Ahsay Online Backup Manager v8

Cloud File Backup & Restore Guide for MacOS

Ahsay Systems Corporation Limited

11 October 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
23 September 2020	Updated PDIC diagram in Ch. 5	Modification
7 April 2021	Updated Ch. 5; Added sub-chapters for the detailed process diagrams in Ch. 5.1, 5.2, 5.2.1, 5.2.2 and 5.3	New / Modifications
25 May 2021	Added requirement in Ch. 2.11; added Limitations in Ch. 2.13 and added notes for Periodic Data Integrity Check (PDIC) Process in Ch. 5.1	New
11 October 2021	Added different login instructions in Ch. 3	New

Table of Contents

1 Overview

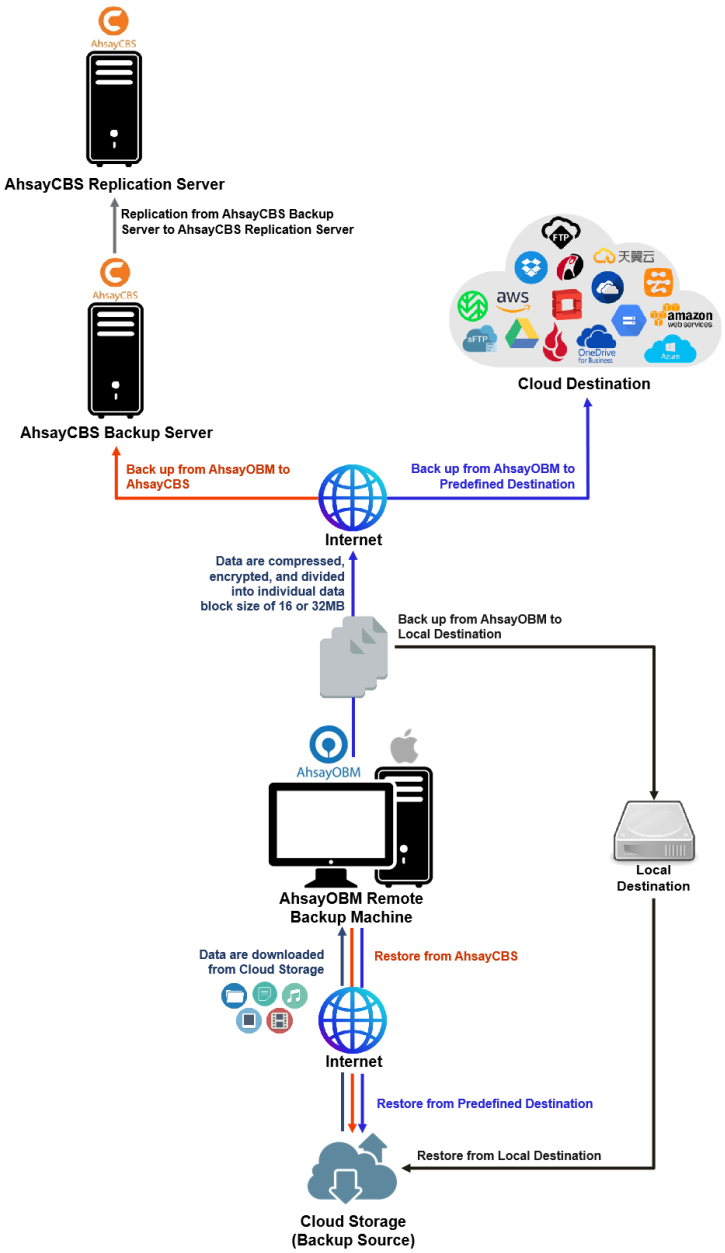
1.1 What is this software?

Ahsay brings you specialized client backup software, namely AhsayOBM, that allows you to back up your data stored on the cloud storage to either the AhsayCBS backup server, another cloud or predefined storage, and local destination. This provides set of tools that include backup and recovery of individual files with versioning and retention policy to protect your data on cloud storages.

1.2 System Architecture

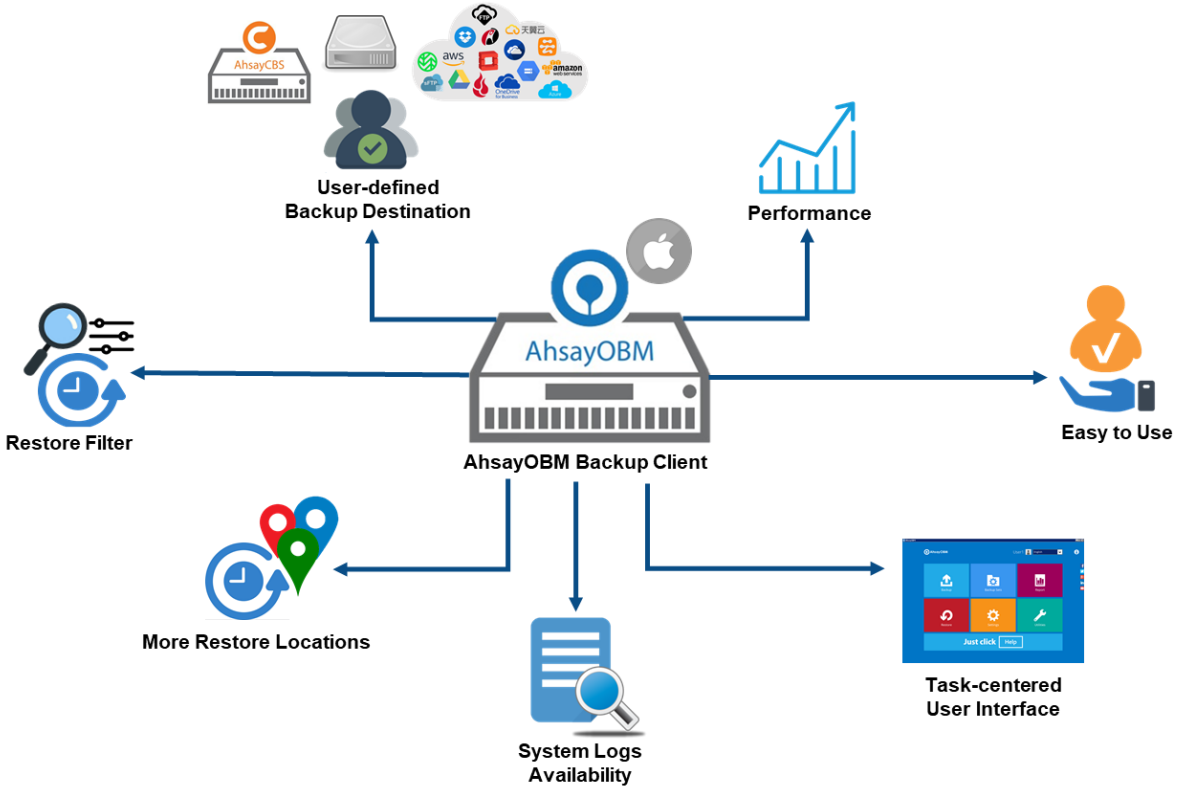
For agent-based backup and restore, the AhsayOBM initiates connection to the cloud storage (backup source) through the internet via the deployed backup agent on the customer's site.

Below is the system architecture diagram illustrating the major elements involved in the backup and restore process using the AhsayOBM Run on Client (Agent-based) backup configuration.



1.3 Why should I use AhsayOBM (Agent-based) Solution to back up my cloud data?

We are committed to bringing you a comprehensive Run on Client (Agent-based) cloud backup and recovery solution with AhsayOBM. Below are some key areas that we can help to make your backup experience a better one.



User-defined Backup Destination

Backup users have more options in assigning a backup destination (i.e., AhsayCBS, Cloud or Predefined destinations, and standard and local destination).

Performance

Agent-based backup is performed on a physical machine or computer with resources that is dedicated for backup and restore operations. Once the backup client is deployed on the machine, the user have more control on the hardware which affects the overall backup and restore performance.

Easy to Use

Agent-based backup solution has a traditional backup approach that is well understood by most administrators and end users who would only need minimal effort and time to understand the backup and/or restore operations.

Task-centered User Interface

Agent-based backup solution make it a good option for users to have more control on the individual backup/restore and resources management.

System Logs Availability

System logs for data integrity check and space freeing up results is accessible for the end users and can be reviewed anytime. Unlike with the agentless backup where system logs will only be available upon request from the backup service provider.

More Restore Locations

Agent-based backup offers you three (3) restore locations such as the local machine, original location (or the cloud storage where you backed up them), and alternate location (which is through the same cloud storage but on a different folder).

Restore Filter

Agent-based backup has a restore filter feature which allows users to easily search directories, files, and/or folders to restore.

High Level of Security

We understand that the data on your cloud storage may contain sensitive information that requires to be protected, that is why we ensure that your backup data will be encrypted with the highest level of security measure.

- ***Un-hackable Encryption Key*** – to provide the best protection to your backup data, the encryption feature which will default encrypt the backup data locally with an AES 256-bit randomized encryption key.
- ***Encryption Key Recovery*** – Furthermore, we have a backup plan for you to recover your encryption key in case you have lost it. Your backup service provider can make it mandatory for you to upload the encryption key to the centralized management console, the encryption key will be uploaded in hashed format and will only be used when you request for a recovery.

Cloud Destinations Backup

By default, the AhsayCBS is set as the storage destination in creating a cloud file backup set. However, you may add another storage destination(s) as provided by your backup service provider. Below is a list of supported cloud destinations:

- Aliyun (阿里云)*
- CTYun (中国电信天翼云)*
- Amazon S3
- AWS S3 Compatible Cloud Storage
- Wasabi
- Backblaze
- Google Cloud Storage
- Google Drive
- Microsoft Azure
- Microsoft OneDrive
- Microsoft OneDrive for Business
- Rackspace
- OpenStack
- Dropbox
- FTP
- SFTP

NOTE

For more details, please contact your backup service provider.

Run on Client

A Run on Client Cloud File Backup Set provides you with an agent-based backup solution. Manual, scheduled, or continuous backup job is performed on the client computer. A backup agent needs to be installed on the client machine in order to back up your data on cloud storage(s).

Differences between a Run on Client and Run on Server Backup Set

The following table summarizes the differences in backup options available between a Run on Client and Run on Server cloud file backup set, and the tool to use (client agent or web console) when performing a backup and restore:

Features/Functions	Run on Client Cloud File Backup Set	Run on Server Cloud File Backup Set
General Settings	✓	✓
Backup Source	✓	✓
Backup Schedule	✓	✓
Continuous Backup	AhsayOBM / AhsayACB for Windows only	✓
Destination	AhsayCBS, Predefined Destinations, Standard and Local	AhsayCBS or Predefined Destinations only
Multiple Destinations	✓	✘
In-File Delta	✓	✓
Retention Policy	✓	✓
Command Line Tool	AhsayOBM for Windows only	✘
Reminder	AhsayOBM / AhsayACB for Windows only	✘
Restore Filter	✓	✘
Bandwidth Control	✓	✓
IP Allowed for Restore	✓	✘
System Logs of Data Integrity Check and Space Freeing Up	✓	✘
Others	✓	✓
To Run a Backup	AhsayOBM / AhsayACB	AhsayCBS User Web Console only
To Run a Restore	AhsayOBM / AhsayACB / AhsayOBR	AhsayCBS User Web Console only

Aside from the backup options, the table below shows other operations that can be performed using client agent and web console:

Features/Functions	Run on Client Cloud File Backup Set	Run on Server Cloud File Backup Set
Data Integrity Check	✓	✓
Space Freeing Up	✓	✓
Delete Backup Data	✓	✓
Decrypt Backup Data	✓	✘

NOTE

For more details on the Run on Server backup option, please refer to the following guides:
AhsayCBS v8 User Guide – Cloud File Run on Server (Agentless) Backup and Restore Guide

1.4 About This Document

What is the purpose of this document?

This document aims at providing all necessary information for you to get started with setting up your system for Run on Client Cloud File backup and restore, followed by step-by-step instructions on a creating a backup set, running a backup and restoring backup data using the AhsayOBM client.

The document can be divided into three (3) main parts.

Part 1: Preparing for Cloud File Backup & Restore

Requirements
Requirements on hardware & software installation

Best Practices and Recommendations
Items recommended to pay attention to before performing backup and restore

Part 2: Performing a Cloud File Backup

Logging in to AhsayOBM client
Log in to AhsayOBM

Creating a Backup Set
Create a backup set using AhsayOBM

Running a Backup Set
Run a backup set using AhsayOBM

Part 3: Restoring a Cloud File Backup

Restoring a Backup Set using AhsayOBM client
Restore a backup set using AhsayOBM

What should I expect from this document?

After reading through this documentation, you can expect to have sufficient knowledge to set up your system to backup data on Cloud storage using the client agent, as well as to carry out an end-to-end backup and restore process.

Who should read this document?

This documentation is intended for backup administrators and IT professionals who are responsible for the Cloud File backup and restore.

2 Preparing for Backup and Restore

2.1 Hardware Requirement

To achieve the optimal performance when running AhsayOBM on your machine, refer to the following article for the list of hardware requirements.
FAQ: Ahsay Hardware Requirement List (HRL) for version 8.1 or above

2.2 Software Requirement

Refer to the following article for the list of compatible operating systems and application version.
FAQ: Ahsay Software Compatibility List (SCL) for version 8.1 or above

2.3 Internet / Network Connection

In order to allow access to the cloud storage, a stable internet connection must be available on the computer where the AhsayOBM is installed. If large amounts of data are backed up from a cloud storage account then a fast internet connection is required.

2.4 AhsayOBM Installation

Make sure that AhsayOBM is installed on a computer with Internet access for connection to the cloud storage.

2.5 Valid AhsayOBM User Account

A valid AhsayOBM user account is required before you can log in to the AhsayOBM client.

2.6 Ahsay License Requirements

- **Licenses**

  The Cloud File Backup module is included in the basic AhsayOBM license. There is no limit on the number of Cloud File backup sets in an AhsayOBM user account.

  For more details, please contact your backup service provider.

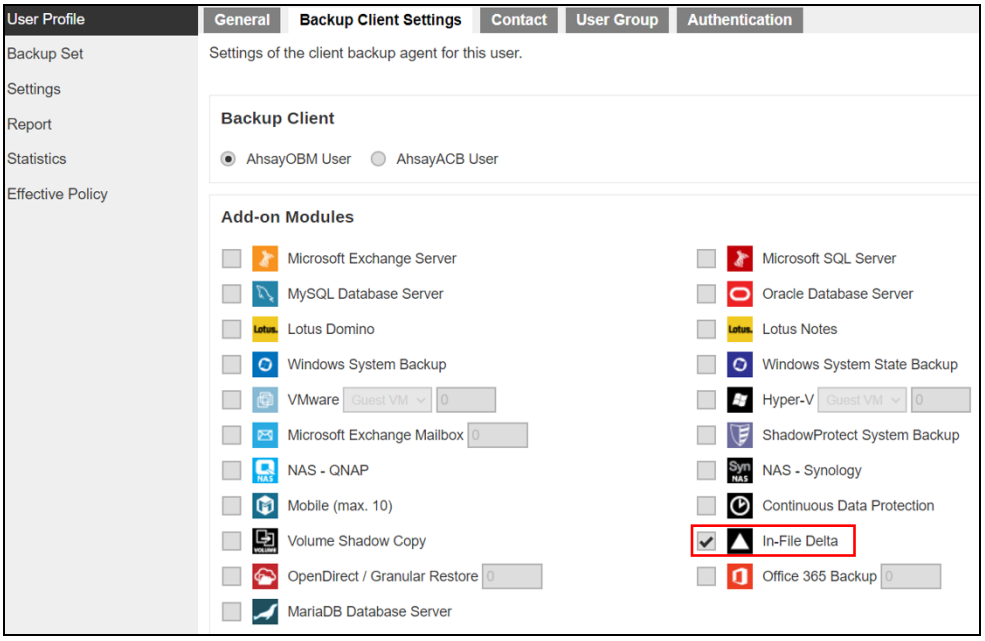
2.7 Add-on Module Requirements

- **In-File Delta**

  The In-File Delta add-on module must be added on the AhsayOBM user account if you would like to use this feature.

  NOTE

  This add-on module must be enabled on the AhsayOBM user account. Please contact your backup service provider for details.



2.8 Backup Quota Requirement

Make sure that your AhsayOBM user account has sufficient quota assigned to accommodate the storage for the cloud file backup set(s) and retention policy.

2.9 Cloud Sources

The AhsayOBM Run on Client (Agent-based) Backup Solution supports the following cloud sources to back up as provided by your backup service provider:

- Aliyun (阿里云)*
- CTYun (中国电信天翼云)*
- Amazon S3
- AWS S3 Compatible Cloud Storage
- Wasabi
- Backblaze
- Google Cloud Storage
- Google Drive
- Microsoft Azure
- Microsoft OneDrive
- Microsoft OneDrive for Business
- Rackspace
- OpenStack
- Dropbox
- FTP
- SFTP

2.10 Login Credentials to Cloud Storage

To allow access to the cloud storage (backup source) in performing a backup, make sure to have the correct login credentials to the cloud storage service.

2.11 Network Bandwidth

10 Mbps or above connection speed.

2.12 Best Practices and Recommendations

The following are some best practices and recommendations we strongly recommend you follow for optimized backup and restore performance:

Backup Destination

To provide maximum data protection and flexible restore options for agent-based backup, it is recommended to configure:

- At least one offsite or cloud destination
- At least one local destination for fast recovery

Temporary Directory Folder Location

Temporary directory folder is used by the AhsayOBM for storing backup set index files and any incremental or differential backup files generated during a backup job. To ensure optimal backup/restoration performance, it is recommended that the temporary directory folder is set to a local drive.

Performance Recommendations

Schedule backup jobs when system activity is low to achieve the best possible performance.

Bucket Management for Enterprise Cloud Storage Providers

If you have chosen to back up files from an enterprise cloud storage (e.g., Amazon S3, Wasabi, Microsoft Azure, Google Cloud Storage, etc.), you will have to select a bucket name during the creation of cloud file backup set. Each bucket has a single compartment, and an access key is associated with a single bucket. Therefore, each backup set can back up one bucket.

For account with multiple buckets, the backup should be organized into one bucket per backup set. For best practice, make sure to assign one bucket name per backup set so you can ensure that you are selecting the correct file(s) to back up.

Test Restore Operations

Perform test restores periodically to ensure your backup is setup and backed up properly. Performing recovery test can also help identify potential issues or gaps in your recovery plan. It is important that you do not try to make the test easier, as the objective of a successful test is not to demonstrate that everything is flawless, but to discover faults in your recovery plan. There might be flaws identified in the plan throughout the test and it is important to identify those flaws.

- **Periodic Backup Schedule**

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

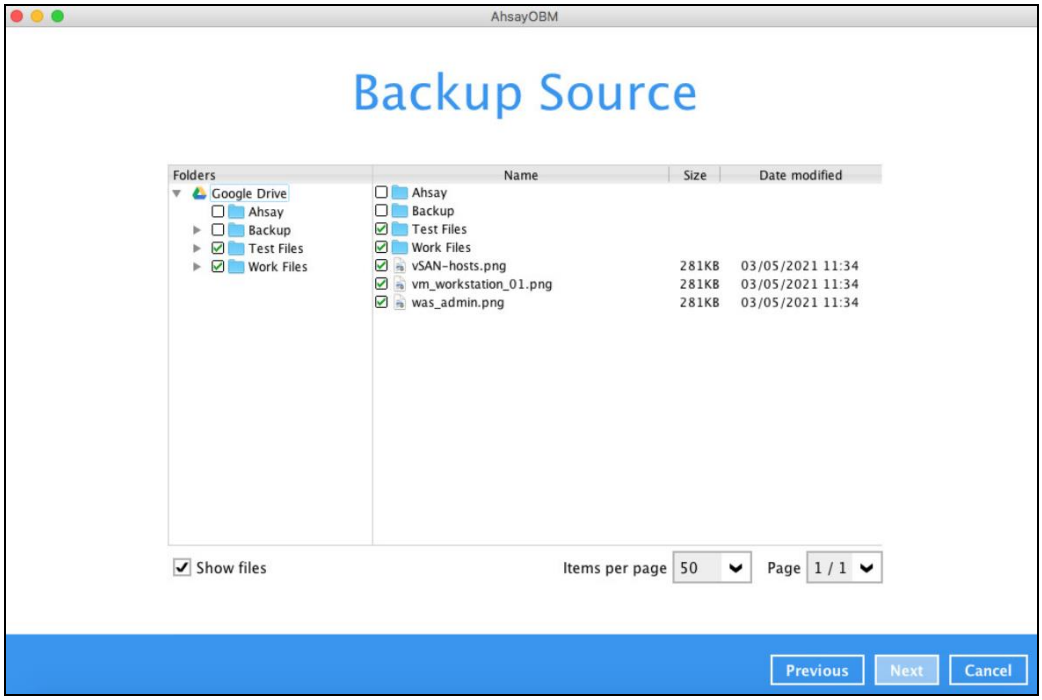
  Consider the following key points to efficiently handle backup sets with periodic backup schedule.

  - Hardware – to achieve optimal performance, compatible hardware requirements is a must. Ensure you have the backup machine's appropriate hardware specifications to accommodate frequency of backups,
    - so that the data is always backed up within the periodic backup interval
    - so that the backup frequency does not affect the performance of the production server
  - Retention Policy - also make sure to consider the retention policy settings and retention area storage management which can grow because of the changes in the backup data for each backup job.

