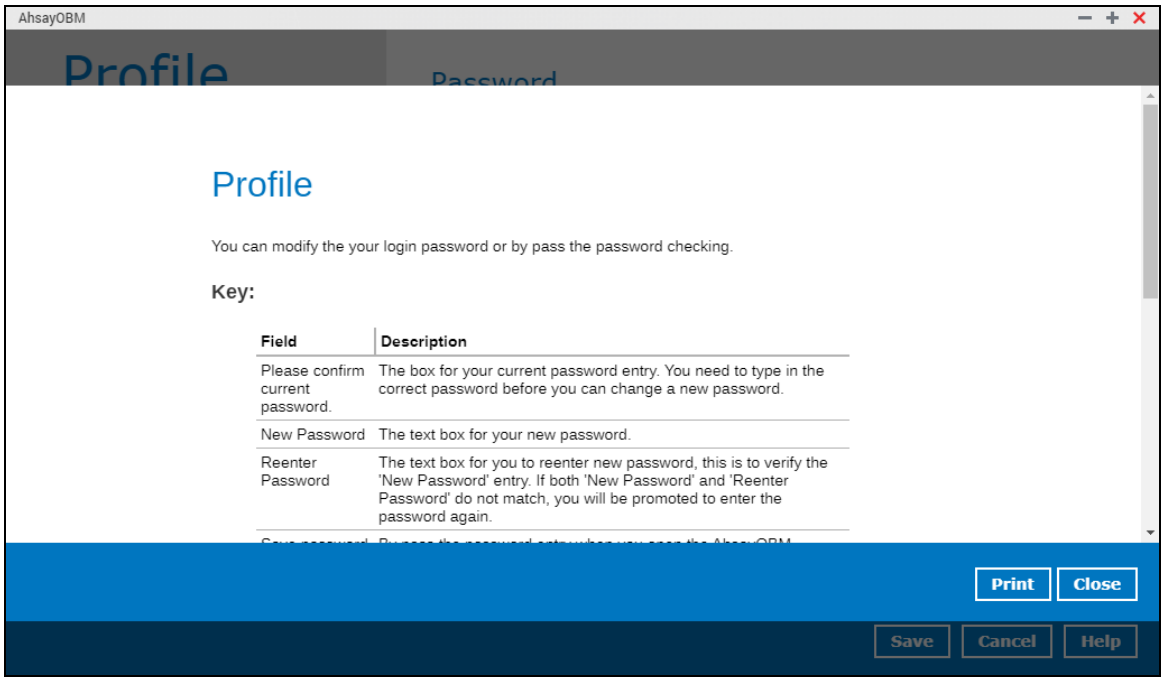
Select the country and enter the phone number, then click **Add**.



6.2 Online Help

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





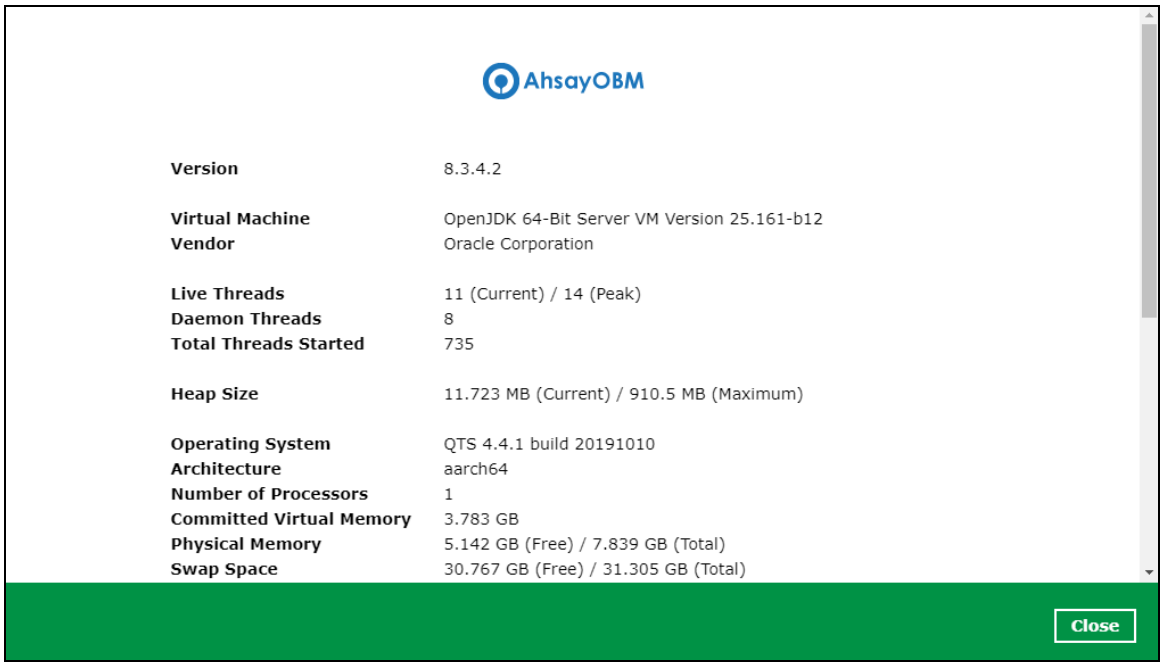
6.3 Language

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

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

6.4 Information

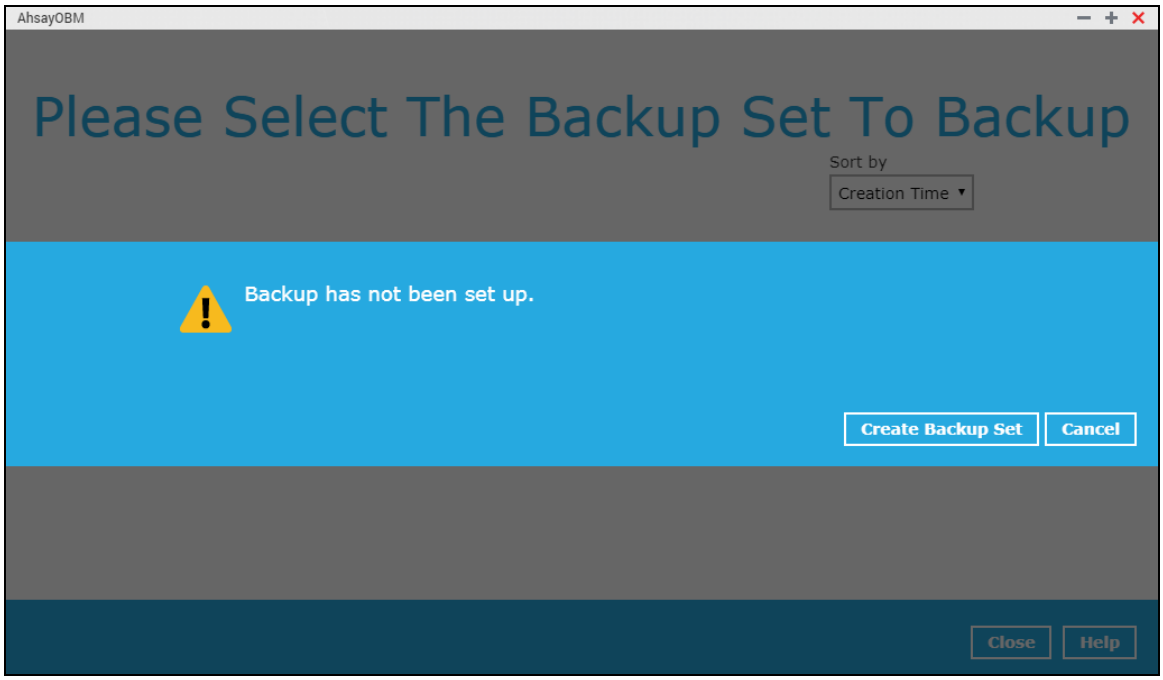
The **information** icon displays the product version and system information of the machine where the AhsayOBM is installed.



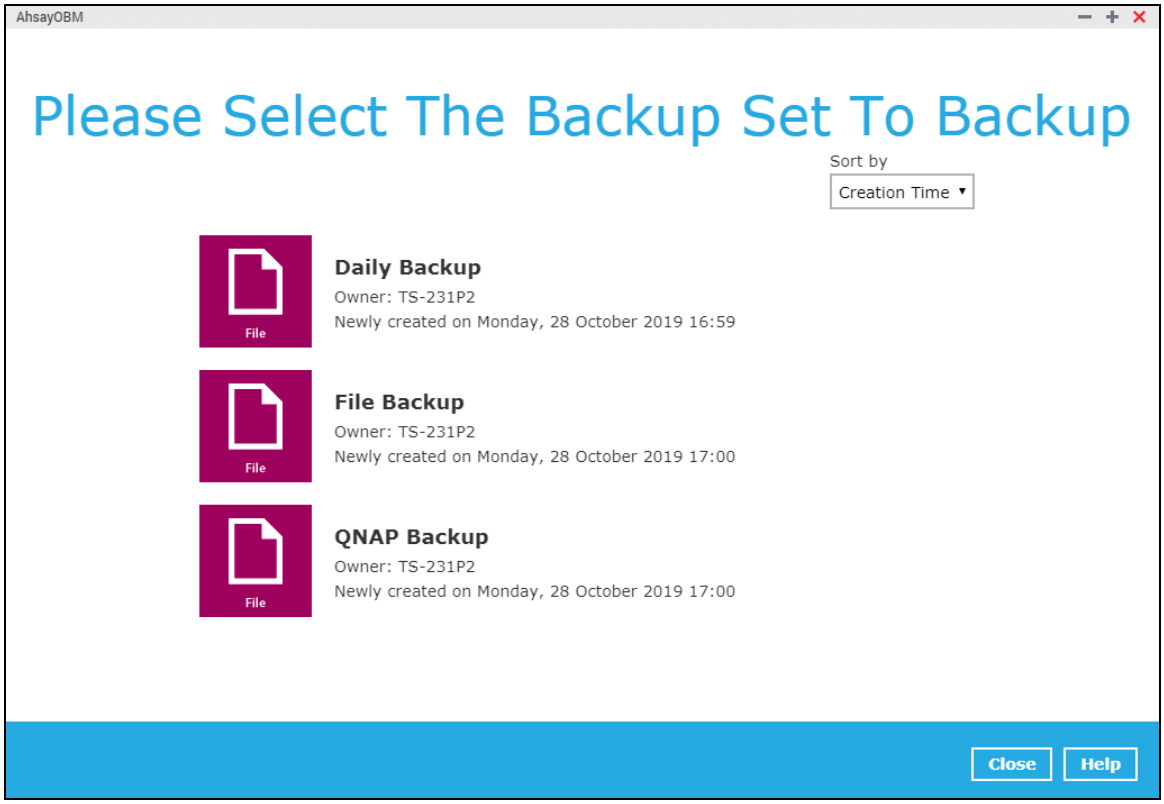
6.5 Backup

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

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



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



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

- **Full** – this type of backup will capture all the data that you want to secure. When you run a backup job for the first time, AhsayOBM will run a full backup regardless of the in-file delta setting.

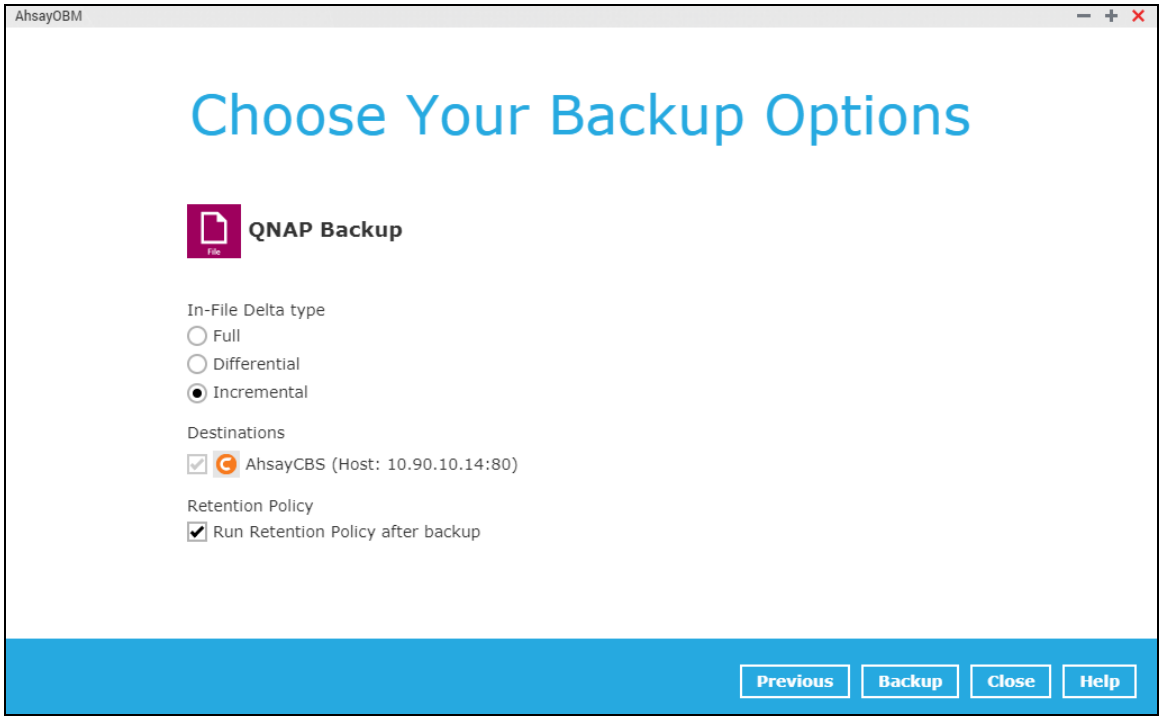
- **Differential** – this type of backup captures only the changes made as compared with the last uploaded full file only and not since the last differential backup.

- **Incremental** – this type of backup captures only the changes compared with the last uploaded full or delta file.

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

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

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



6.6 Backup Sets

A backup set is a place for files and/or folders of your backed-up data. This feature allows the user to select files individually or an entire folder to backup. It is also used to delete backup set/s.

To create or modify a backup set, follow the instructions on Chapter 7 Creating a File Backup Set.

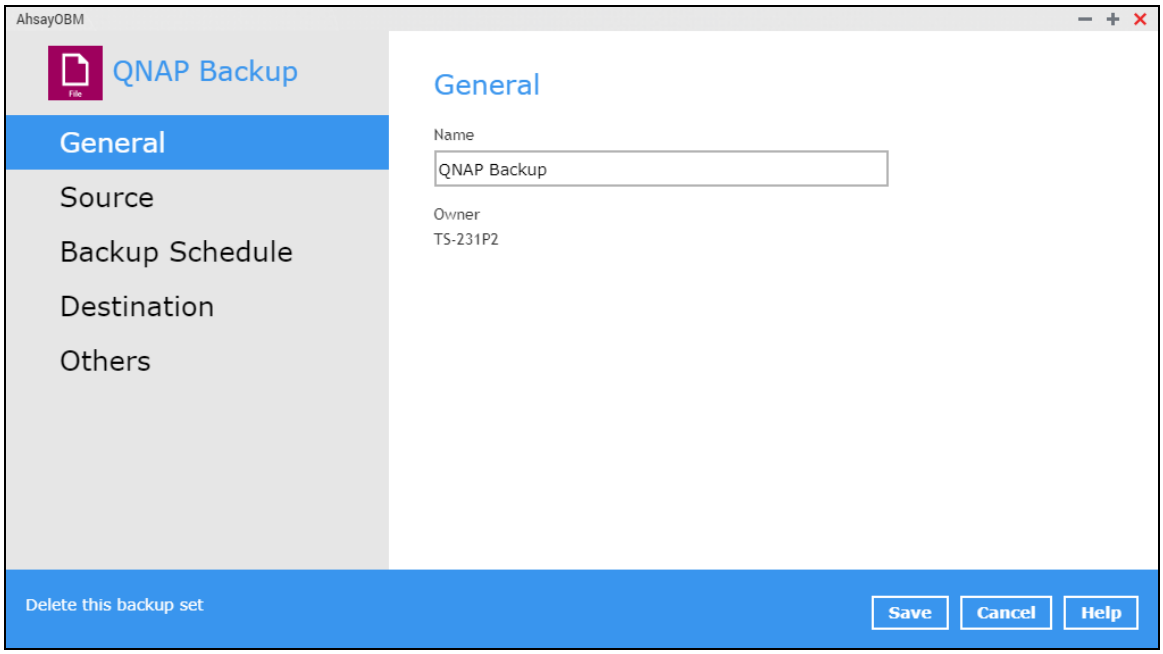
Backup Set Settings

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

- General
- Source
- Backup Schedule
- Destination
- Others

General

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

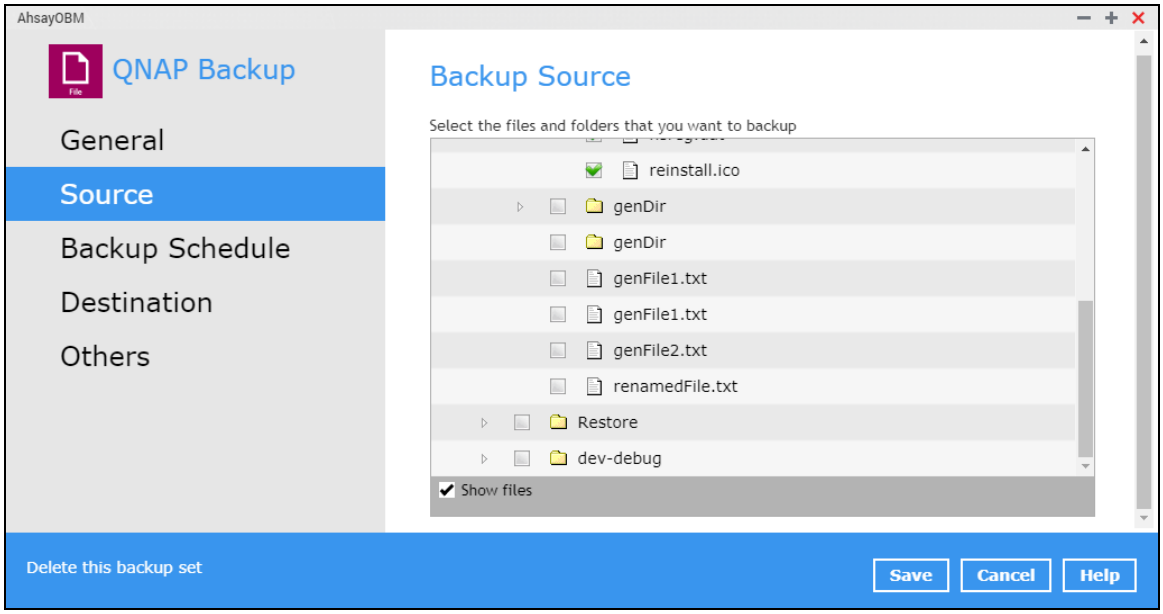


To modify the backup set name, follow the instructions below:

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

Source

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

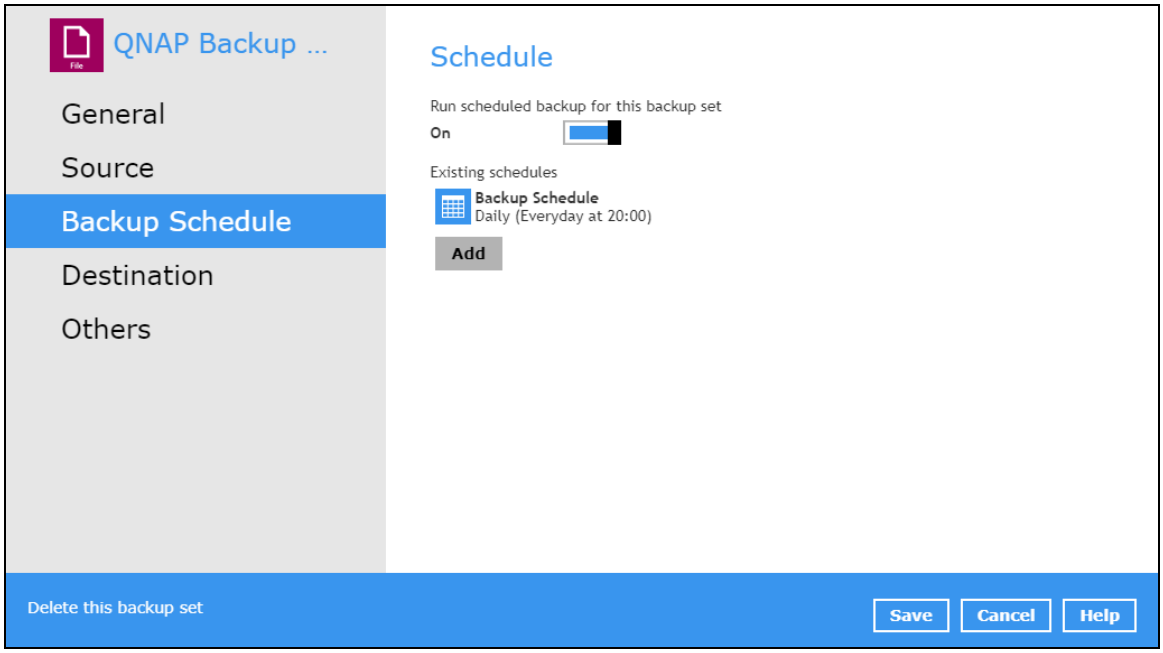


To add backup source, follow the instructions below:

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

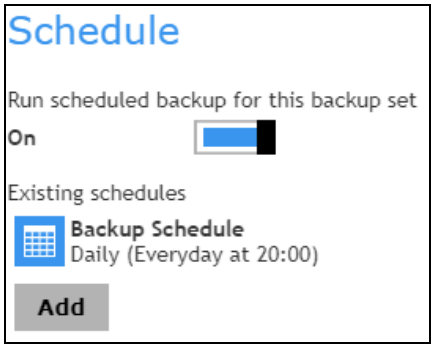
Backup Schedule

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

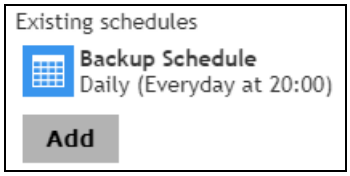


To configure a backup schedule, follow the steps below:

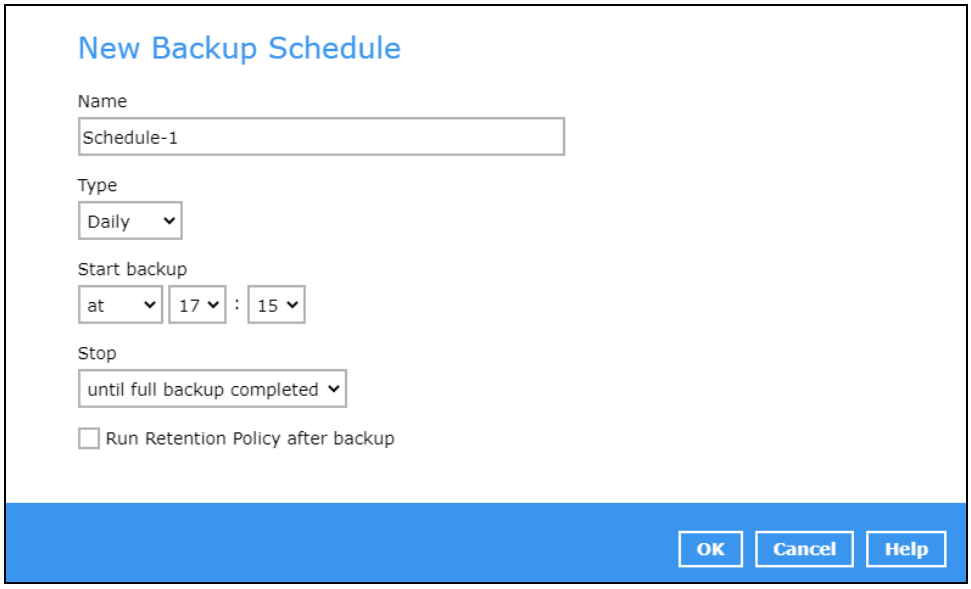
1. Swipe the lever to the right to turn on the backup schedule setting. The backup schedule is configured as “Daily at 20:00” by default.



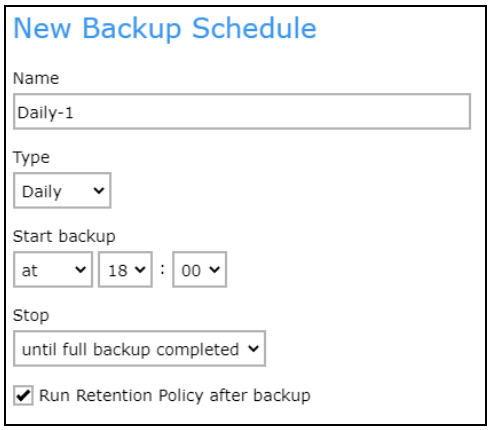
2. Select an existing backup schedule to modify or click the **[Add]** button to create a new one.



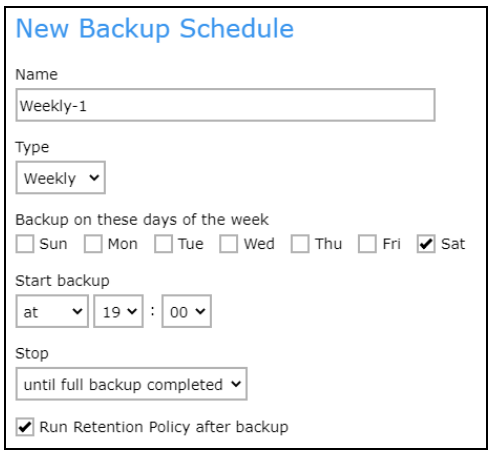
3. In the New Backup Schedule window, configure the following backup schedule settings.



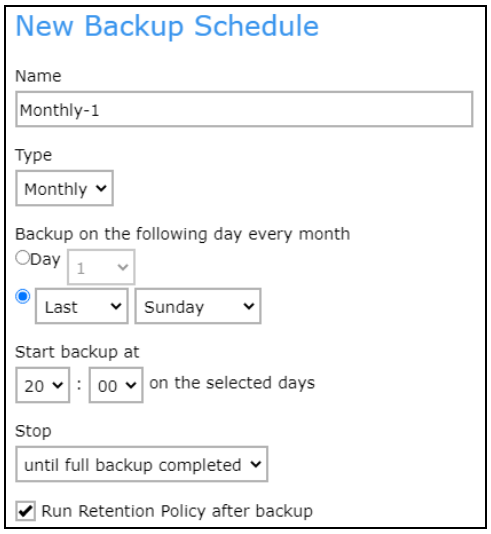
- **Name** – the name of the backup schedule.
- **Type** – the type of the backup schedule. There are four (4) different types of backup schedule: Daily, Weekly, Monthly and Custom.
  - **Daily** – the time of the day when the backup job will run.



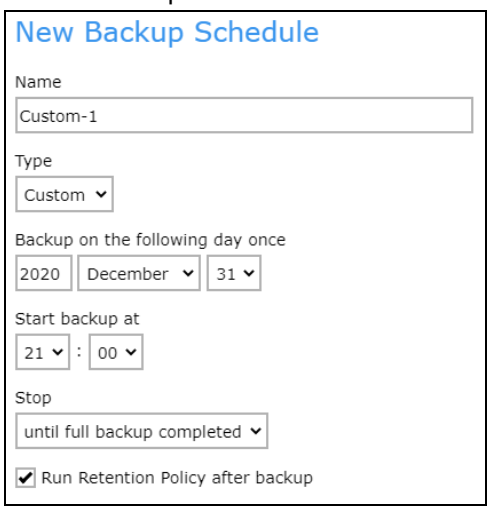
  - **Weekly** – the day of the week and the time of the day when the backup job will run.



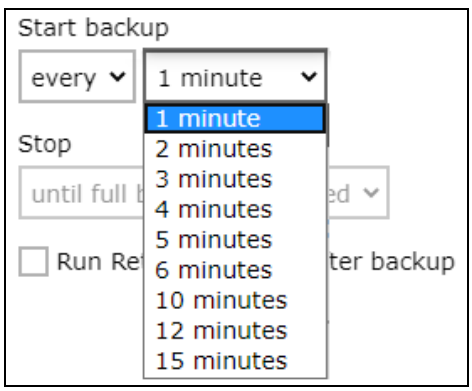
- **Monthly** – the day of the month and the time of the day when the backup job will run.

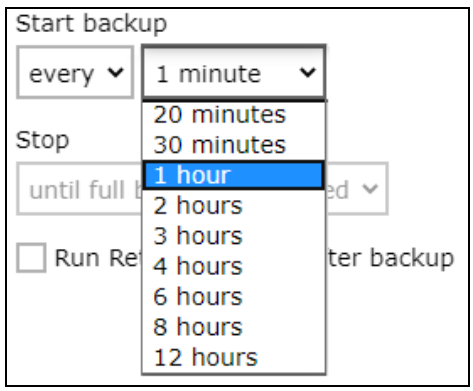


- **Custom** – a specific date and the time when the backup job will run.



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





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

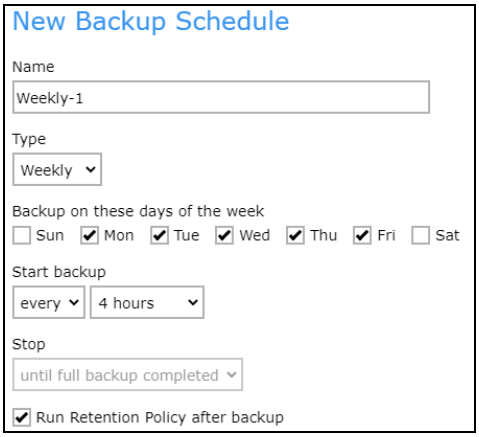


Figure 1.1

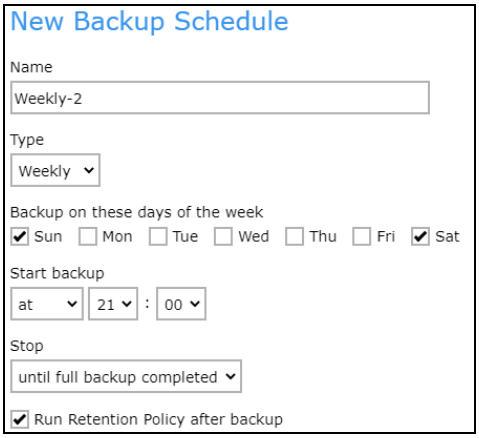


Figure 1.2

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.

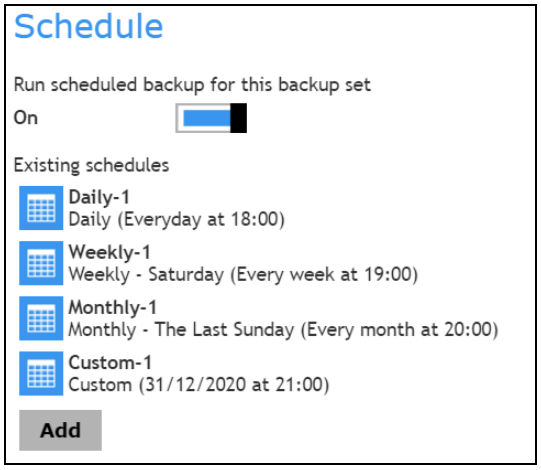
    The partially backed up data will have to be removed by running the data integrity check.

    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.