2.13 Limitations

For backup source selection:

1. It is currently not possible to select the entire contents of the Cloud drive. Existing top level folders and/or files must be selected individually. If you need to back up the contents of the entire Cloud drive, then all top level folders and/or files must be selected.

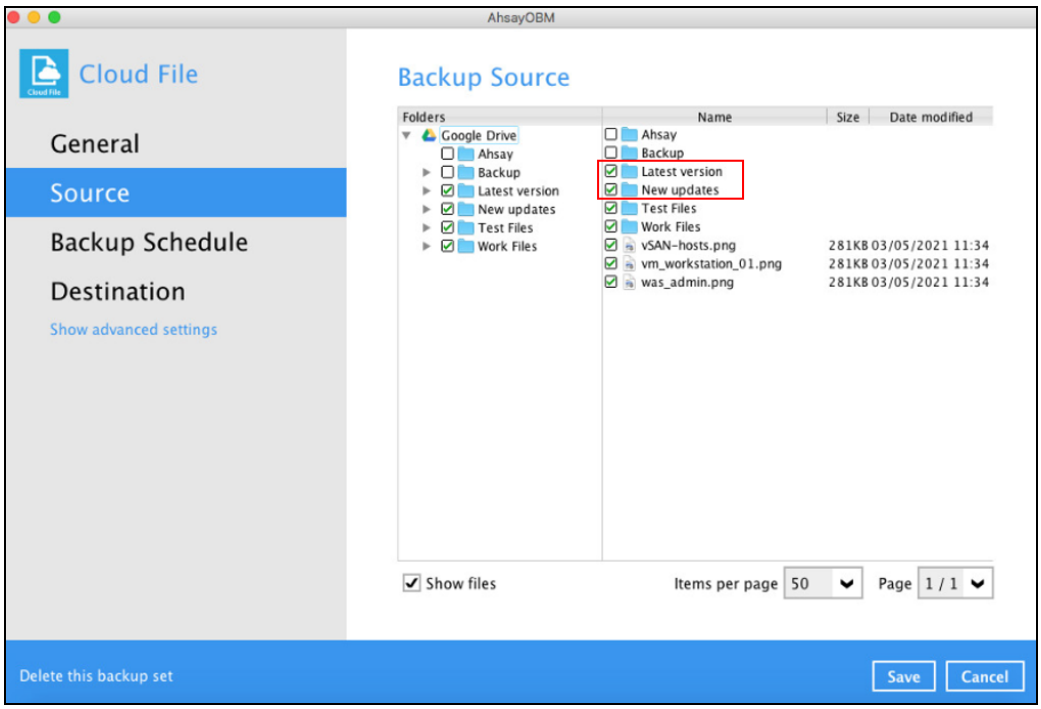


2. If there are any top level folders and/or files added to the Cloud drive after the backup set is created, they will not be added in the backup source automatically. The backup

set will have to be manually updated to include the new top level folders and/or files before they can be backed up.

Example:

If the “Latest version” and “New updates” folders were created after the creation of the backup set, and the contents of these folders must be backed up, then you must manually select these folders to be included in the backup.

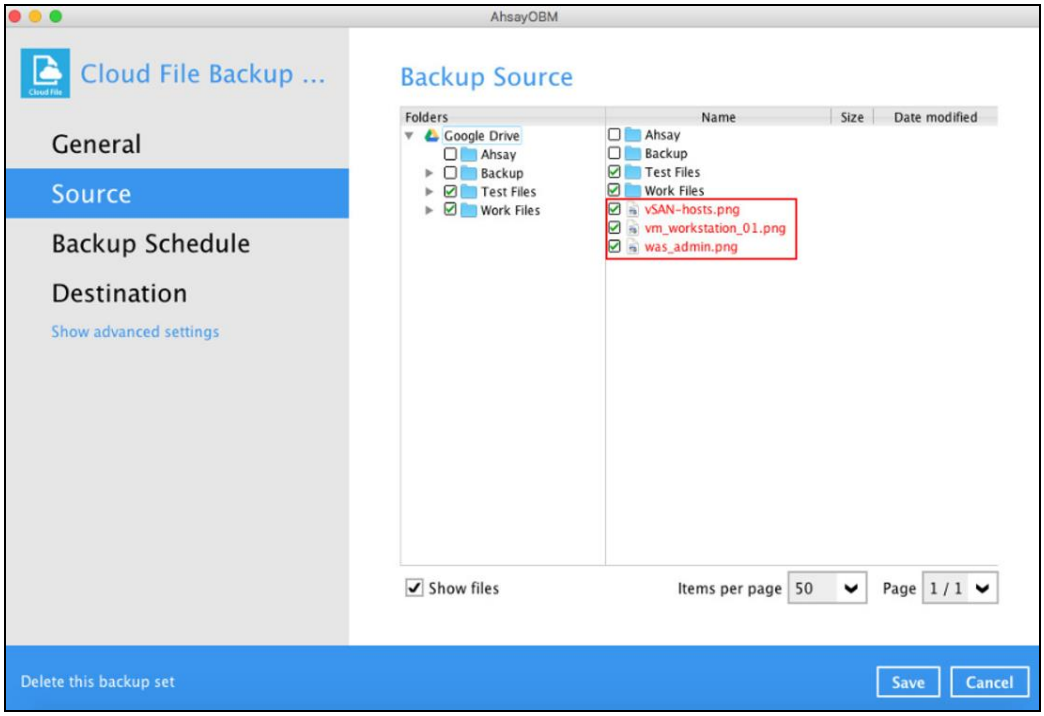


3. If there are any top level folders and/or files which have been deleted from the Cloud drive since the last backup job, they will not be removed from the backup source automatically. The backup set will have to be manually updated to unselect the deleted top level folders and/or files. Otherwise, the backup job will be completed with warnings.

   Example:

   The following files were backed up but subsequently deleted from the top level backup source of the Cloud drive: **was_admin.png**, **vm_workstation_01.png**, **vSAN-hosts.png**. The next backup job will encounter the following warnings until these deleted files are unselected from the backup source.

   The deleted files are highlighted in red on the backup source to indicate that they no longer exist on the Cloud storage account.



Backup log

```
[2021/05/04 09:56:50] [warn] [1620092933022] Backup source "was_admin.png" does not exist !

[2021/05/04 09:56:50] [cbs] [1620092933022] warn,"Backup source \"was_admin.png\" does not exist !",0,0,0,,,

[2021/05/04 09:56:50] [warn] [1620092933022] Backup source "vm_workstation_01.png" does not exist !

[2021/05/04 09:56:50] [cbs] [1620092933022] warn,"Backup source \"vm_workstation_01.png\" does not exist !",0,0,0,,,

[2021/05/04 09:56:50] [warn] [1620092933022] Backup source "vSAN-hosts.png" does not exist !

[2021/05/04 09:56:50] [cbs] [1620092933022] warn,"Backup source \"vSAN-hosts.png\" does not exist !",0,0,0,,,
```

3 Logging in to AhsayOBM

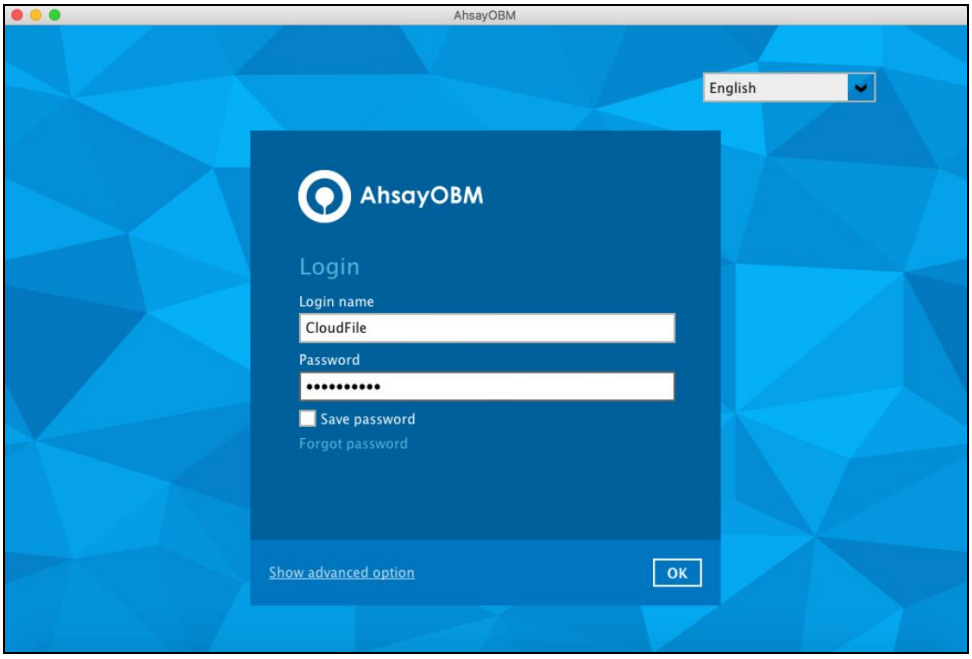
Starting with AhsayOBM v8.5.0.0 there are several login scenarios depending on the setting of the account you are using. The different scenarios will be discussed below:

- Login without 2FA
- Login with 2FA using authenticator app
- Login with 2FA using Twilio

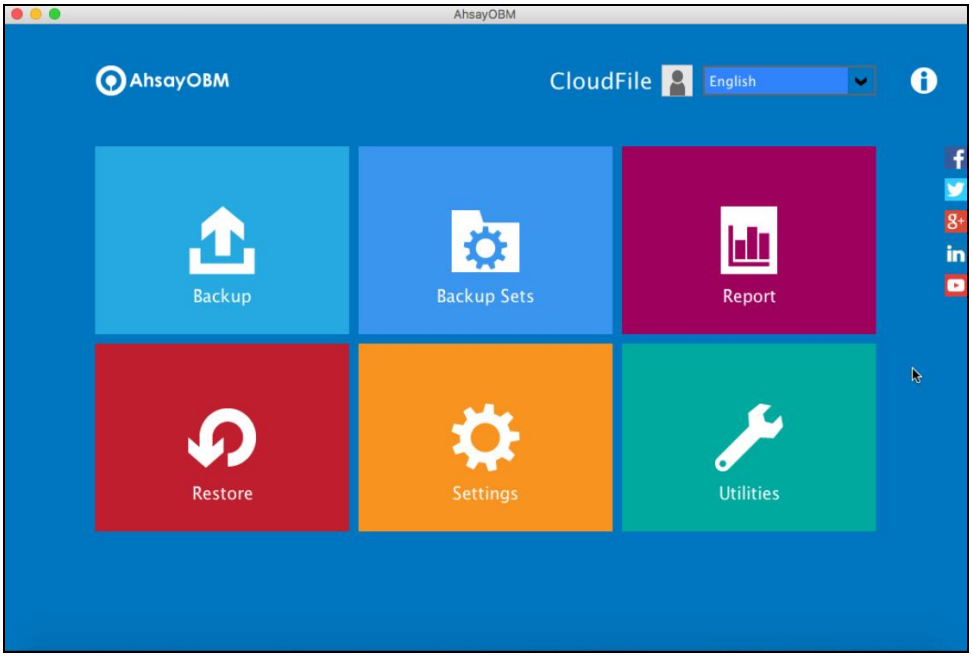
3.1 Login to AhsayOBM without 2FA

1. Log in to the AhsayOBM application user interface. Double click the AhsayOBM icon to launch the application.

2. Enter the **Login name** and **Password** of your AhsayOBM account then click **OK** to login.



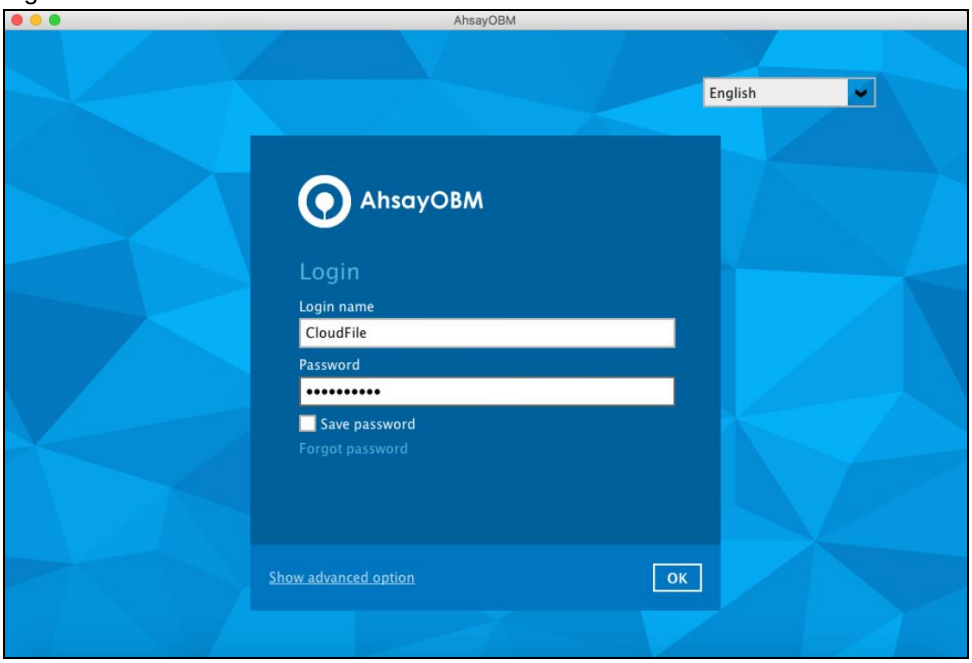
3. After successful login, the following screen will appear.



3.2 Login to AhsayOBM with 2FA using authenticator app

1. Log in to the AhsayOBM application user interface. Double click the AhsayOBM icon to launch the application.

2. Enter the **Login name** and **Password** of your AhsayOBM account then click **OK** to login.



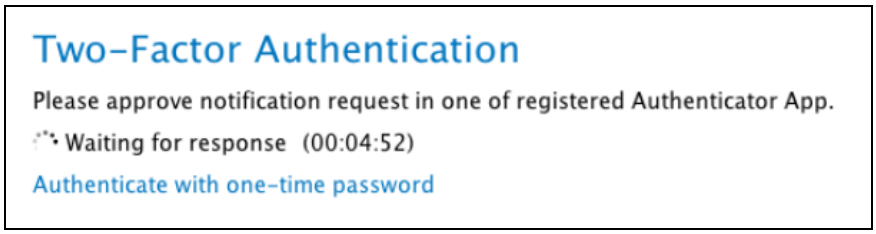
3. One of the two authentication methods will be displayed to continue with the login:

- Push Notification and TOTP when using Ahsay Mobile app
- TOTP only

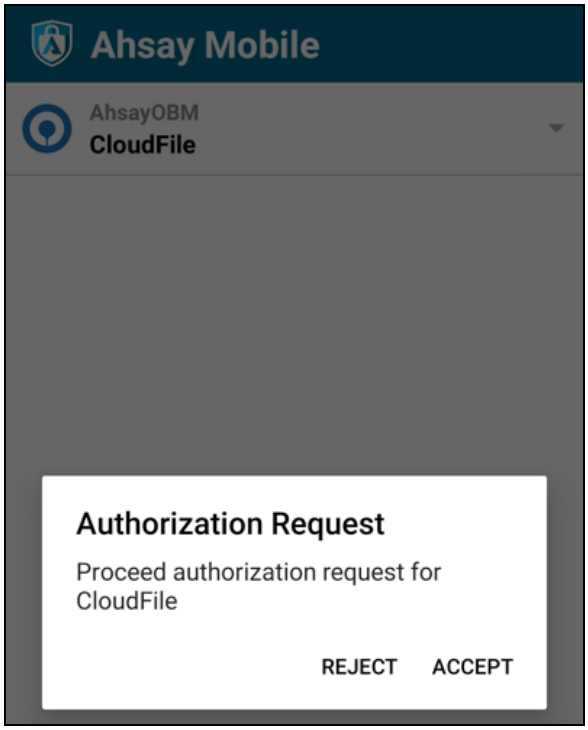
- If **Ahsay Mobile app** was configured to use Push Notification and TOTP then there are two 2FA modes that can be used:

  - Push Notification (default)

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

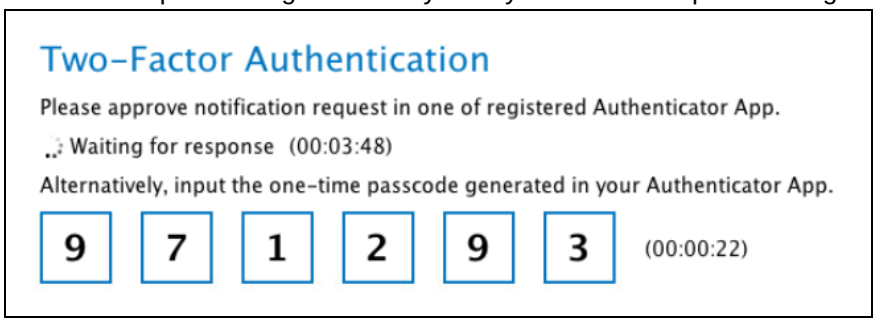
    Example of the login request sent to the Ahsay Mobile app.

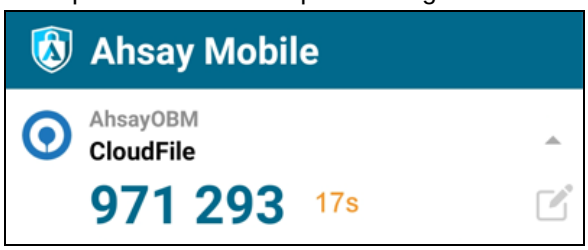
  - TOTP

    However, if push notification is not working or you prefer to use one-time passcode, click the Authenticate with one-time password link, then input

the one-time passcode generated by Ahsay Mobile to complete the login.

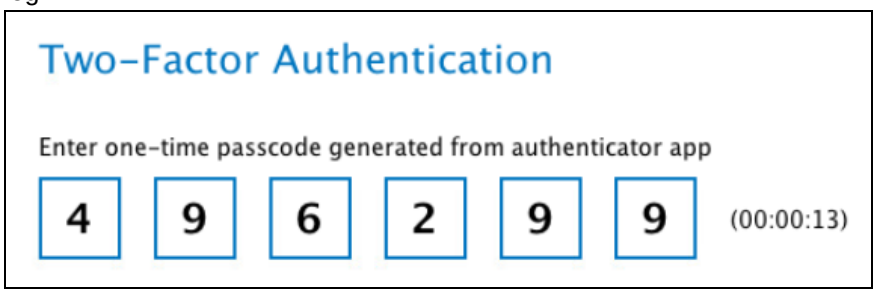


Example of the one-time passcode generated in Ahsay Mobile.

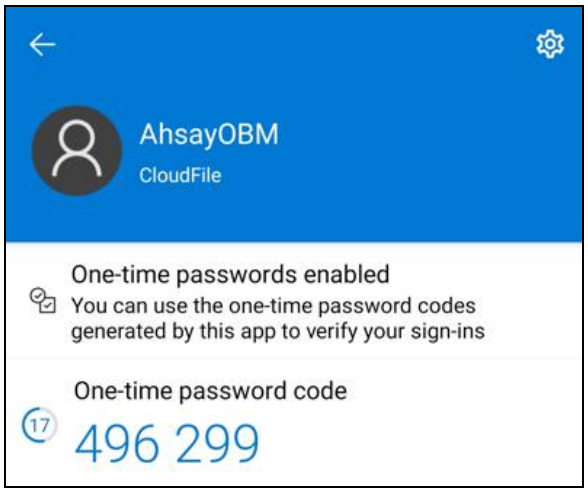


- TOTP only

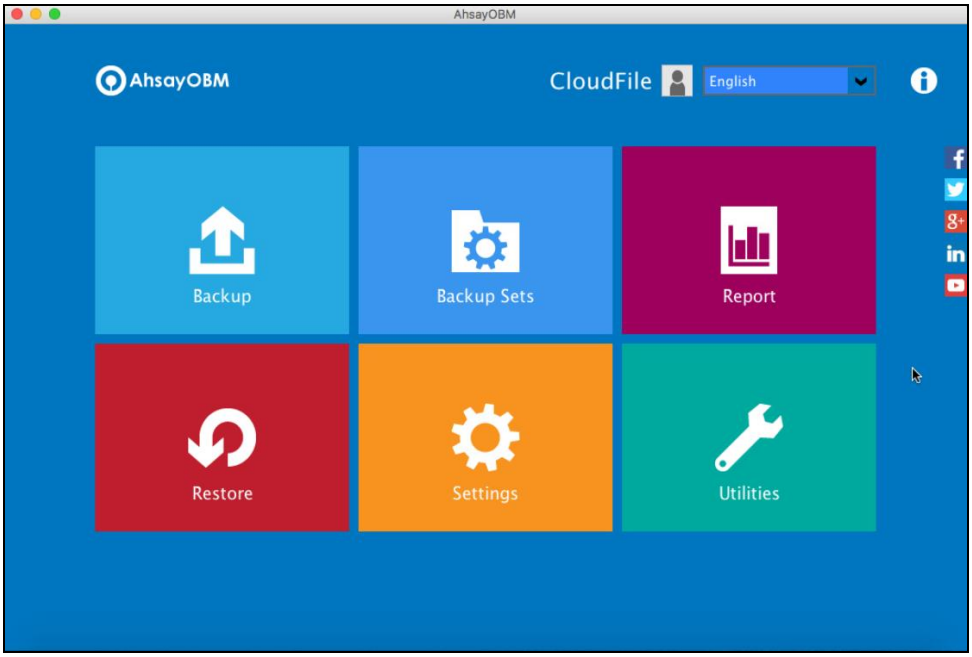
Enter the one-time passcode generated by the authenticator app to complete the login.