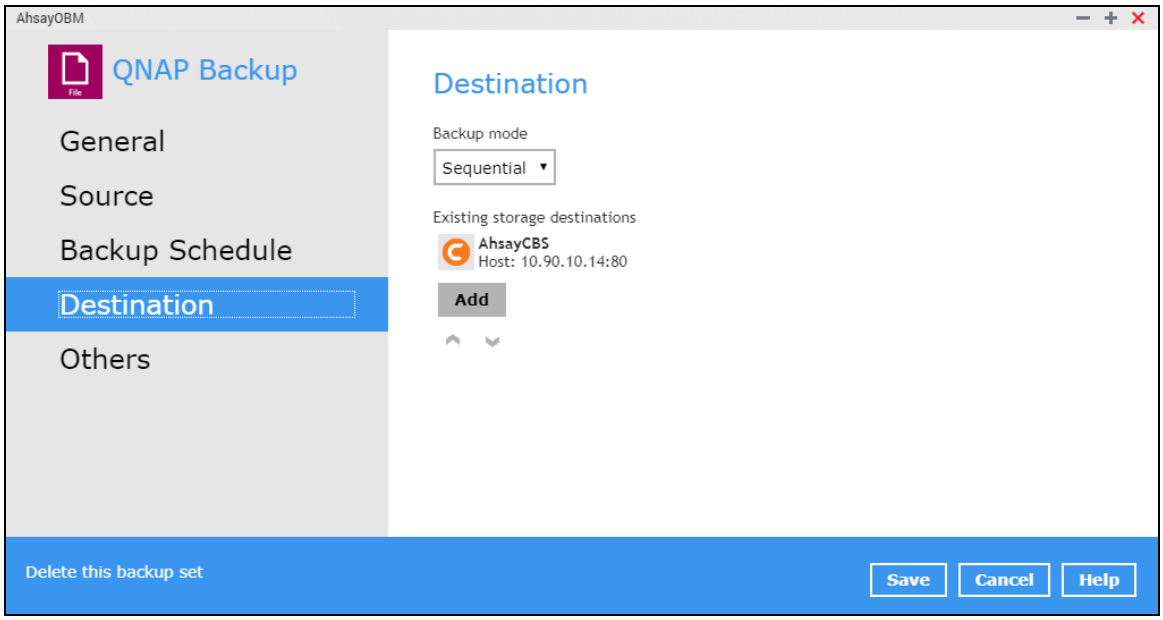


NOTE

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

Destination

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



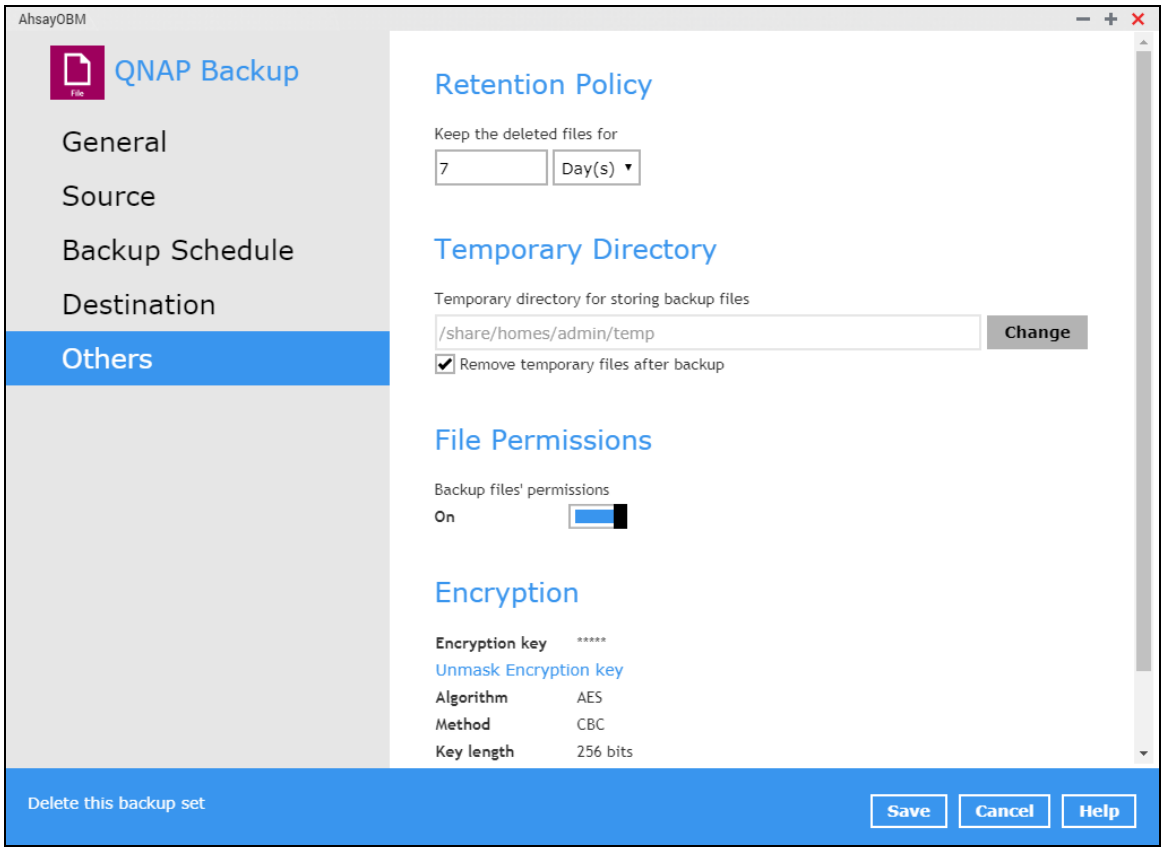
To add a destination, follow the instructions below:

1. Select [Destination].
2. Click the [Add] button.
3. Complete the following fields:
   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.

Others

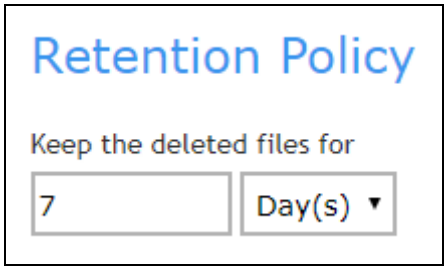
These are the list of other backup set settings that can be configured.

- Retention Policy
- Temporary Directory
- File Permissions
- Encryption



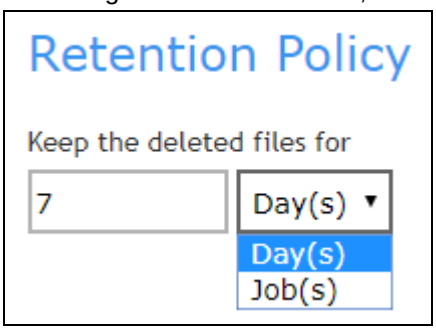
Retention Policy

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:

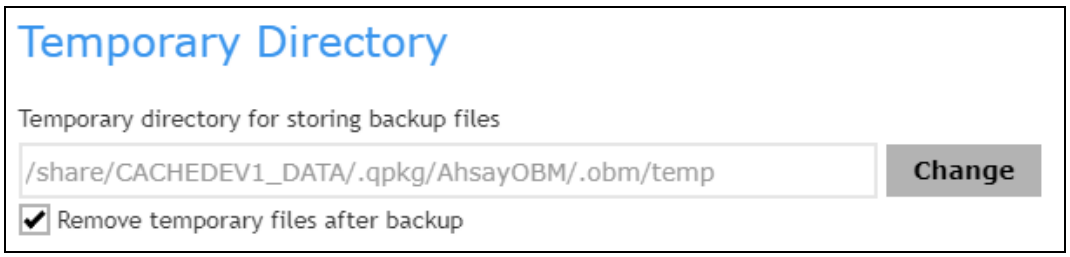
1. Select [Others].
2. On the right side of the screen, select from the two (2) options: Day(s) or Job(s).



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.

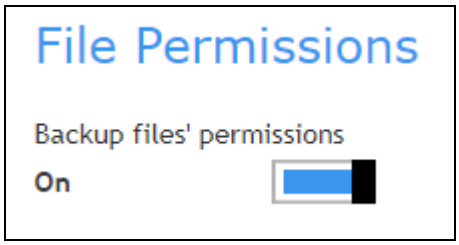


To configure the temporary directory, follow the instructions below:

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 backups the operating system file permission of the data selected as backup source.

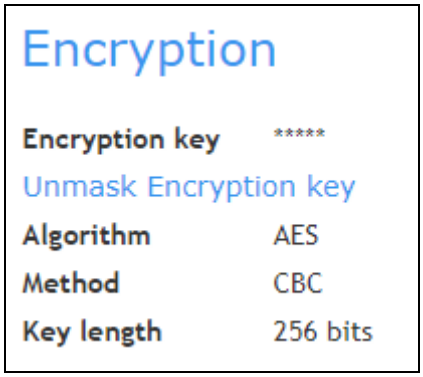


1. Slide the lever to the right to turn on the File Permissions option. Otherwise, slide to the left to turn it off.

2. Click the [Save] button to save the settings.

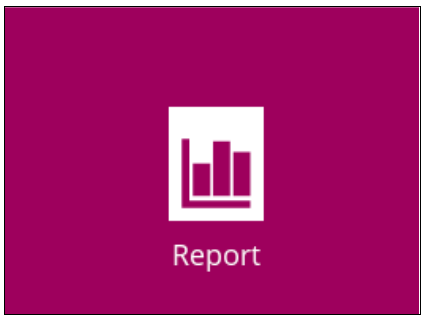
Encryption

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**.



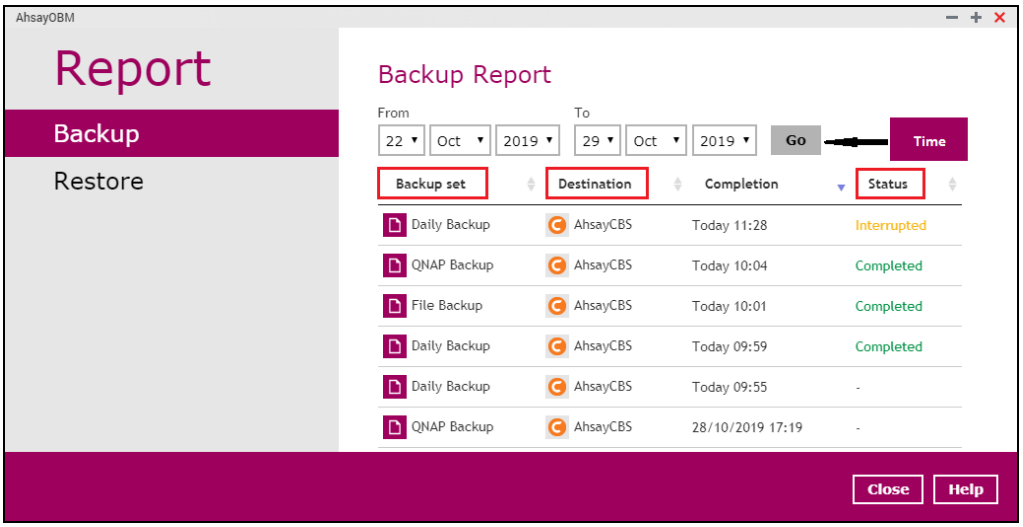
There are two (2) functions that are available for this feature:

- **Backup**
- **Restore**

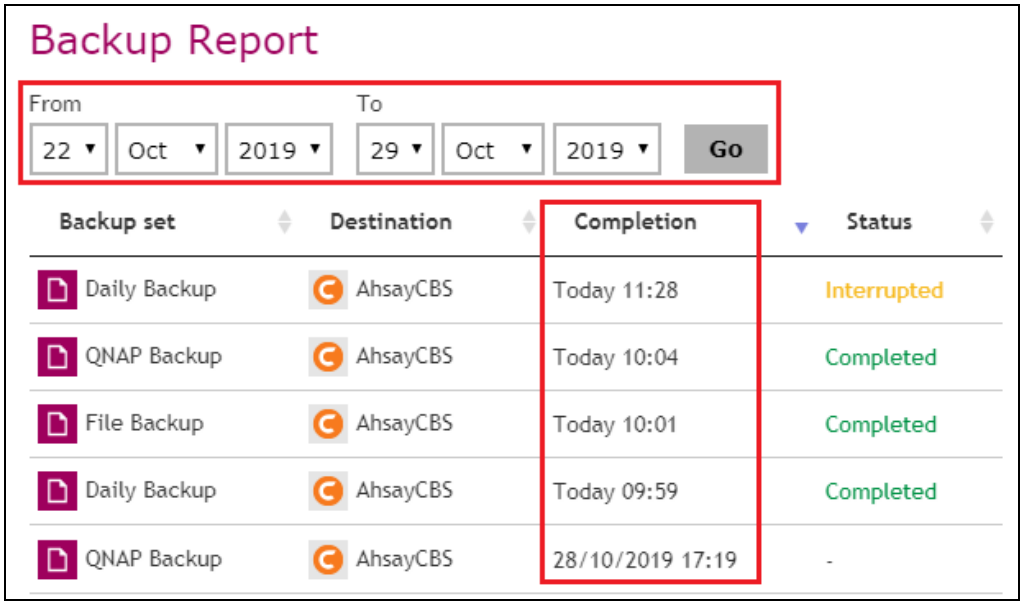
6.7.1 Backup

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

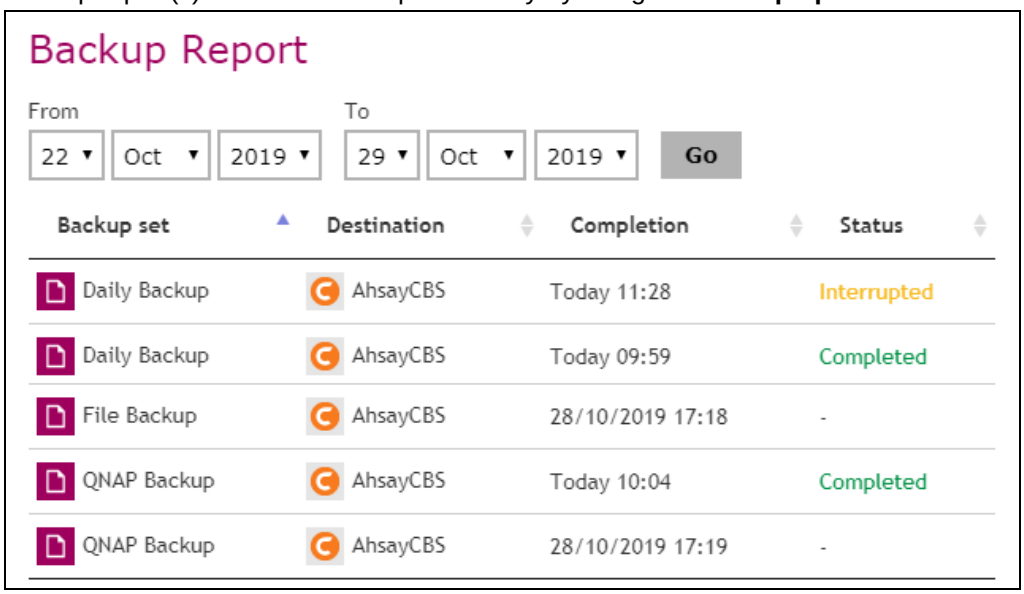
- **Time**
- **Backup set**
- **Destination**
- **Status**



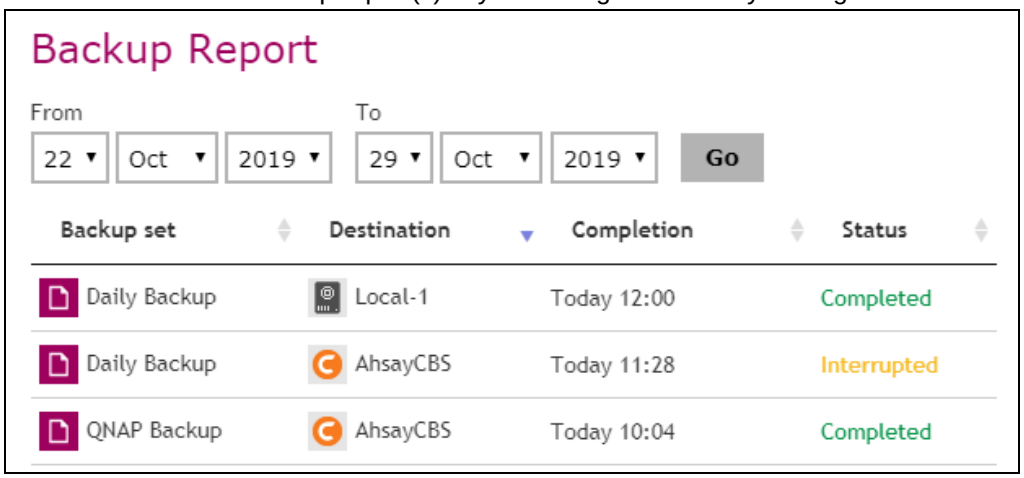
By setting the **time**, you will see the list of all backup report(s) within that period.



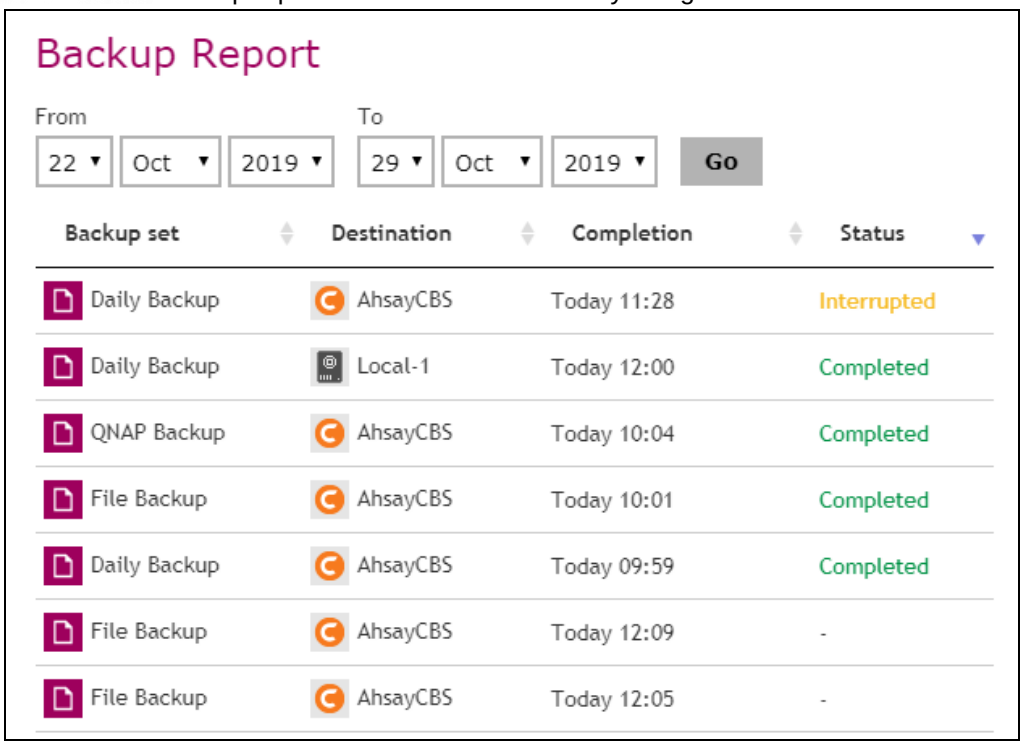
Backup report(s) can be sorted alphabetically by using the **backup up set** filter.



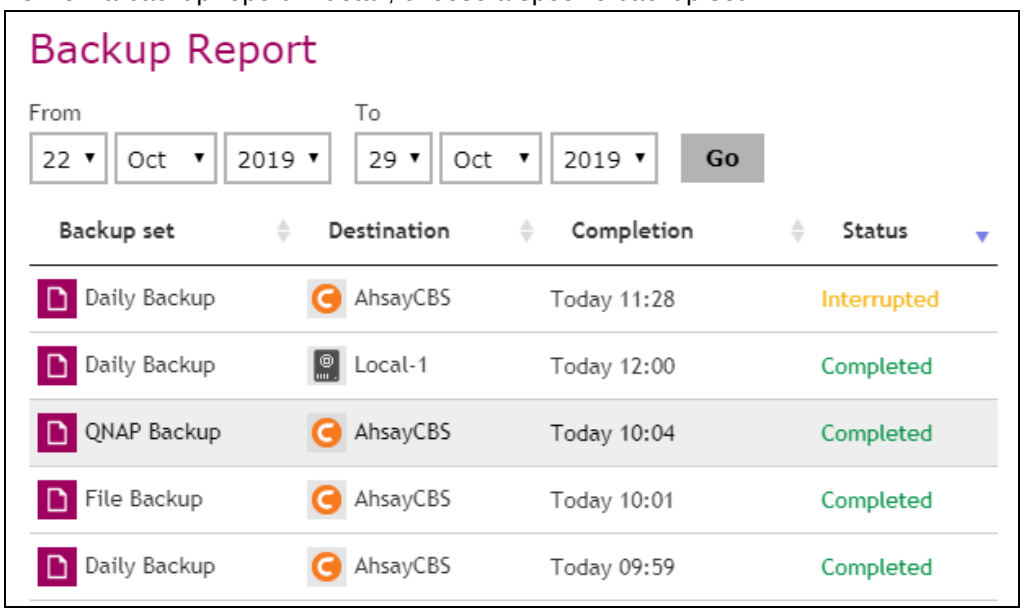
You can view all the backup report(s) in your storage location by sorting the **destination** filter.



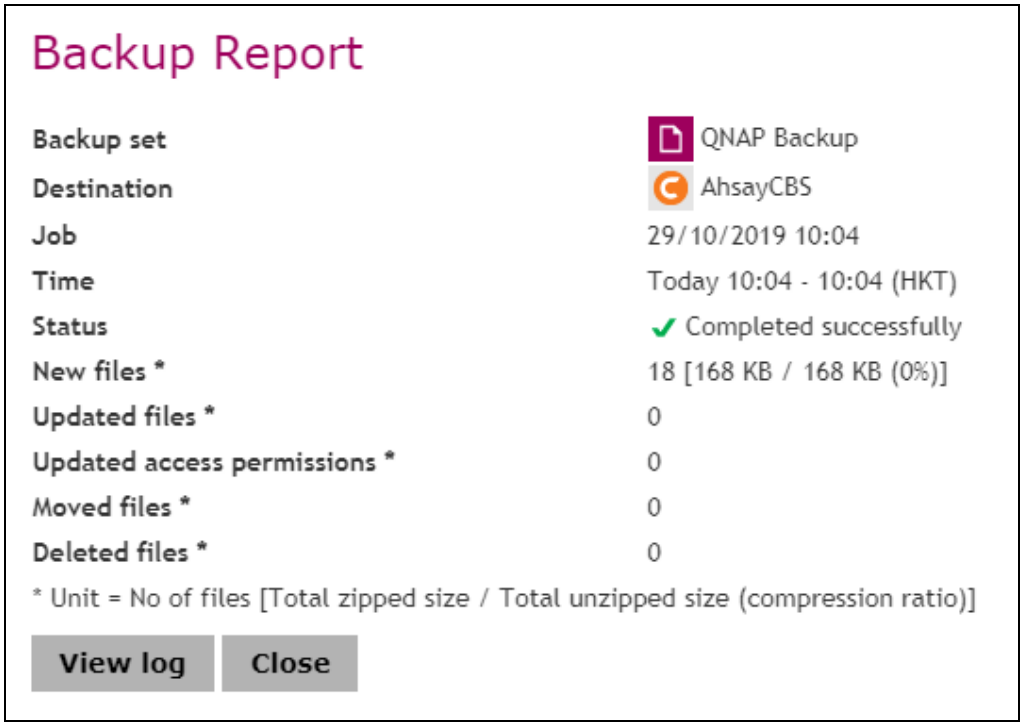
You can sort backup reports with the same status by using the **status** filter.

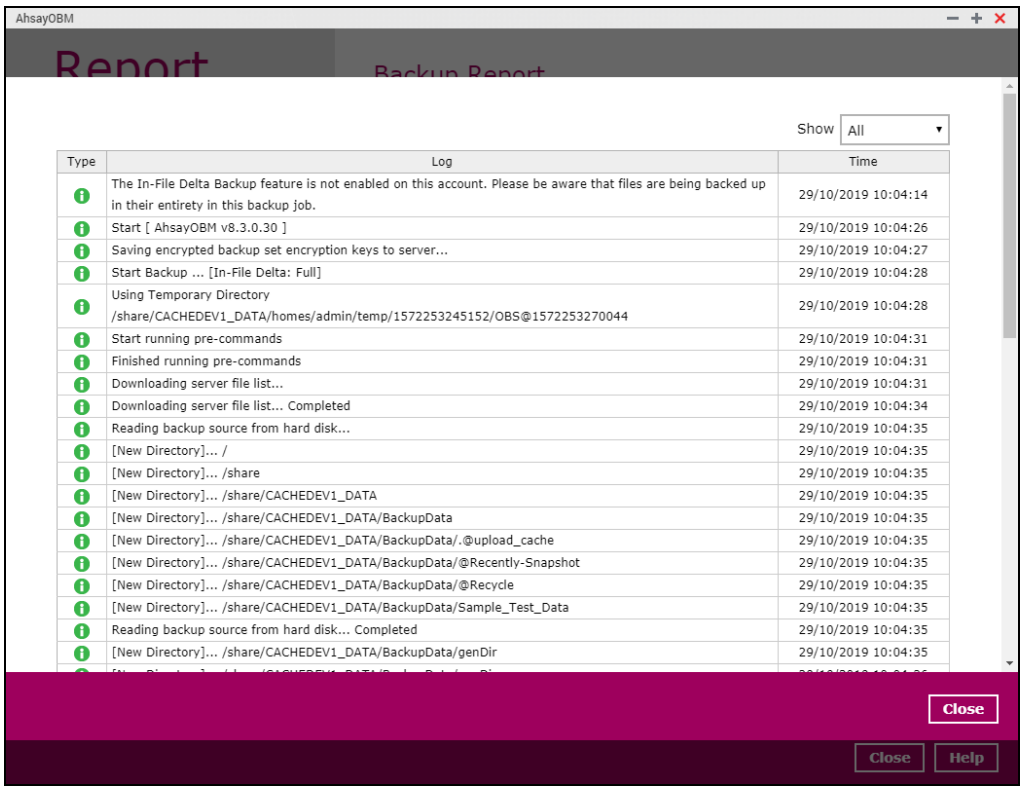


To view a backup report in detail, choose a specific backup set.

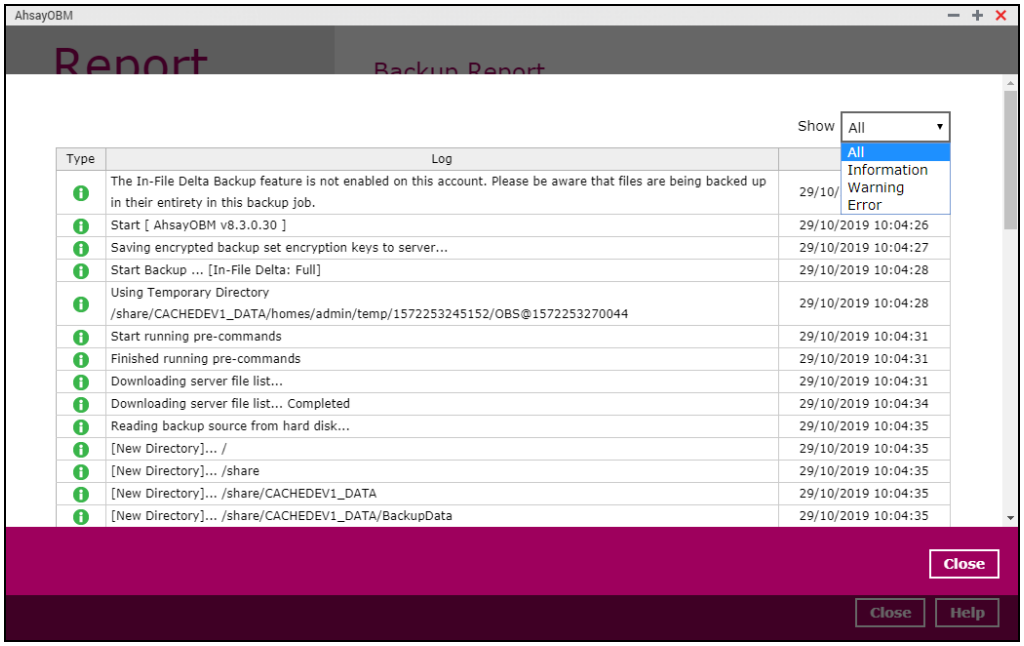


Click **view log** to show the event log during a backup.

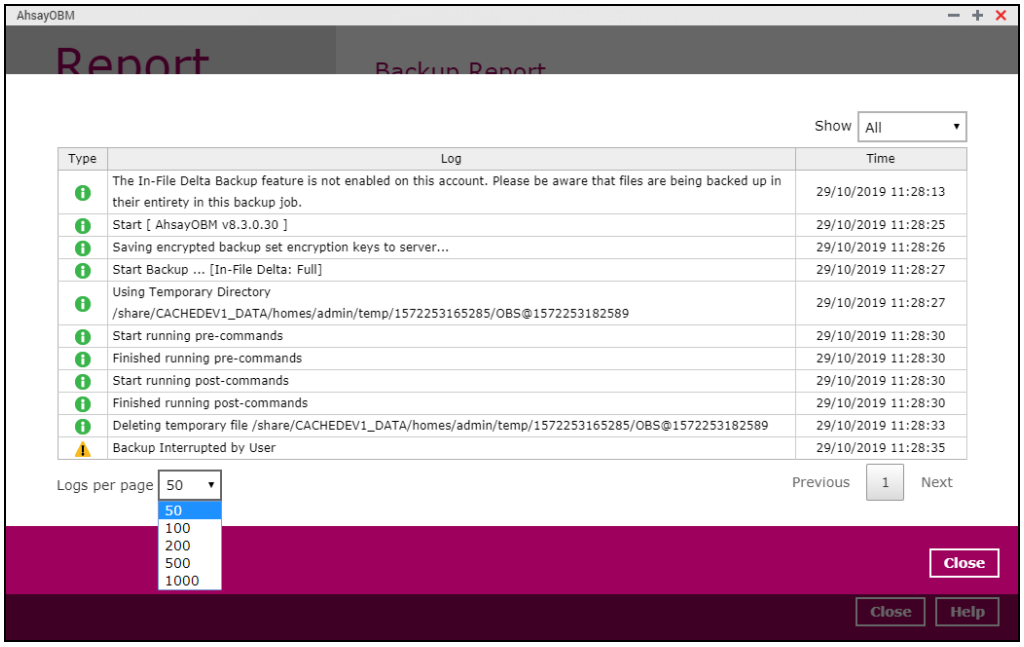




You can apply filter on the status of the event by clicking the drop-down list.

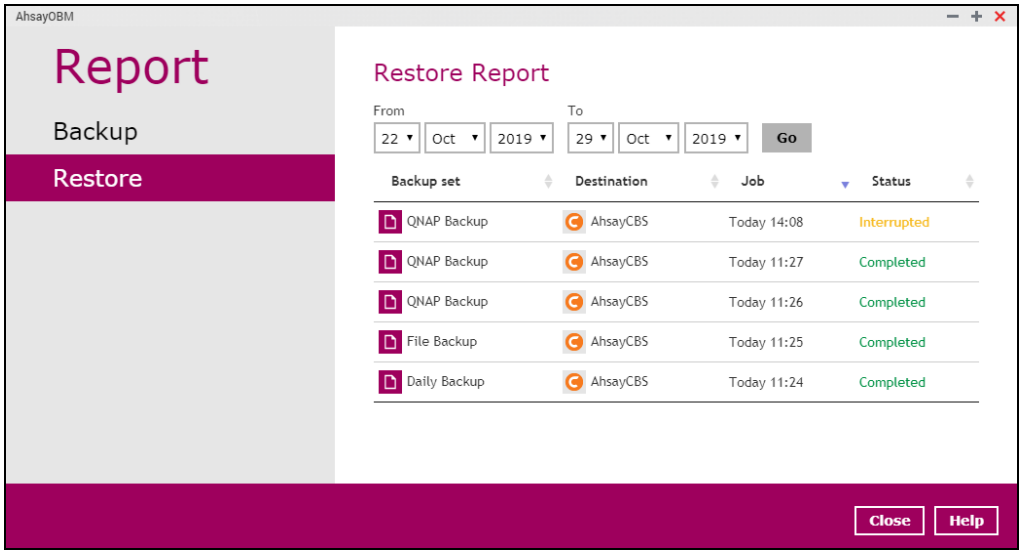


You can choose to view the number of logs per page by clicking the drop-down list.



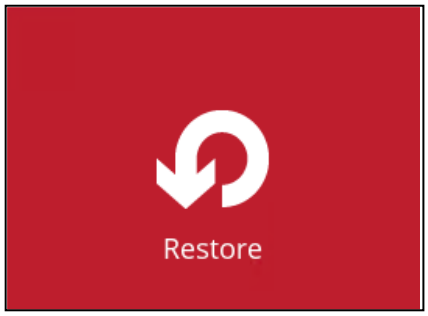
6.7.2 Restore

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

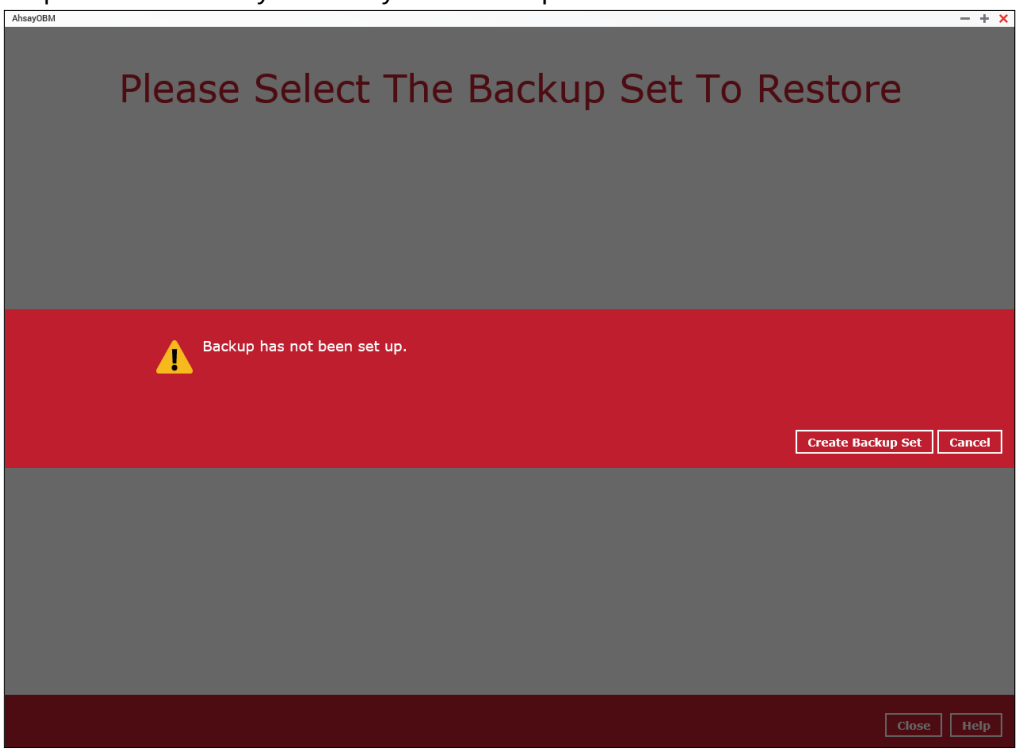


6.8 Restore

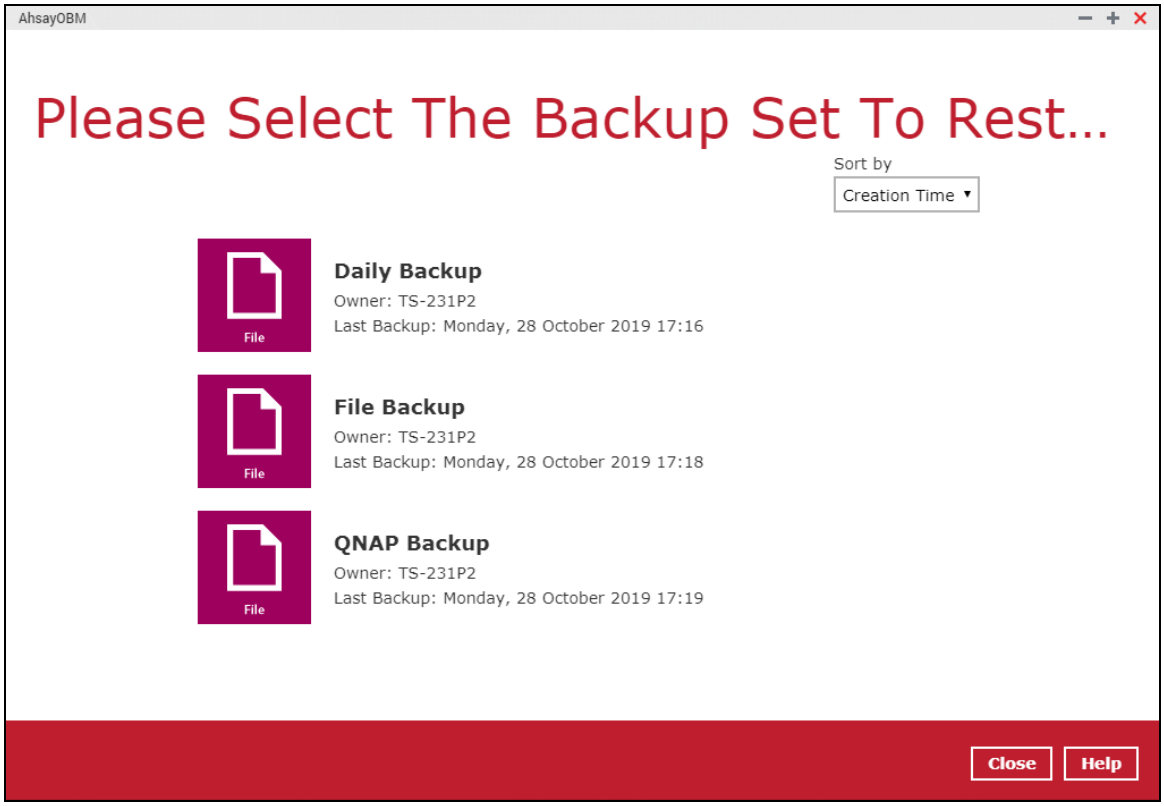
This feature is used to copy the backed-up file(s) from the backup set and restoring it to its original location or new location.



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.

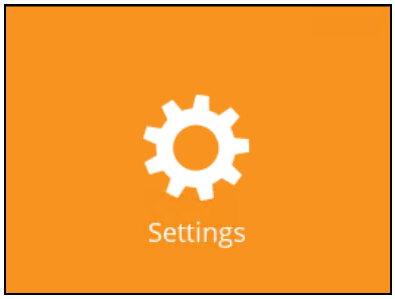


If a backup job has been performed, select a backup set you wish to restore.



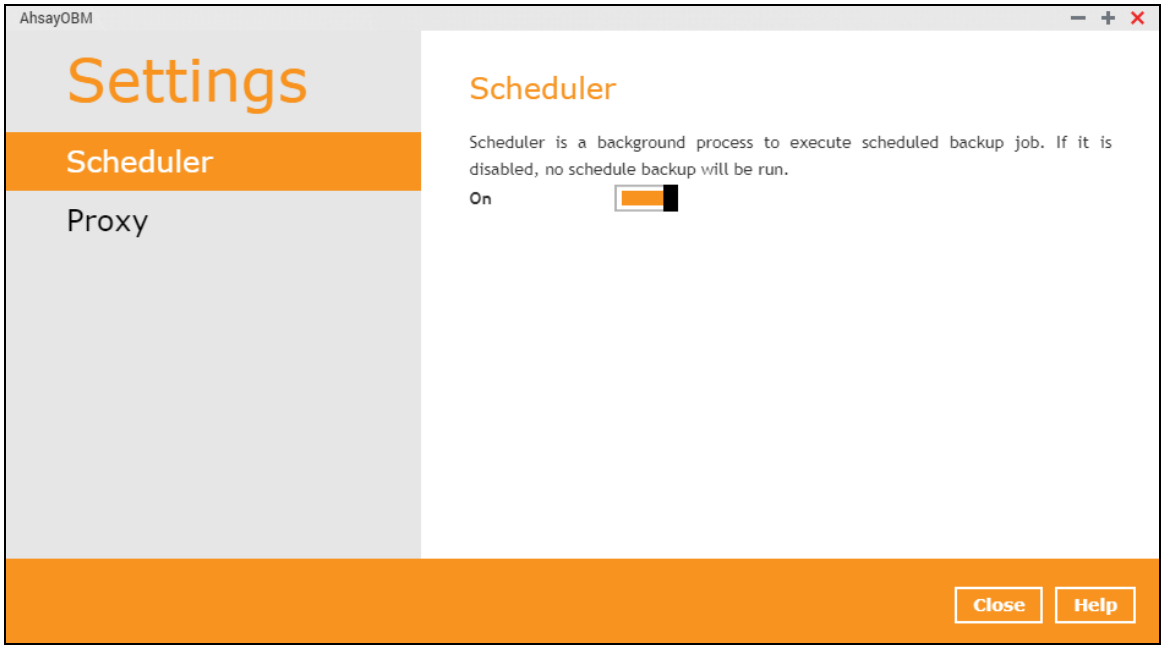
6.9 Settings

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



6.9.1 Scheduler

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

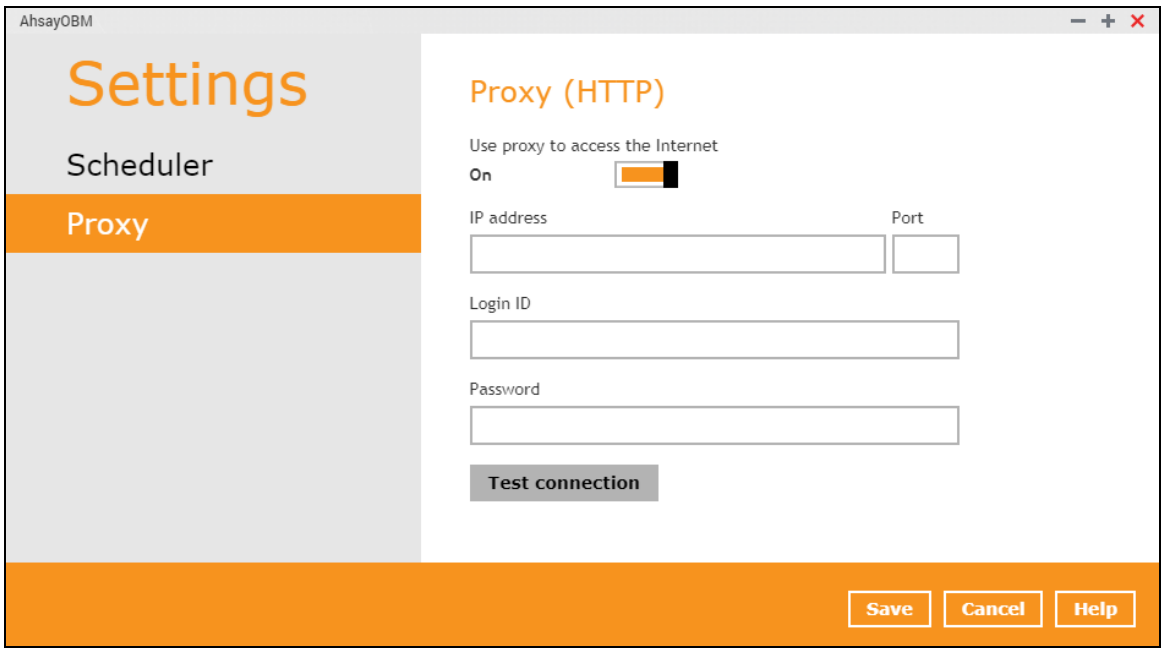


Note

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

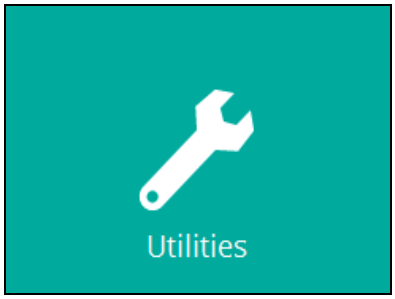
6.9.2 Proxy

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



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:

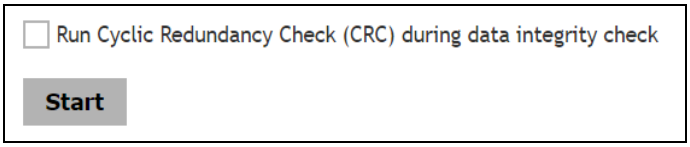
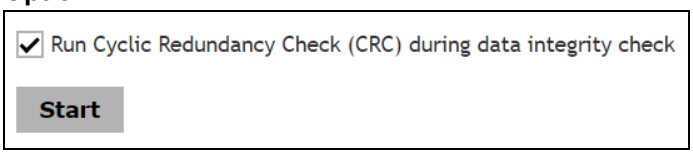
- Data Integrity Check
- Delete Backup Data

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).

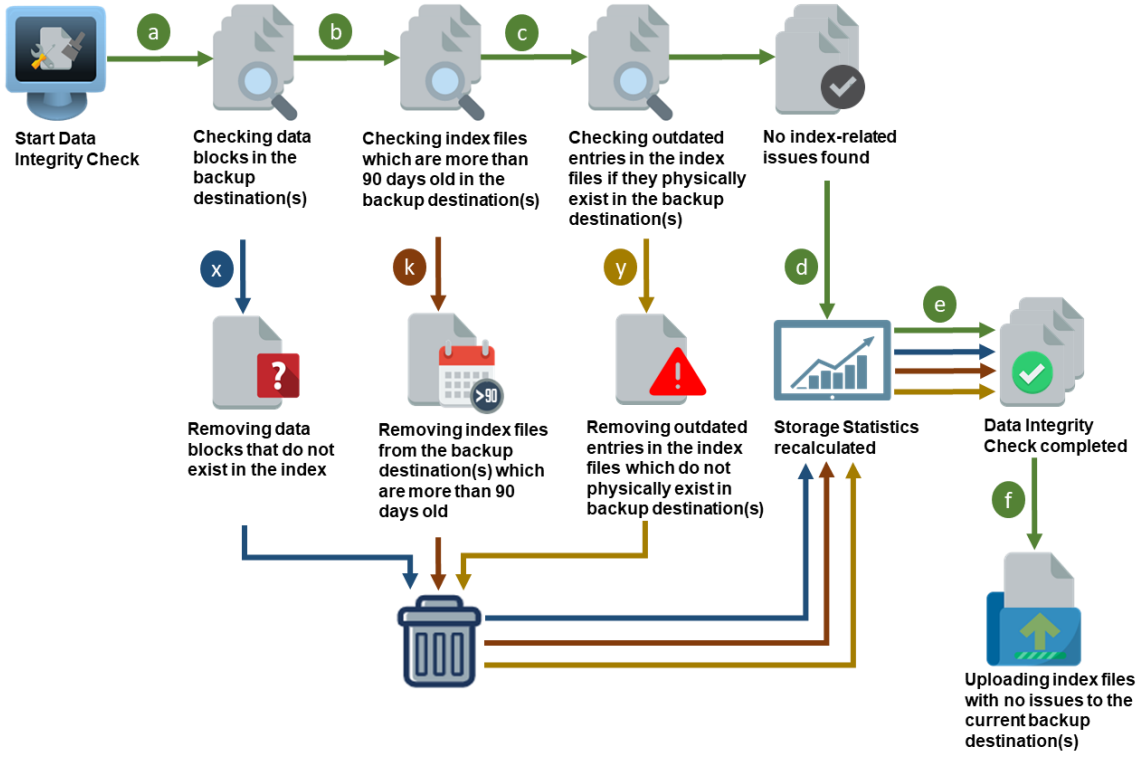
There are two (2) options in performing the Data Integrity Check:

Option 1 	For checking of index and data.
Option 2 	For checking of index and integrity of files against the checksum file generated at the time of the backup job.

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

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

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



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

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

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

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

e Data integrity check is completed.

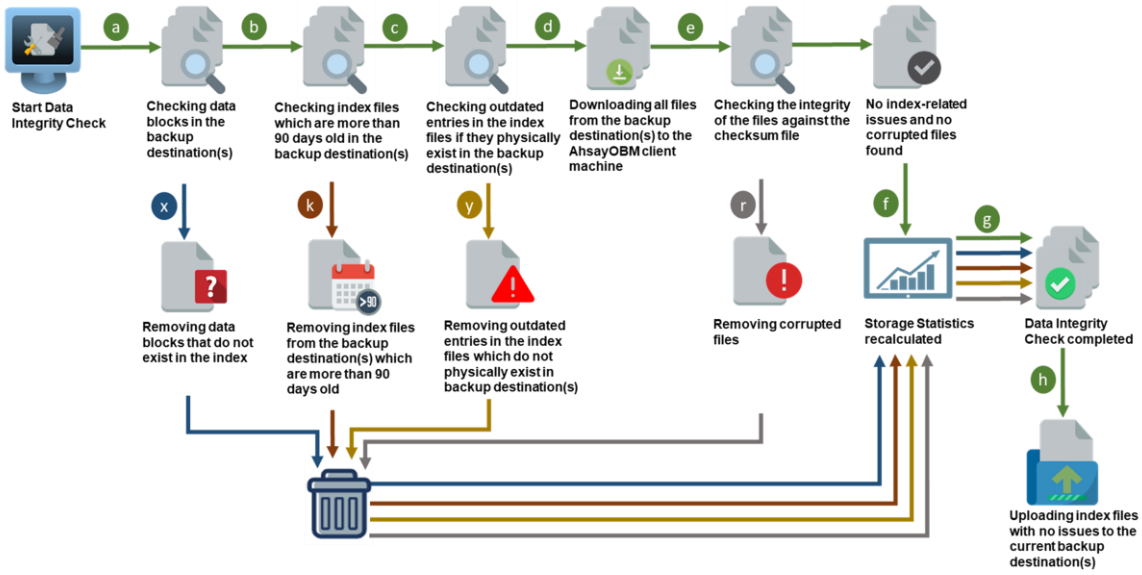
f Index files with no issues will be uploaded to the current backup destination(s).

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

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

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

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



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

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

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

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

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

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

g Data integrity check is completed.

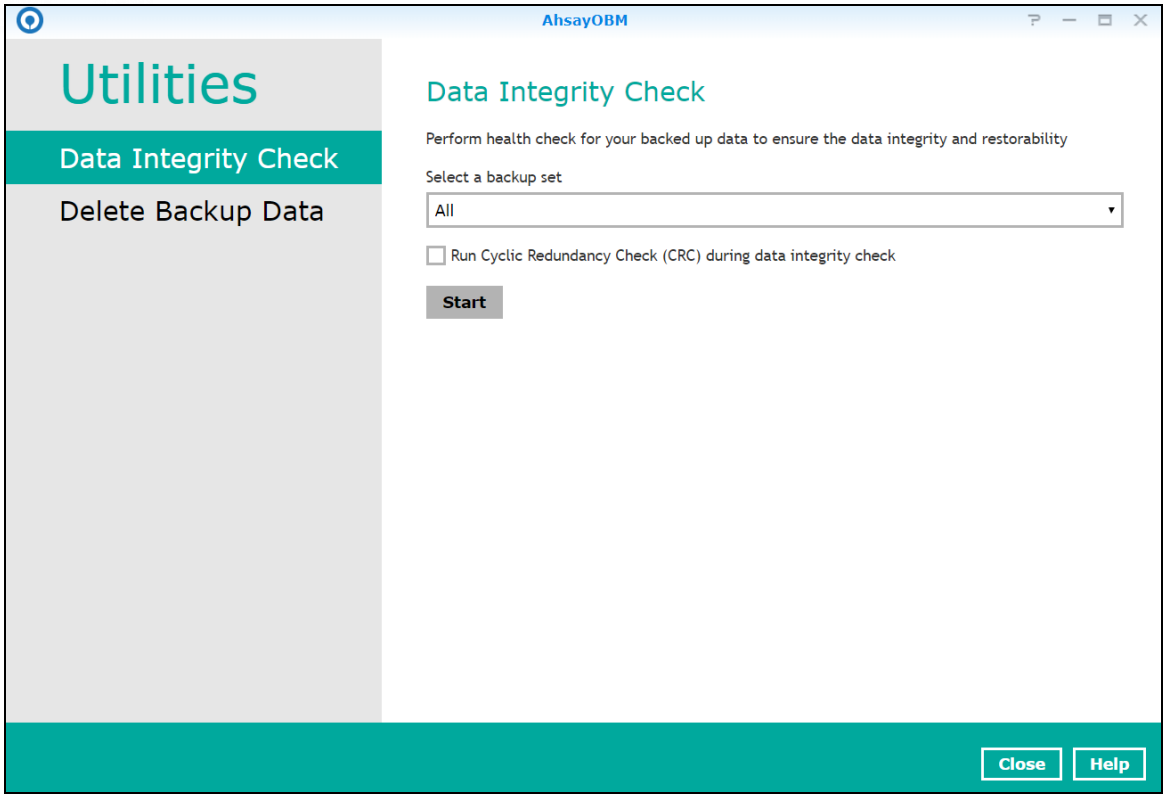
h Index files with no issues will be uploaded to the current backup destination(s).

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

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

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

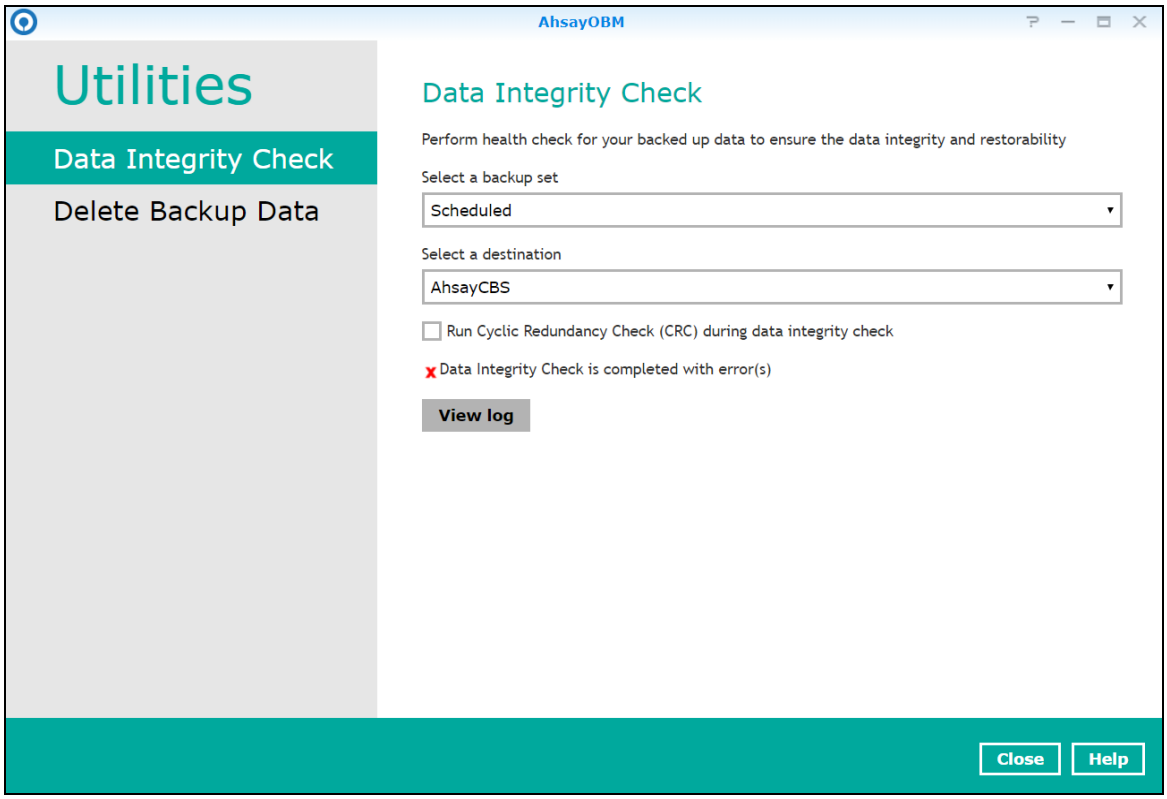
r Corrupted files will be automatically removed from the backup destination(s).

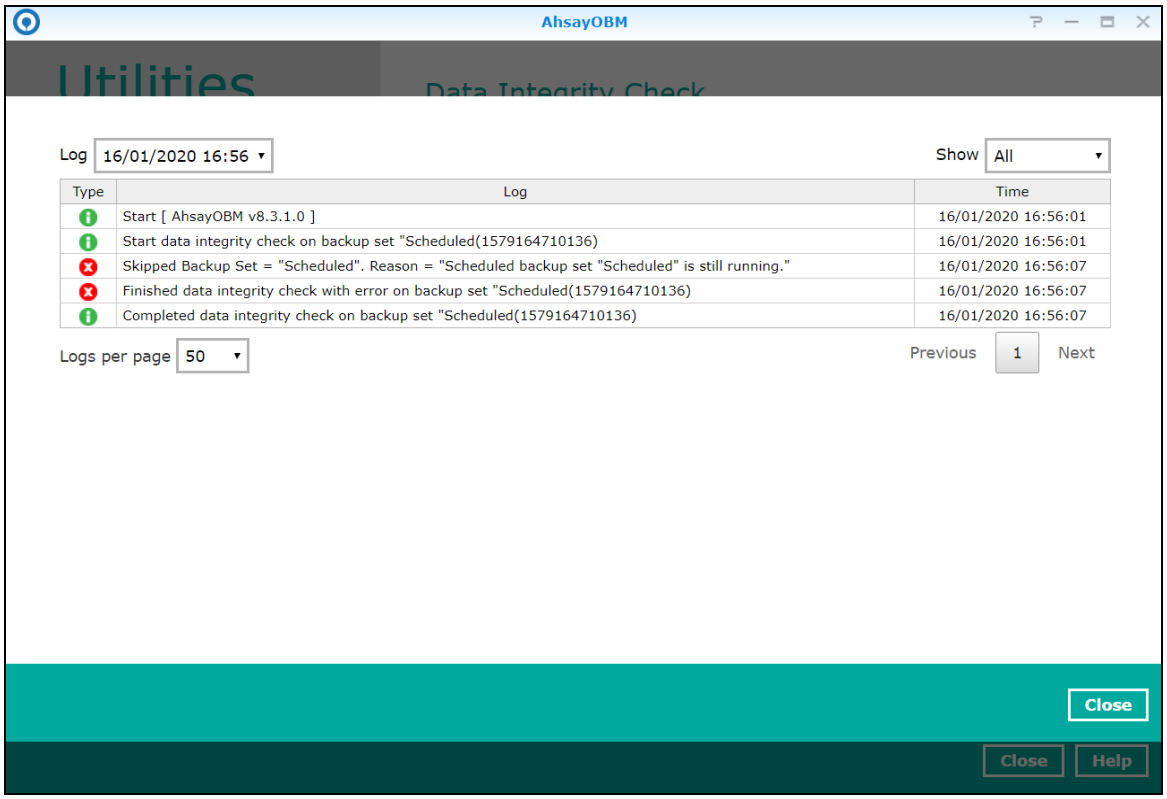


NOTES

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

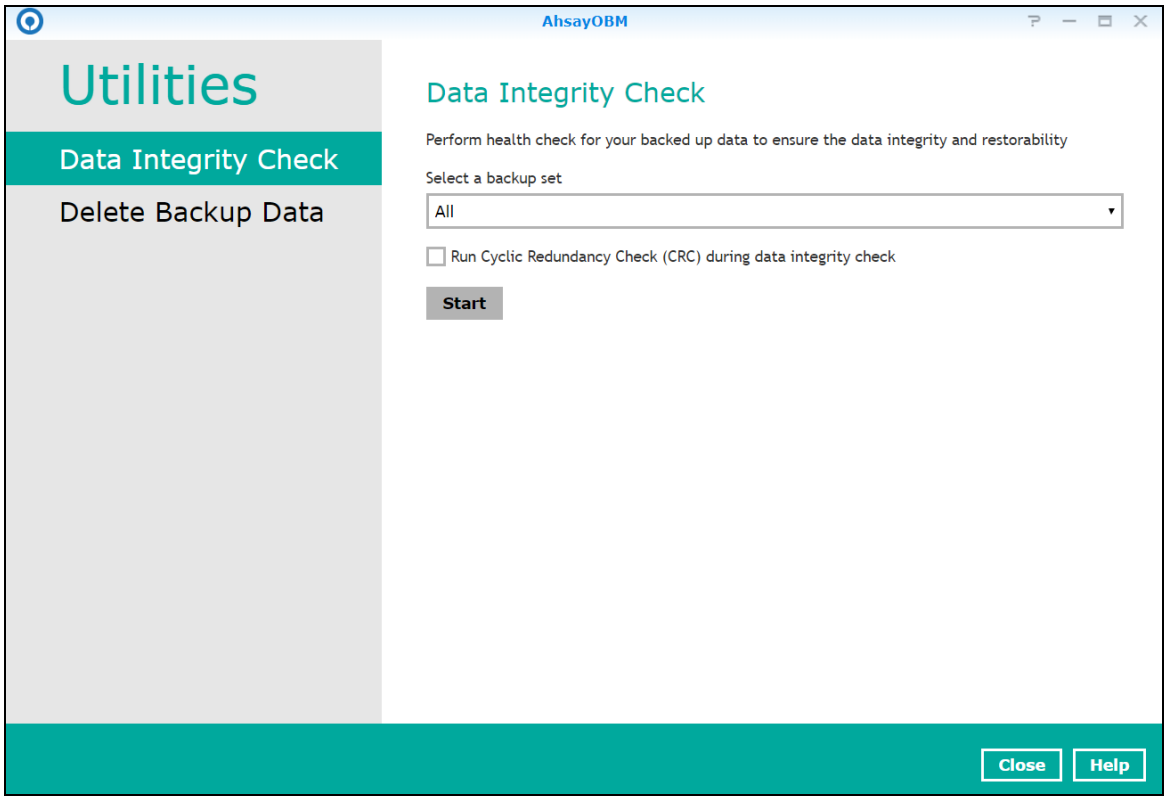
The following screenshot is an example of a Data Integrity Check completed with error(s). A Data Integrity Check is run on a backup set with an active backup job running which resulted the Data Integrity Check to stop with error(s). Clicking the **View log** button will display the details of the Data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



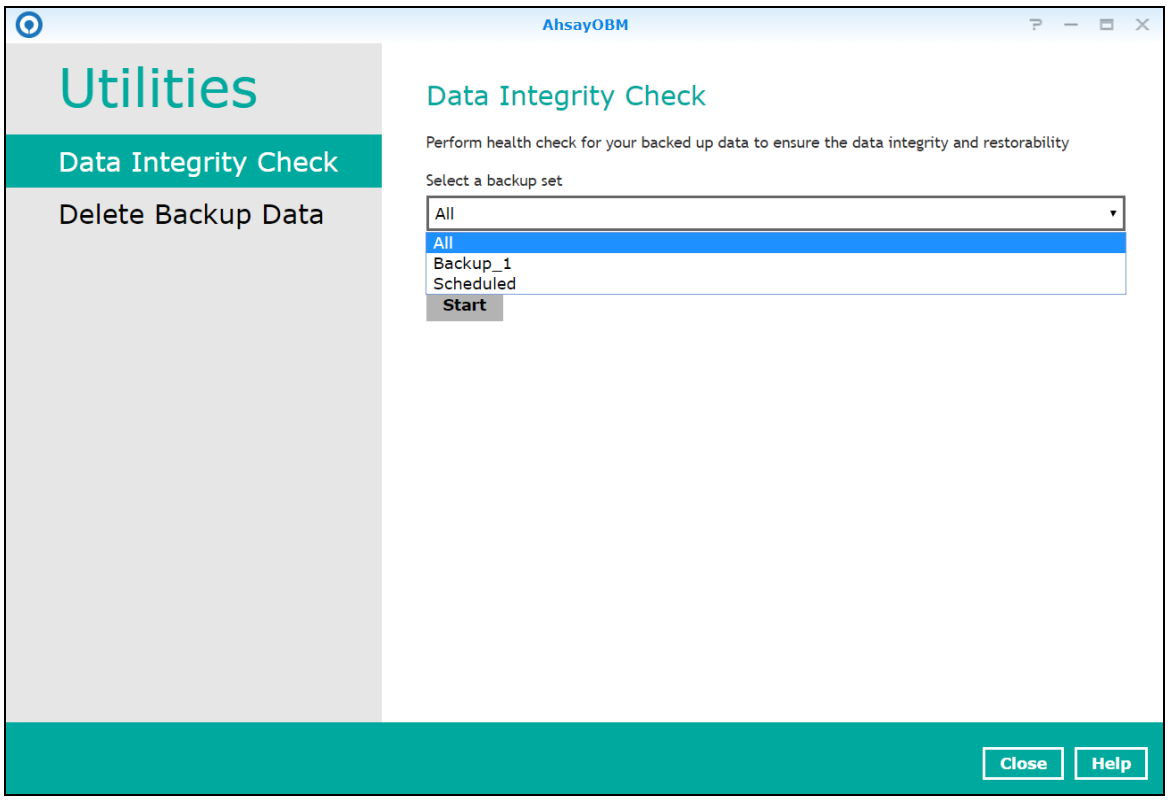


To perform a Data Integrity Check, follow the instructions below:

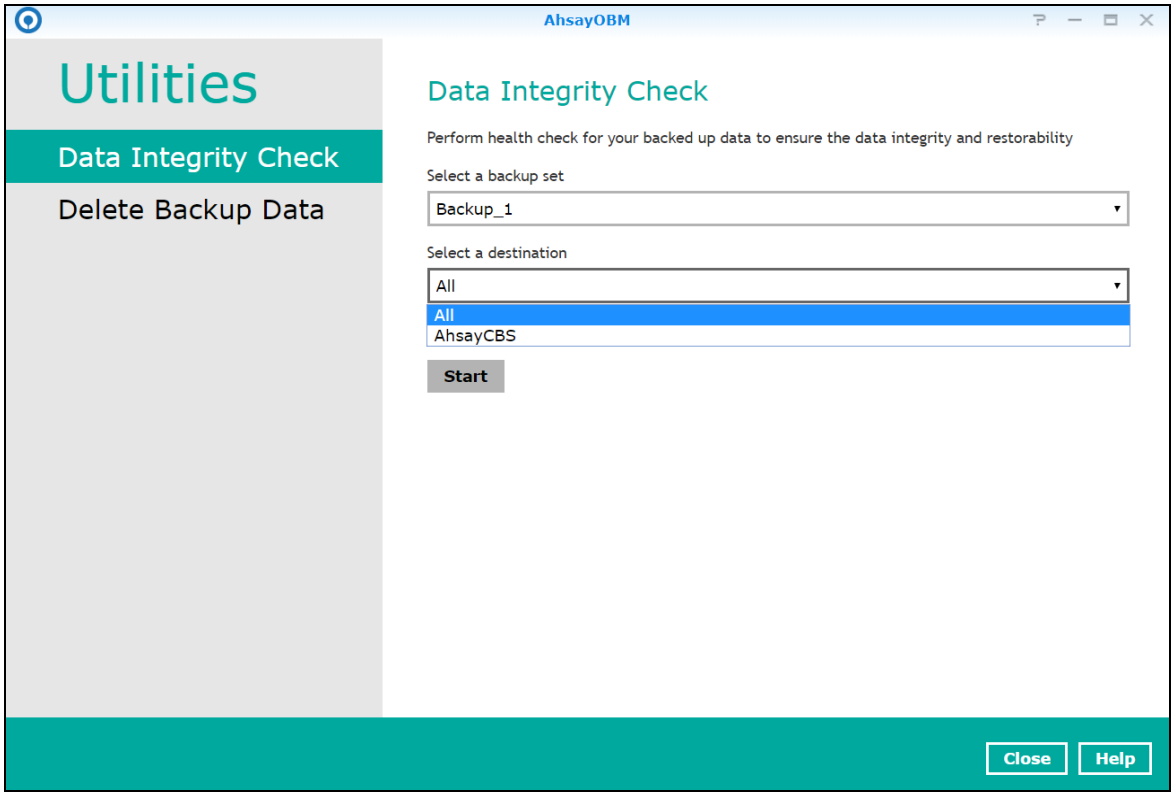
1. Go to the Data Integrity Check tab in the Utilities menu.