Example of the one-time passcode generated in the third party authenticator app Microsoft Authenticator.



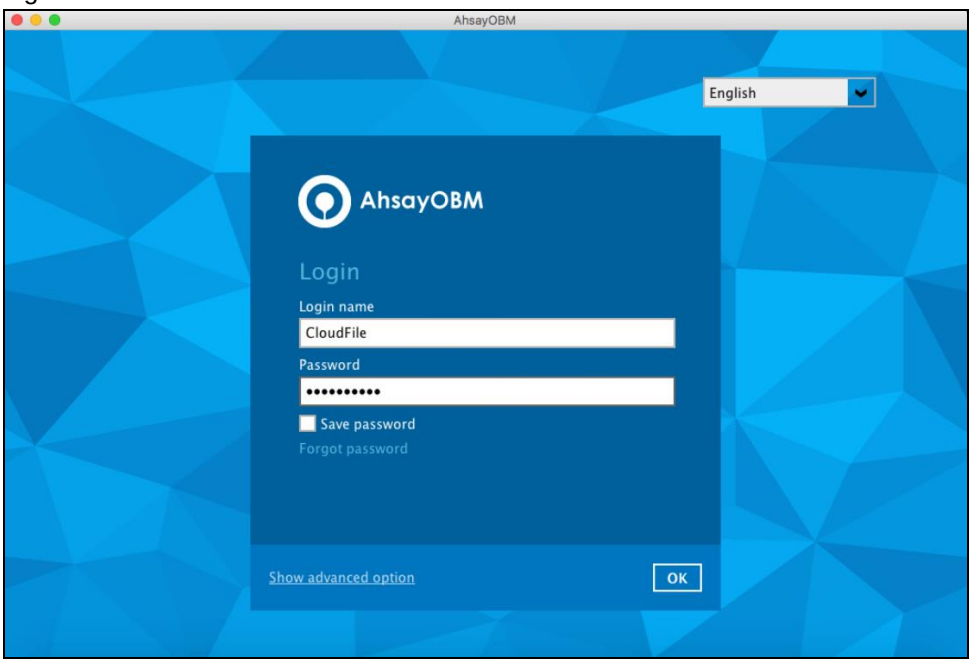
4. After successful login, the following screen will appear.



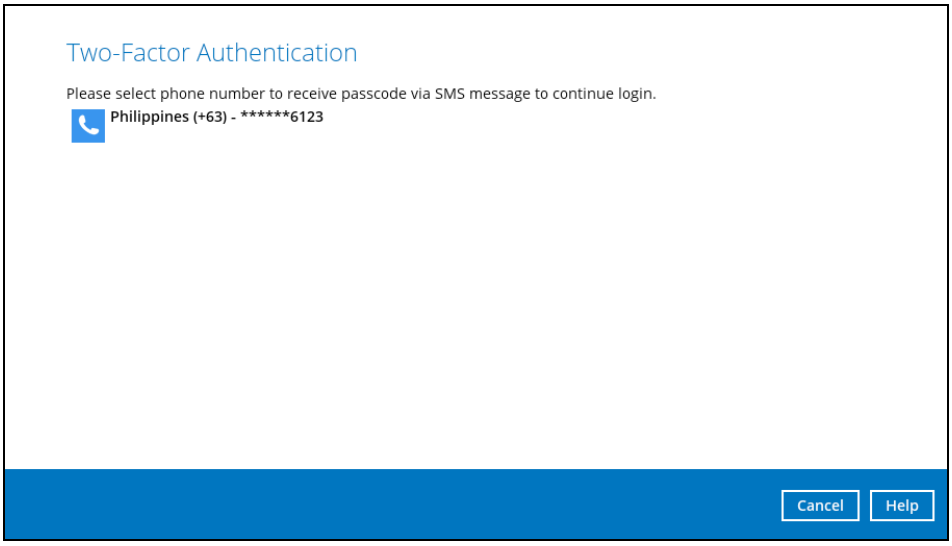
3.3 Login to AhsayOBM with 2FA using Twilio

1. Log in to the AhsayOBM application user interface. Double click the AhsayOBM icon to launch the application.

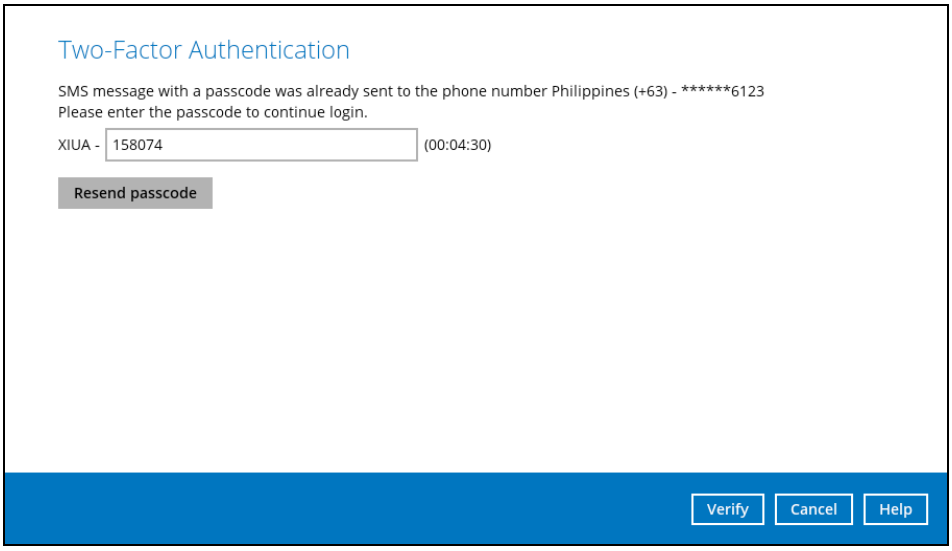
2. Enter the **Login name** and **Password** of your AhsayOBM account then click **OK** to login.



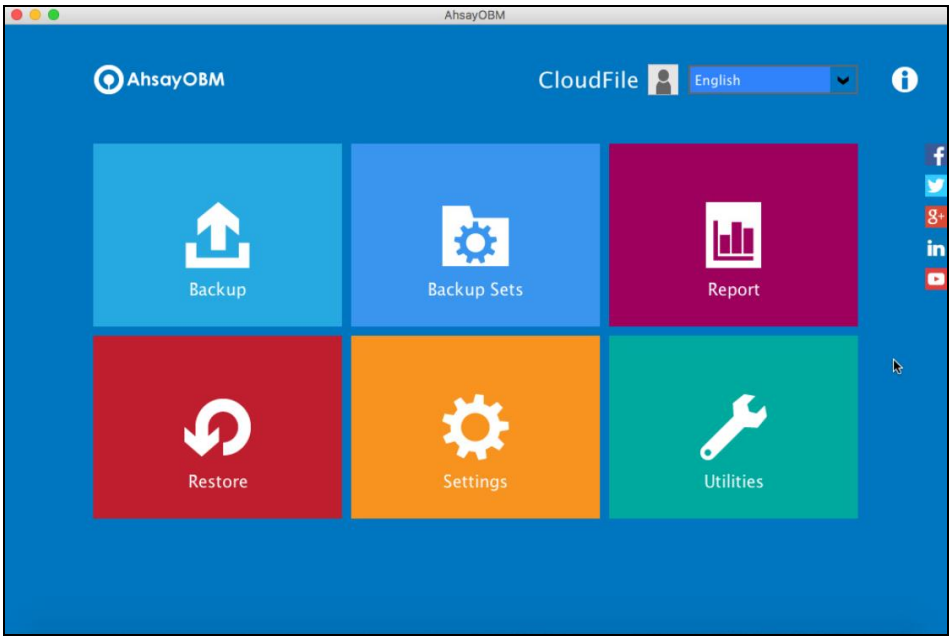
3. Select your phone number to receive the passcode.



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

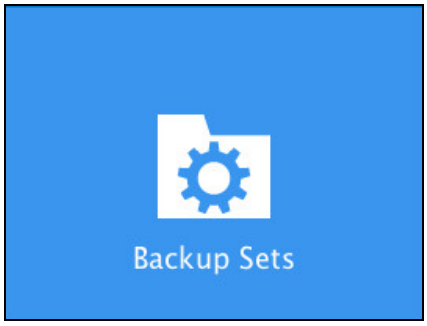


5. After successful login, the following screen will appear.

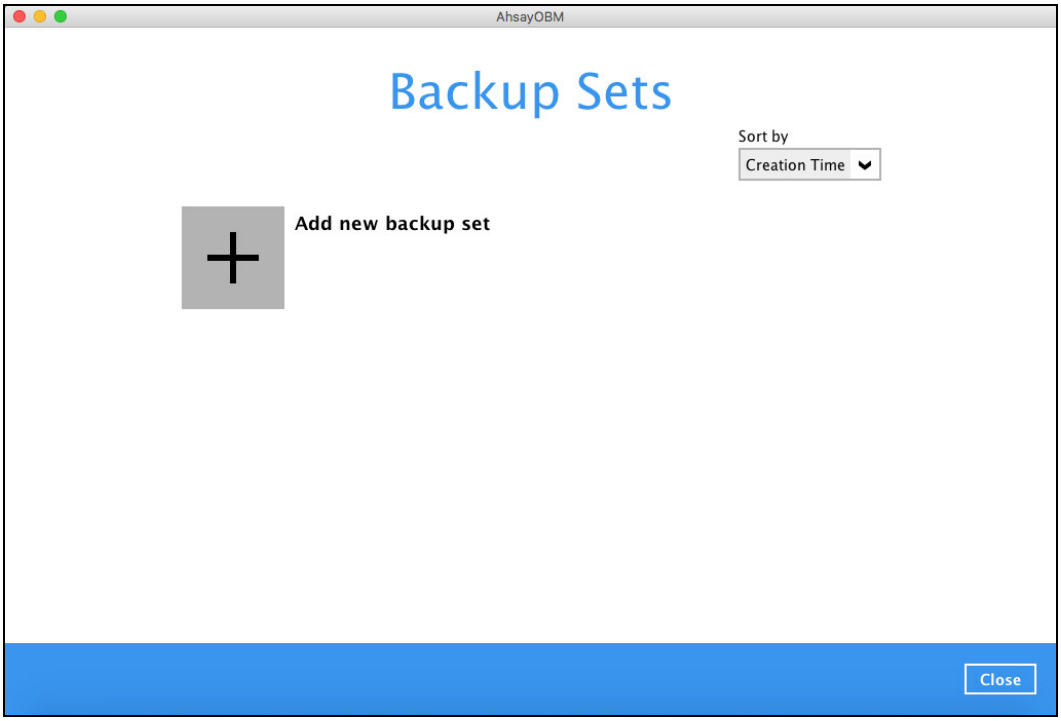


4 Creating a Cloud File Backup Set

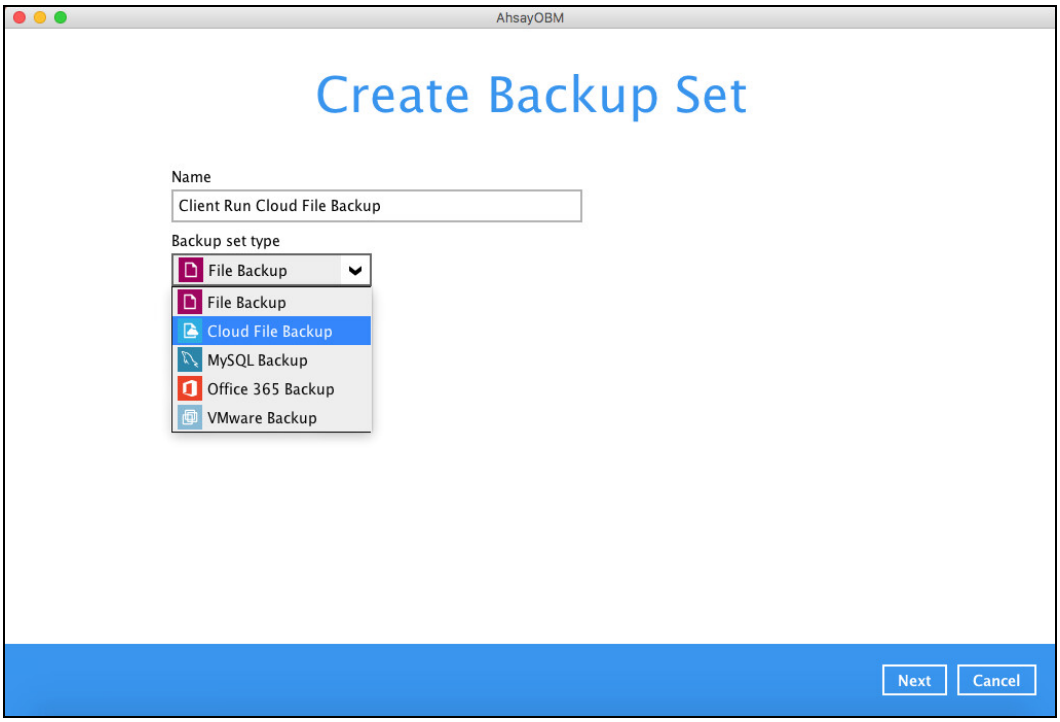
1. In the AhsayOBM main interface, click **Backup Sets**.



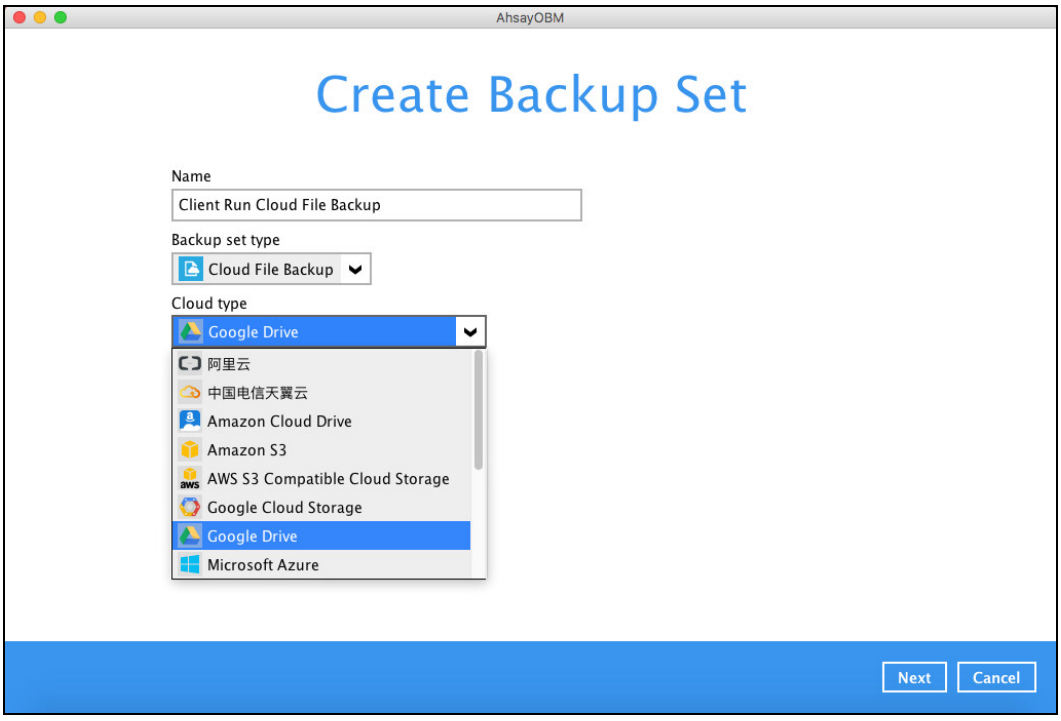
2. Create a Cloud File backup set by clicking the "+" icon next to **Add new backup set**.



3. Enter a **Name** for your backup set and select **Cloud File Backup** as the **Backup set type**.



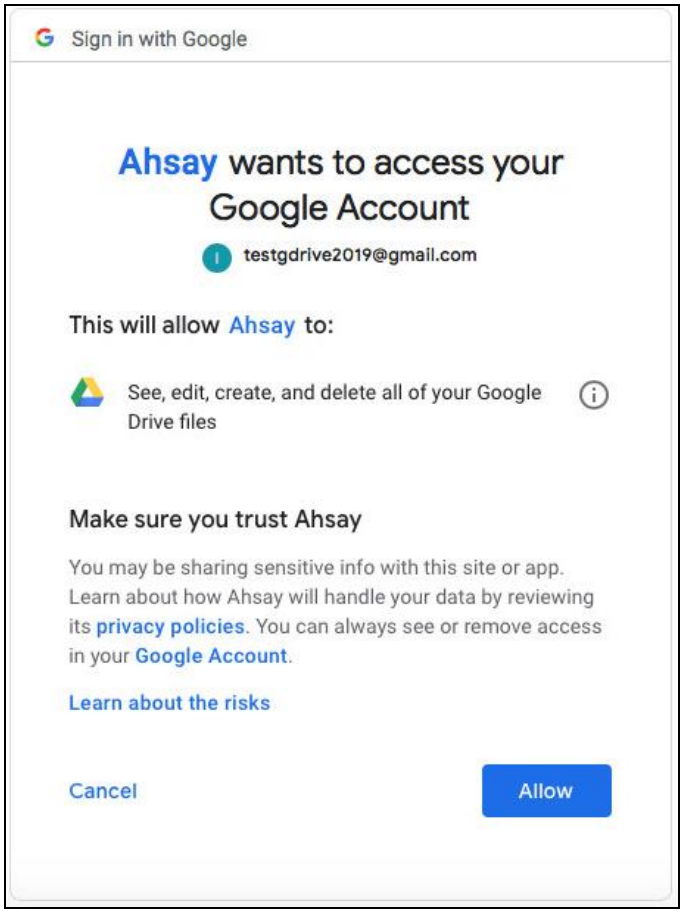
4. Select the **Cloud type** of the cloud storage that contain the data that you want to backup.

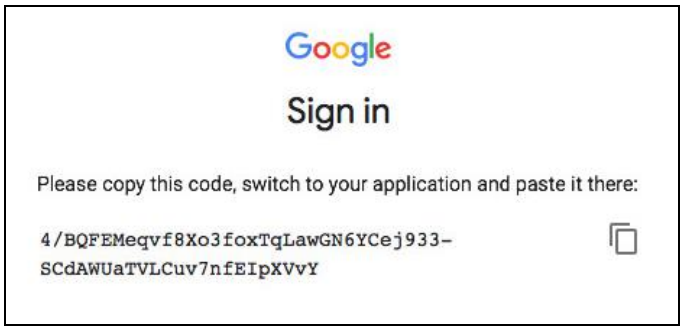


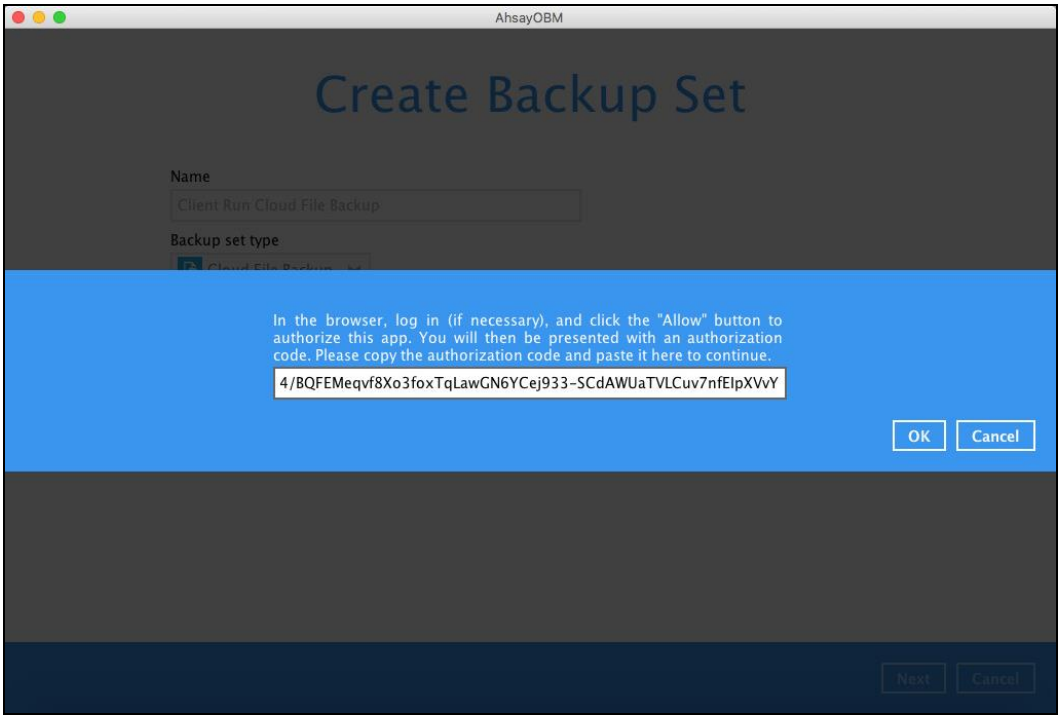
5. Depending on the cloud type you have selected, you will be prompted to enter the cloud service login details in either way below.