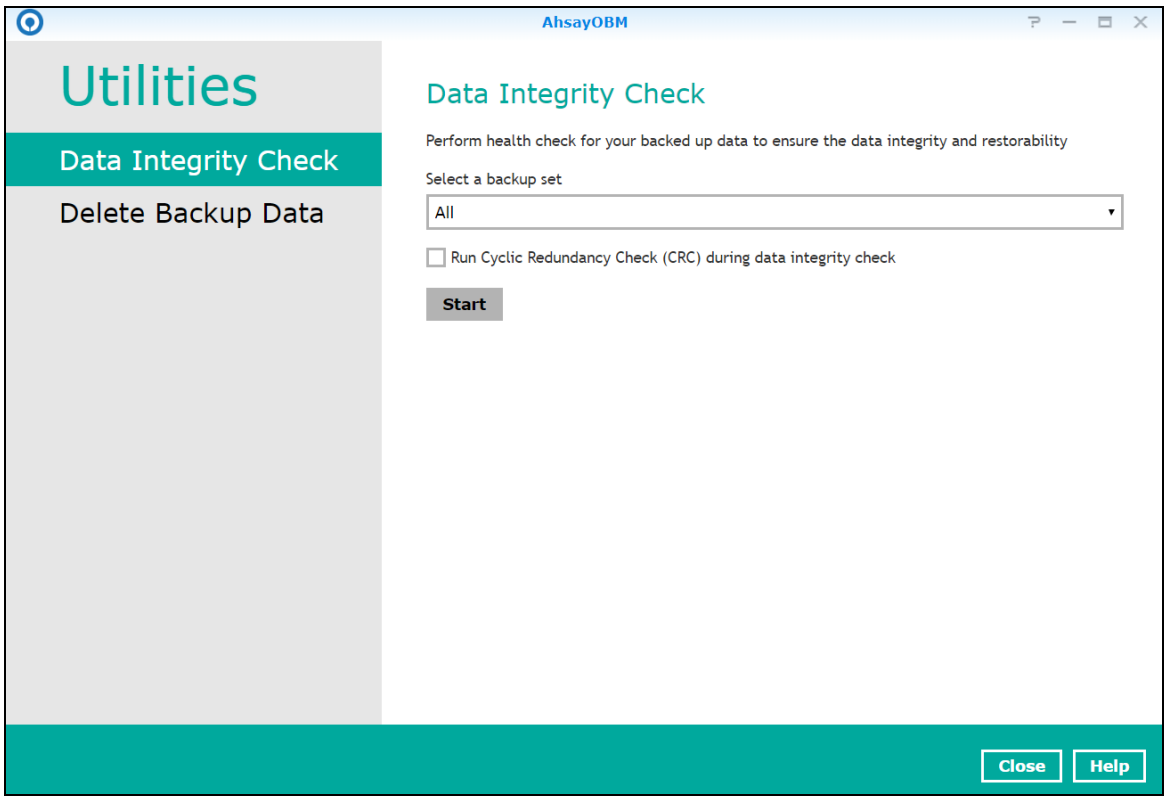
2. Click the drop-down button to select a backup set.



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



4. Unchecked Run Cyclic Redundancy Check (CRC) option is the default setting of data integrity check.



Run Cyclic Redundancy Check (CRC)

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

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

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

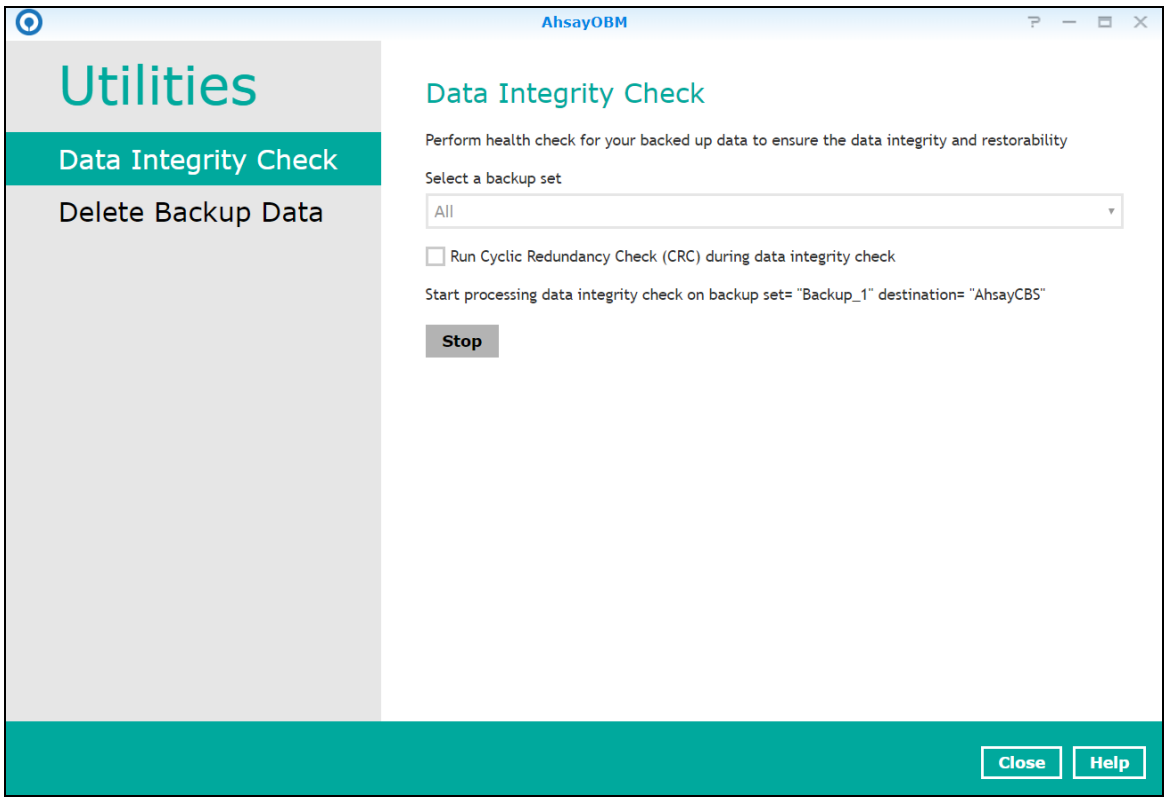
The time required to complete a data integrity check depends on the number of factors such as:

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

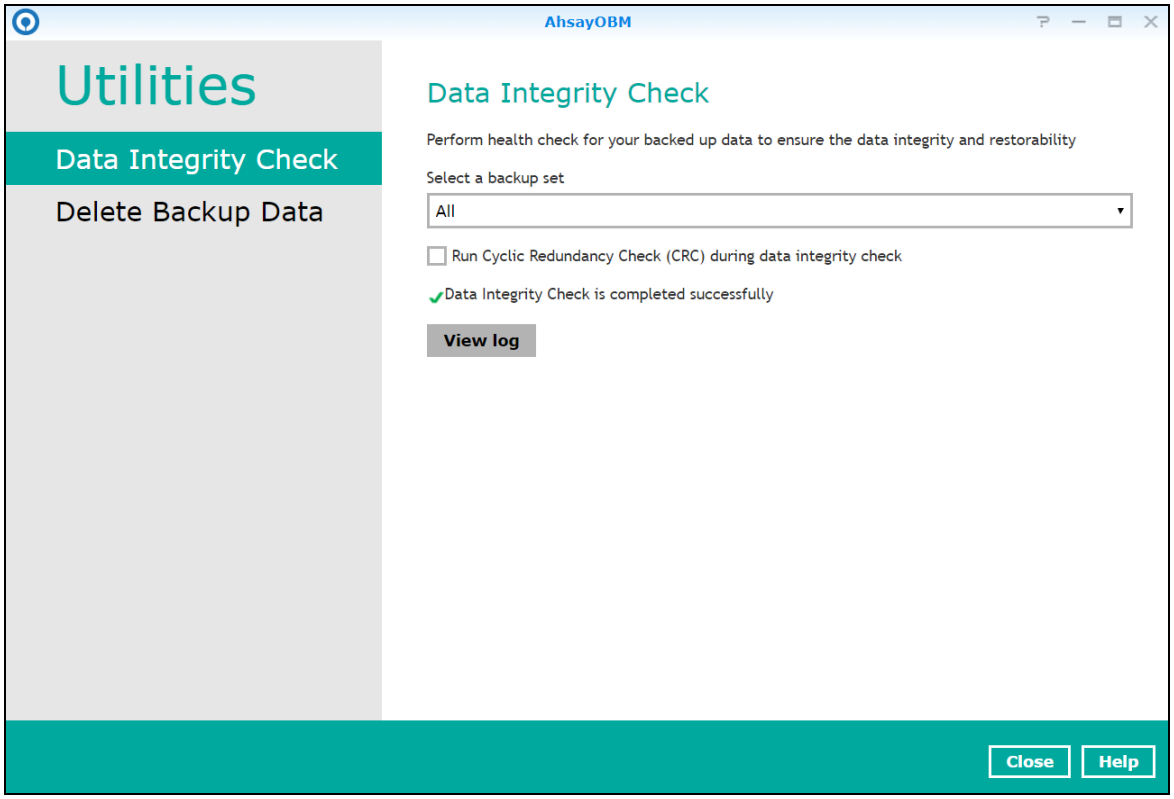
NOTE

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

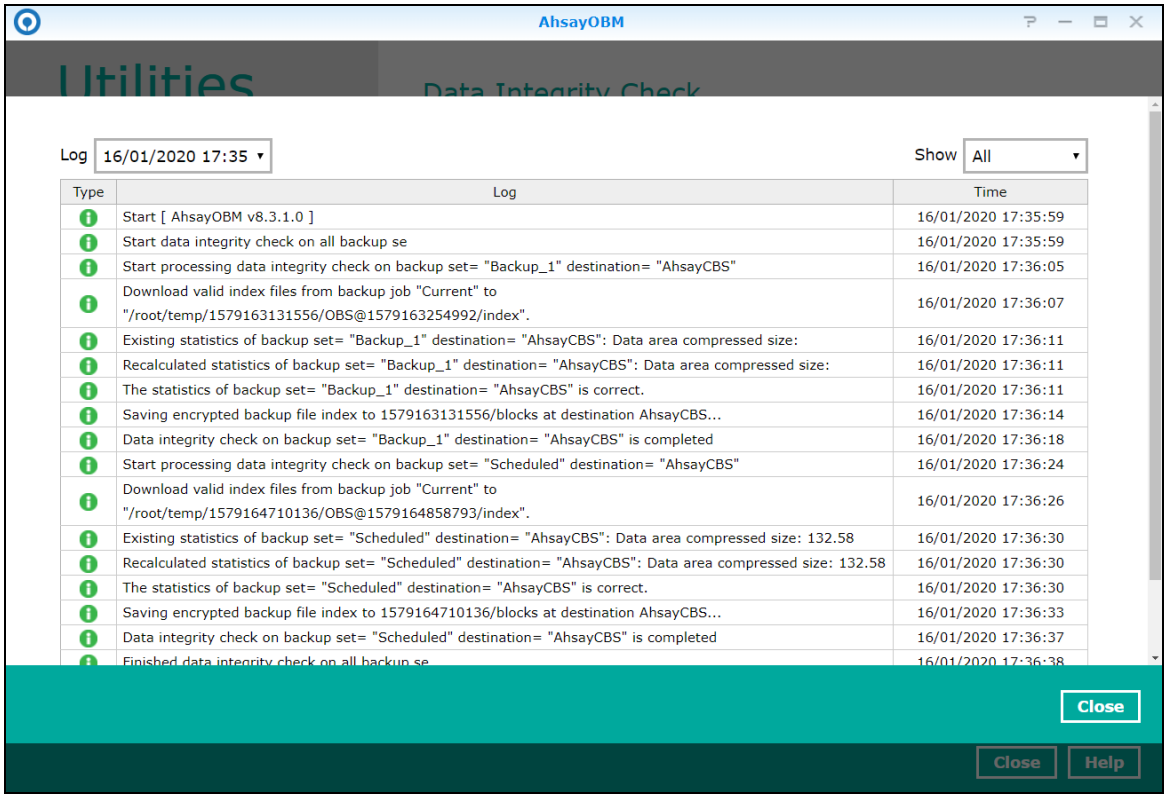
5. Click the [Start] button to begin the Data Integrity Check.
6. Data Integrity Check will start running on the selected backup set(s) and backup destination(s).



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

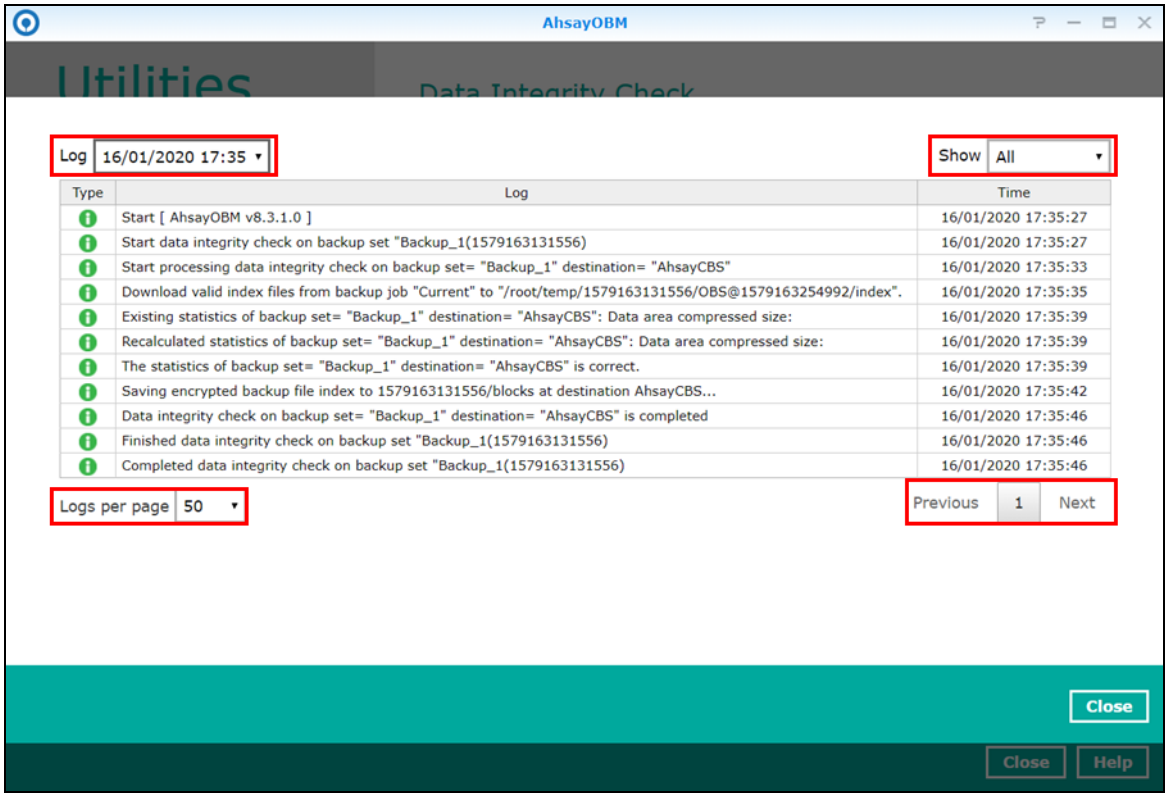


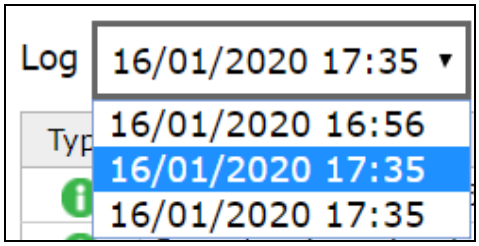
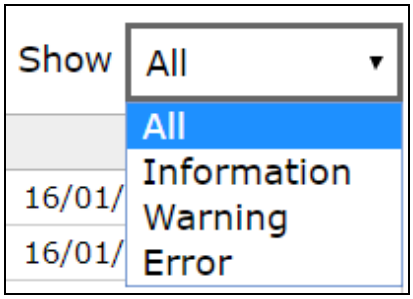
8. The detailed log of data integrity check process will be displayed.

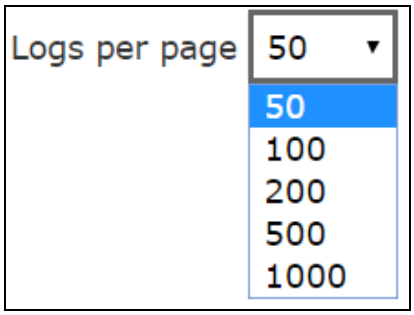


The following options can be used for further viewing of the detailed DIC log:

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



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

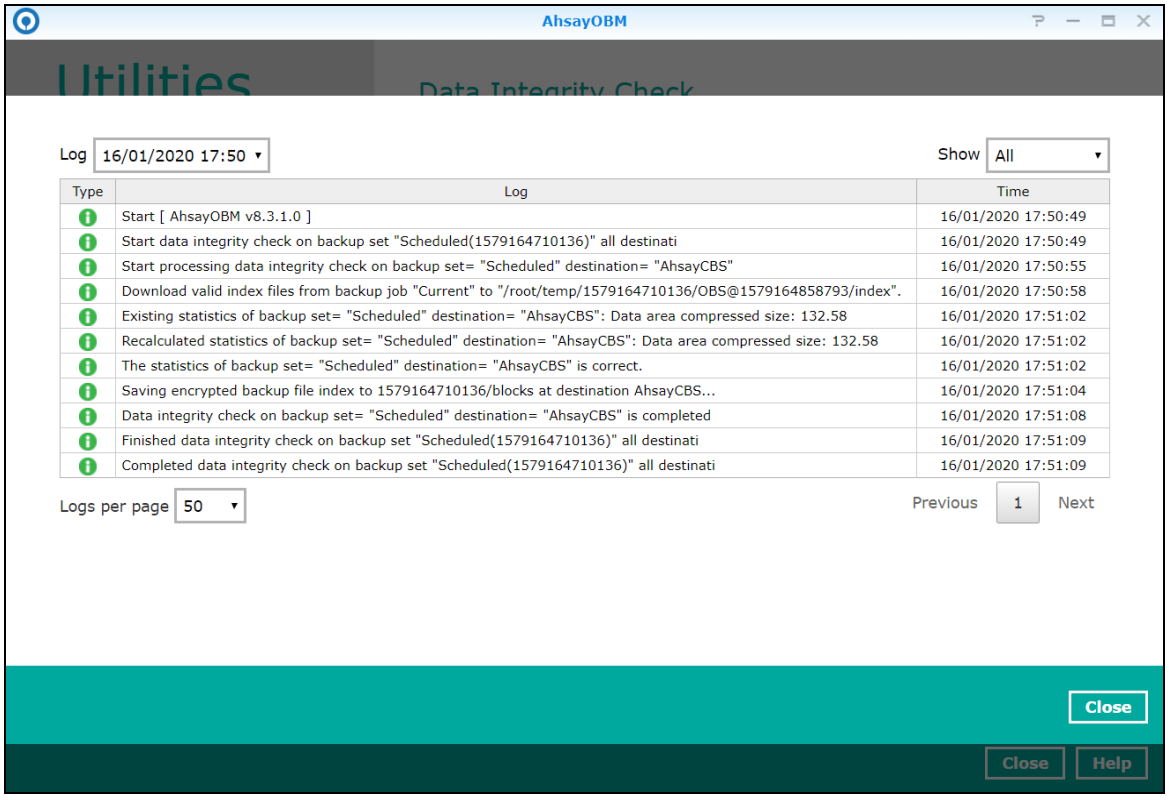
Logs per page		This option allows user to control the displayed number of logs per page.
Page		This option allows user to navigate the logs to the next page(s).

Data Integrity Check Result

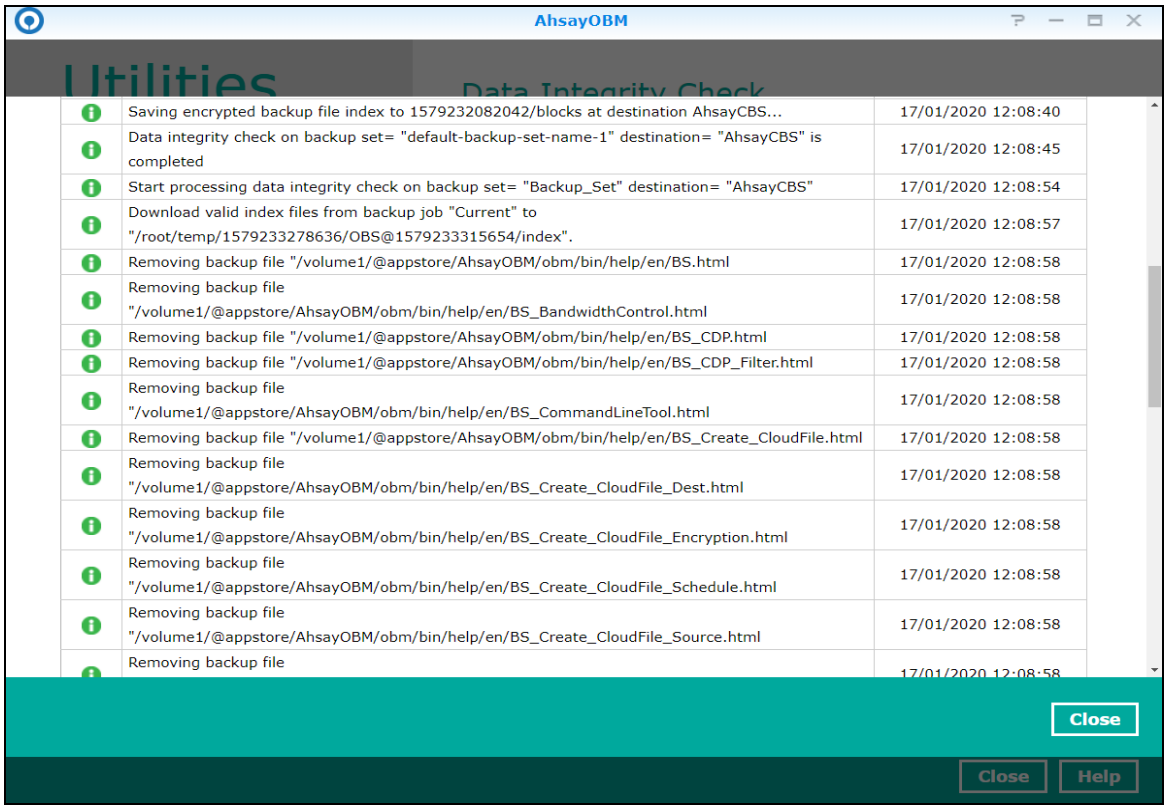
There are two possible outcomes after the completion of a data integrity check:

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

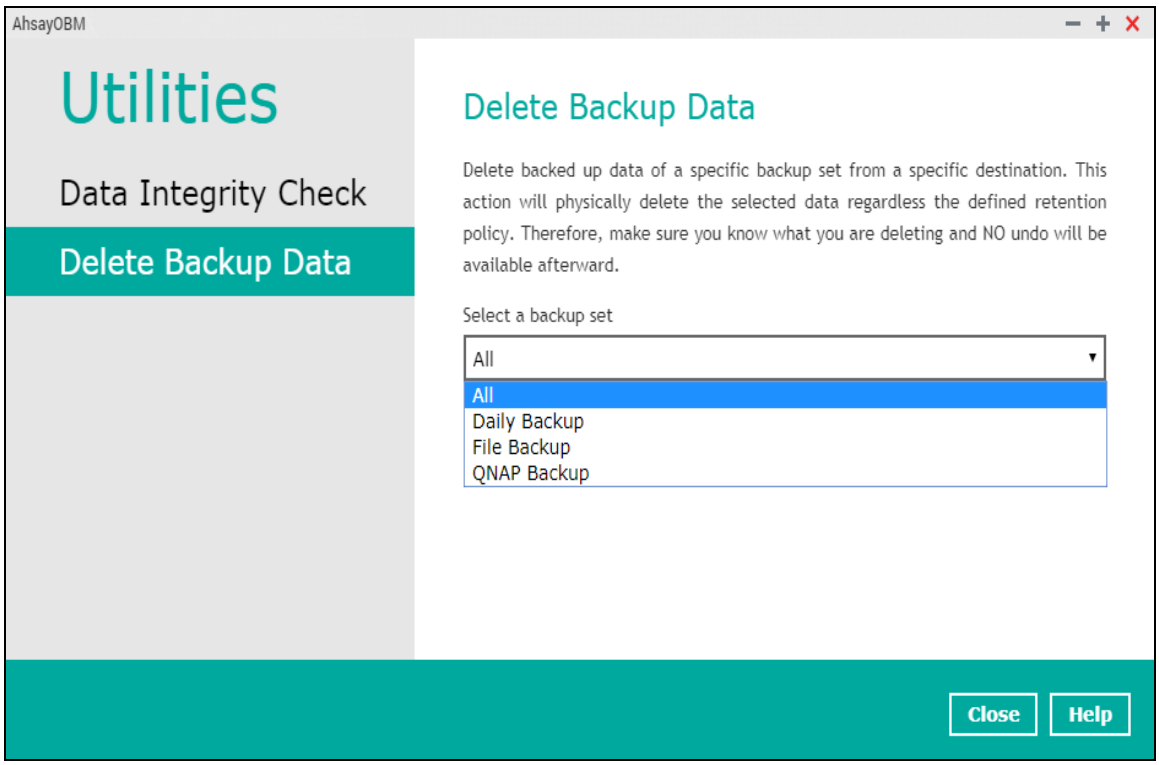
${system_volume_path}/homes/admin/.obm/system/IntegrityCheck

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.

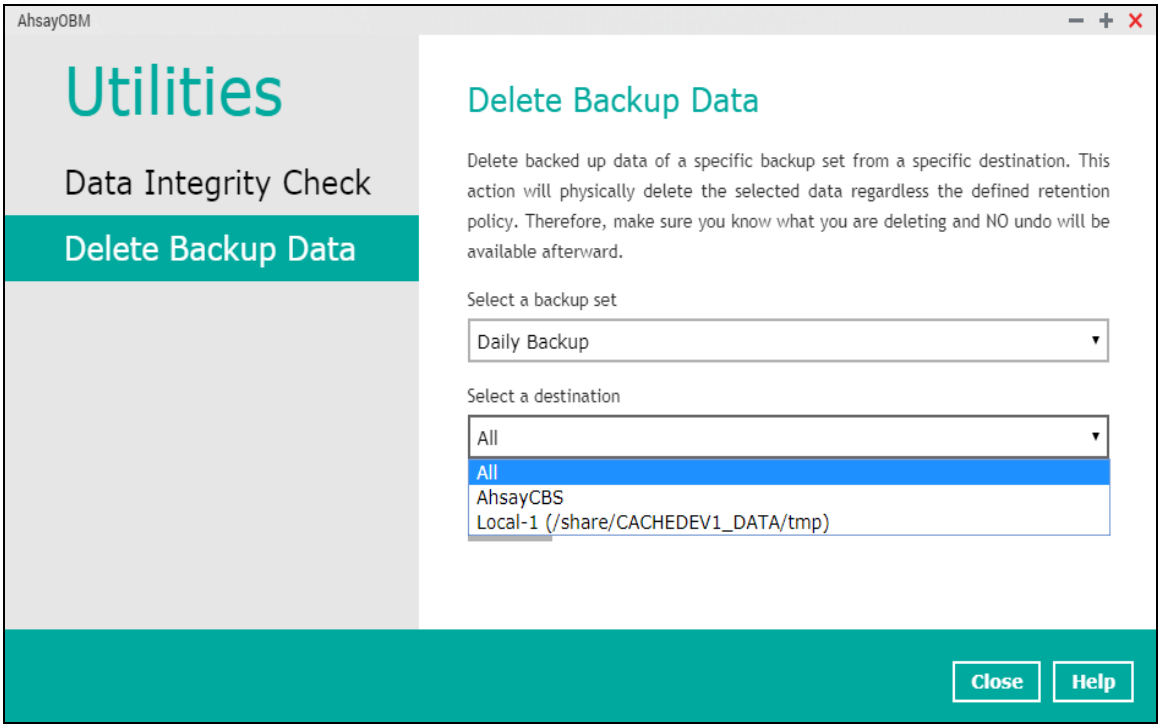
To perform deletion of backup data, follow the instructions below:

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

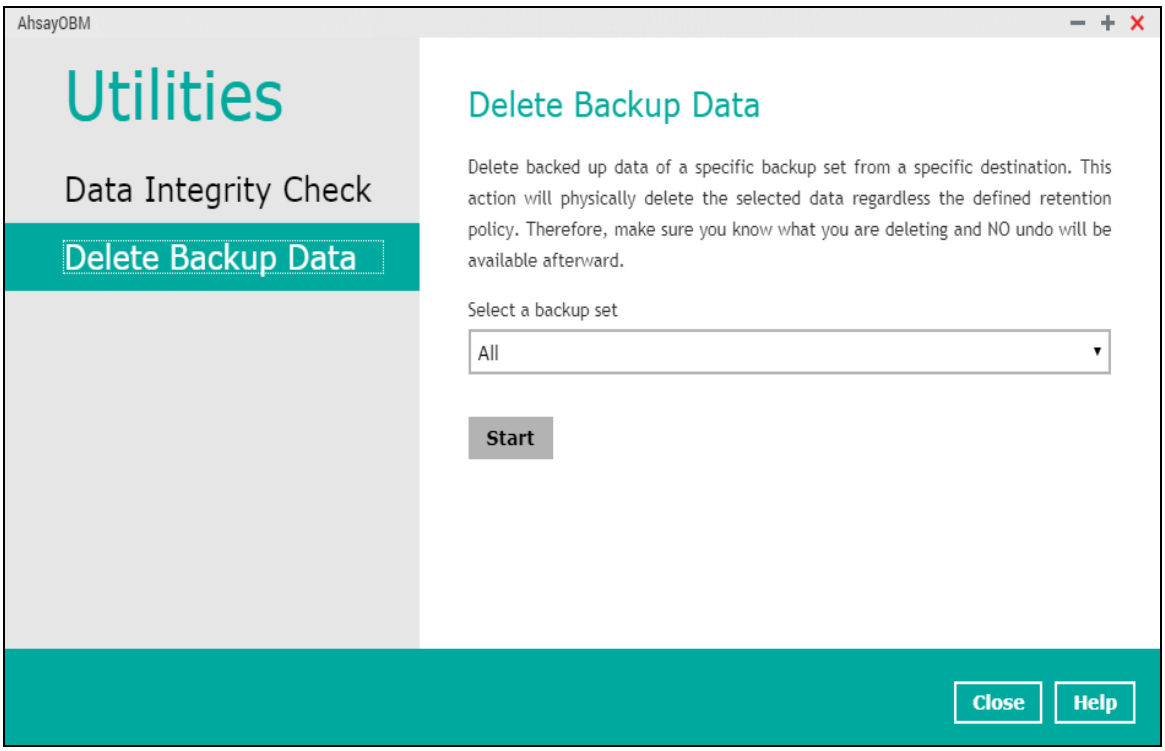


NOTE: This will only delete the backed up files in a backup set(s) and destination(s), but the backup set and destination will remain.