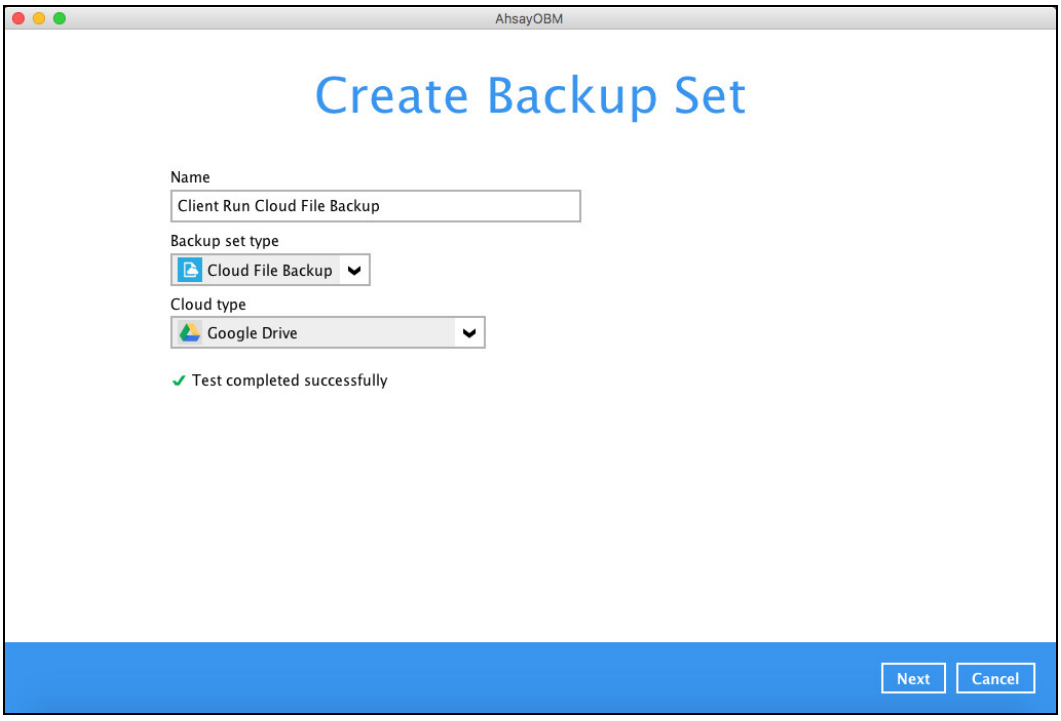
   - Click **Test** to get redirected to the login page of the cloud service provider on your default browser, then enter the login details there. Click **Allow** to permit AhsayOBM to access the cloud storage. Copy and paste the code generated by the cloud service provider to AhsayOBM where you will be prompted to

enter, then click **OK** to confirm.





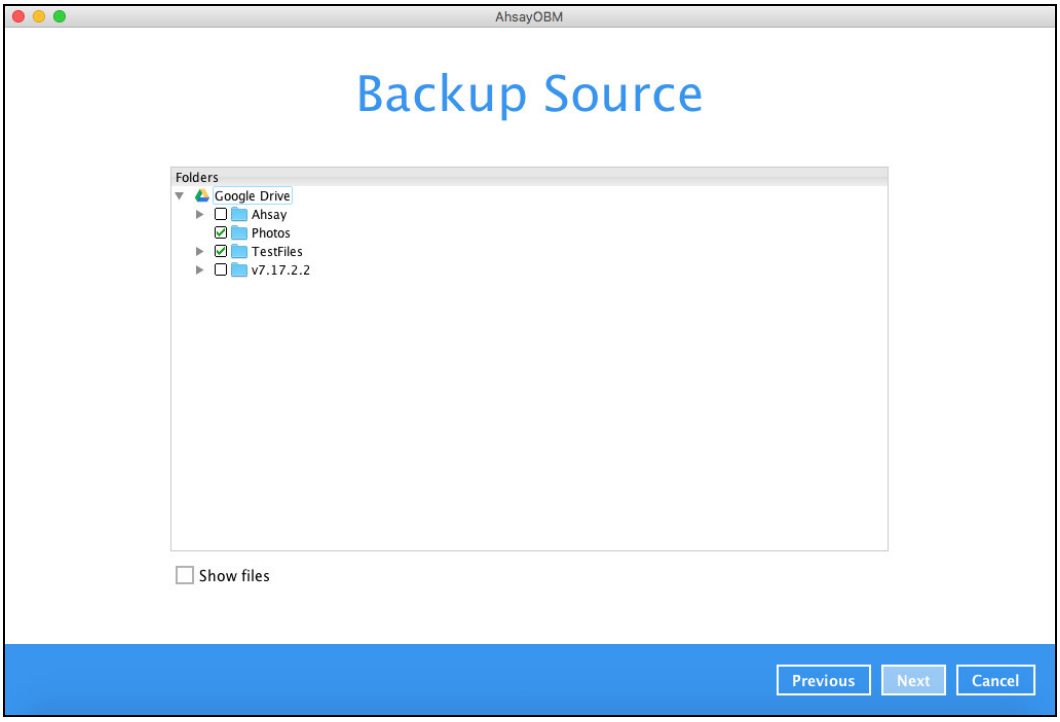




NOTE

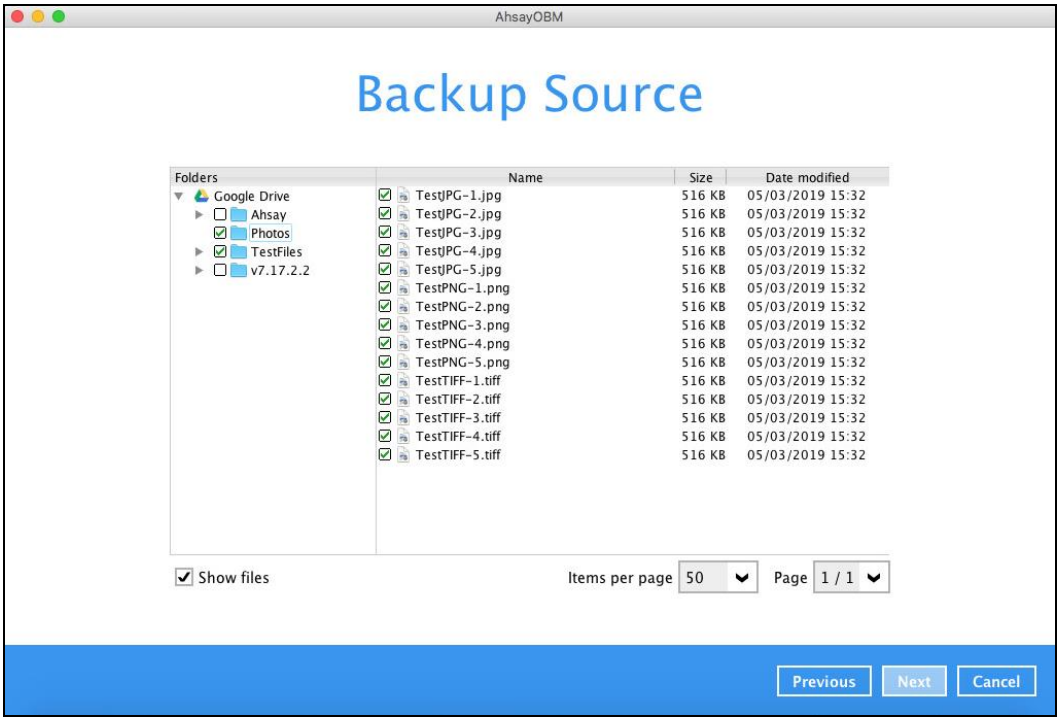
The authentication request will be opened in a new tab or window. Ensure that the pop-up window is not blocked, and pop-up blocker is disabled in your browser.

6. In the **Backup Source** menu, select the folder / files that you would like to backup.

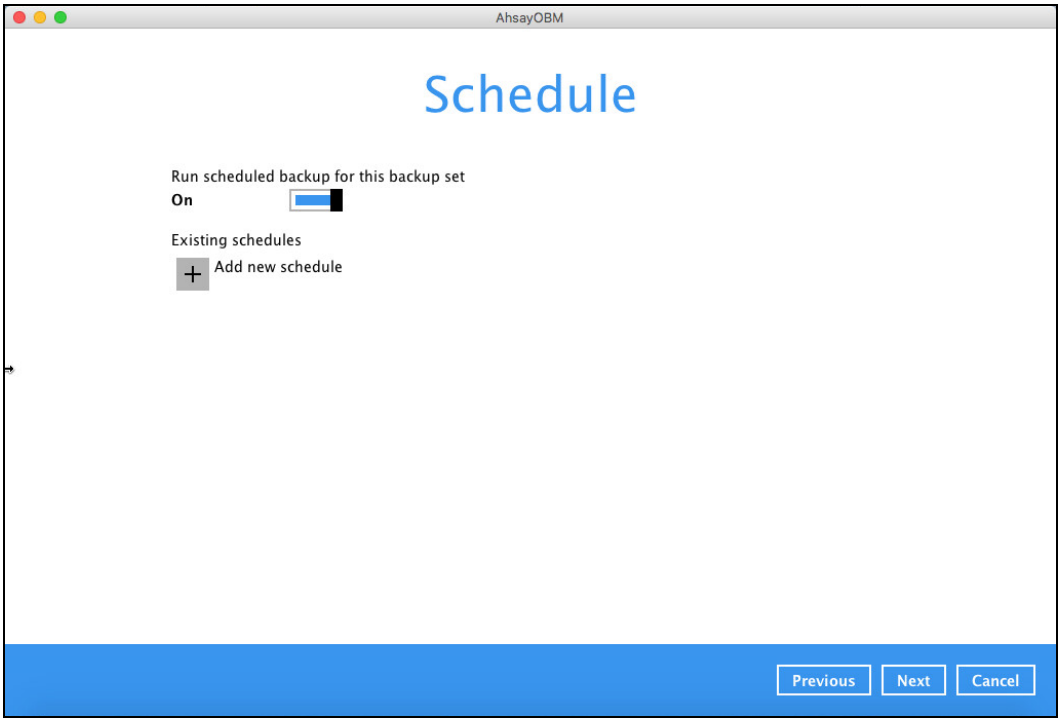


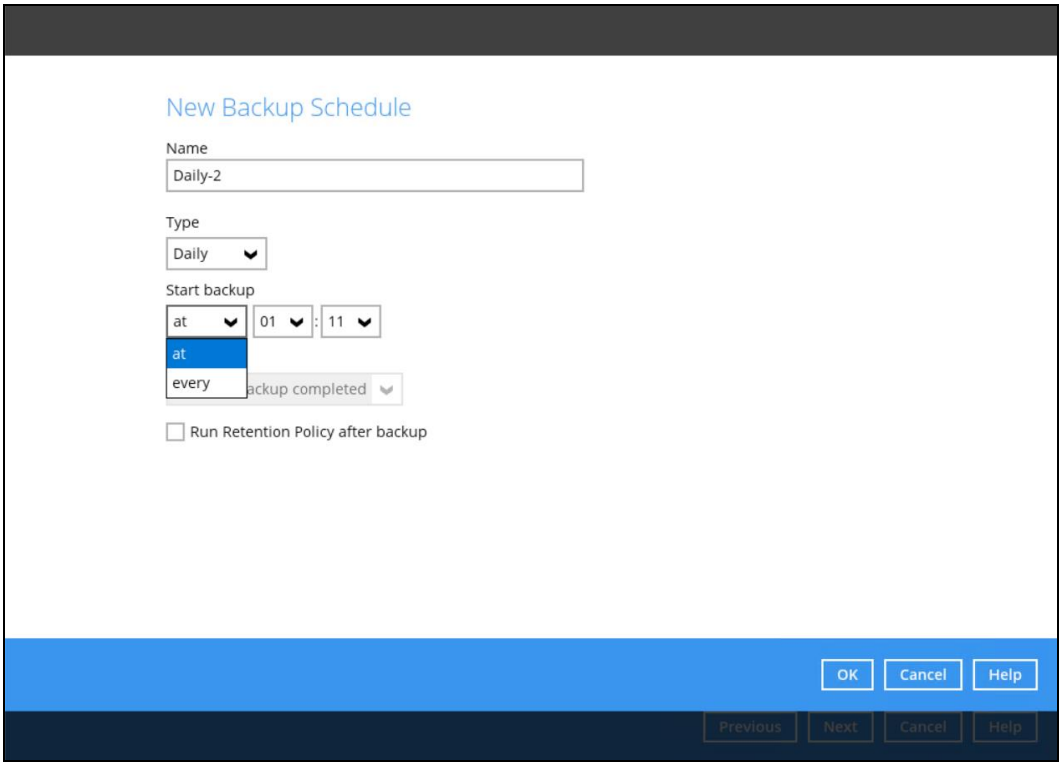
NOTE: There are limitations in selecting files and/or folders in the backup source menu. For further details, please refer to Ch. 2.13 Limitations.

Enable the **Show files** checkbox at the bottom left corner if you would like to choose individual file for backup. Click **Next** to proceed when you are done with the selection.



7. In the Schedule menu, configure a backup schedule for backup job to run automatically at your specified time interval. Slide the on/off button to turn on this feature, then click **Add new schedule** to add a new schedule, then click **Next** to proceed afterward.

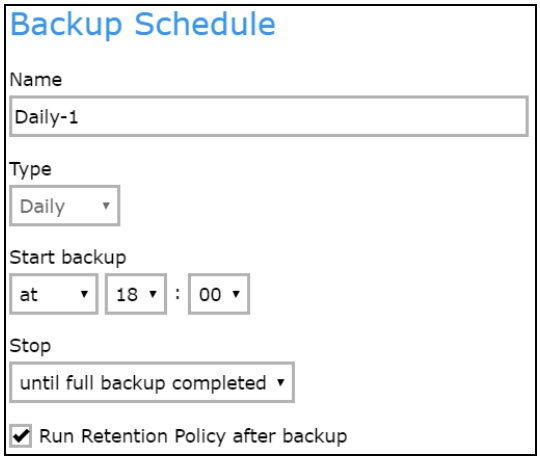




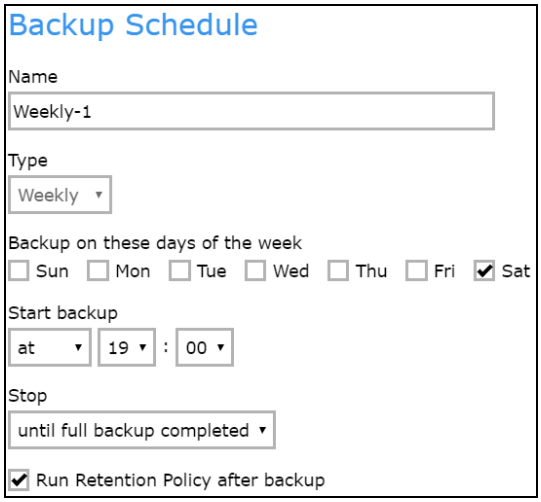
In the New Backup Schedule window, configure the following backup schedule settings.

- **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.

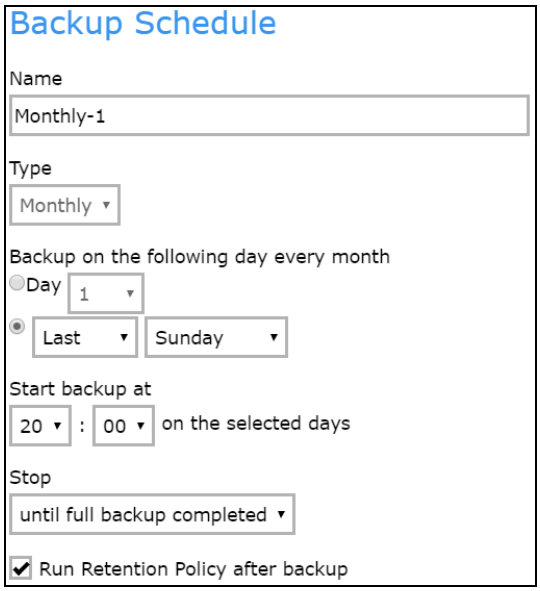
Daily – the time of the day or interval in minutes/hours when the backup job will run.



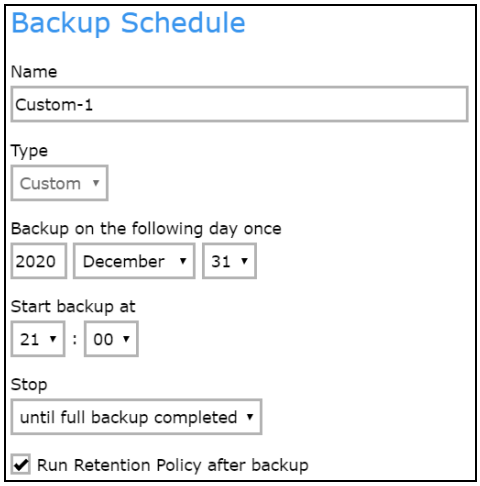
Weekly – the day of the week and the time of the day or interval in minutes/hours when the backup job will run.



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



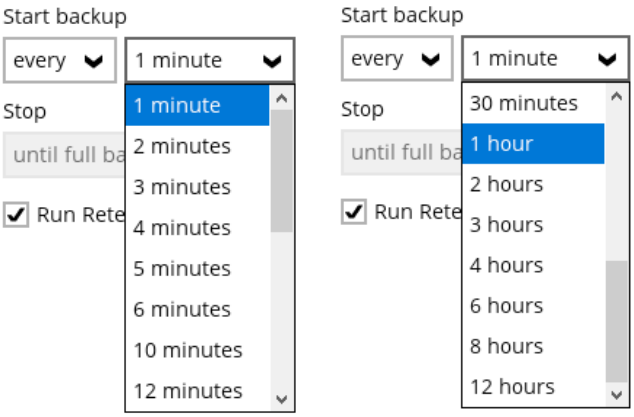
Custom – a specific date and the time when the backup job will run.



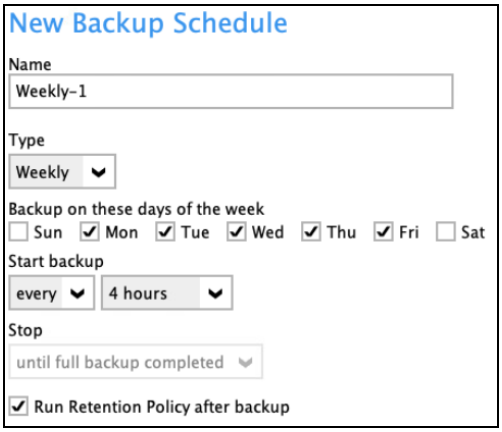
- **Start backup** – the start time of the backup job.

  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 backup set that has a daily and weekly backup schedule.



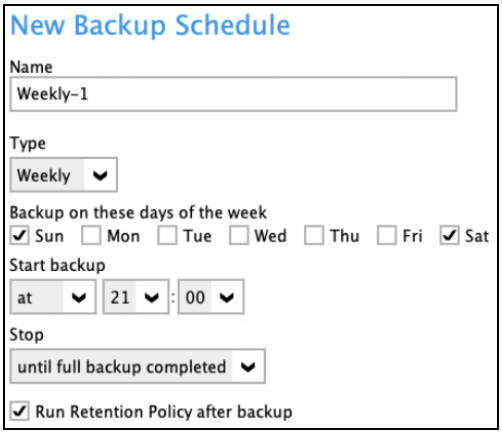


Figure 1.1 ***Figure 1.2***

Figure 1.1 – Periodic scheduled every 4 hours Monday - Friday for business hours

Figure 1.2 – Normal schedule run at 21:00 or 9:00 PM daily on Saturday & Sunday for 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.

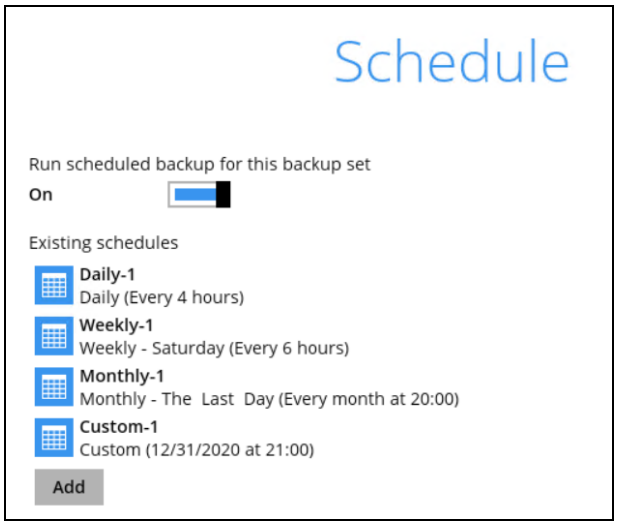
  The partially backed up data will have to be removed by running the data integrity check.

  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.