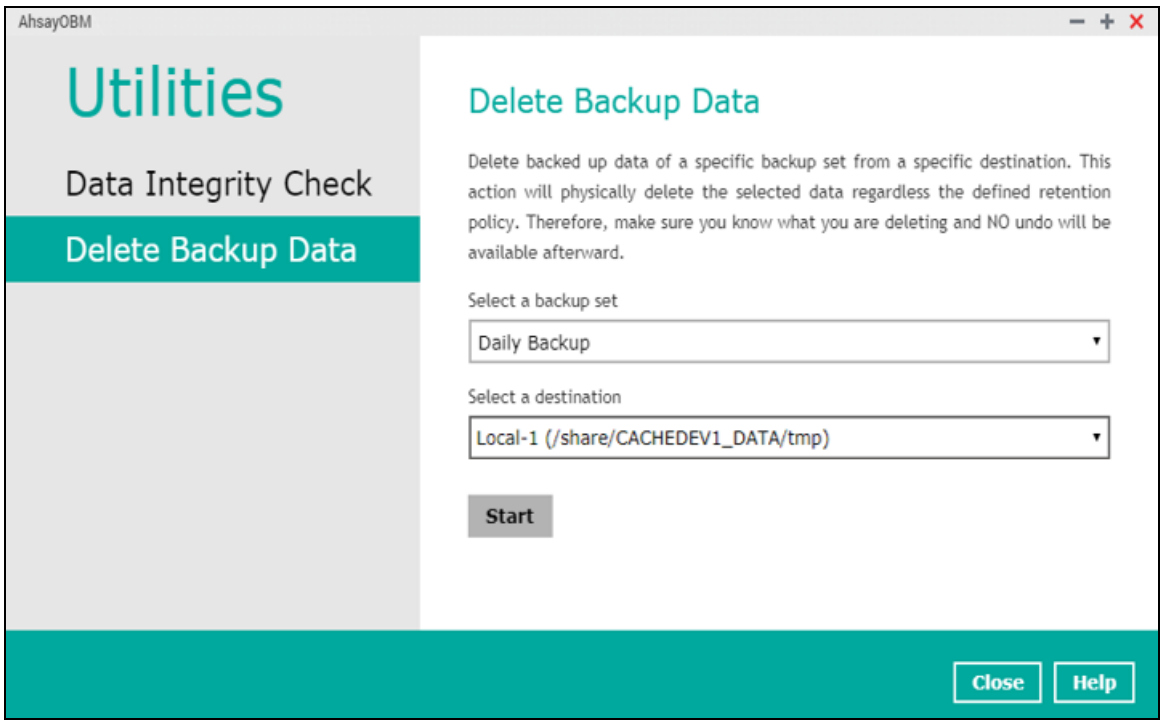
If you select a specific backup set, then you will also have to select a specific destination or all destinations.

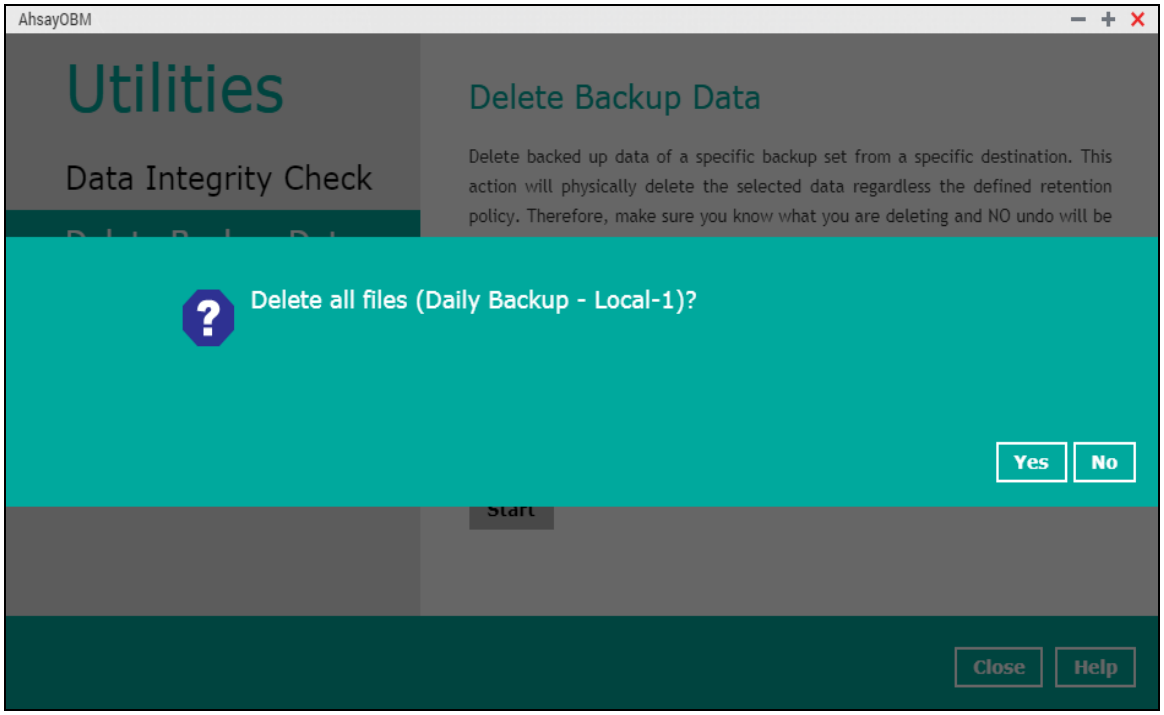


If you select **All** backup sets, then there is no need to select a destination.

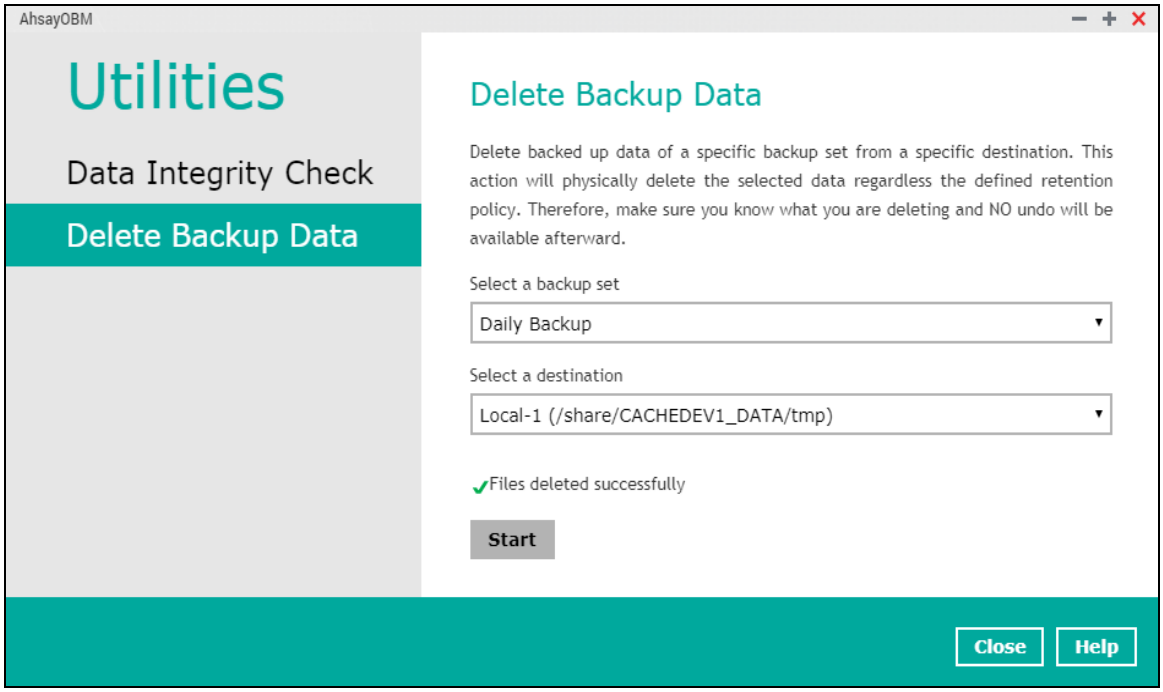


2. Click the [Start] button, then click [Yes] to proceed. This process will delete backed up data on the selected backup set(s) and destination(s).





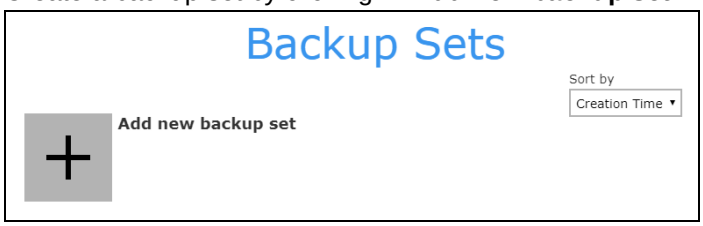
3. Files are successfully deleted.



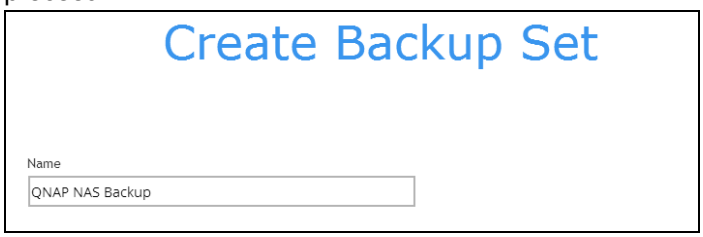
7 Create a Backup Set

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

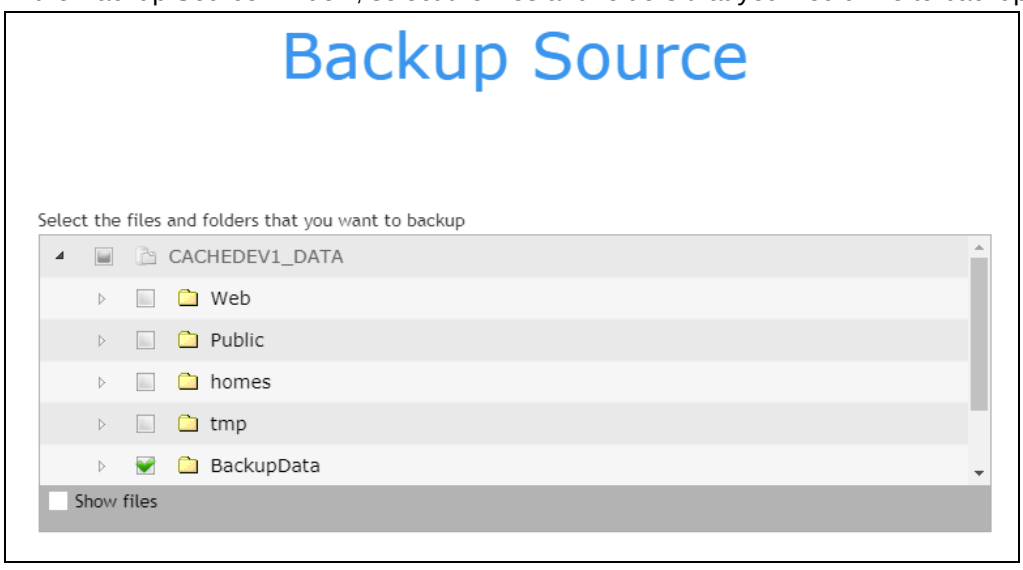
2. Create a backup set by clicking "**+ Add new backup set**".



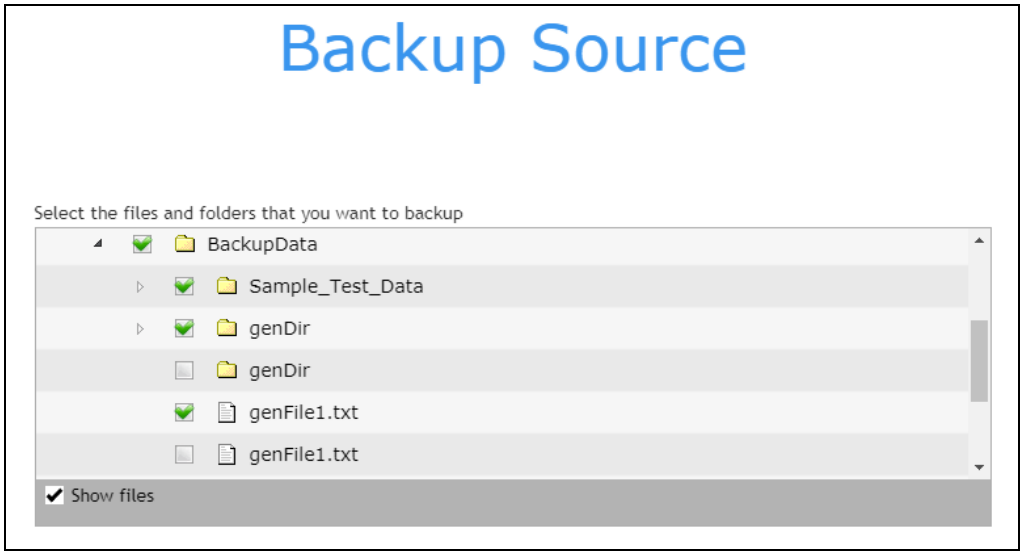
3. When the Create Backup Set window appears, name your new backup set, then click **Next** to proceed.



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



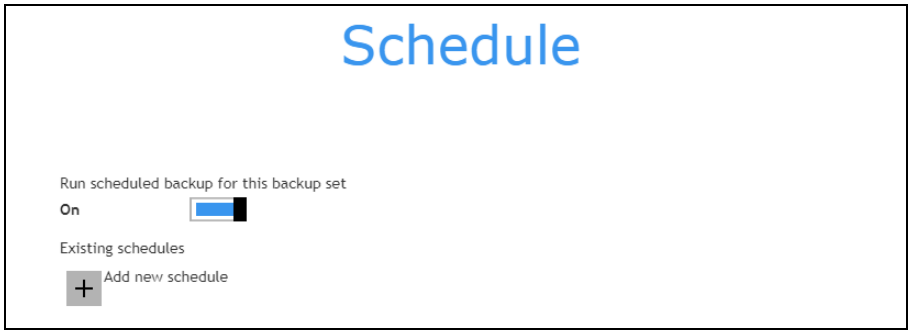
5. Click the **Show files** checkbox if you want to select individual file(s) for backup.



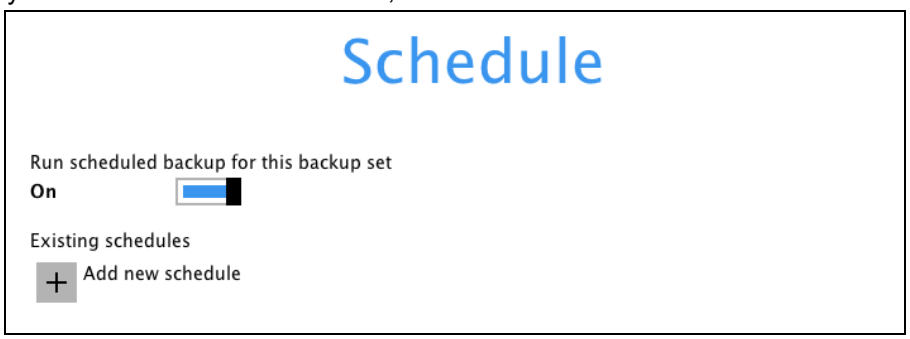
After selecting the backup source, click **Next** to proceed.

6. 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.

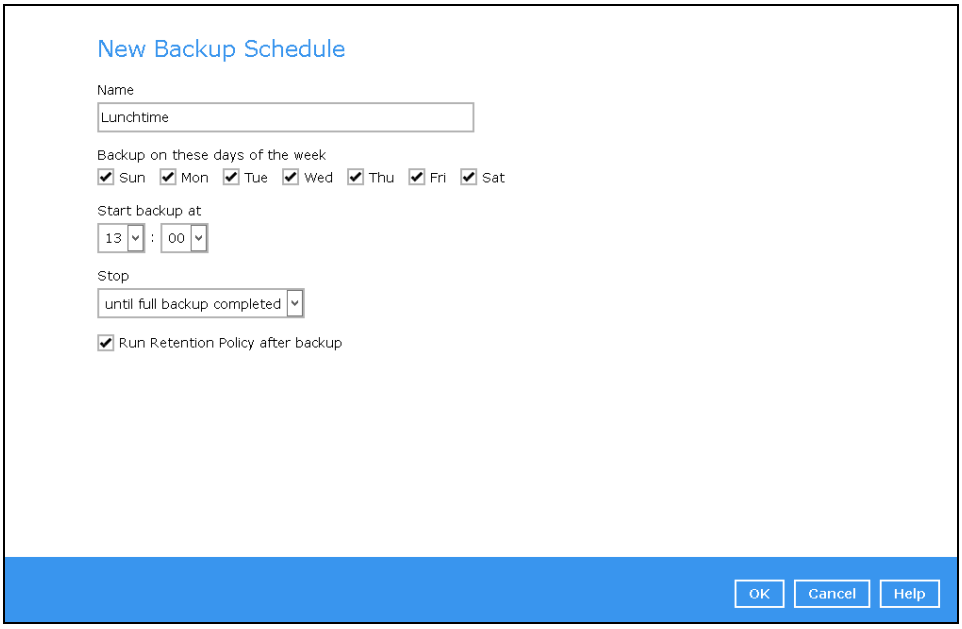
- You can leave it as is or you can turn it **Off** if you do not want to add a schedule again.



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

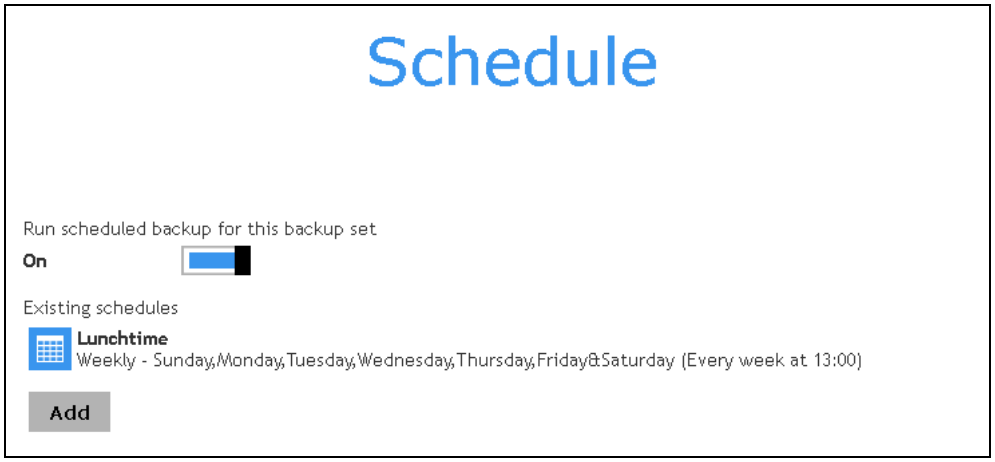


When the **New Backup Schedule** window appears, specify your backup schedule. Then, click **OK** to save your changes and close the New Backup Schedule window.



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

7. 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.



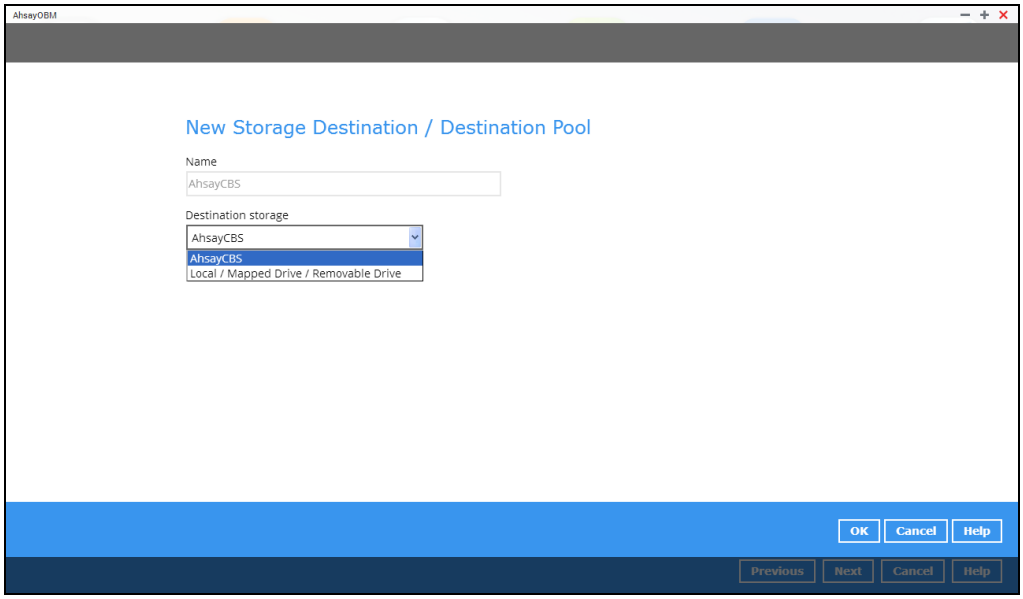
8. The Destination window will appear.

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

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

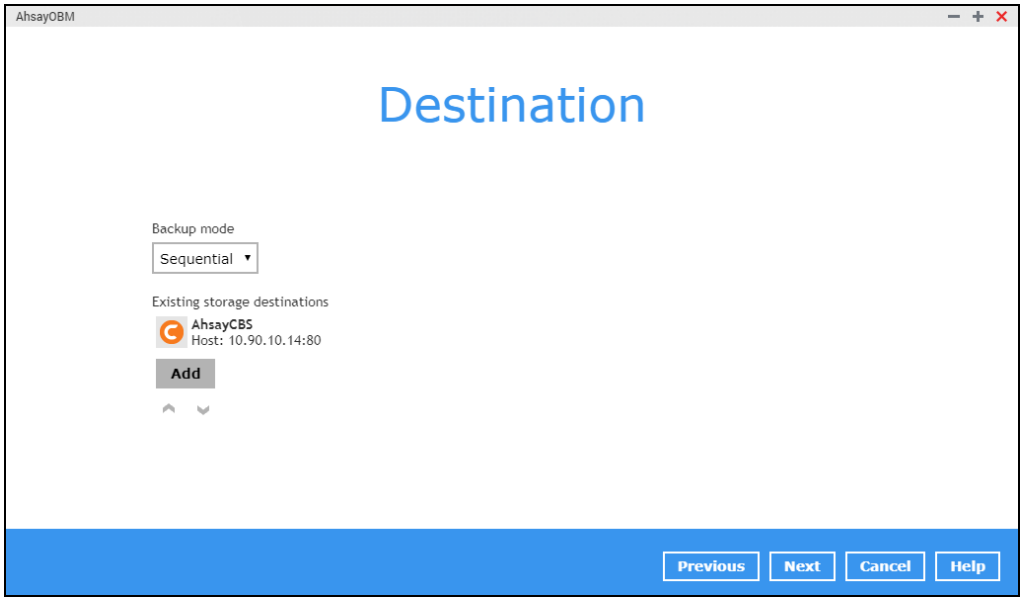
To select a backup destination for the backup data storage, click the "**+**" icon next to **Add new storage destination / destination pool**.

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

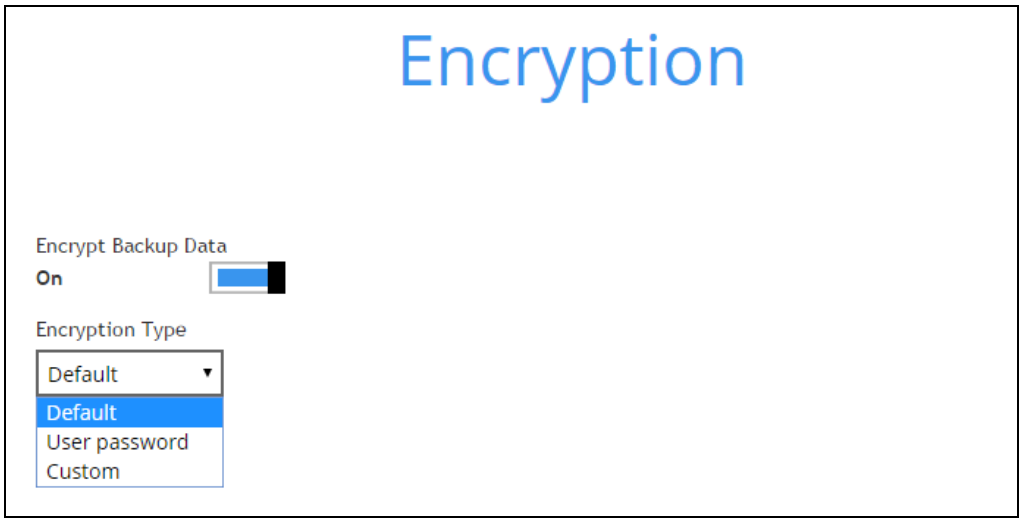


Note: *For more details on configuration of cloud storage as backup destination, refer to Appendix A in this guide.*

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



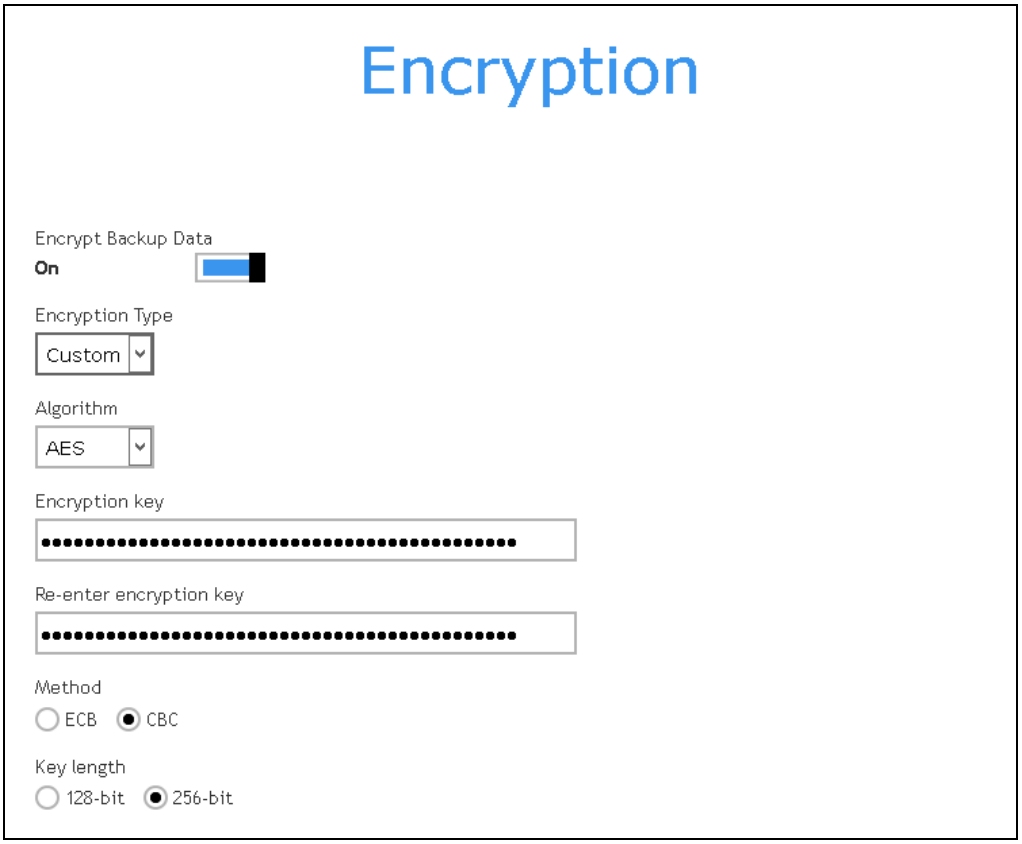
11. In the Encryption window, the default **Encrypt Backup Data** option is enabled with an encryption key preset by the system which provides the most secure protection.



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.

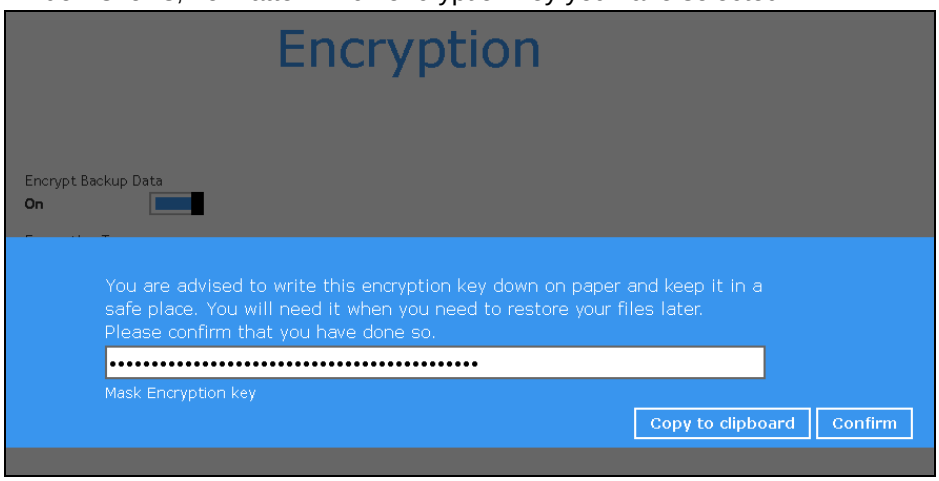
- **Custom** – you can customize your encryption key, where you can set your own algorithm, encryption key, method and key length.



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

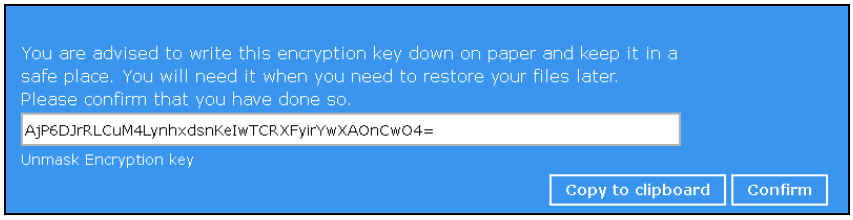
Click **Save** when you are done with the settings.