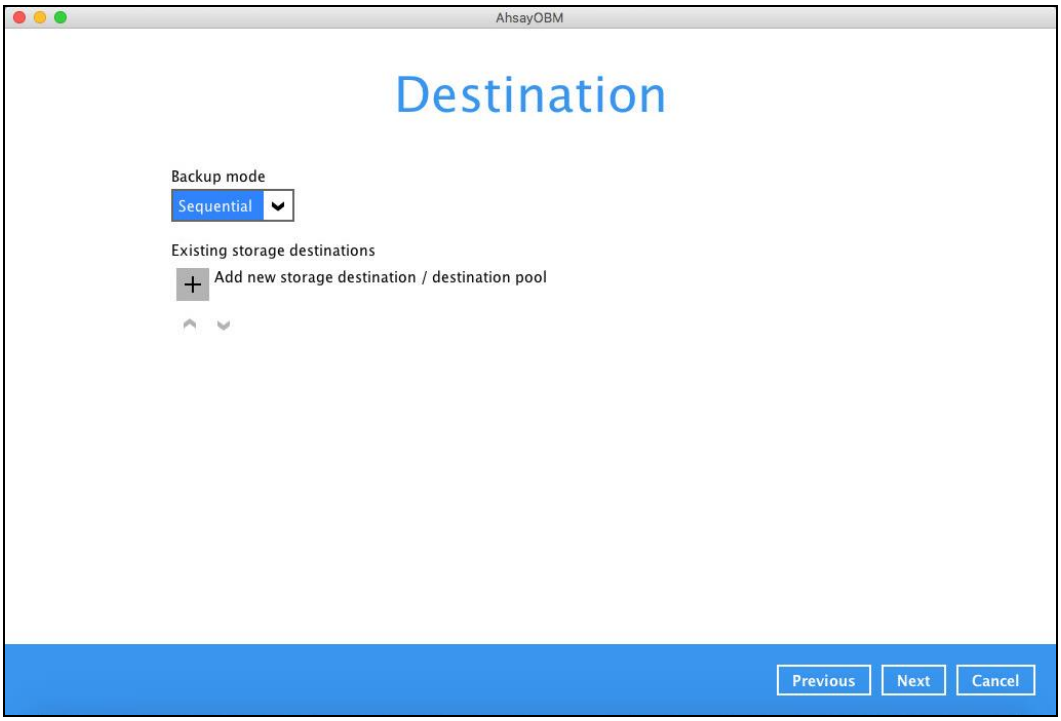
Click the **[OK]** button to save the configured backup schedule settings.

Multiple backup schedules can be created, as an example; the four types of backup schedules may look like the following.



Click Next to proceed.

8. In the **Destination** menu, select a backup destination where the backup data will be stored. Click the "+" icon next to **Add new storage destination / destination pool**.

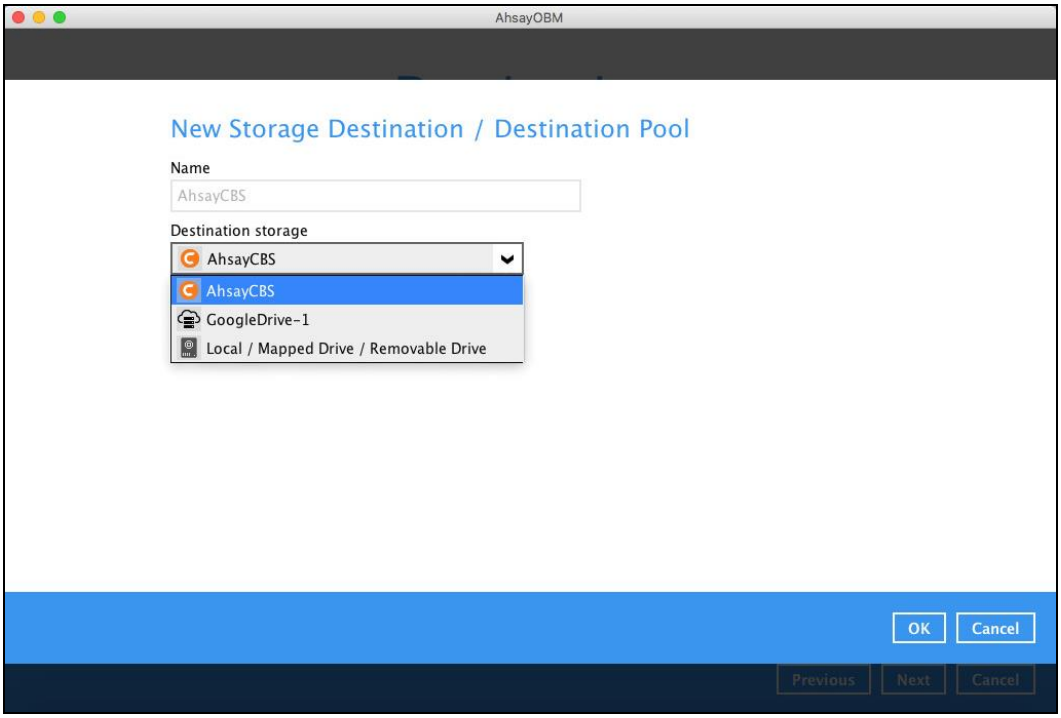


NOTE

For more details on Backup Destination, refer to this article:

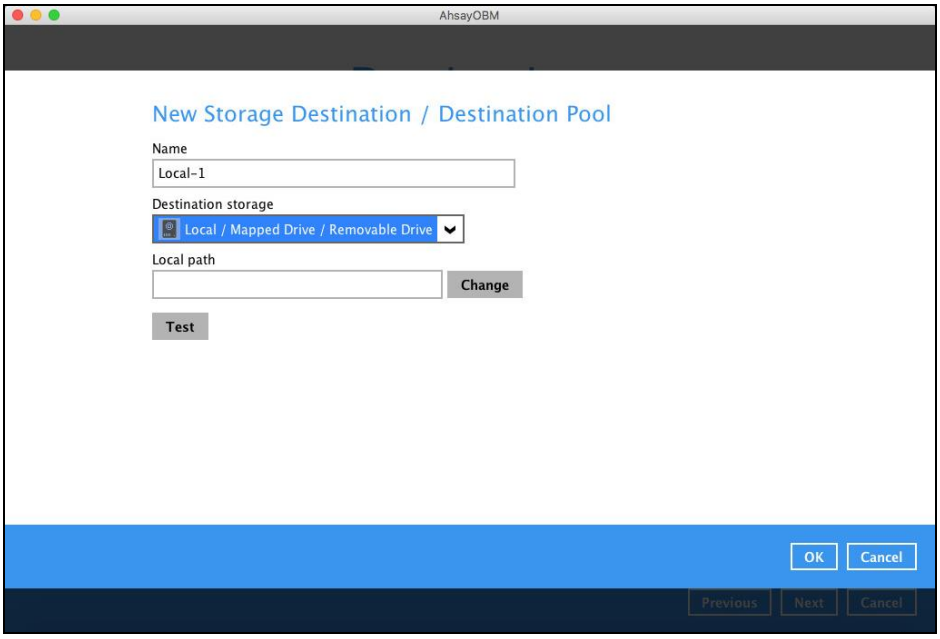
FAQ: Frequently Asked Questions on Backup Destination

9. Select the Destination storage.

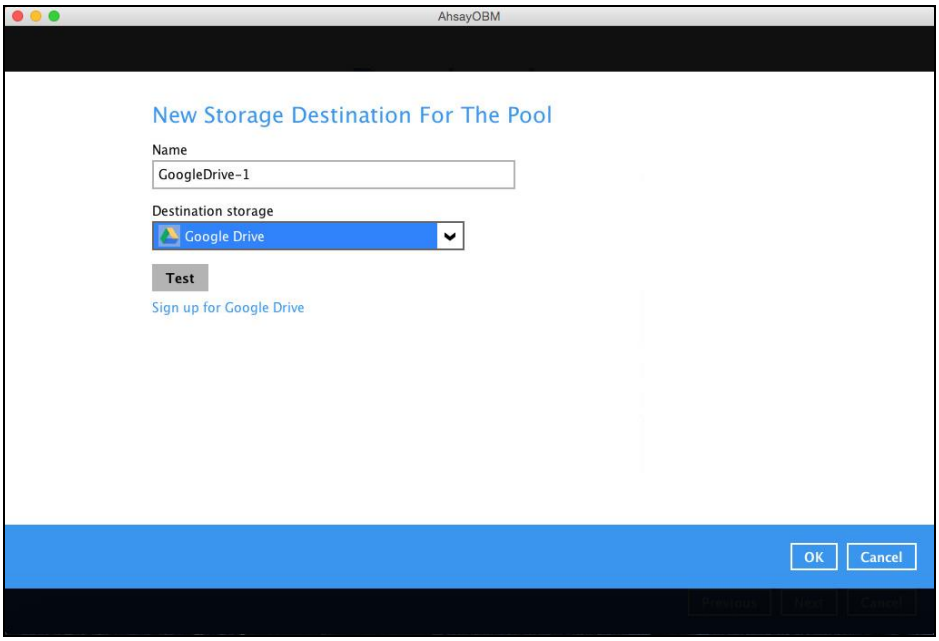


You can choose a storage combination of the Local/Mapped drive/Removable Drive, Cloud storage or FTP. Click **OK** to proceed when you are done with the settings.

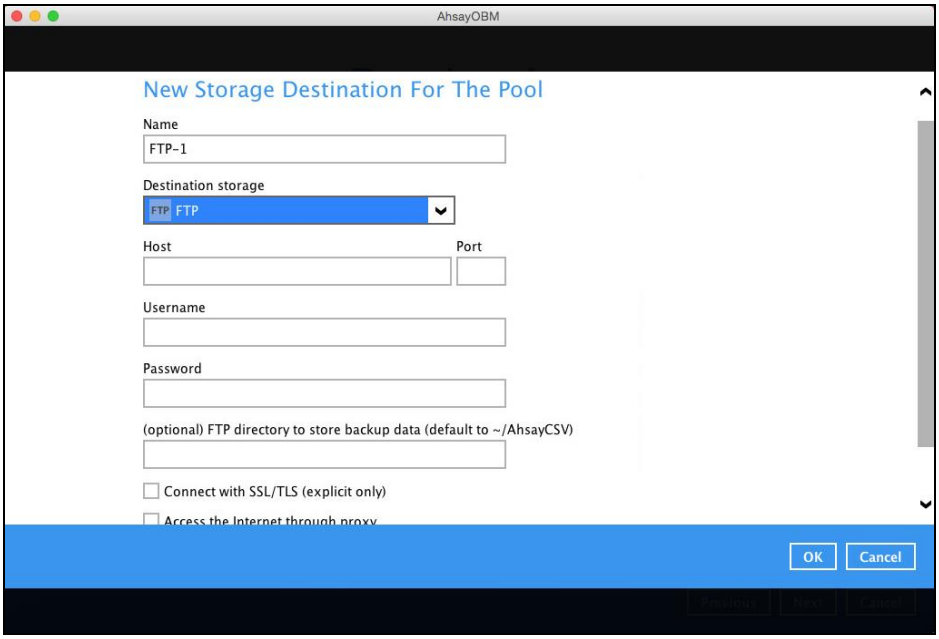
- If you have chosen the Local/Mapped Drive/Removable Drive option, click **Change** to browse to a directory path where backup data will be stored, then click **Test** to validate the path. **Test completed successfully** shows when the validation is done.



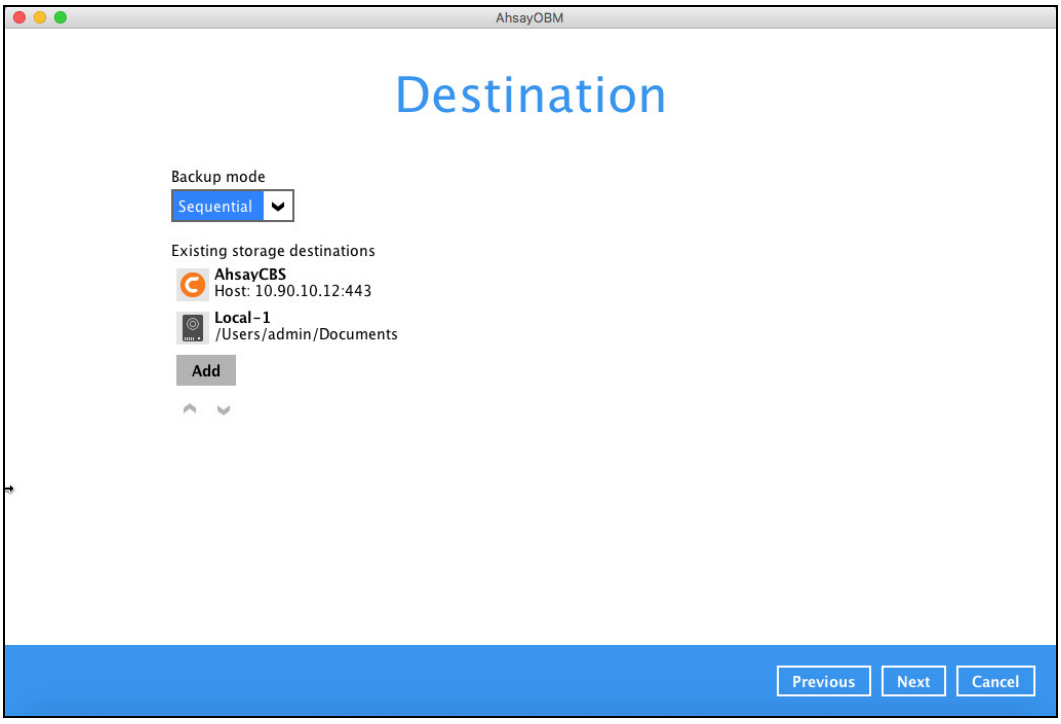
- If you have chosen the Cloud Storage, click **Test** to log in to the corresponding cloud storage service.



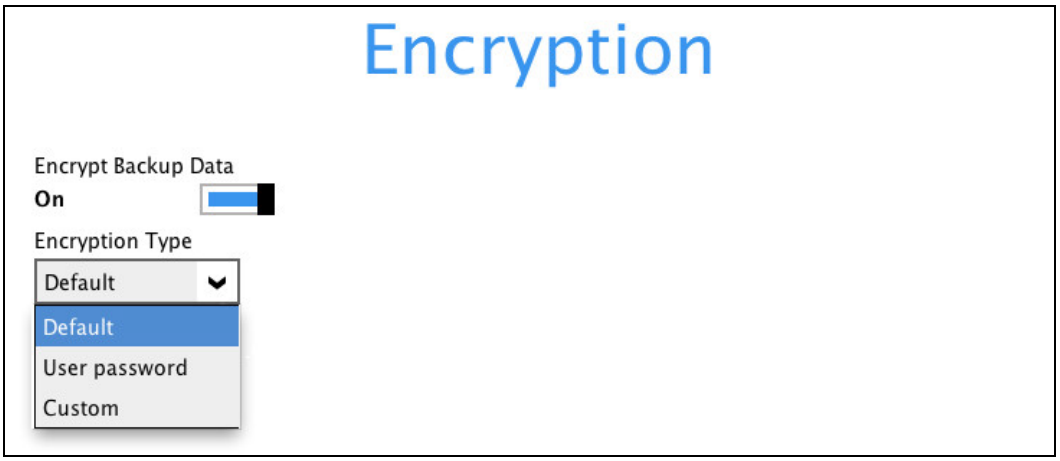
- If you have chosen the FTP as the destination, enter the the Host, Username and Password details.



10. You can add multiple storage destinations. The backup data will be uploaded to all the destinations you have selected in the order you added them. Press the icon to alter the order. Click **Next** to proceed when you are done with the selection.

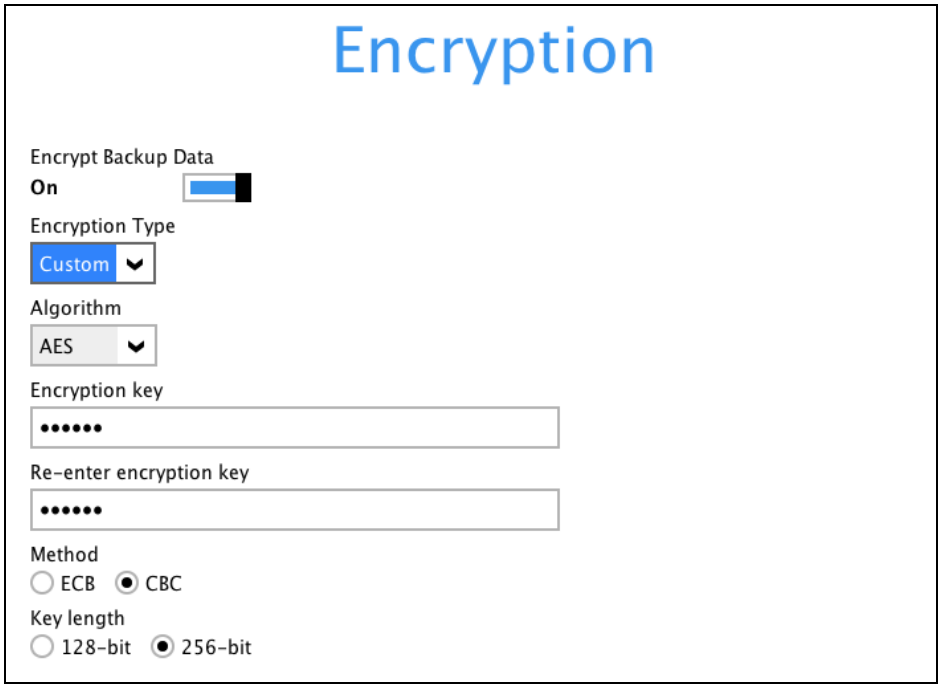


11. In the Encryption window, the default **Encrypt Backup Data** option is enabled with an encryption key preset by the system which provides the most secure protection.



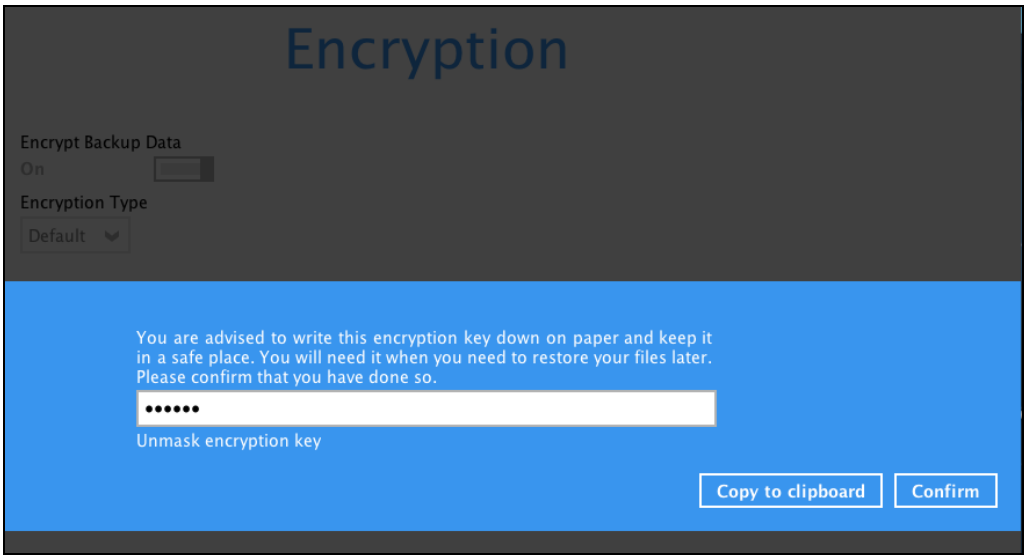
You can choose from one of the following three Encryption Type options:

- **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 set 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.



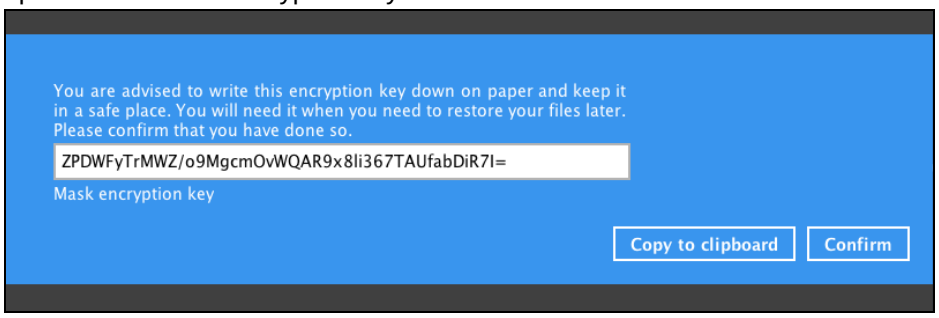
Click **Next** when you are done setting.

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

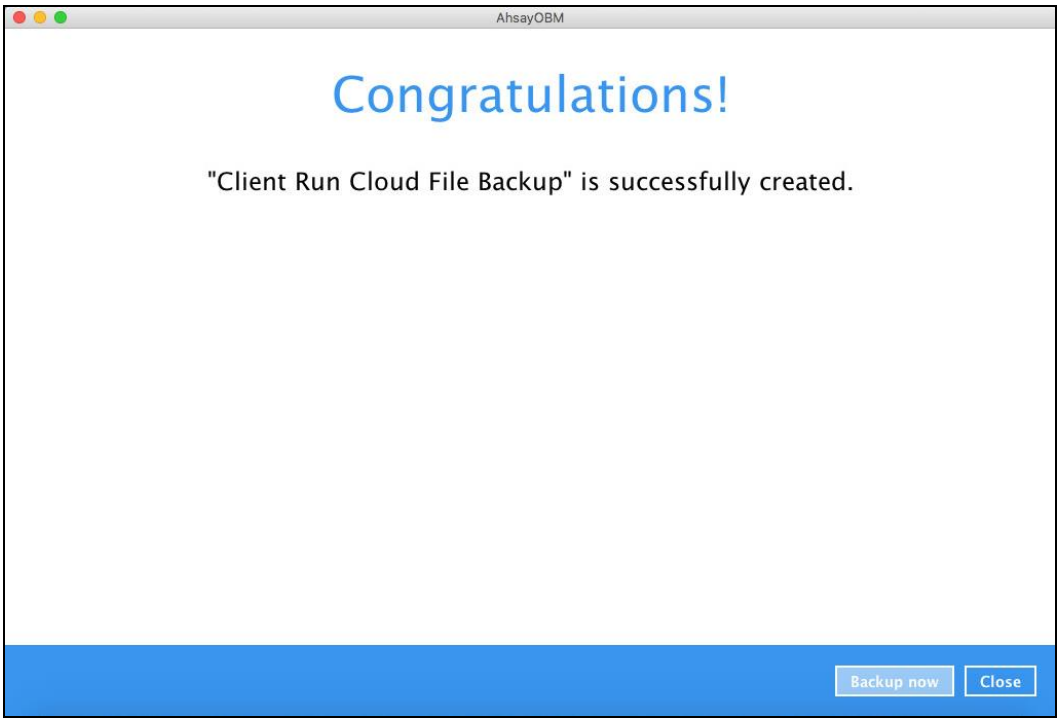


- **Copy to clipboard** – Click to copy the encryption key, then you can paste it in another location of your choice.