12. 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:

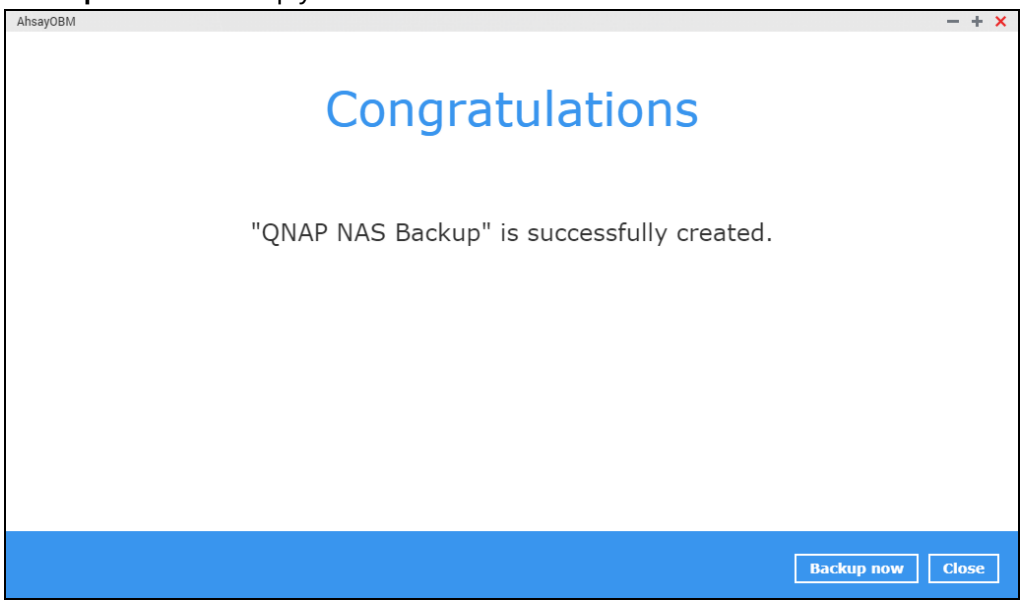
- **Unmask encryption key** – The encryption key is masked by default. Click this option to show the encryption key.



- **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.

13. 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 5)**
  - Completed Backup Job **(Step 12)**
- Data Validation Check Process **(Step 10)**

8.1 Periodic Data Integrity Check (PDIC) Process

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

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

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

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

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

NOTE: The PDIC schedule cannot be changed.

Example:

Backup set ID: 1594627447932

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

2	**Wednesday**

In this example:

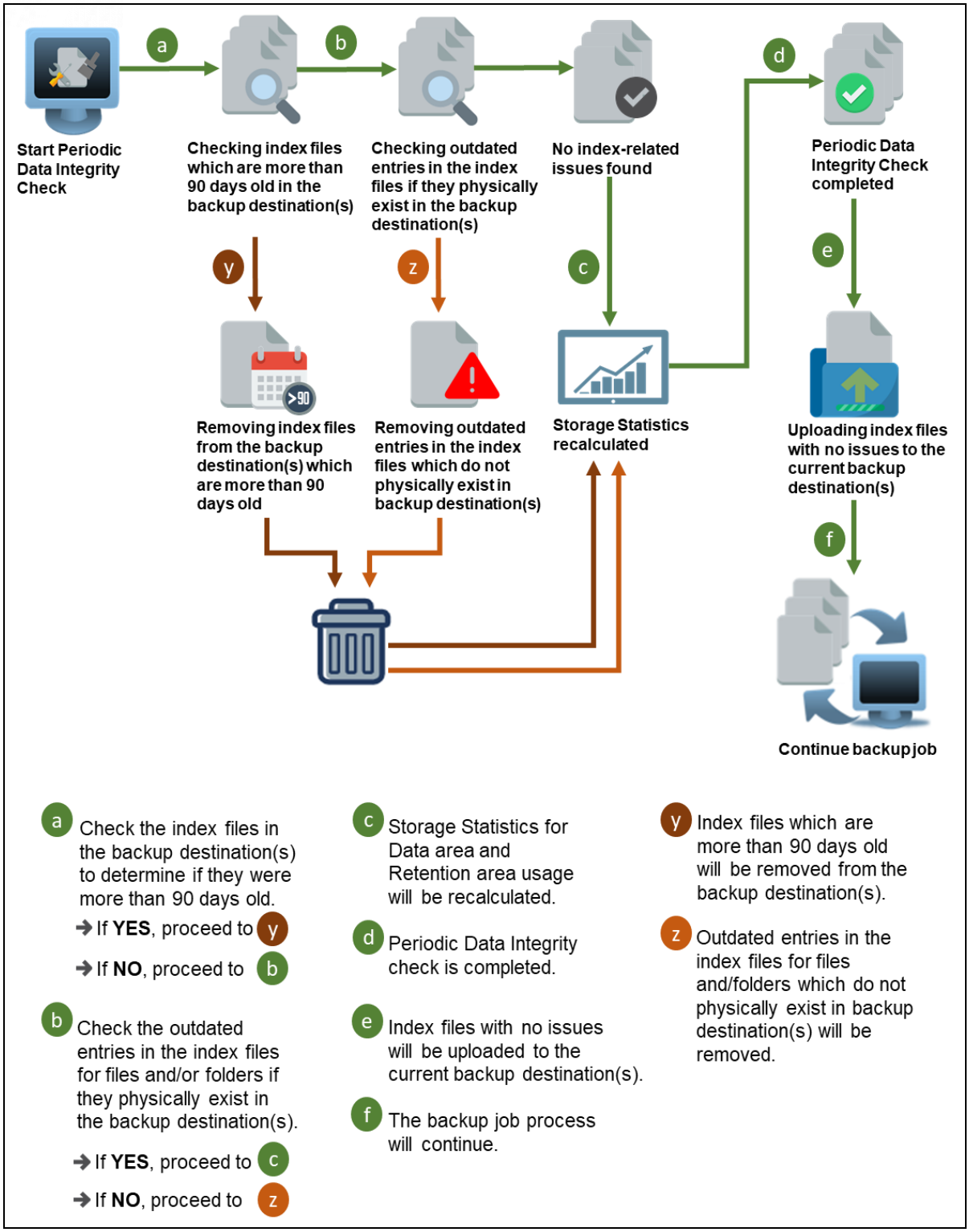
- the PDIC will run on the first backup job that falls on Wednesday; or
- if there is no active backup job(s) running from Monday to Friday, then the PDIC will run on the next available backup job.

NOTE

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

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

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



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.

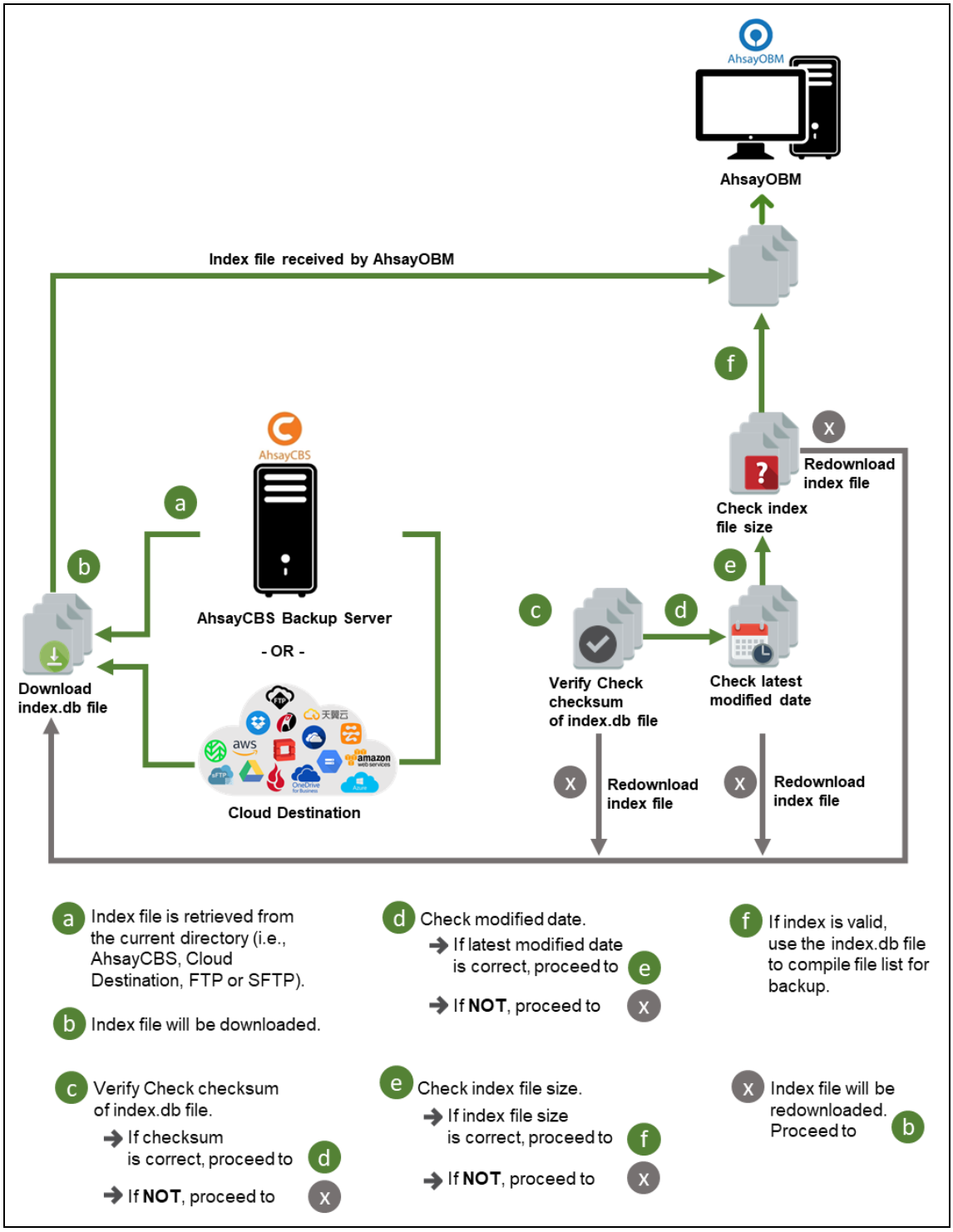
y Index files which are more than 90 days old will be removed from the backup destination(s).

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

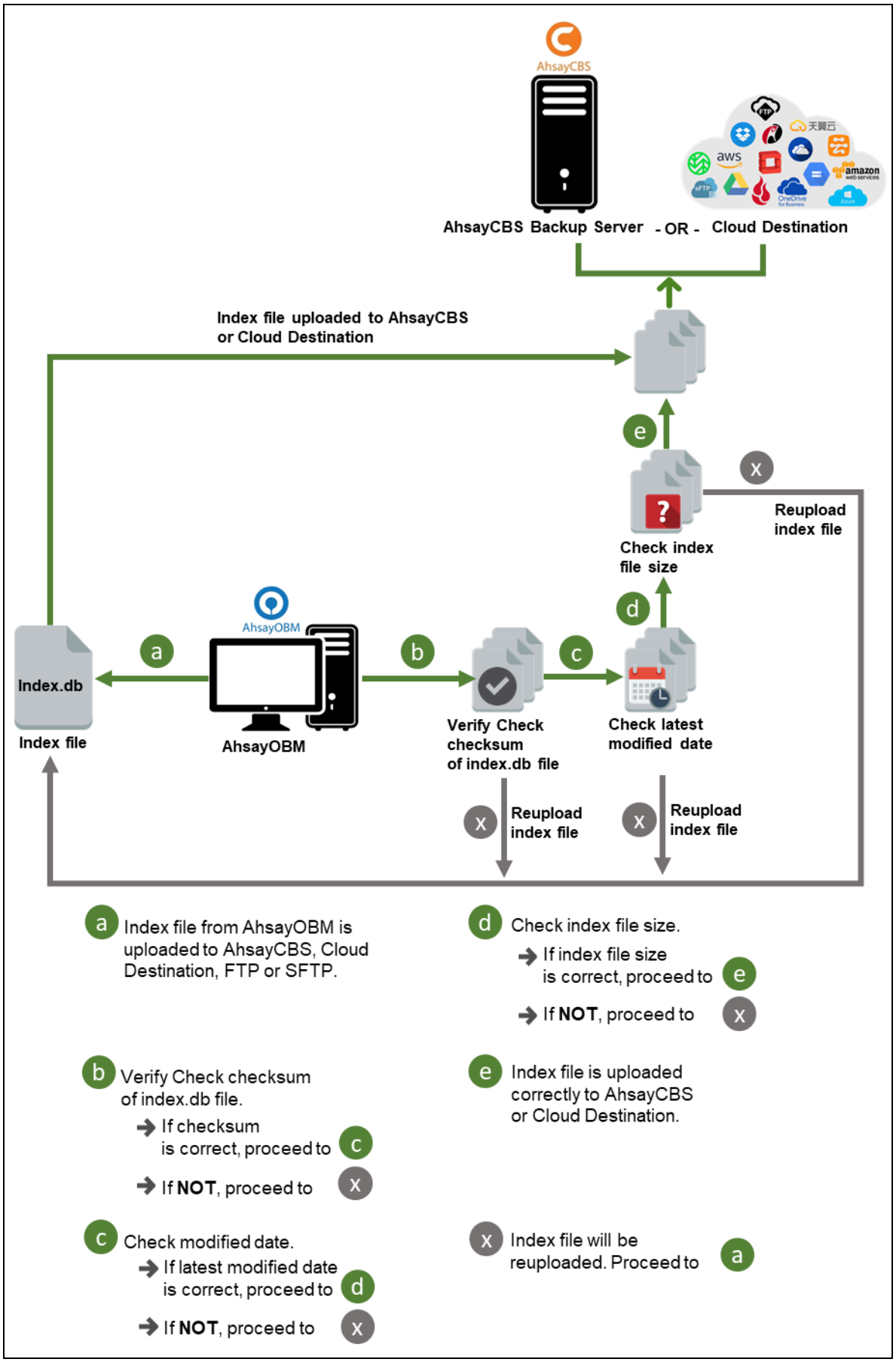
8.2 Backup Set Index Handling Process

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

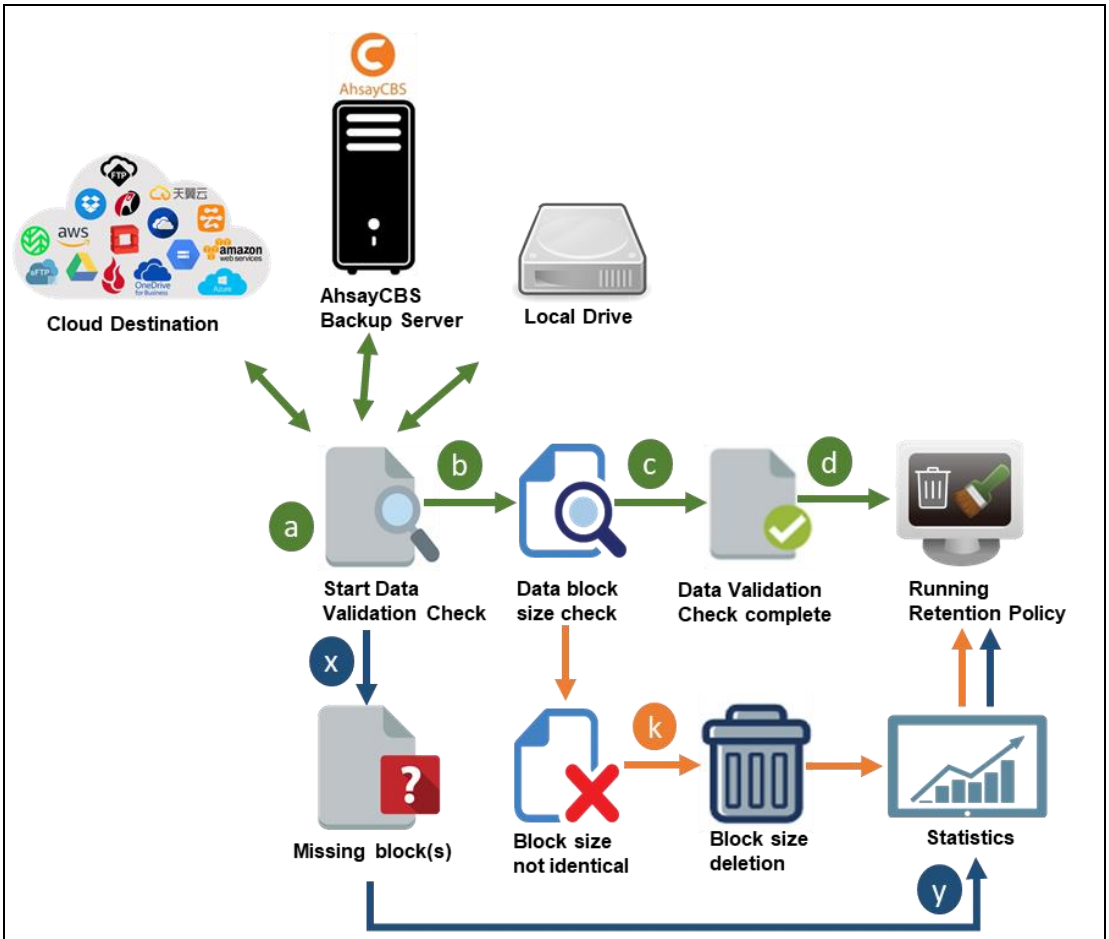


8.2.2 Completed Backup Job



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



a Check the number of 16 or 32 MB data blocks in the backup destination(s) is identical to the number of blocks transferred.

→ If YES, proceed to b

→ If NO, proceed to x

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

→ If YES, proceed to c

→ If NO, proceed to k

c Data validation check is complete.

d Retention policy will run (if enabled).

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

y Statistics will be updated according to the files removed.

Proceed to d

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

Proceed to y then

Proceed to d

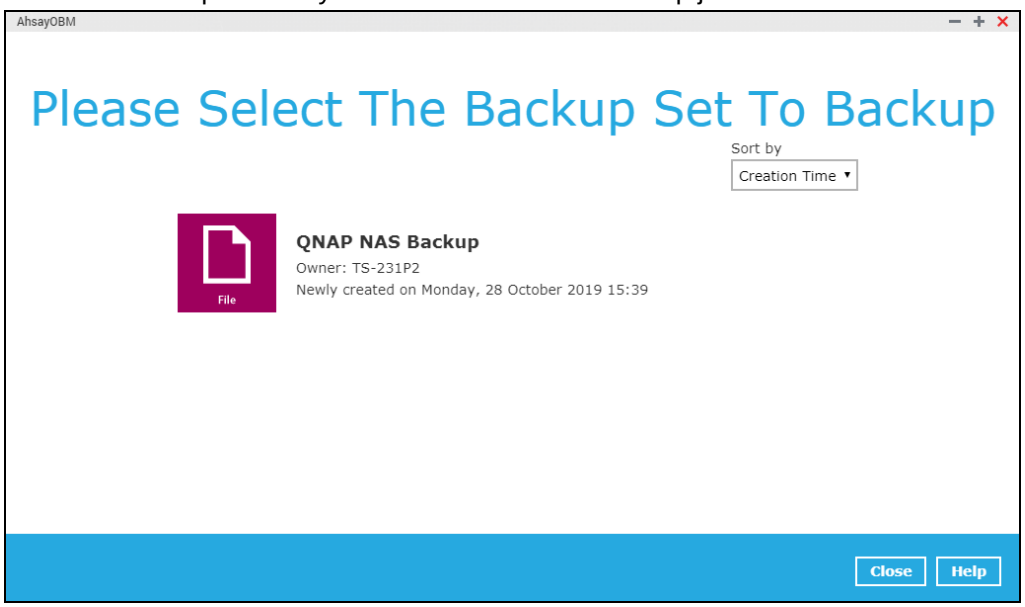
9 Run Backup Jobs

9.1 Start a Manual Backup

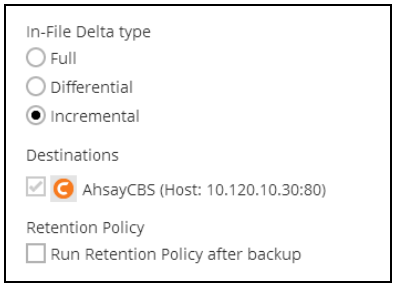
1. Login to the AhsayOBM application with the instructions provided in Login to AhsayOBM.

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

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

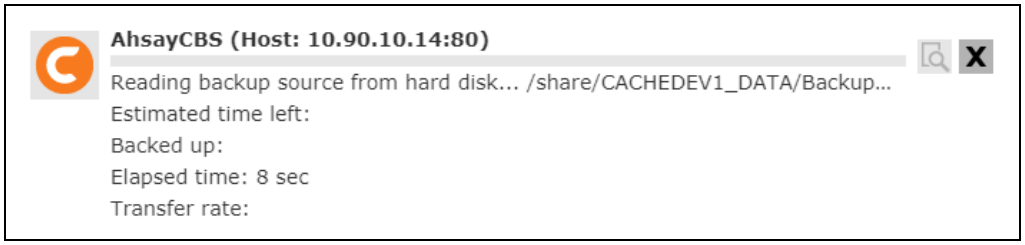


4. When the following options are shown, it is recommended that you tick the checkbox next to **Run Retention Policy after backup** in the Retention Policy section at the bottom. This will help you save hard disk quota in the long run. In the In-File Delta type section, the following three options are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

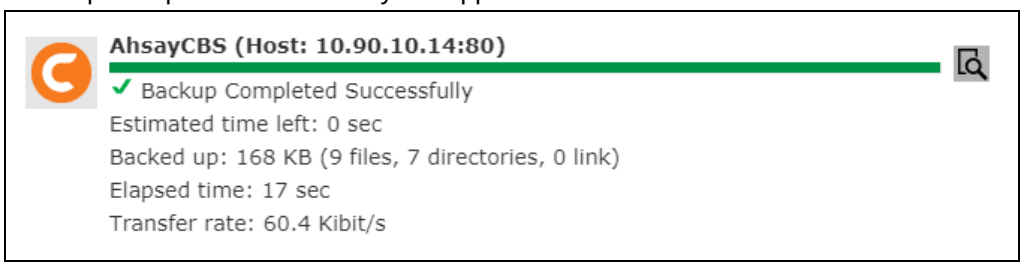


- **Full** – A full backup captures all the data that you want to protect. When you run a backup job for the first time, AhsayOBM will run a full backup regardless of the in-file delta setting.
- **Differential** – A differential backup captures only the changes made as compared with the last uploaded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

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.



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

Show All

Type	Log	Time
	Start [AhsayOBM v8.3.0.30]	28/10/2019 15:41:25
	Saving encrypted backup set encryption keys to server...	28/10/2019 15:41:25
	Start Backup ... [In-File Delta: Incremental]	28/10/2019 15:41:26
	Using Temporary Directory /share/CACHEDEV1_DATA/homes/admin/temp/1572248343679/OBS@1572248370655	28/10/2019 15:41:26
	Start running pre-commands	28/10/2019 15:41:30
	Finished running pre-commands	28/10/2019 15:41:30
	Downloading server file list...	28/10/2019 15:41:30
	Downloading server file list... Completed	28/10/2019 15:41:33
	Reading backup source from hard disk...	28/10/2019 15:41:34
	Reading backup source from hard disk... Completed	28/10/2019 15:41:34
	[New Directory]... /	28/10/2019 15:41:34
	[New Directory]... /share	28/10/2019 15:41:35
	[New Directory]... /share/CACHEDEV1_DATA	28/10/2019 15:41:35
	[New Directory]... /share/CACHEDEV1_DATA/BackupData	28/10/2019 15:41:35
	[New Directory]... /share/CACHEDEV1_DATA/BackupData/Sample_Test_Data	28/10/2019 15:41:35
	[New Directory]... /share/CACHEDEV1_DATA/BackupData/Sample_Test_Data/empty_files	28/10/2019 15:41:35
	[New Directory]... /share/CACHEDEV1_DATA/BackupData/Sample_Test_Data/empty_files/abc	28/10/2019 15:41:35
	[New File]... 100% of "/share/CACHEDEV1_DATA/BackupData/Sample_Test_Data/reinstall.ico"	28/10/2019 15:41:35
	[New File]... 100% of "/share/CACHEDEV1_DATA/BackupData/Sample_Test_Data/nsreg.dat"	28/10/2019 15:41:35
	[New File]... 100% of "/share/CACHEDEV1_DATA/BackupData/Sample_Test_Data/empty_files/0.test"	28/10/2019 15:41:35
	[New File]... 100% of "/share/CACHEDEV1_DATA/BackupData/Sample_Test_Data/empty_files/Copy (3) of empty.txt"	28/10/2019 15:41:35
	[New File]... 100% of "/share/CACHEDEV1_DATA/BackupData/Sample_Test_Data/empty_files/Copy (4) of empty.txt"	28/10/2019 15:41:35
	[New File]... 100% of "/share/CACHEDEV1_DATA/BackupData/Sample_Test_Data/empty_files/empty.txt"	28/10/2019 15:41:35
	[New File]... 100% of "/share/CACHEDEV1_DATA/BackupData/Sample_Test_Data/empty_files/Copy of empty.txt"	28/10/2019 15:41:35
	[New File]... 19% of "/share/CACHEDEV1_DATA/BackupData/Sample_Test_Data/empty_files/tail.exe"	28/10/2019 15:41:35
	[New File]... 34% of "/share/CACHEDEV1_DATA/BackupData/Sample_Test_Data/empty_files/tail.exe"	28/10/2019 15:41:35
	[New File]... 48% of "/share/CACHEDEV1_DATA/BackupData/Sample_Test_Data/empty_files/tail.exe"	28/10/2019 15:41:35
	[New File]... 63% of "/share/CACHEDEV1_DATA/BackupData/Sample_Test_Data/empty_files/tail.exe"	28/10/2019 15:41:35
	[New File]... 78% of "/share/CACHEDEV1_DATA/BackupData/Sample_Test_Data/empty_files/tail.exe"	28/10/2019 15:41:35
	[New File]... 92% of "/share/CACHEDEV1_DATA/BackupData/Sample_Test_Data/empty_files/tail.exe"	28/10/2019 15:41:35
	[New File]... 100% of "/share/CACHEDEV1_DATA/BackupData/Sample_Test_Data/empty_files/tail.exe"	28/10/2019 15:41:35
	[New File]... 100% of "/share/CACHEDEV1_DATA/BackupData/Sample_Test_Data/empty_files/abc/test.txt"	28/10/2019 15:41:35
	Start validating the presence and size of backup data in destination "AhsayCBS"...	28/10/2019 15:41:36
	File: "1572248343679/blocks/2019-10-28-15-41-07/0/000000.bak", Size: 171,648, OK	28/10/2019 15:41:36
	Finished validating the presence and size of backup data in destination "AhsayCBS"	28/10/2019 15:41:36
	Total New Files = 9	28/10/2019 15:41:36
	Total New Directories = 7	28/10/2019 15:41:36
	Total New Links = 0	28/10/2019 15:41:36
	Total Updated Files = 0	28/10/2019 15:41:36
	Total Attributes Changed Files = 0	28/10/2019 15:41:36
	Total Deleted Files = 0	28/10/2019 15:41:36
	Total Deleted Directories = 0	28/10/2019 15:41:36
	Total Deleted Links = 0	28/10/2019 15:41:36
	Total Moved Files = 0	28/10/2019 15:41:36
	Start running retention policy on backup set "QNAP NAS Backup(1572248343679)", "AhsayCBS(1572248370655)"	28/10/2019 15:41:36
	Start processing space freeing up on backup set= "QNAP NAS Backup (1572248343679)" destination= "AhsayCBS (1572248370655)"	28/10/2019 15:41:36
	Space freeing up on backup set= "QNAP NAS Backup (1572248343679)" destination= "AhsayCBS (1572248370655)" is completed	28/10/2019 15:41:36
	Finished running retention policy on backup set "QNAP NAS Backup(1572248343679)", "AhsayCBS(1572248370655)"	28/10/2019 15:41:36
	Saving encrypted backup file index to 1572248343679/blocks at destination AhsayCBS...	28/10/2019 15:41:37
	Saving encrypted backup file index to 1572248343679/blocks/2019-10-28-15-41-07 at destination AhsayCBS...	28/10/2019 15:41:37
	Start running post-commands	28/10/2019 15:41:39
	Finished running post-commands	28/10/2019 15:41:39
	Deleting temporary file /share/CACHEDEV1_DATA/homes/admin/temp/1572248343679/OBS@1572248370655	28/10/2019 15:41:42
	Backup Completed Successfully	28/10/2019 15:41:43

Logs per page 100 Previous 1 Next

10 Restore Data

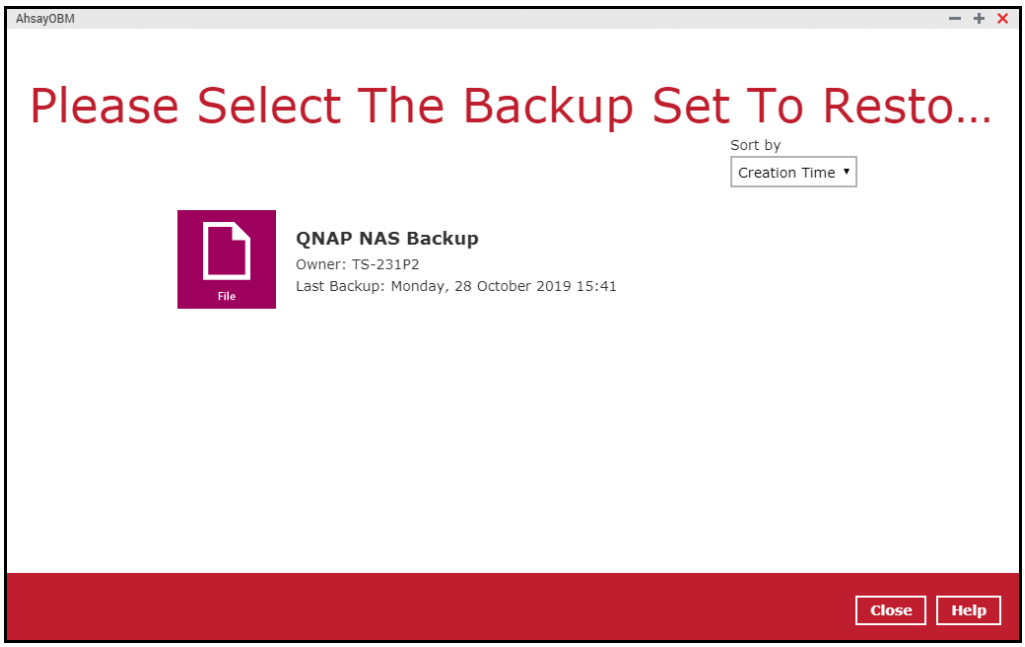
10.1 Login to AhsayOBM

Login to the AhsayOBM application with the instructions provided in Login to AhsayOBM.

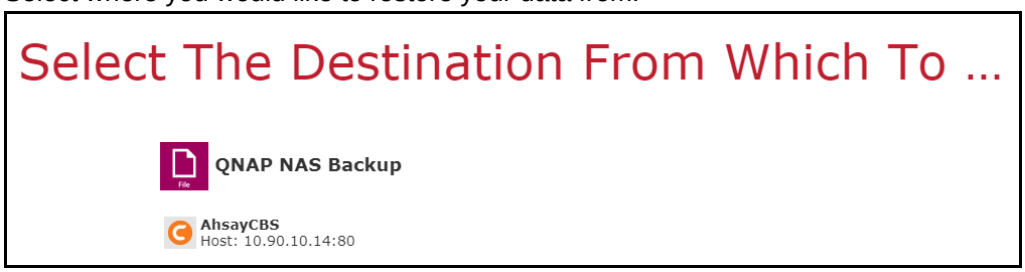
10.2 Restore Data

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

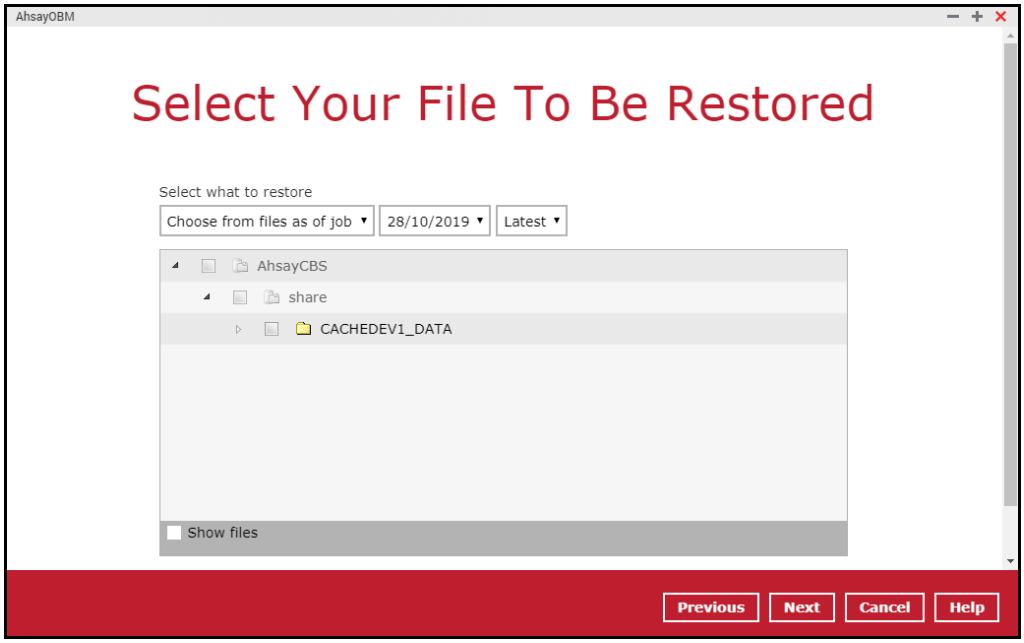
2. All the available backup sets for restore will be listed. Select the backup set that you would like to restore the data from.



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.

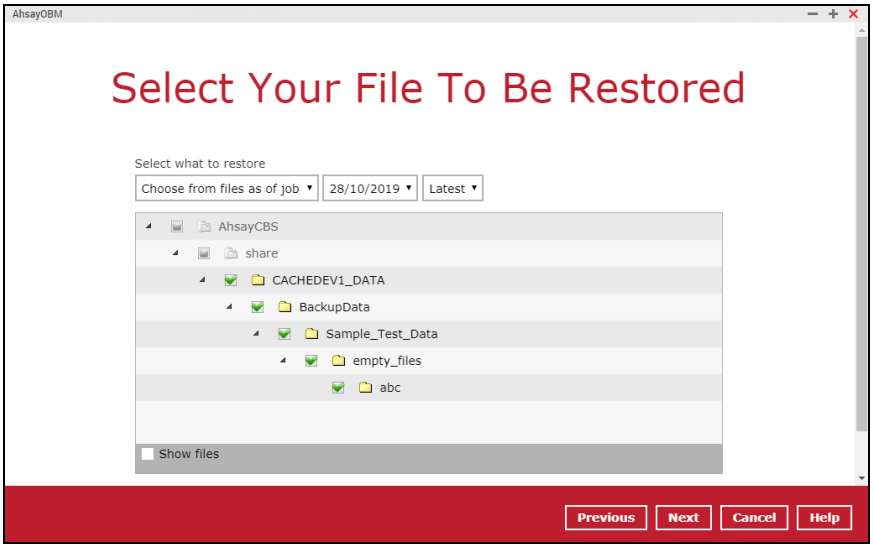


There are two options from the **Select what to restore** drop-down menu:

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

- 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

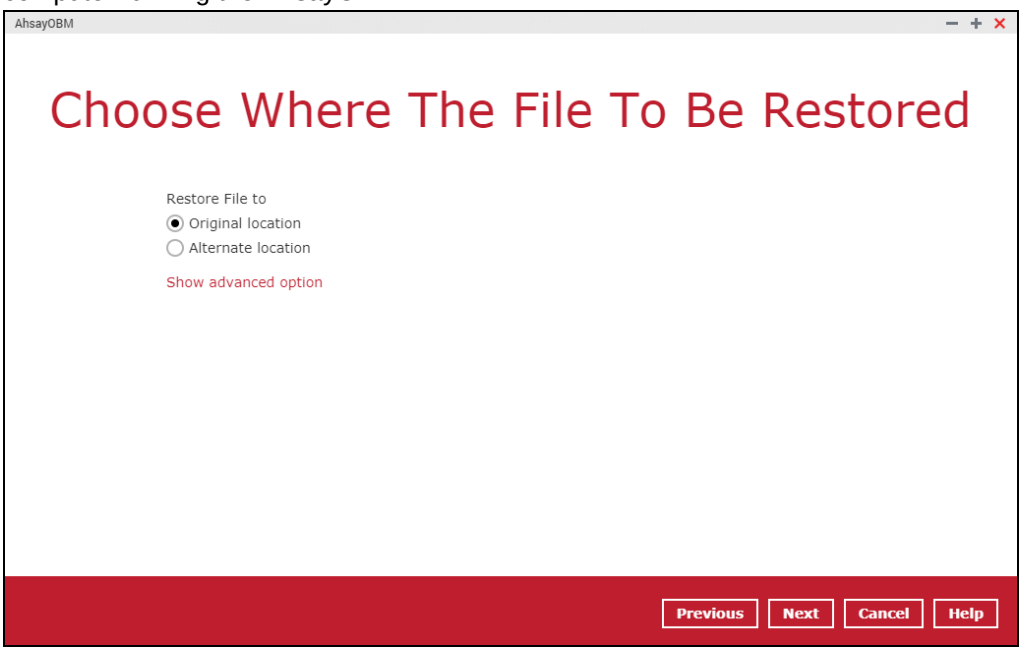
even select only some of the backup files or folders to restore.



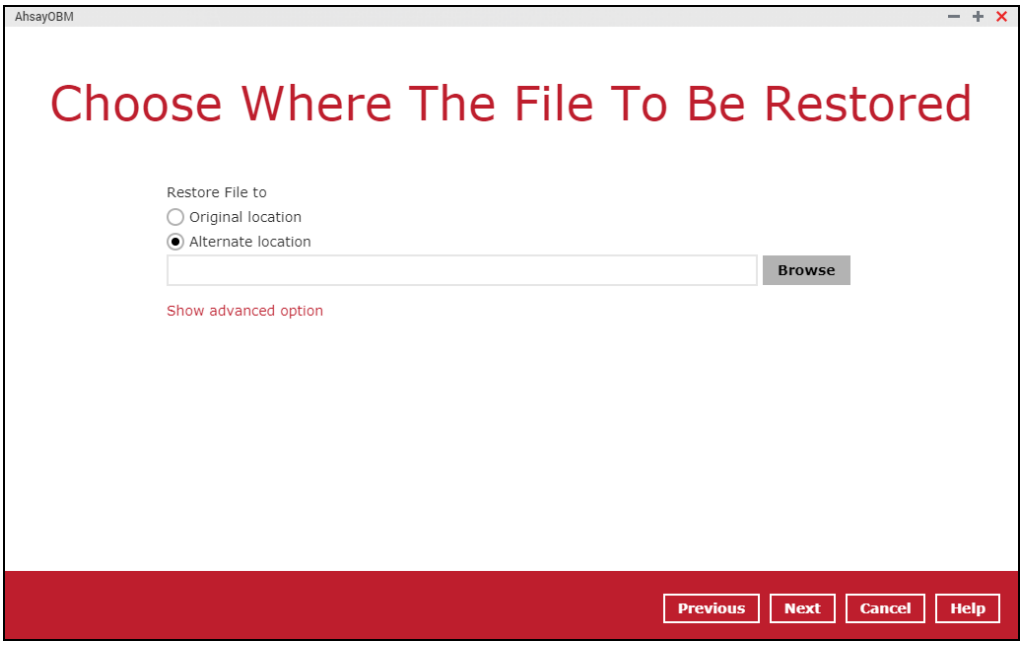
5. Click the **Show files** checkbox to select individual files for restoration. Click **Next** to proceed when you are done with the selections.

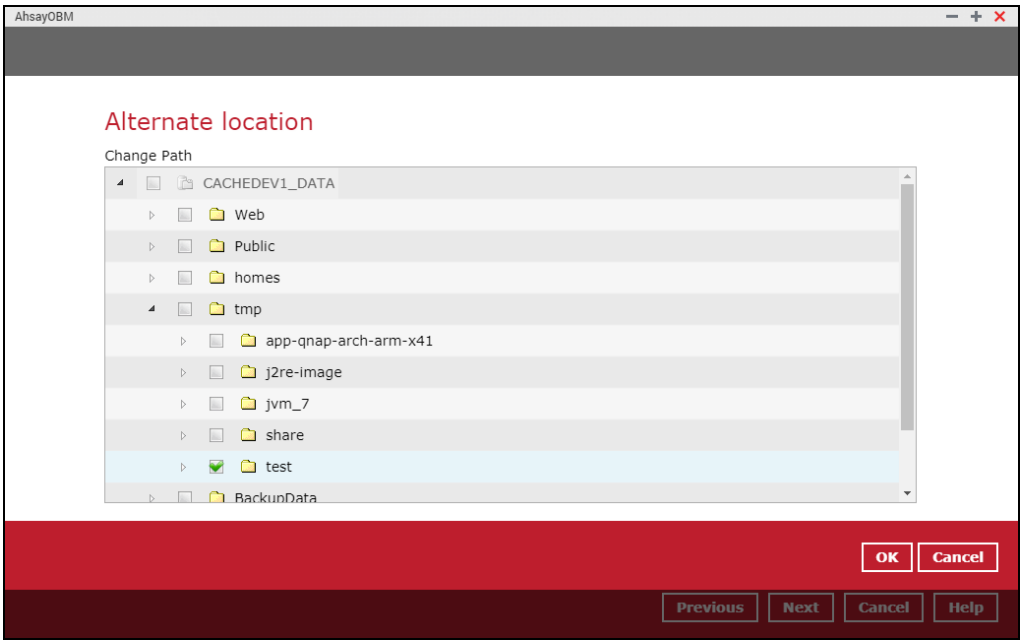
6. Select to restore the files to their **Original location**, or to an **Alternate location**. Then click **Next** to proceed.

   - **Original location** – the backed up data will be restored to the computer running the AhsayOBM under the same directory path as on the machine storing the backup source. For example, if the backup source files are stored under **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.

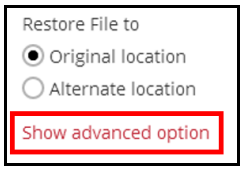


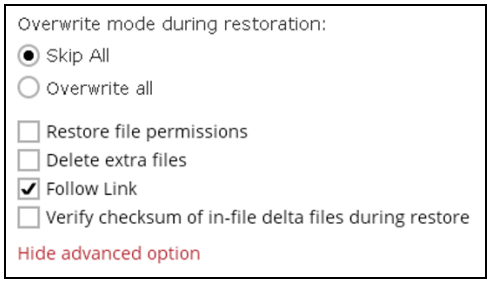
- **Alternate location** – you can choose to restore the data to a location of your choice on the computer where AhsayOBM is running.





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





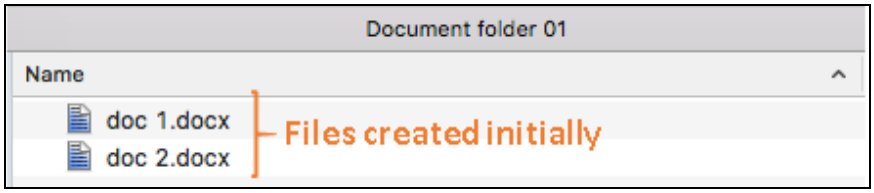
- **Overwrite mode during restoration**
  When there are file name conflicts during restoration, you can choose to skip them all or overwrite all existing files in the restore destination.

- **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.

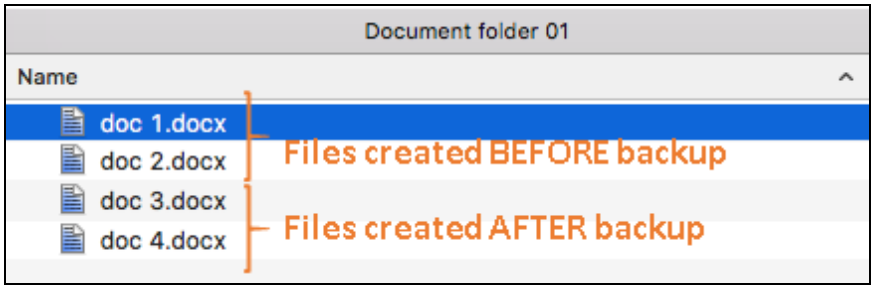
- **Delete extra files**
  Synchronize the selected restore source with the restore destination.
  By enabling this option, the restore process will attempt to synchronize the selected restore source with the restore destination, making sure the data in the restore destination is exactly the same as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

  Example:

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

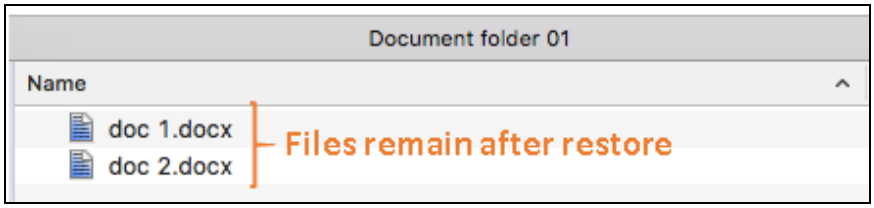


  - A backup is performed for folder Document folder 01.
  - Two new files are created, namely doc 3 & doc 4.



  - A restore is performed for the Document folder 01, with Delete extra files 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 is deleted.

Prior to the data restore and synchronization, a warning message shows as the one shown below. Only clicking **Yes** will the "extra file" be deleted. You can click **Apply to all** to confirm deleting all the "extra files" at a time.

- **Follow Link (Enabled by default)**
  When this option is enabled, not only the symbolic link or junction point will be restored, the directories and files that the symbolic link or junction point links to will also be restored.

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

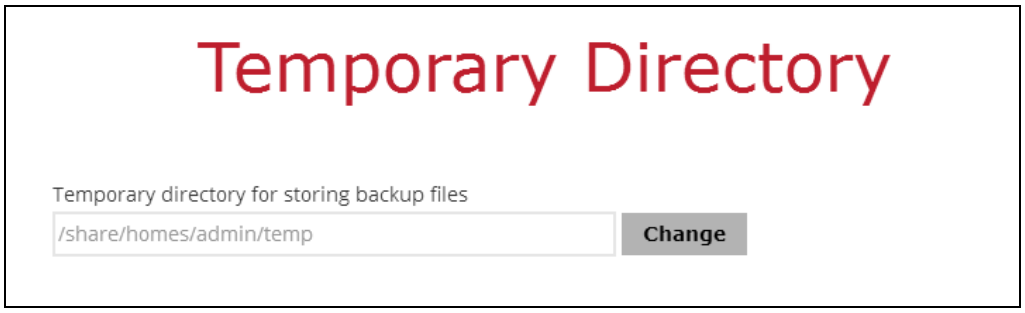
Follow Link	Restore to	Behavior
Enabled	**Original location**	Symbolic link or junction point is restored to the original backup location. Target directories or files are also restored to the original backup location.
	Alternate location	Symbolic link or junction point is restored to the location specified.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

- **Verify checksum of in-file delta files during restore**
  Verify checksum of in-file delta files during restore is disabled by default. You can enable the feature by ticking the checkbox so that the checksum of in-file delta files will be verified.

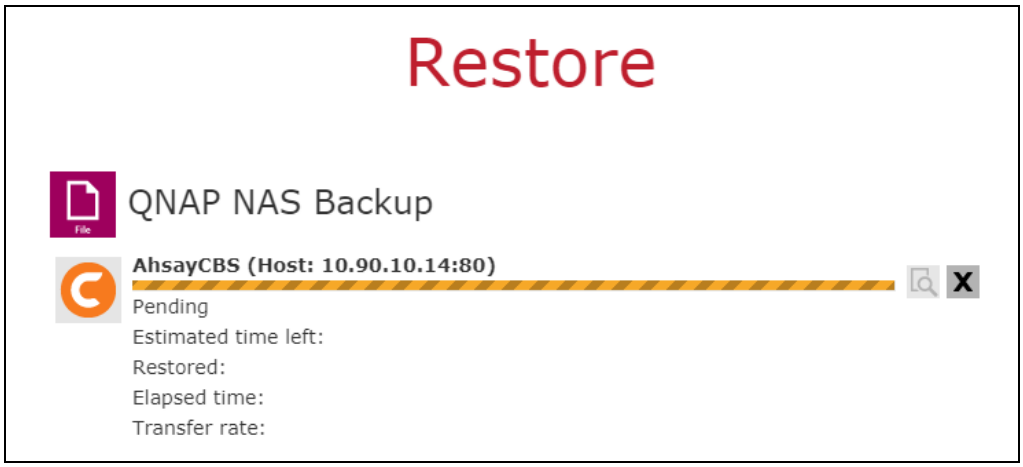
As the feature will make the restore process time longer, it is recommended to enable the feature only if you want to verify whether the merged file were correct.

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

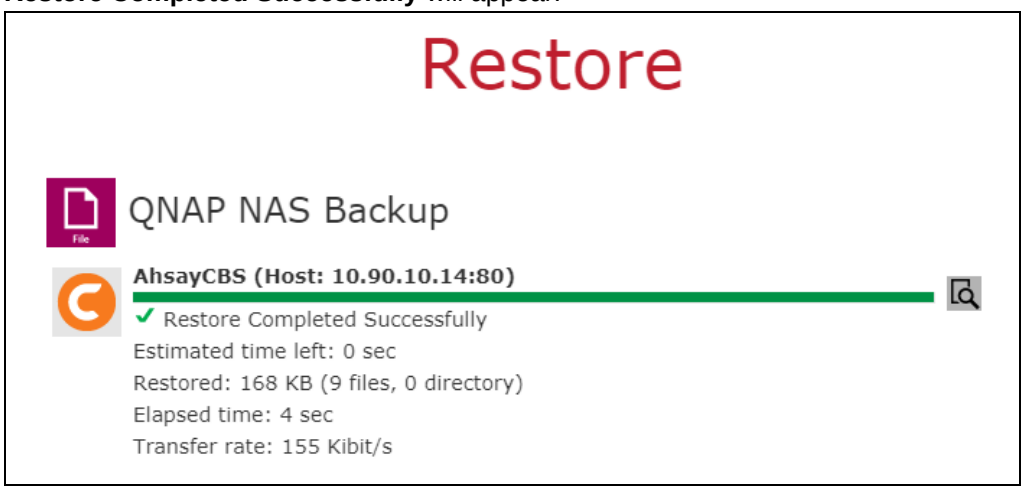
9. Select the temporary directory for storing temporary files, such as delta files when they are being merged.



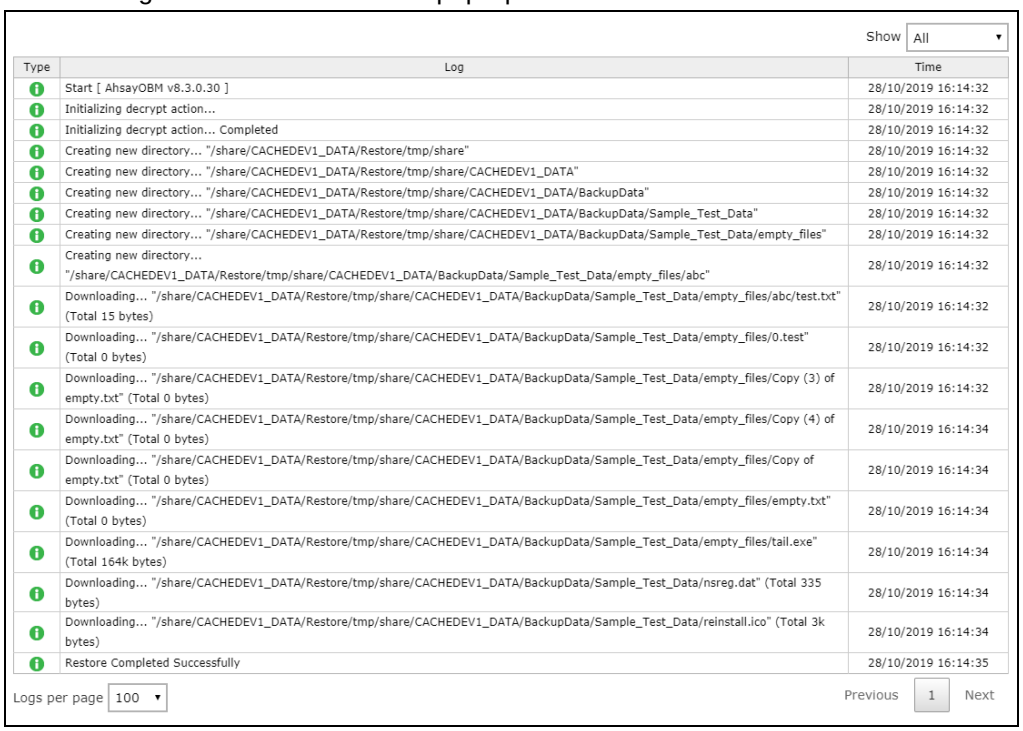
10. Click **Restore** to start the restore. The status will be shown.



11. 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.



Show All

Type	Log	Time
ⓘ	Start [AhsayOBM v8.3.0.30]	28/10/2019 16:14:32
ⓘ	Initializing decrypt action...	28/10/2019 16:14:32
ⓘ	Initializing decrypt action... Completed	28/10/2019 16:14:32
ⓘ	Creating new directory... "/share/CACHEDEV1_DATA/Restore/tmp/share"	28/10/2019 16:14:32
ⓘ	Creating new directory... "/share/CACHEDEV1_DATA/Restore/tmp/share/CACHEDEV1_DATA"	28/10/2019 16:14:32
ⓘ	Creating new directory... "/share/CACHEDEV1_DATA/Restore/tmp/share/CACHEDEV1_DATA/BackupData"	28/10/2019 16:14:32
ⓘ	Creating new directory... "/share/CACHEDEV1_DATA/Restore/tmp/share/CACHEDEV1_DATA/BackupData/Sample_Test_Data"	28/10/2019 16:14:32
ⓘ	Creating new directory... "/share/CACHEDEV1_DATA/Restore/tmp/share/CACHEDEV1_DATA/BackupData/Sample_Test_Data/empty_files"	28/10/2019 16:14:32
ⓘ	Creating new directory... "/share/CACHEDEV1_DATA/Restore/tmp/share/CACHEDEV1_DATA/BackupData/Sample_Test_Data/empty_files/abc"	28/10/2019 16:14:32
ⓘ	Downloading... "/share/CACHEDEV1_DATA/Restore/tmp/share/CACHEDEV1_DATA/BackupData/Sample_Test_Data/empty_files/abc/test.txt" (Total 15 bytes)	28/10/2019 16:14:32
ⓘ	Downloading... "/share/CACHEDEV1_DATA/Restore/tmp/share/CACHEDEV1_DATA/BackupData/Sample_Test_Data/empty_files/0.test" (Total 0 bytes)	28/10/2019 16:14:32
ⓘ	Downloading... "/share/CACHEDEV1_DATA/Restore/tmp/share/CACHEDEV1_DATA/BackupData/Sample_Test_Data/empty_files/Copy (3) of empty.txt" (Total 0 bytes)	28/10/2019 16:14:32
ⓘ	Downloading... "/share/CACHEDEV1_DATA/Restore/tmp/share/CACHEDEV1_DATA/BackupData/Sample_Test_Data/empty_files/Copy (4) of empty.txt" (Total 0 bytes)	28/10/2019 16:14:34
ⓘ	Downloading... "/share/CACHEDEV1_DATA/Restore/tmp/share/CACHEDEV1_DATA/BackupData/Sample_Test_Data/empty_files/Copy of empty.txt" (Total 0 bytes)	28/10/2019 16:14:34
ⓘ	Downloading... "/share/CACHEDEV1_DATA/Restore/tmp/share/CACHEDEV1_DATA/BackupData/Sample_Test_Data/empty_files/empty.txt" (Total 0 bytes)	28/10/2019 16:14:34
ⓘ	Downloading... "/share/CACHEDEV1_DATA/Restore/tmp/share/CACHEDEV1_DATA/BackupData/Sample_Test_Data/empty_files/tail.exe" (Total 164k bytes)	28/10/2019 16:14:34
ⓘ	Downloading... "/share/CACHEDEV1_DATA/Restore/tmp/share/CACHEDEV1_DATA/BackupData/Sample_Test_Data/nsreg.dat" (Total 335 bytes)	28/10/2019 16:14:34
ⓘ	Downloading... "/share/CACHEDEV1_DATA/Restore/tmp/share/CACHEDEV1_DATA/BackupData/Sample_Test_Data/reinstall.ico" (Total 3k bytes)	28/10/2019 16:14:34
ⓘ	Restore Completed Successfully	28/10/2019 16:14:35

Logs per page 100 Previous 1 Next

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

13. To exit AhsayOBM, click the red “x” on the top right corner. If you wish to use the AhsayOBM again, you will then have to launch it again.

11 Contact Ahsay

11.1 Technical Assistance

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

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

11.2 Documentation

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

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

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

Appendix

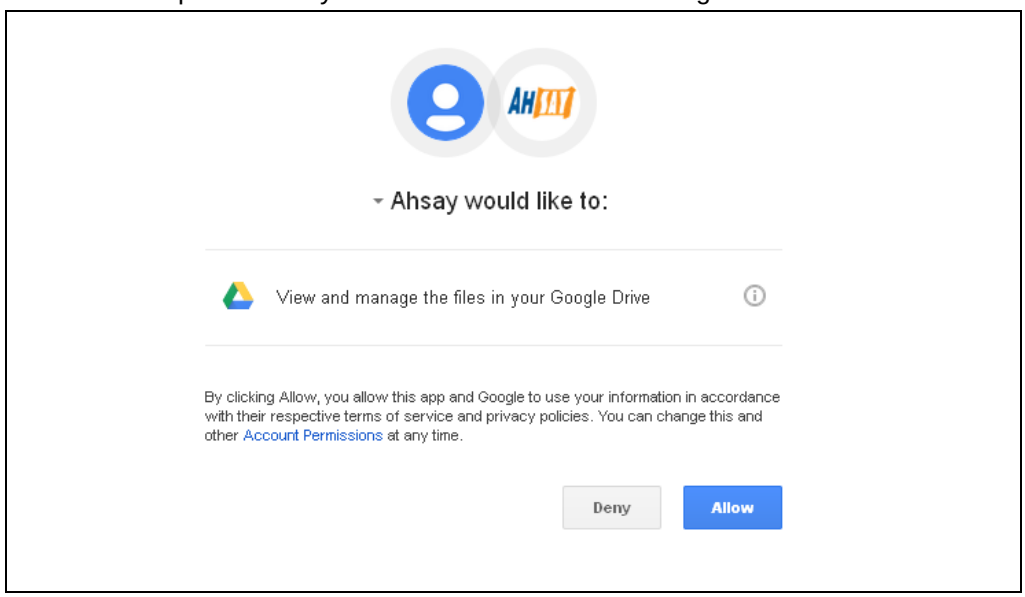
Appendix A: Cloud Storage as Backup Destination

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

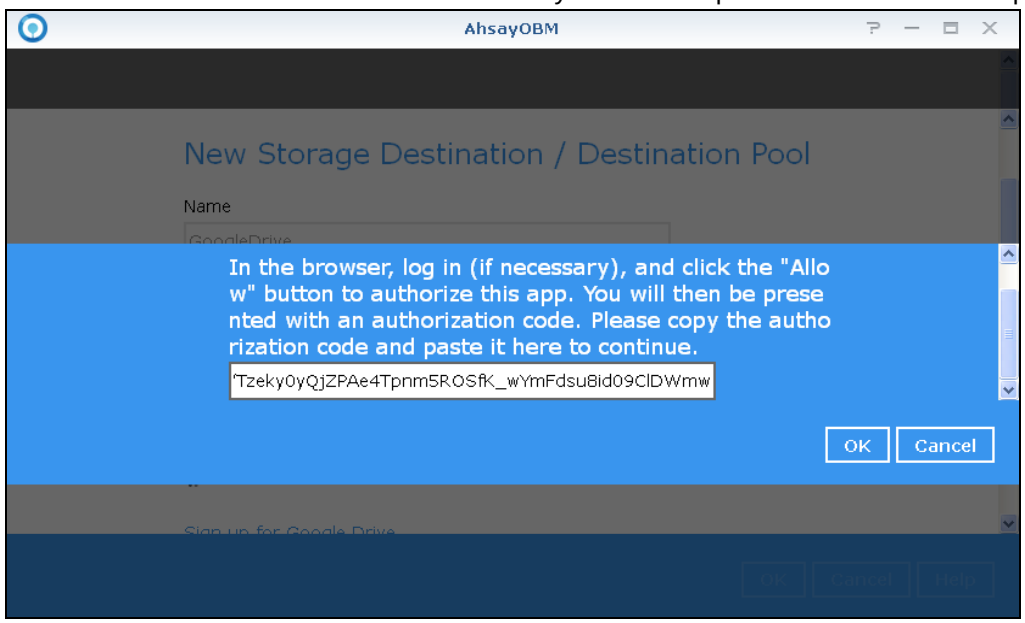
IMPORTANT

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

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.

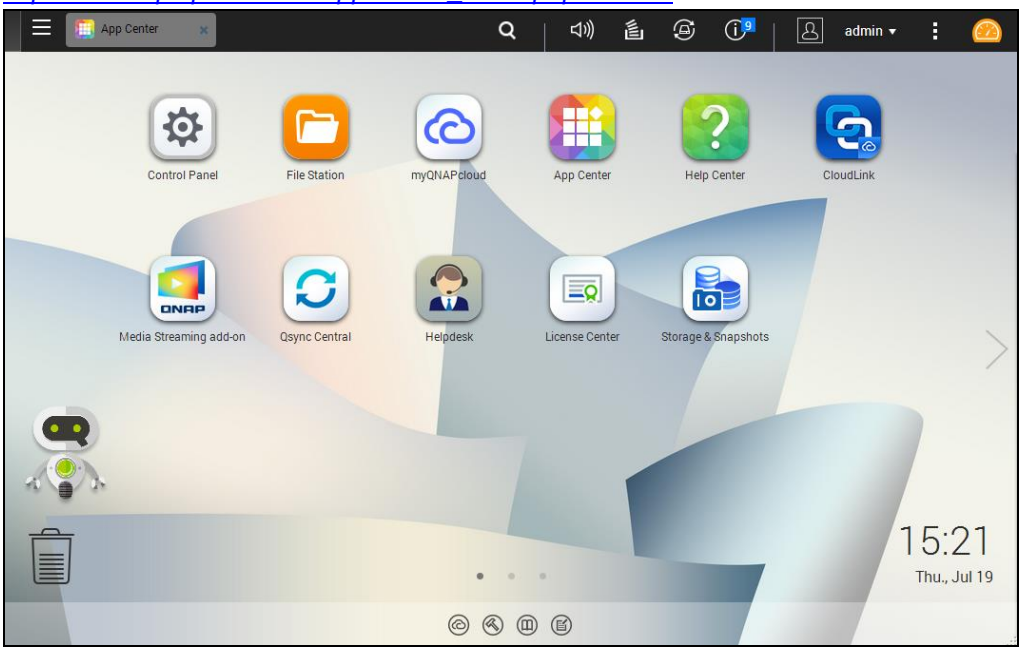
For more details on backup destination, for example which cloud service providers are supported, destination type, or limitation, you can refer to the following article:
http://wiki.ahsay.com/doku.php?id=public:8002_faq:faq_on_backup_destination

Appendix B: Uninstall AhsayOBM

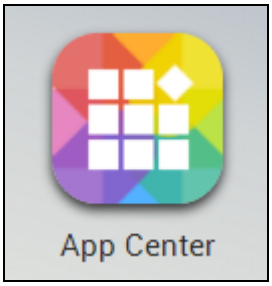
Refer to the following steps to uninstall AhsayOBM.