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

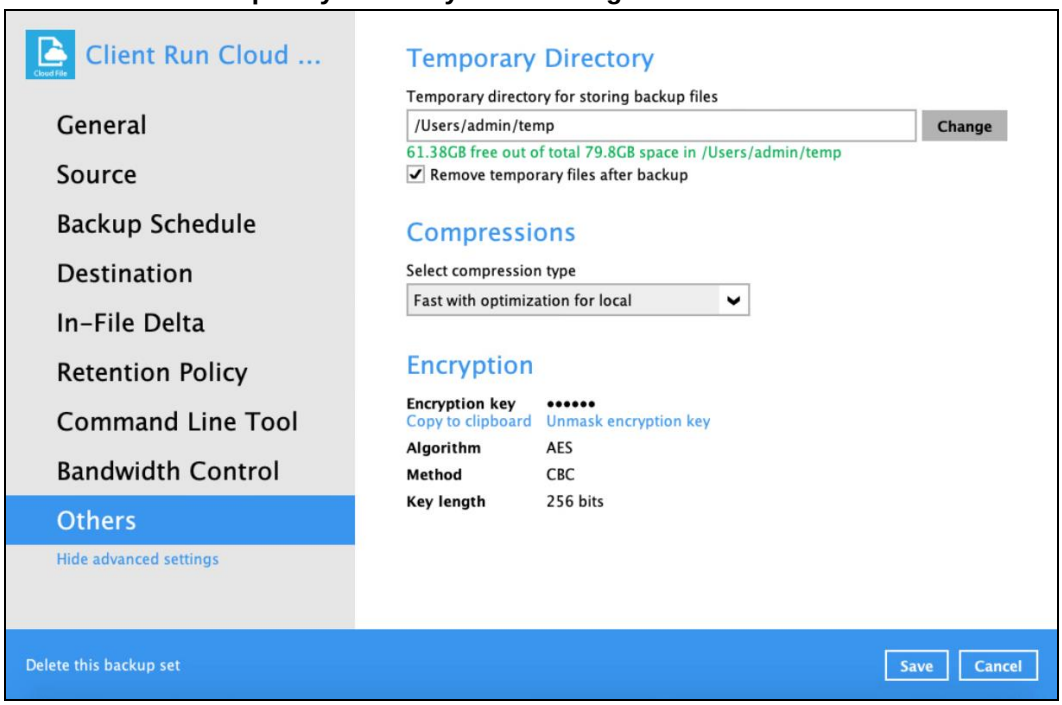
Click **Next** to create the backup set.

13. The following screen is displayed when the Cloud File backup set is created successfully.



14. Based on Best Practices and Recommendations, it is highly recommended to change the Temporary Directory. Select another location with sufficient free disk space other than /Users/admin/temp.

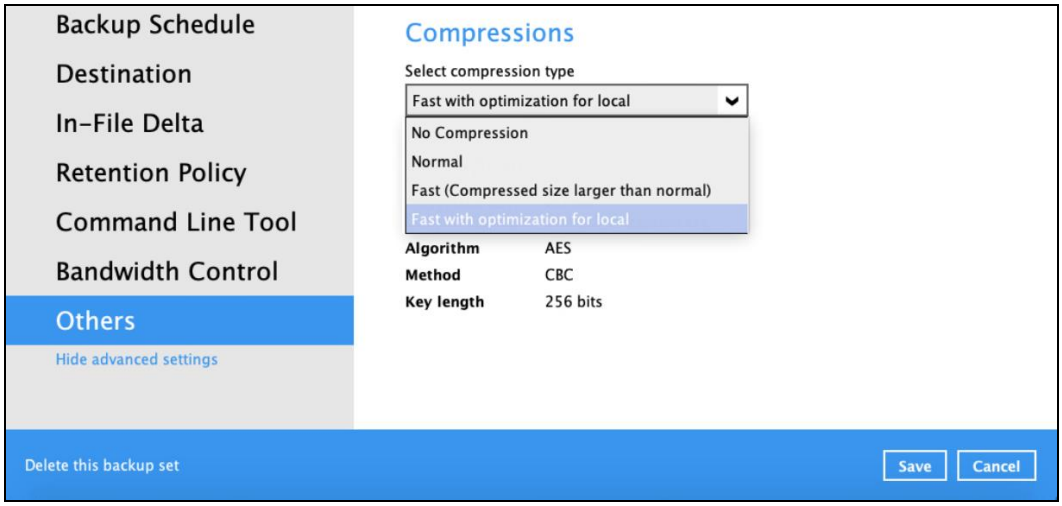
Go to **Others** > **Temporary Directory**. Click **Change** to browse for another location.



15. Optional: Select your preferred **Compression** type. By default, the compression is Fast with optimization for local.

    Go to Others > Compressions. Select from the following list:

    - No Compression
    - Normal
    - Fast (Compressed size larger than normal)
    - Fast with optimization for local



5 Overview of Run on Client Cloud File 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)**

5.1 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:

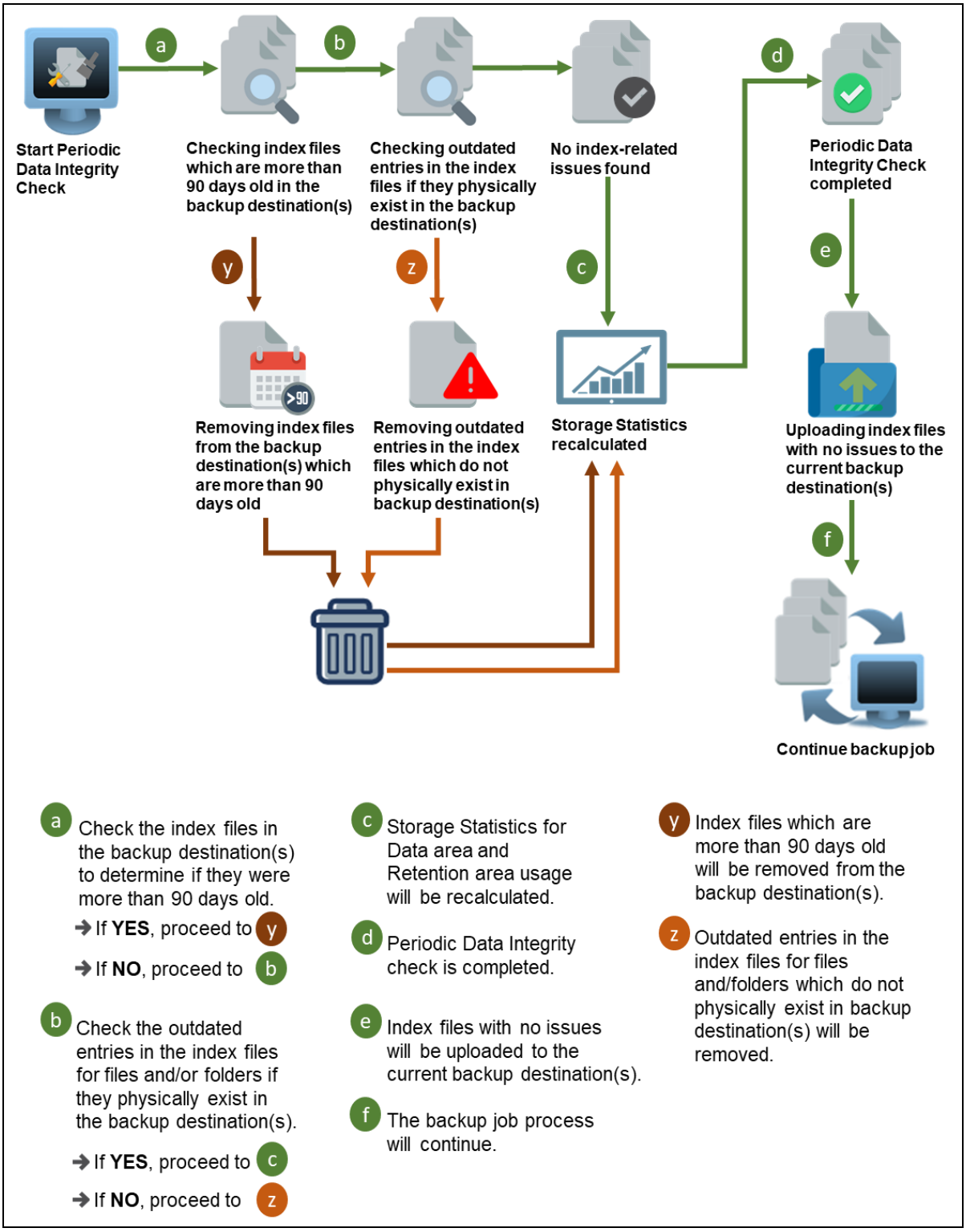
- the PDIC will run on the first backup job that falls on Wednesday; or
- if there is no active backup job(s) running from Monday to Friday, then the PDIC will run on the next available backup job.

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:

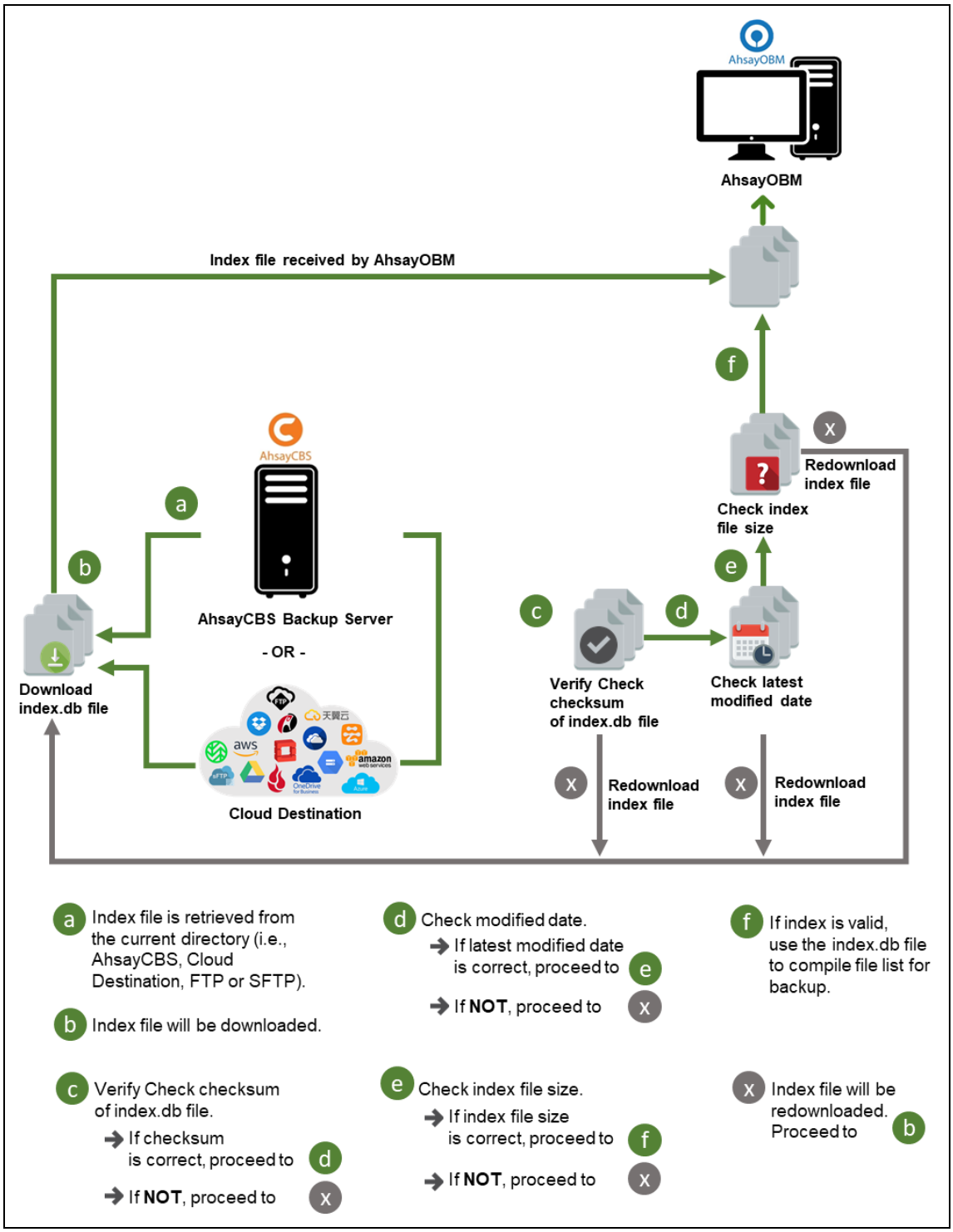
1. If AhsayOBM was upgraded to v8.5 (or above) from an older version v6, v7, or pre-8.3.6.0 version. In this case, the PDIC job will run on the first backup job after upgrade.
2. If backup jobs for a backup set are not run on a regular daily backup schedule (for example: on a weekly or monthly schedule), 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
b
d
Start Periodic Data Integrity Check
Checking index files which are more than 90 days old in the backup destination(s)
Checking outdated entries in the index files if they physically exist in the backup destination(s)
No index-related issues found
Periodic Data Integrity Check completed
y
z
c
e
>90
Removing index files from the backup destination(s) which are more than 90 days old
Removing outdated entries in the index files which do not physically exist in backup destination(s)
Storage Statistics recalculated
Uploading index files with no issues to the current backup destination(s)
f
Continue backup job
a Check the index files in the backup destination(s) to determine if they were more than 90 days old.
➔ If YES, proceed to y
➔ If NO, proceed to b
b Check the outdated entries in the index files for files and/or folders if they physically exist in the backup destination(s).
➔ If YES, proceed to c
➔ If NO, proceed to z
c Storage Statistics for Data area and Retention area usage will be recalculated.
d Periodic Data Integrity check is completed.
e Index files with no issues will be uploaded to the current backup destination(s).
f The backup job process will continue.
y Index files which are more than 90 days old will be removed from the backup destination(s).
z Outdated entries in the index files for files and/folders which do not physically exist in backup destination(s) will be removed.

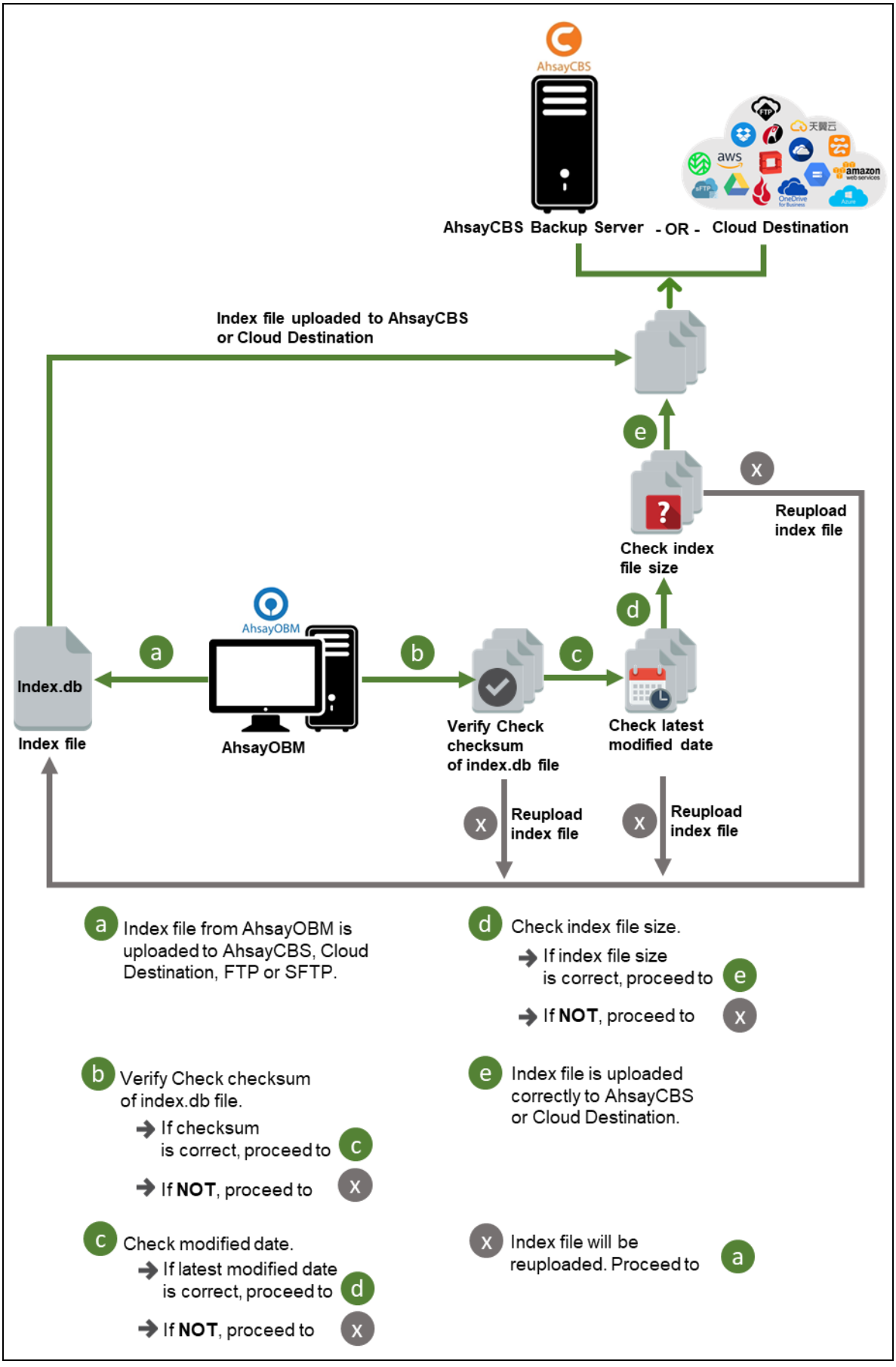
5.2 Backup Set Index Handling Process

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.

5.2.1 Start Backup Job

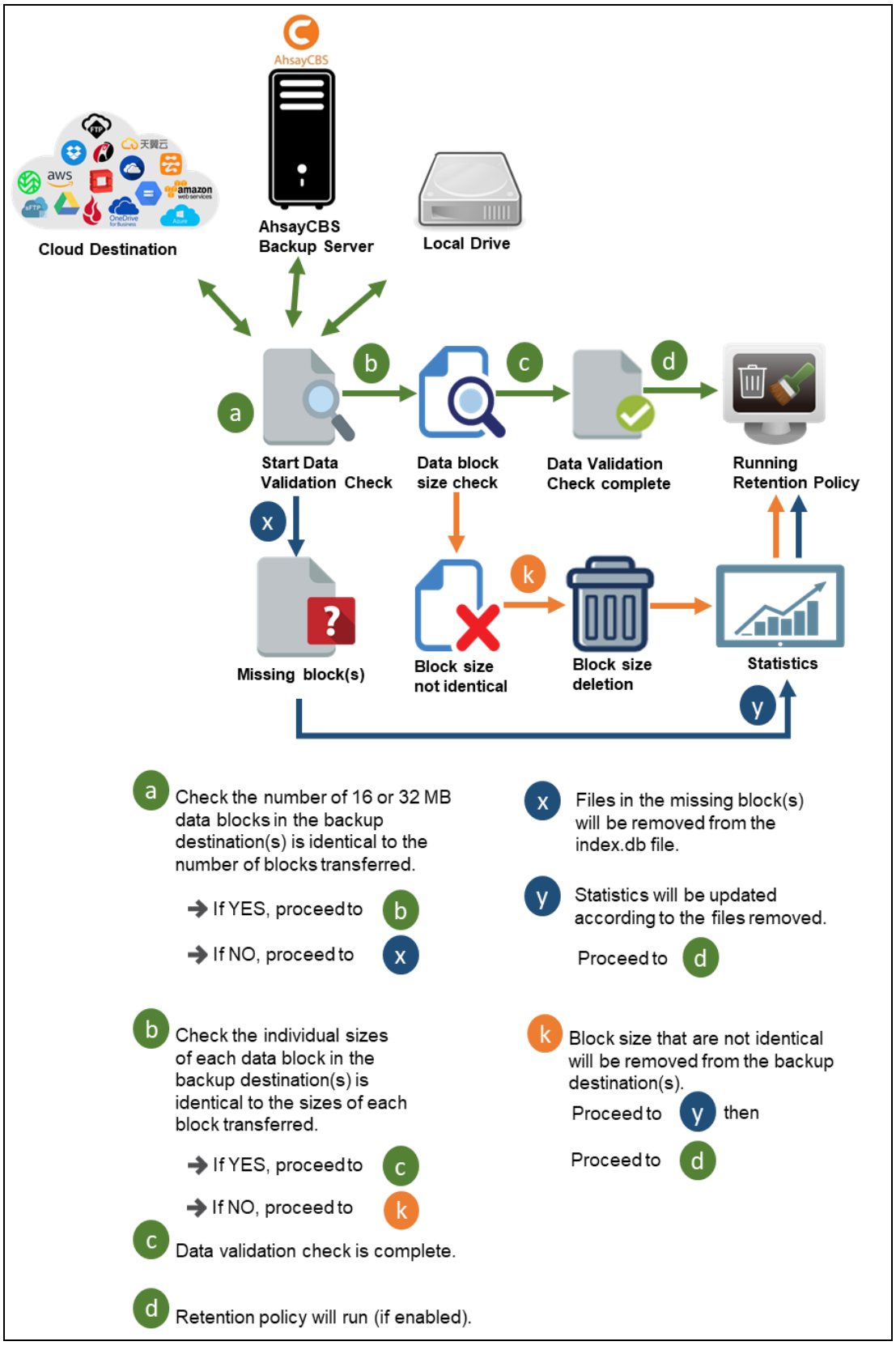


5.2.2 Completed Backup Job



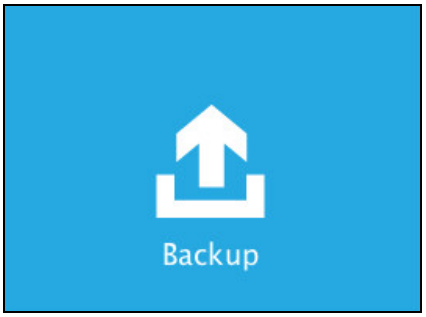
5.3 Data Validation Check Process

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.

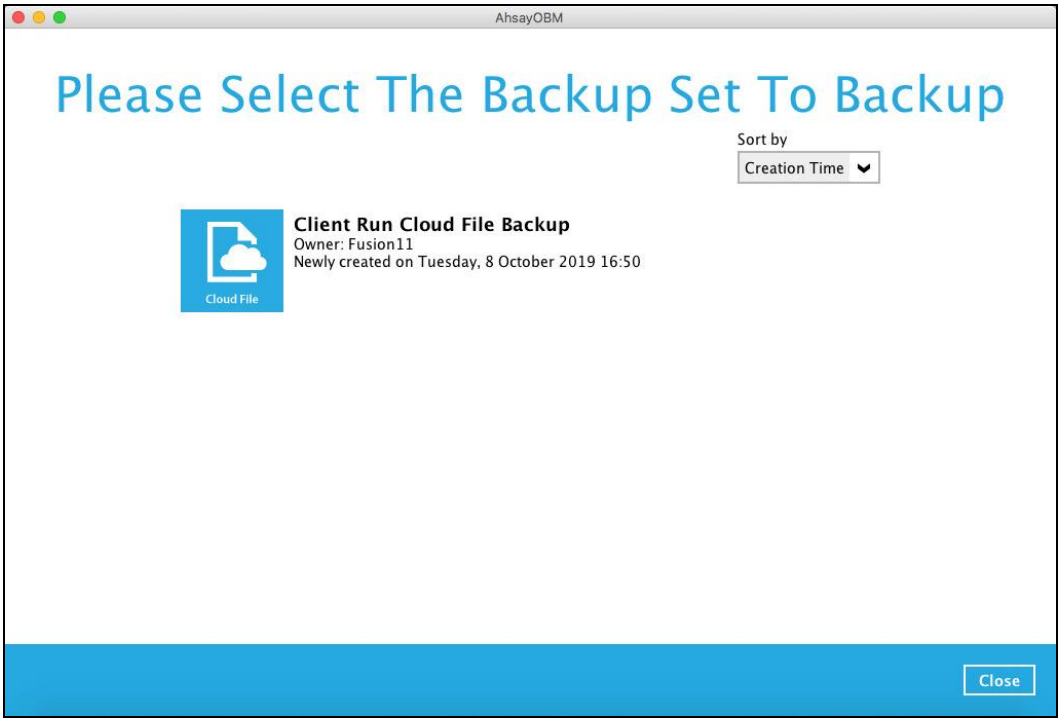


6 Running a Backup

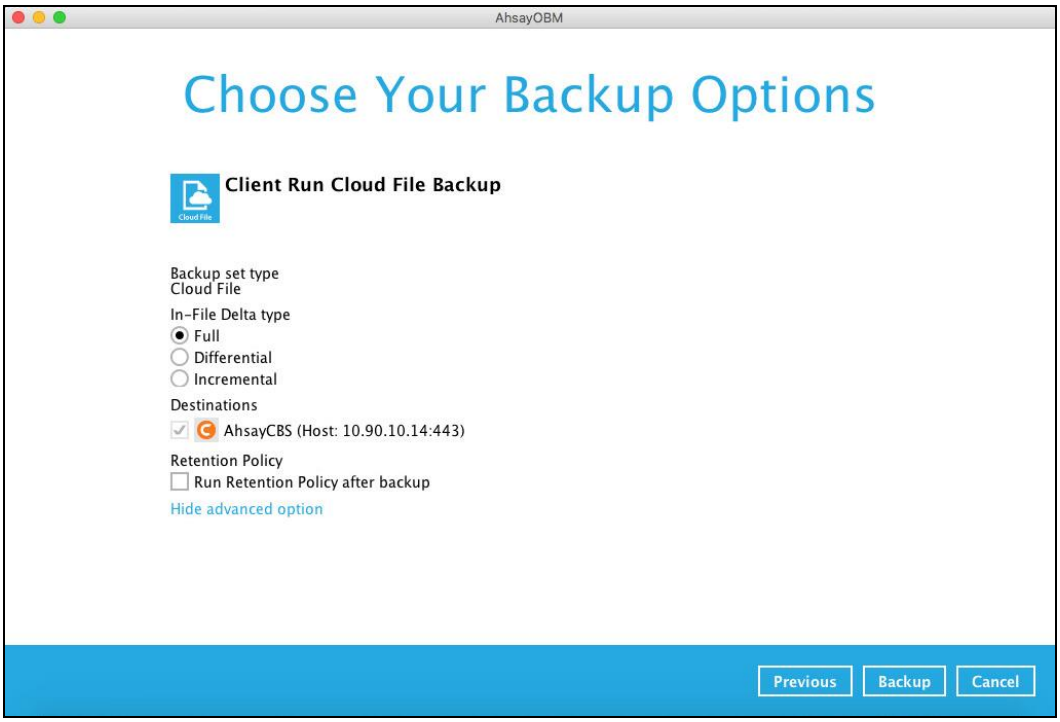
1. Click the **Backup** icon on the main interface of AhsayOBM.



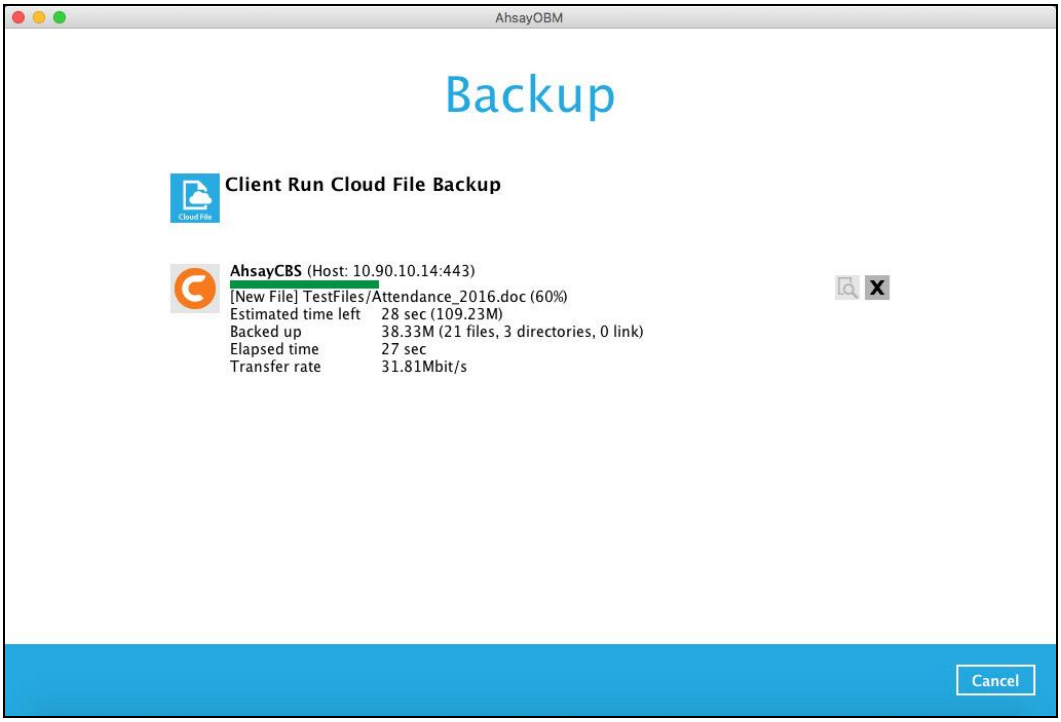
2. Select the backup set which you would like to start a backup for.



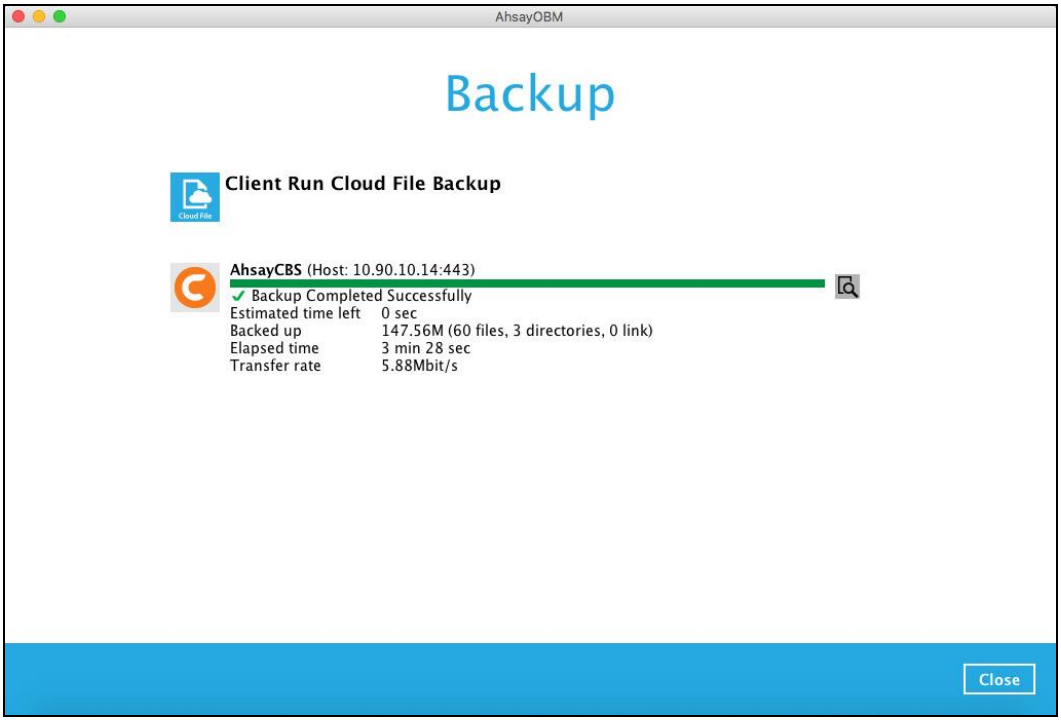
3. If you would like to modify the In-File Delta type, Destinations and Retention Policy Settings, click **Show advanced option**.



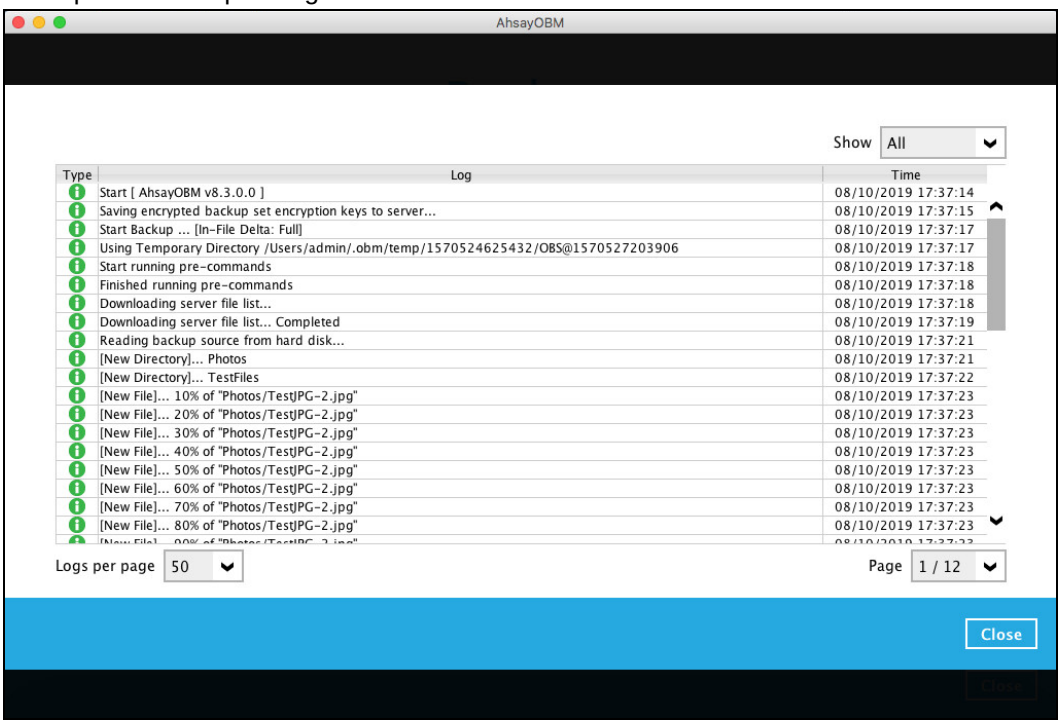
4. Click **Backup** to start the backup and wait until it is finish.



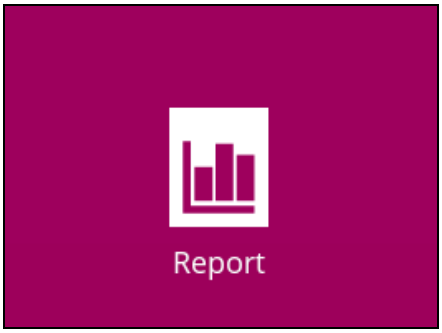
5. The backup through AhsayOBM has been successful.



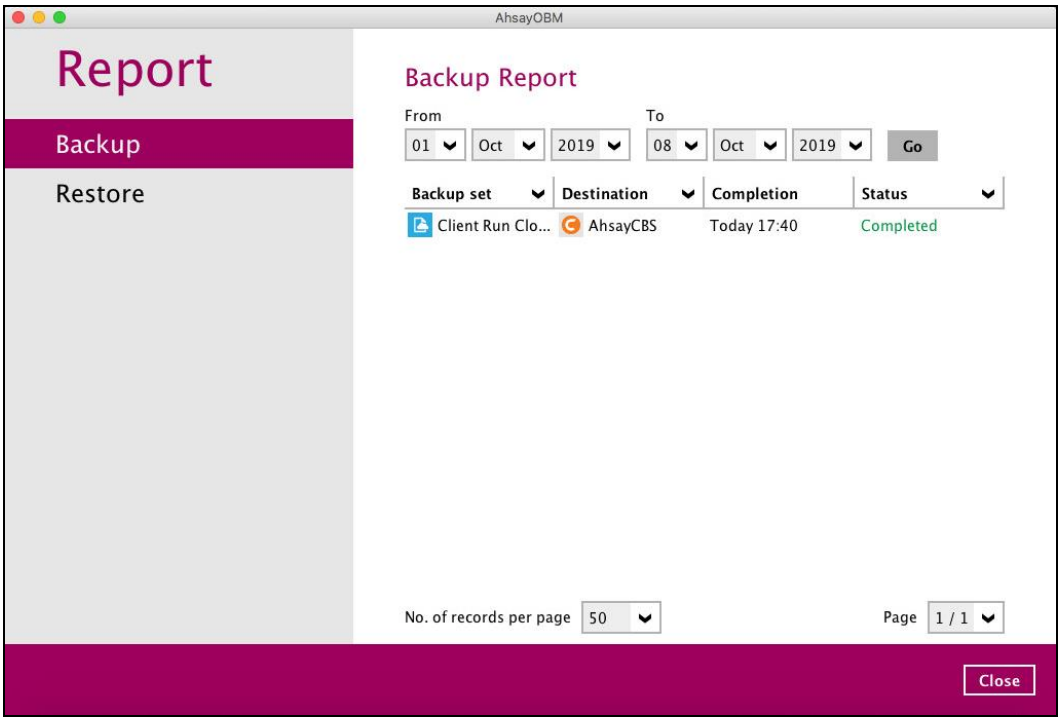
6. Check the log of your backup by clicking this icon  . It will show you the log of your backup with corresponding date and time.



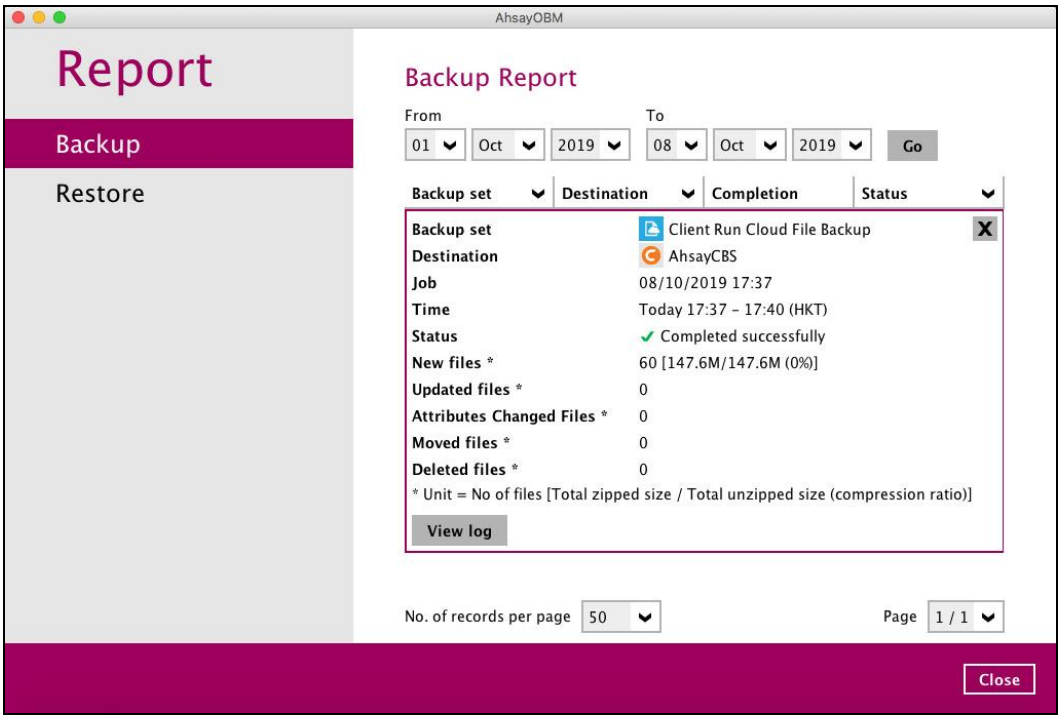
To view the backup report, return to the AhsayOBM main interface then click the following icon.

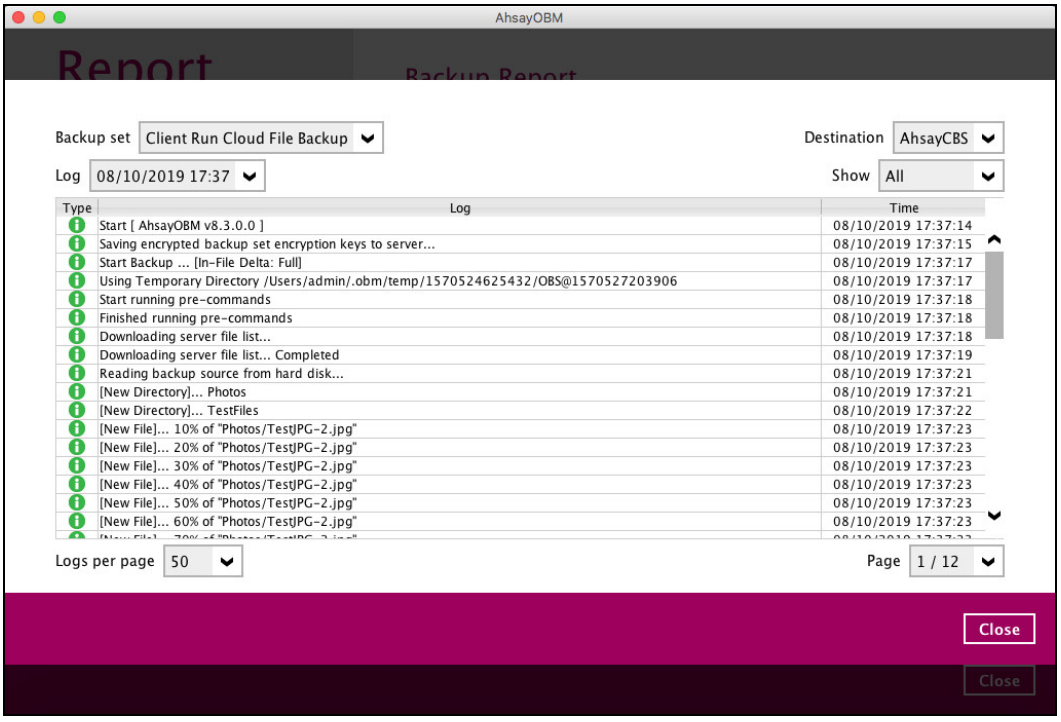


In this Backup Report screen, you can see the backup set with corresponding destination, completion date and time, and status.