1. 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*

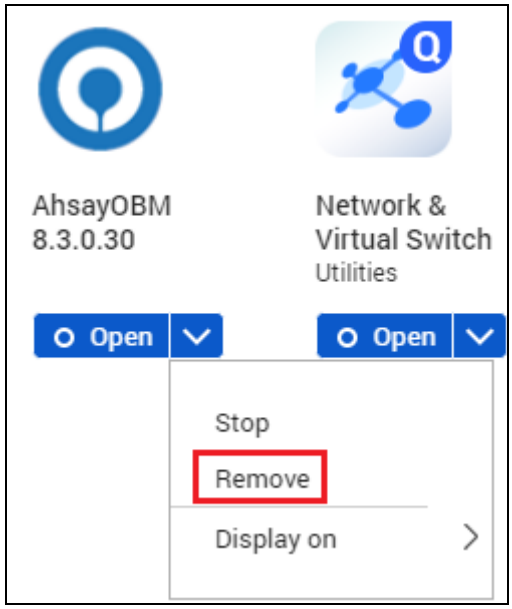


2. Click the App Center icon on the desktop.

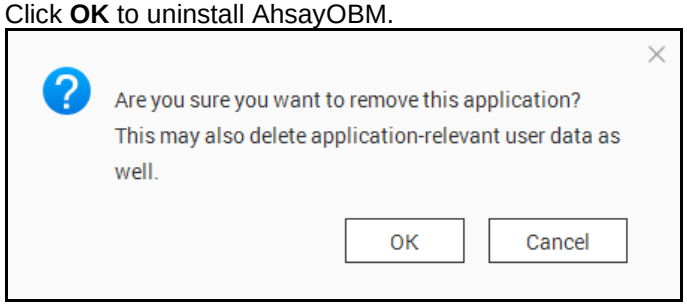


3. When the App Center window appears, click the arrow icon of AhsayOBM.

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

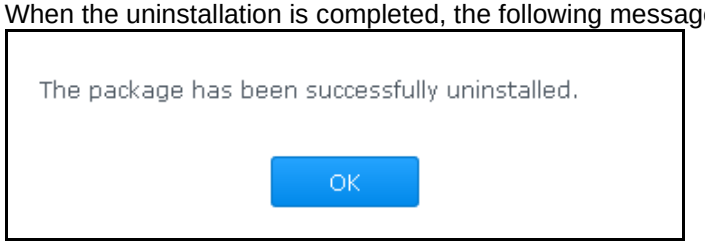


5. Click **OK** to uninstall AhsayOBM.



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

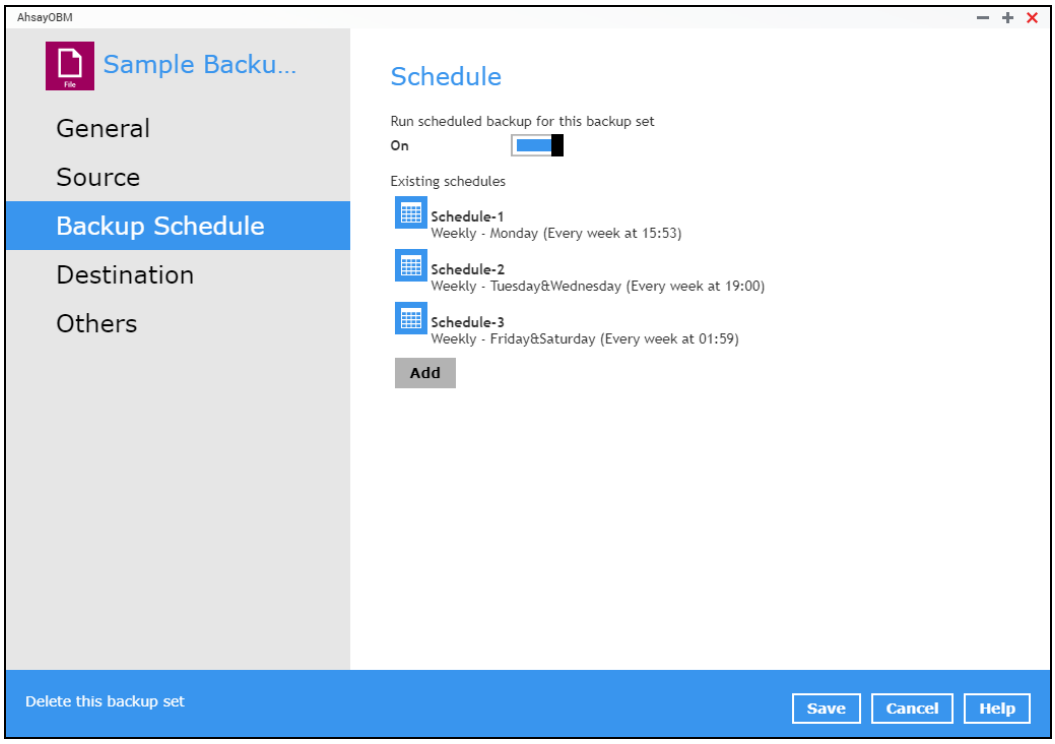
6. When the uninstallation is completed, the following message will appear.



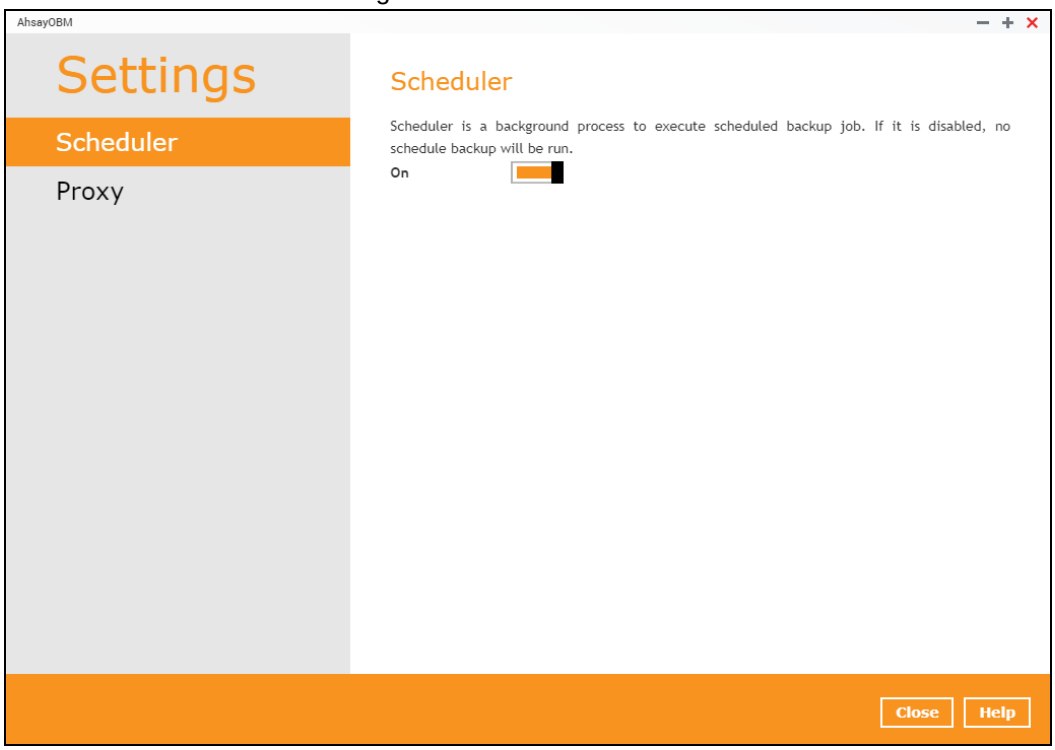
Appendix C: Scheduler Scenarios

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

Level 1: Scheduler under Backup Set Settings

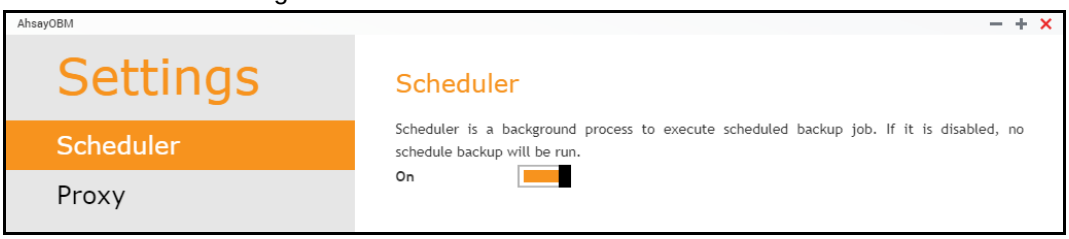


Level 2: Scheduler under Settings

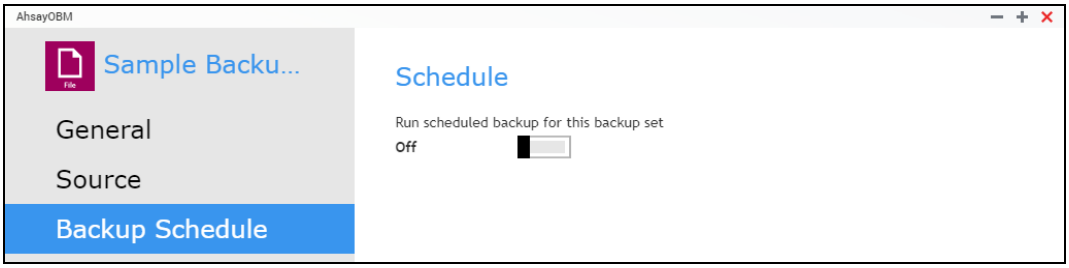


Scenario no. 1: Scheduler under Setting is ON and Scheduler under Backup Set Settings is OFF

Scheduler under Setting



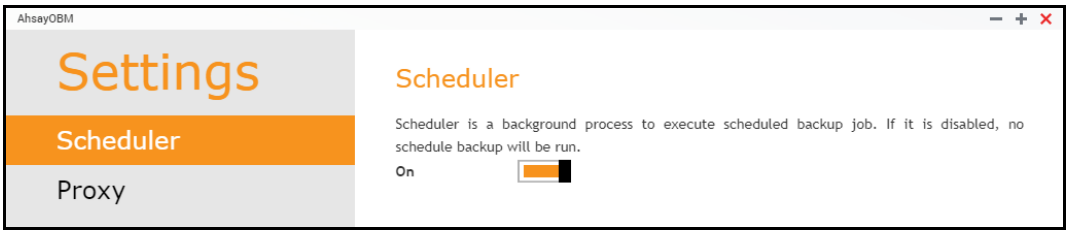
Scheduler under Backup Set Settings



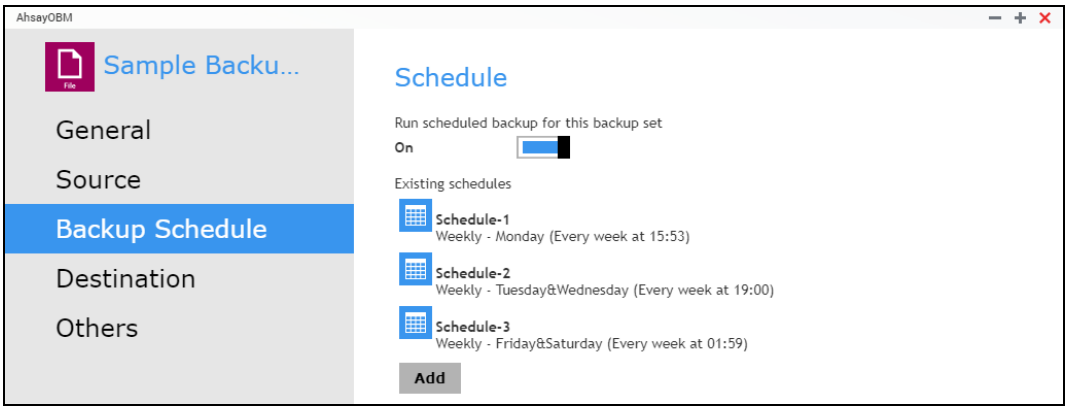
Result: There is no scheduled backup job will be run for the backup set.

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

Scheduler under Setting



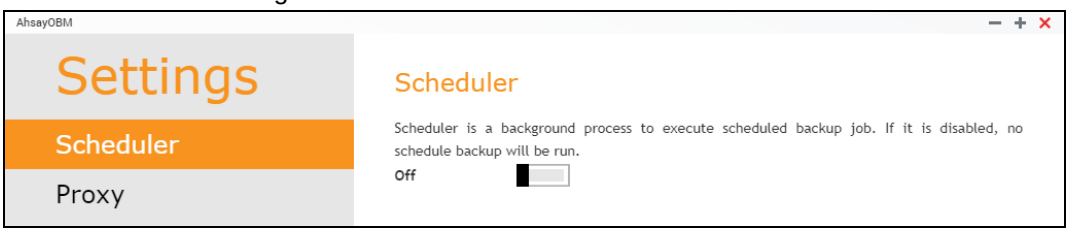
Scheduler under Backup Set Settings



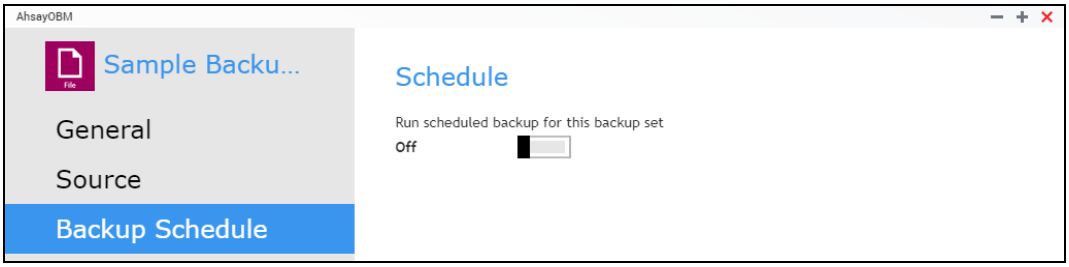
Result: Scheduled backup jobs which are Schedule-1, Schedule-2, and Schedule-3 for the backup set will run.

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

Scheduler under Setting



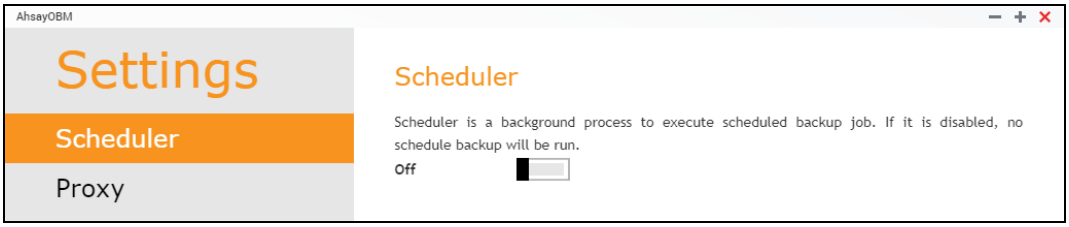
Scheduler under Backup Set Settings



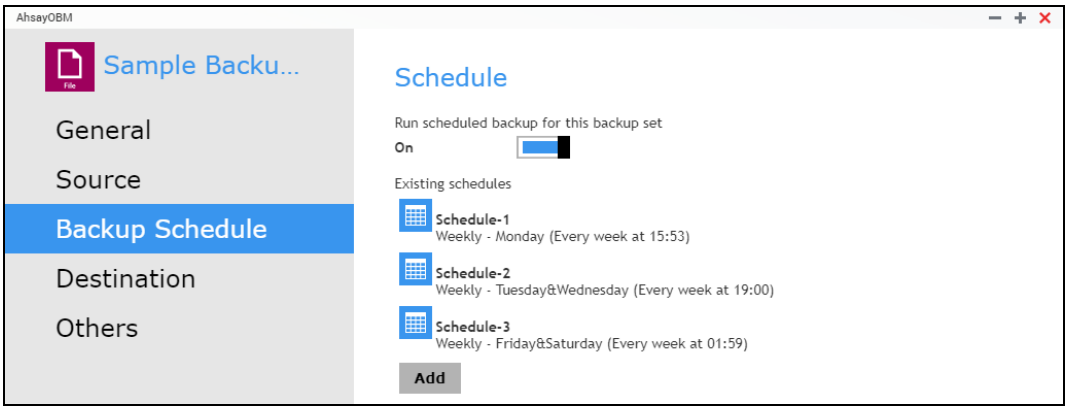
Result: There is no scheduled backup job will be run for the backup set.

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

Scheduler under Setting



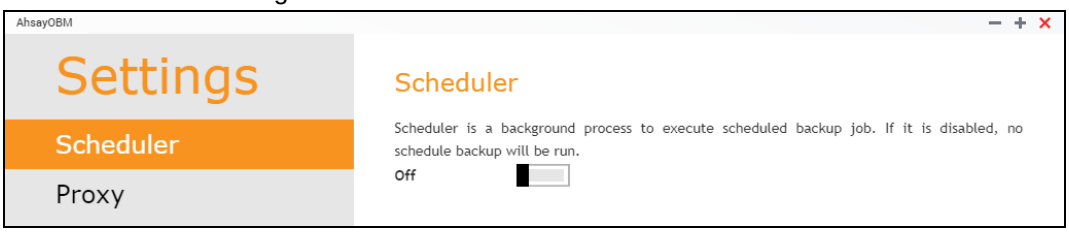
Scheduler under Backup Set Settings



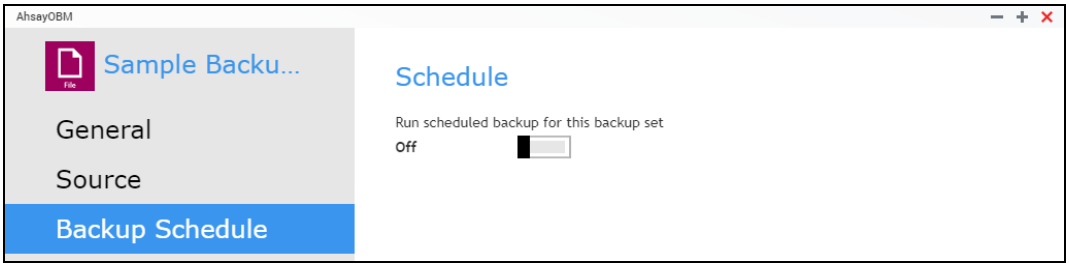
Result: There is no scheduled backup job will be run for the backup set.

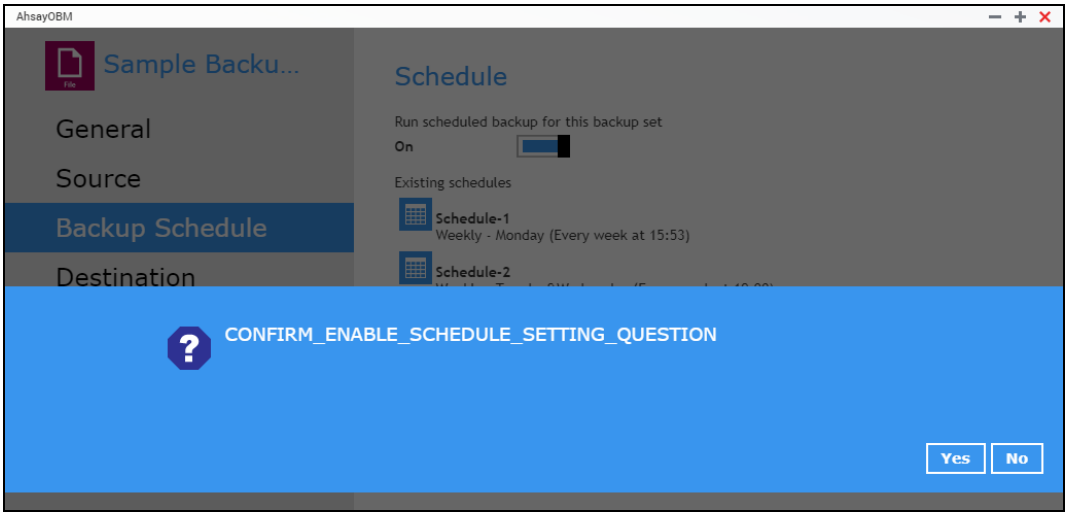
Scenario no. 5: Scheduler under Setting is OFF and turning ON Scheduler under Backup Set Settings

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:

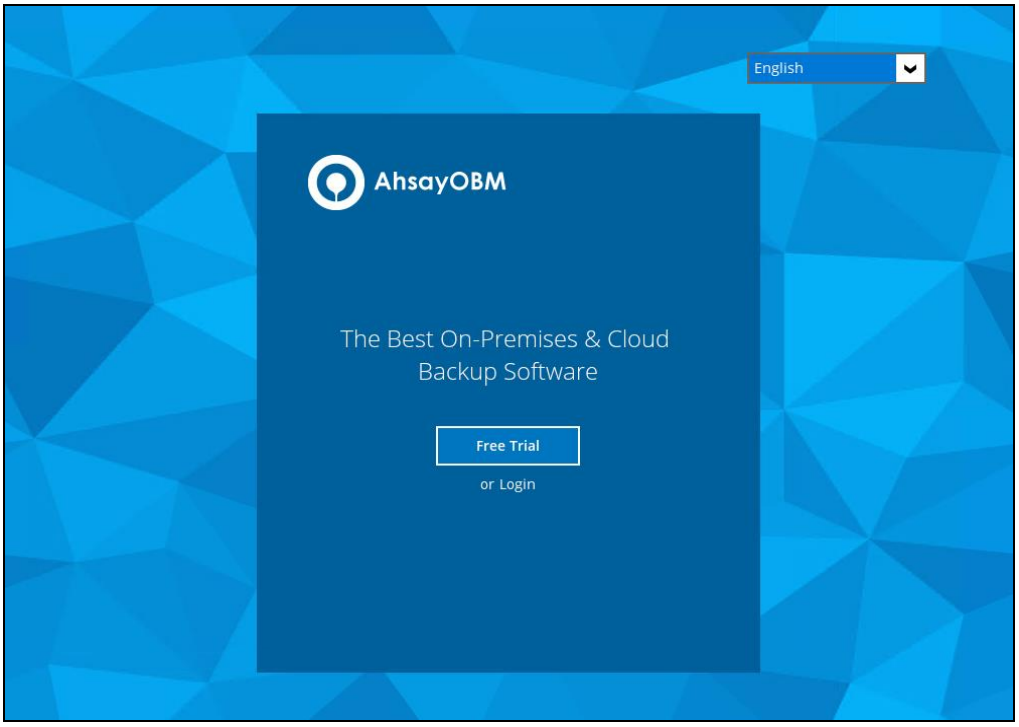
- A valid email address which will be used for receiving notices. A welcome message will also be sent upon creation of the account which specifies the User Setting and Quota set for backup in AhsayCBS.

While here are the limitations of a trial account:

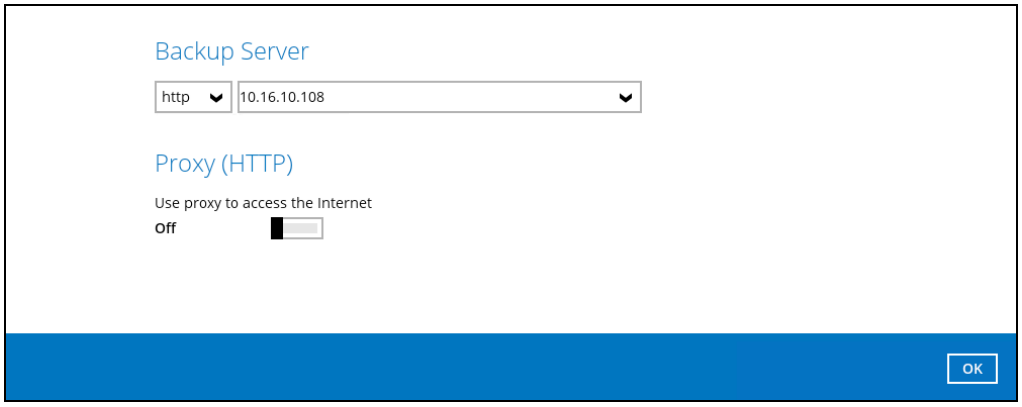
- The Free Trial button will only be displayed once, when the user login for the first time. If you cannot create a free trial account kindly contact your backup service provider.
- Only alphanumeric characters and selected special characters, A to Z, 0 to 9, @, - and _, are allowed to be used for the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

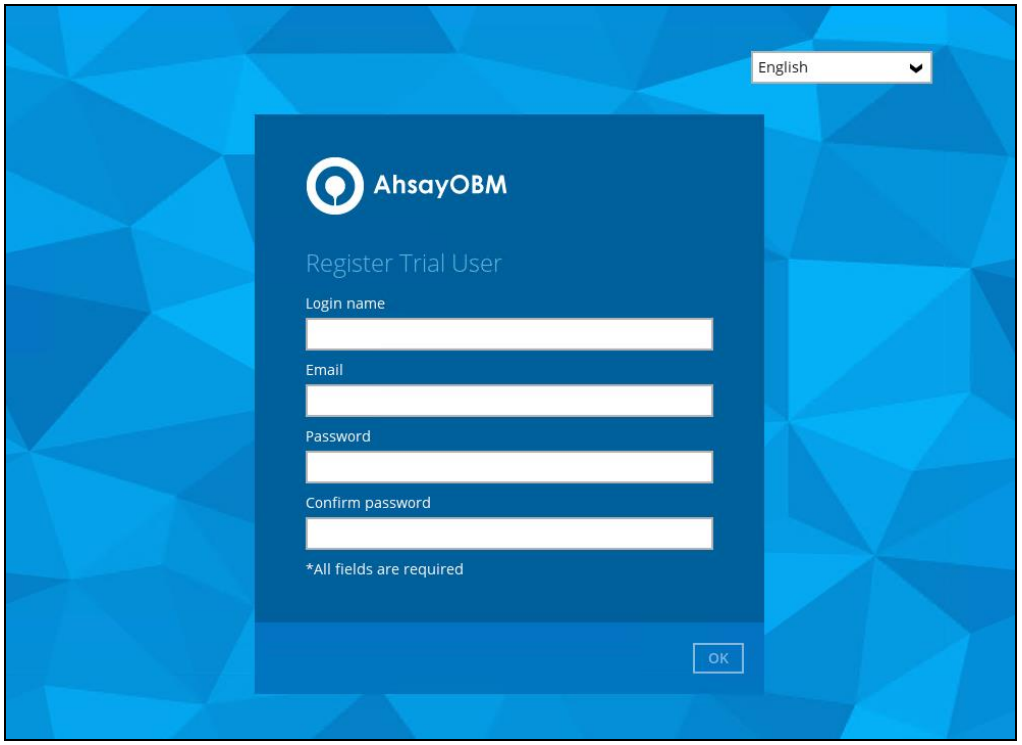
1. Click on **Free Trial**.



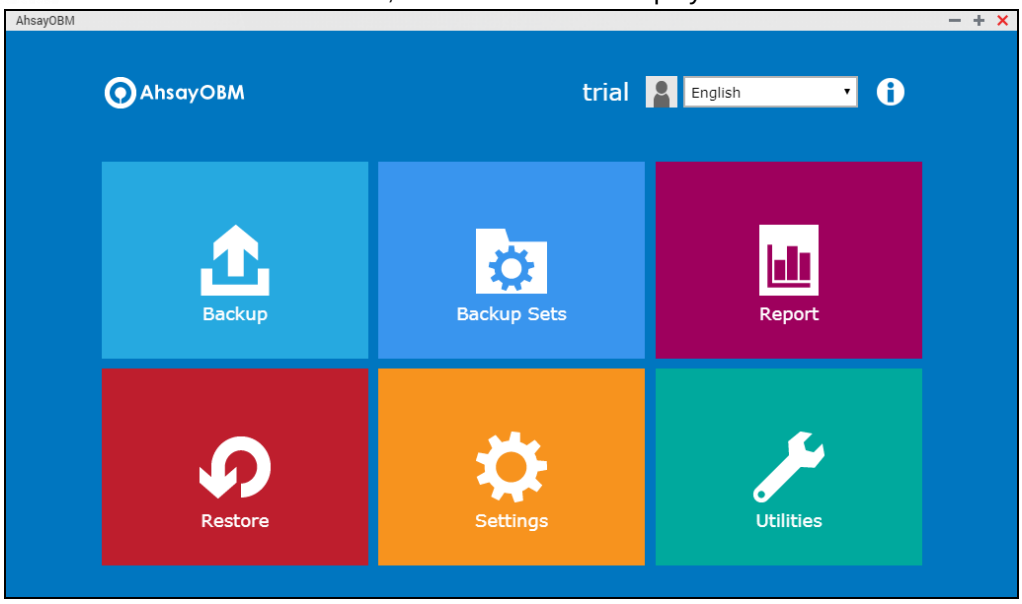
2. Configure your Backup Server settings.



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.



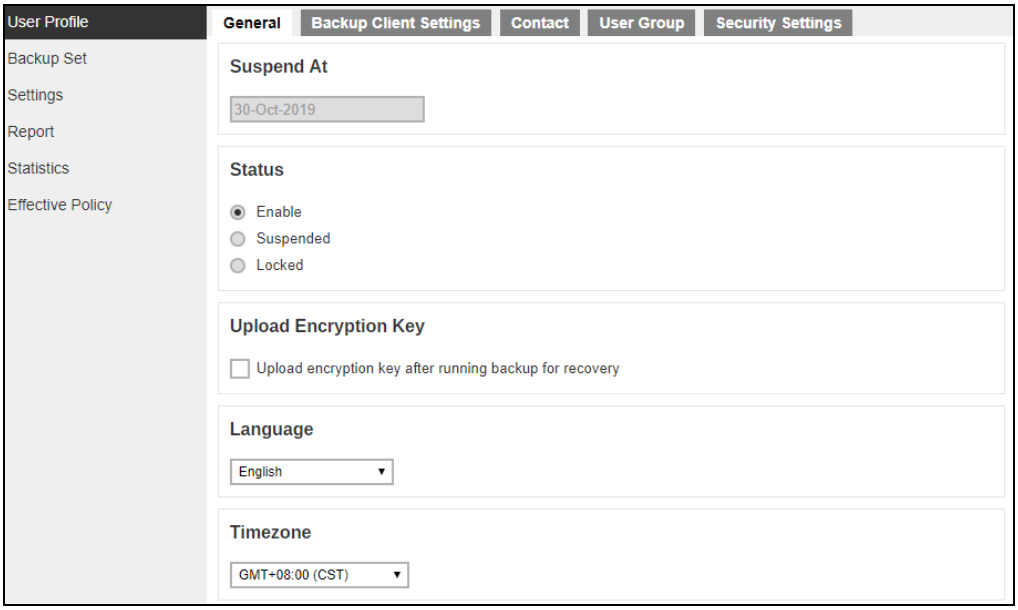
4. Once the trial account is created, this screen will be displayed.



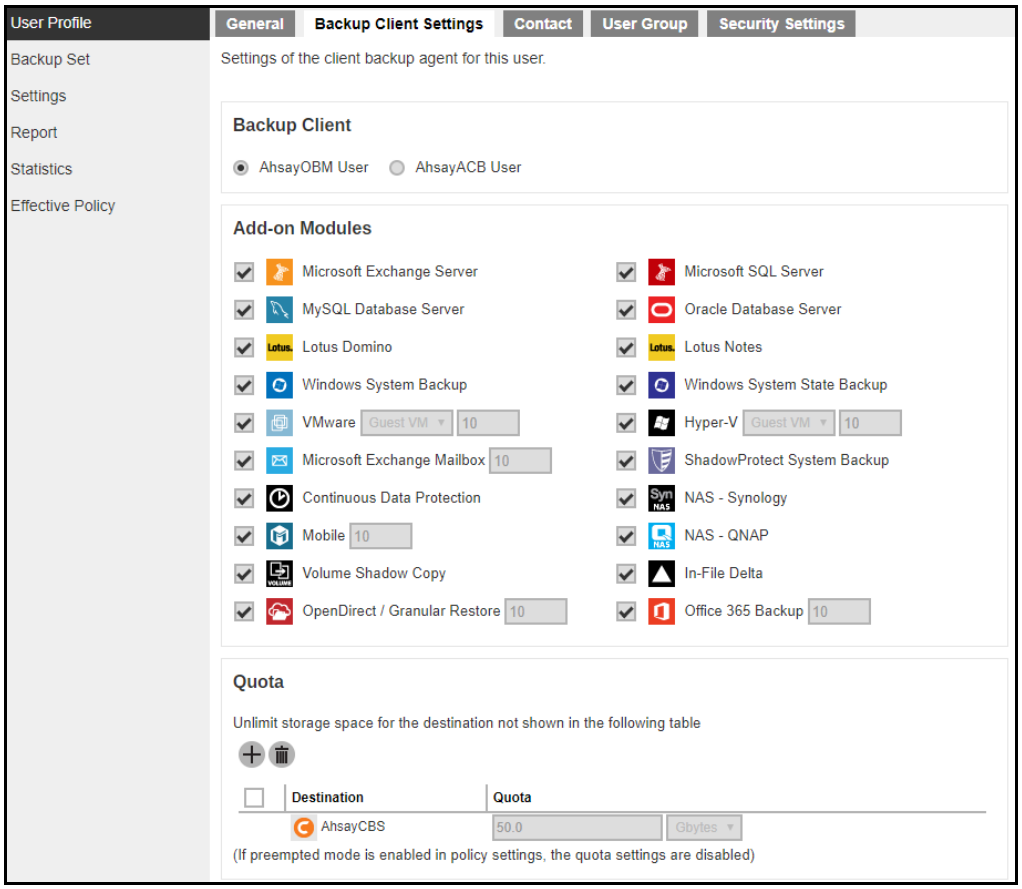
5. After your trial account has been created, you need to check several things:

- 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.



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



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.