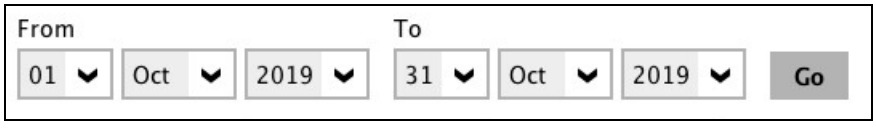


Click the backup report and the summary of the backup will be displayed. You can also click the **View Log**; this will redirect you to the log summary of your backup.

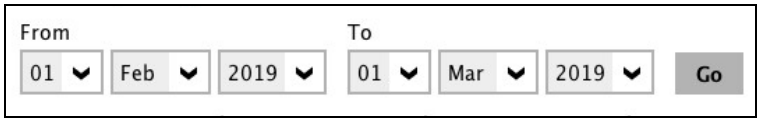


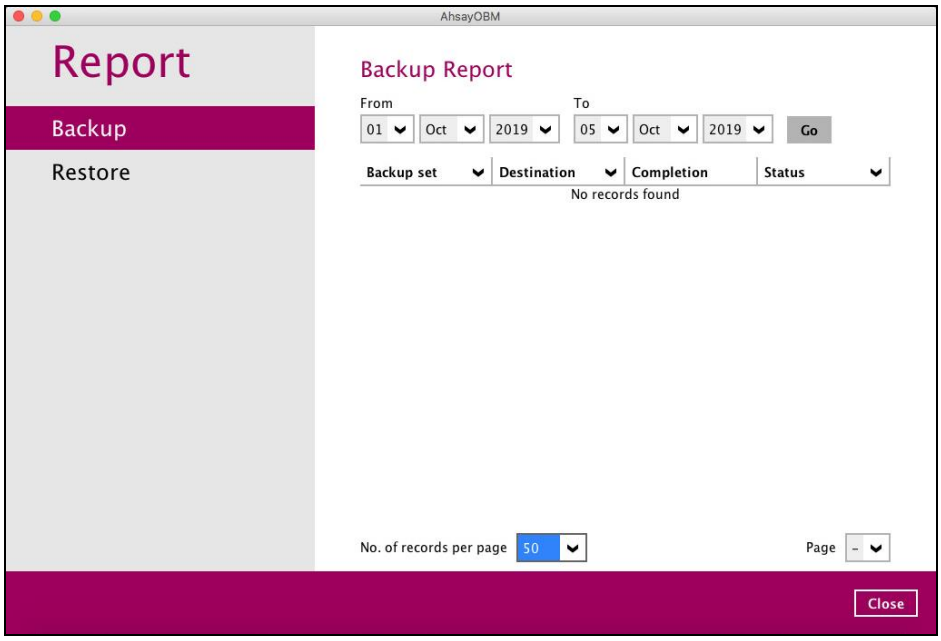


You can also search for backup reports from a specific period of date. For example, we have the **From** date which is, **01 Oct 2019** and the To date which is, **31 October 2019**. Then click the Go button to generate the available reports.



If this is a valid range of dates then backup reports will be displayed unless there were no backup running on the specified dates. A message of **No records found** will be indicated.





7 Restoring with a Cloud File Backup Set

Using AhsayOBM to do the restoration has three (3) options. Through Local machine, Original location, and Alternate location. Below are brief descriptions of the said features. After this quick walkthrough you will see the step-by-step instructions with corresponding screen shots on how to restore your data using the following options below.

- **Local machine**

  Restore your data to your local computer where the AhsayOBM is running.

- **Original location**

  Aside from the location machine option, you are also able to restore your data to your original location, on the cloud storage, where you backed them up.

- **Alternate location**

  Besides the two options above, you can also restore your data to an alternate location which is through the same cloud storage but on a different folder.

NOTE

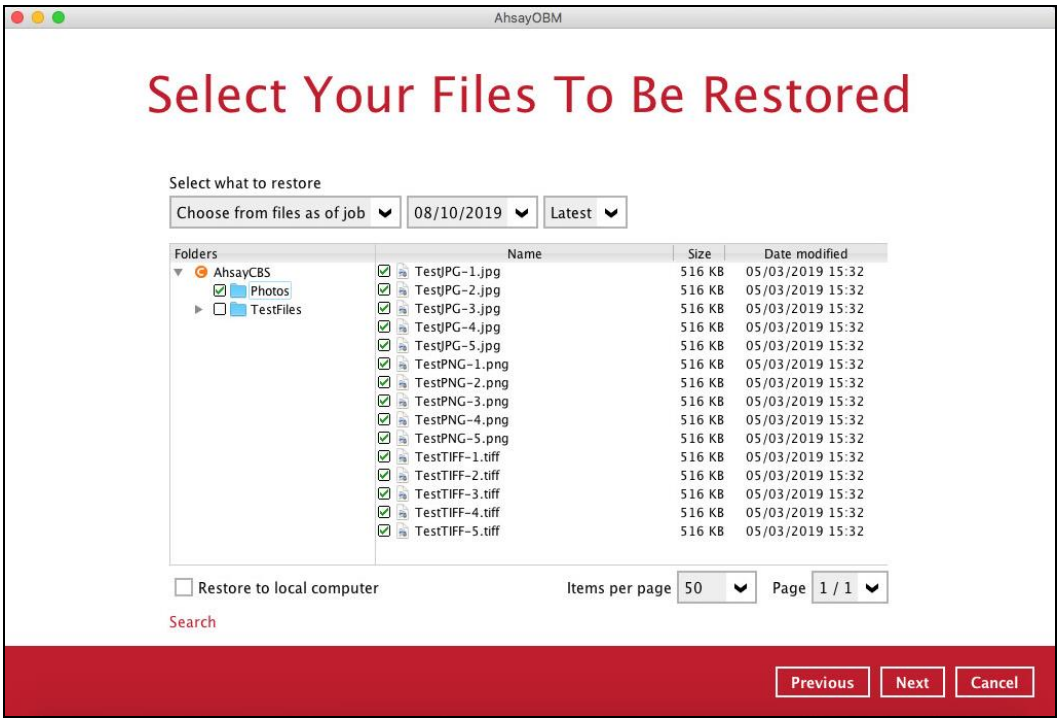
Login to the AhsayOBM application according to the instruction provided in the chapter on Log in to AhsayOBM.

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

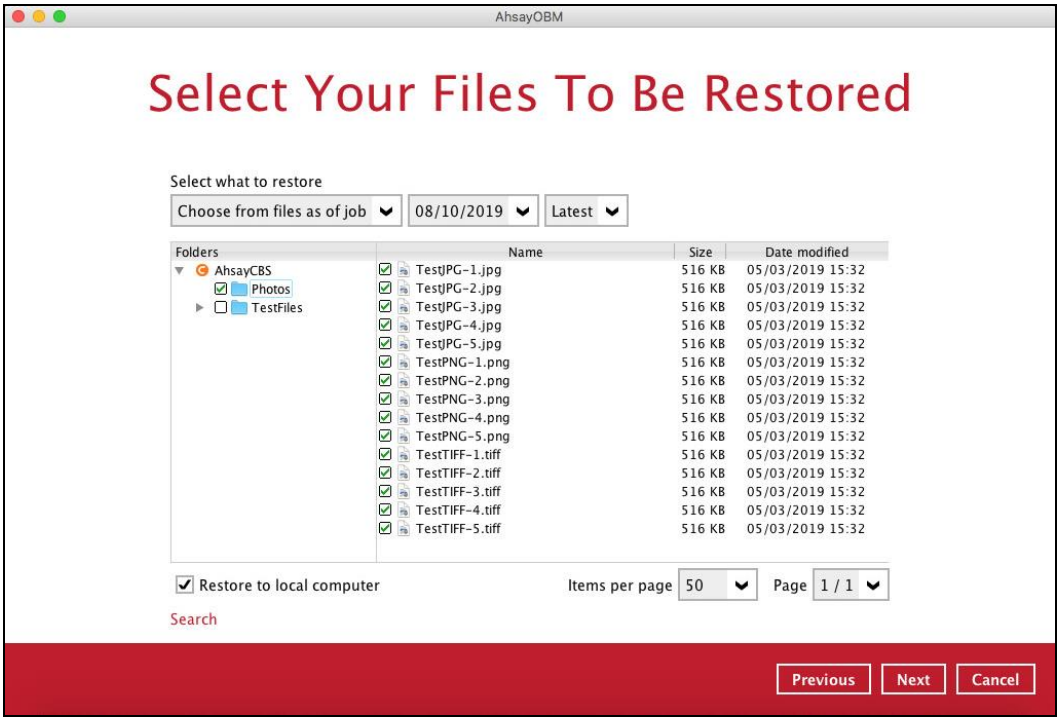
2. Select the backup set that you would like to restore from.

3. Select the backup destination that contains the data that you would like to restore.

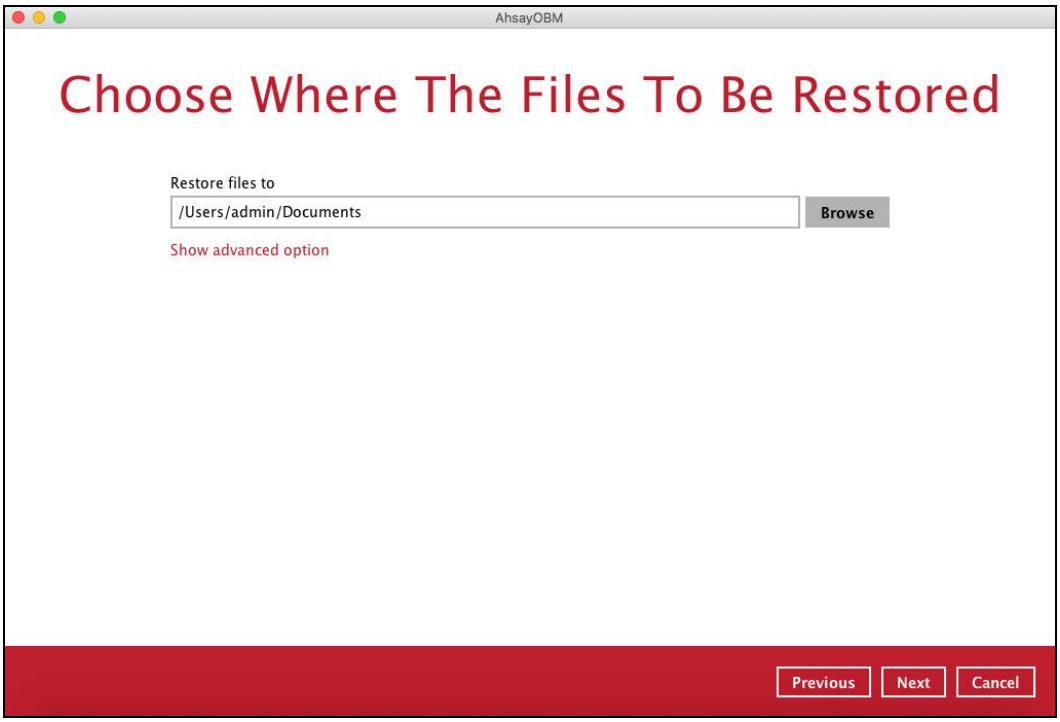
4. Select to restore from a specific backup job, or the latest job available from the **Select what to restore** drop down menu.



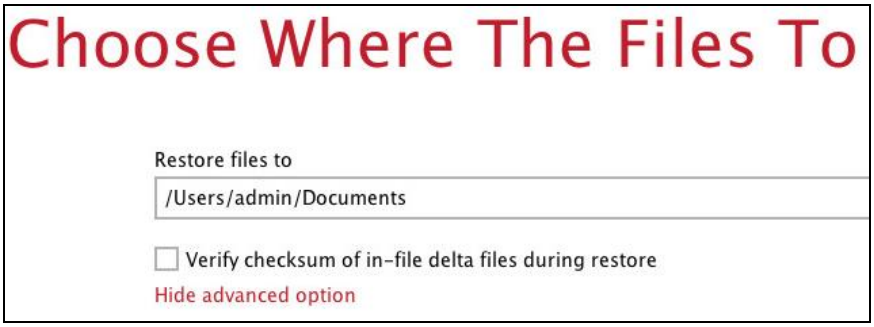
5. Select **Restore to local computer** if you want to restore the backed-up data to the location computer. Click **Next** to continue.



6. If **Restore to local computer** is enabled, browse to the corresponding directory path on the local computer that you want the data to be restored to.



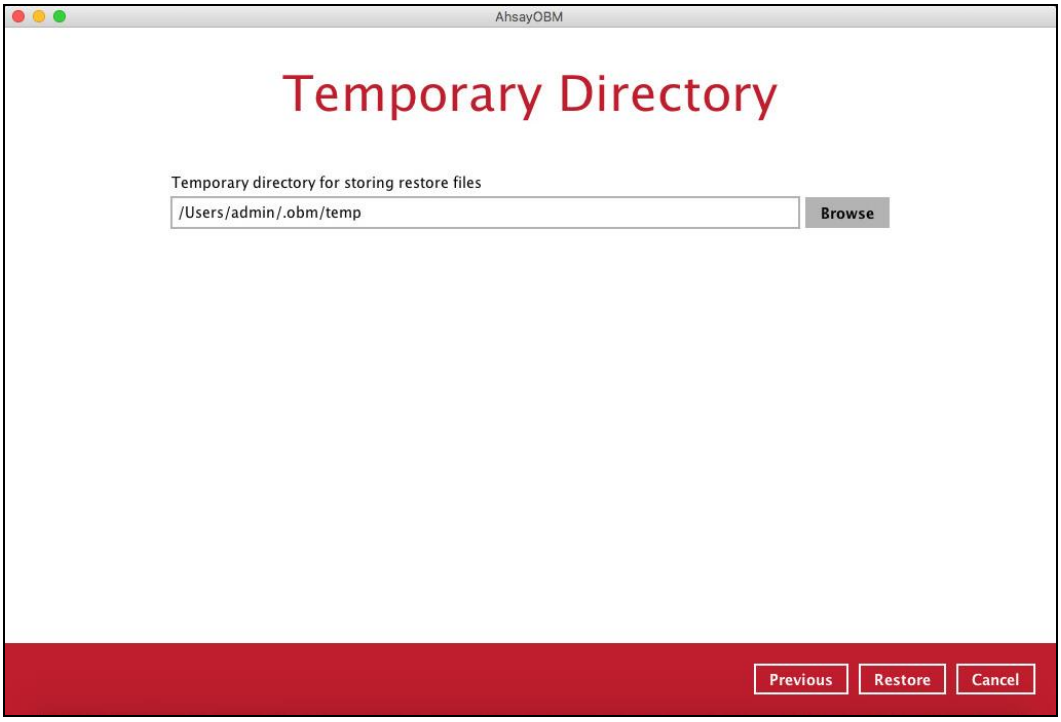
Click **Show advanced option** to configure other restore settings.



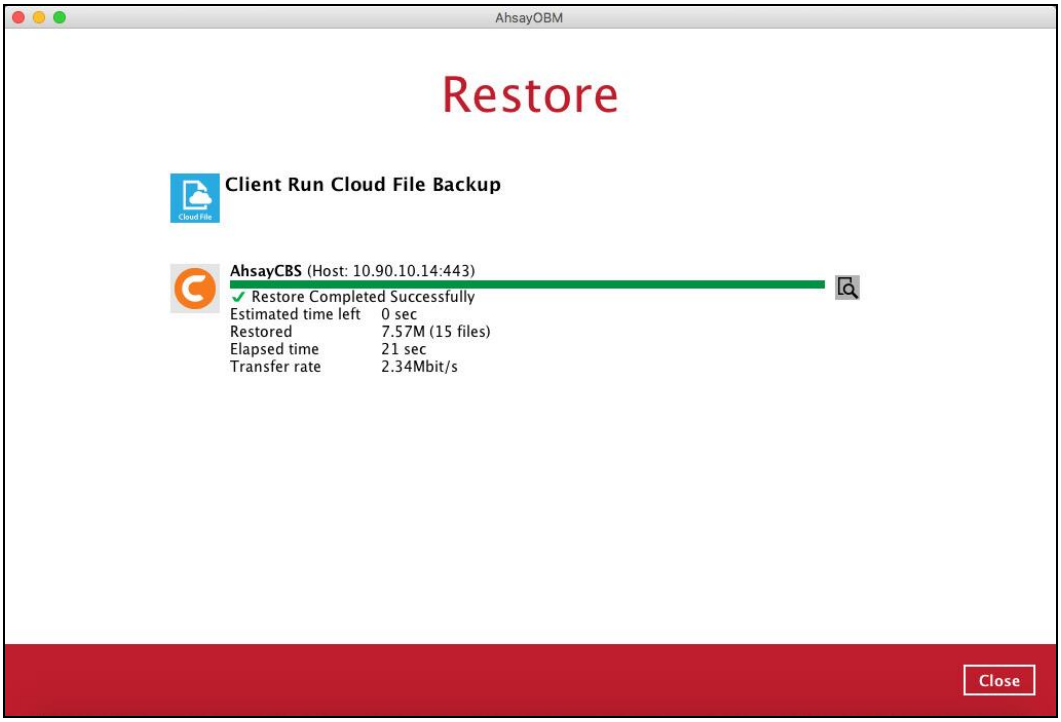
- **Verify checksum of in-file delta files during restore**

By enabling this option, the checksum of in-file delta files will be verified during the restore process. This will check the data for errors during the restore process and create a data summary of the in-file delta files which will be included in the report.

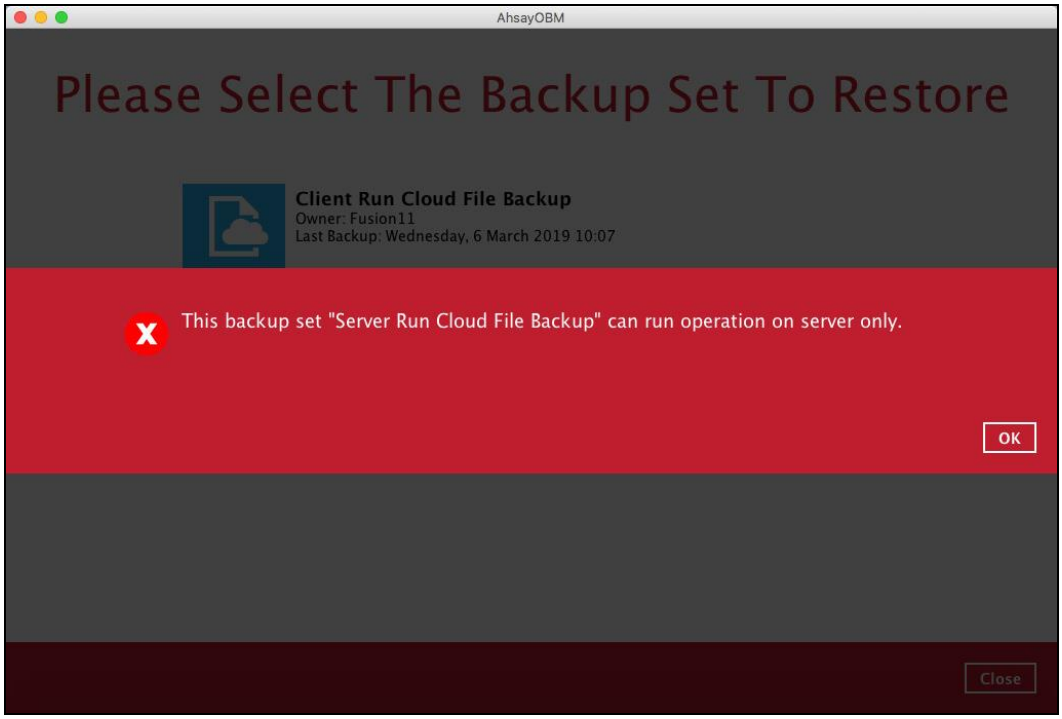
7. Select the temporary directory for storing temporary files.



8. Click **Restore** to start the restoration. The following screen is displayed when the files are restored successfully.



Important: *Data of a **Run on Server** Cloud File backup set can only be restored via the AhsayCBS web console. The following error message will be displayed if you try to restore data of a **Run on Server** Cloud File backup set via the AhsayOBM user interface.*


AhsayOBM
Please Select The Backup Set To Restore
Client Run Cloud File Backup
Owner: Fusion11
Last Backup: Wednesday, 6 March 2019 10:07
This backup set "Server Run Cloud File Backup" can run operation on server only.
OK
Close

8 Contacting Ahsay

8.1 Technical Assistance

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

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

8.2 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.