Ahsay Backup

Ahsay Online Backup Manager v8

Cloud File Backup & Restore Guide for Windows

Ahsay Systems Corporation Limited

25 January 2019

A wholly owned subsidiary of
Ahsay Backup Software Development Company Limited
HKEx Stock Code: 8290

Copyright Notice

Trademarks

Disclaimer

Revision History

Date	Descriptions	Type of modification
25 January 2019	Updated the list of Cloud Destinations Backup in Ch. 1; Updated the FAQ Link for the Hardware Requirement in Ch. 2.1; Updated the FAQ Link for the Software Requirement in Ch. 2.2; Updated screen shots for the creation of Cloud File Backup Set in AhsayOBM, updated the FAQ Link for the Backup Destination, updated the Destination Storage, removed the Single Storage and Destination Pool, and updated the FAQ Link on managing the Encryption Key in Ch. 4.1; Updated screen shots for the creation of Cloud File Backup Set in AhsayCBS User Web Console and Added the destination screen with existing storage destinations in Ch. 4.2; Updated screen shots for the start of manual backup in AhsayOBM and added the steps to generate the backup report in Ch. 6.1; Updated screen shots for the start of manual backup in AhsayCBS User Web Console and added the steps to generate the backup report Ch. 6.2; Updated the screen shots for the configuration of backup schedule in AhsayOBM in Ch. 6.3; Updated the screen shots for the configuration of backup schedule in AhsayCBS User Web Console in Ch. 6.4; Updated the restoration process using the AhsayOBM, added the Show Advanced Options, and Restore Options in Ch. 7.1; Updated the restoration process using the AhsayCBS User Web Console, added the Show Advanced Options, and Restore Options in Ch. 7.2; Updated screen shots in Appendix A;	New/ Modification

Table of Contents

1 Overview

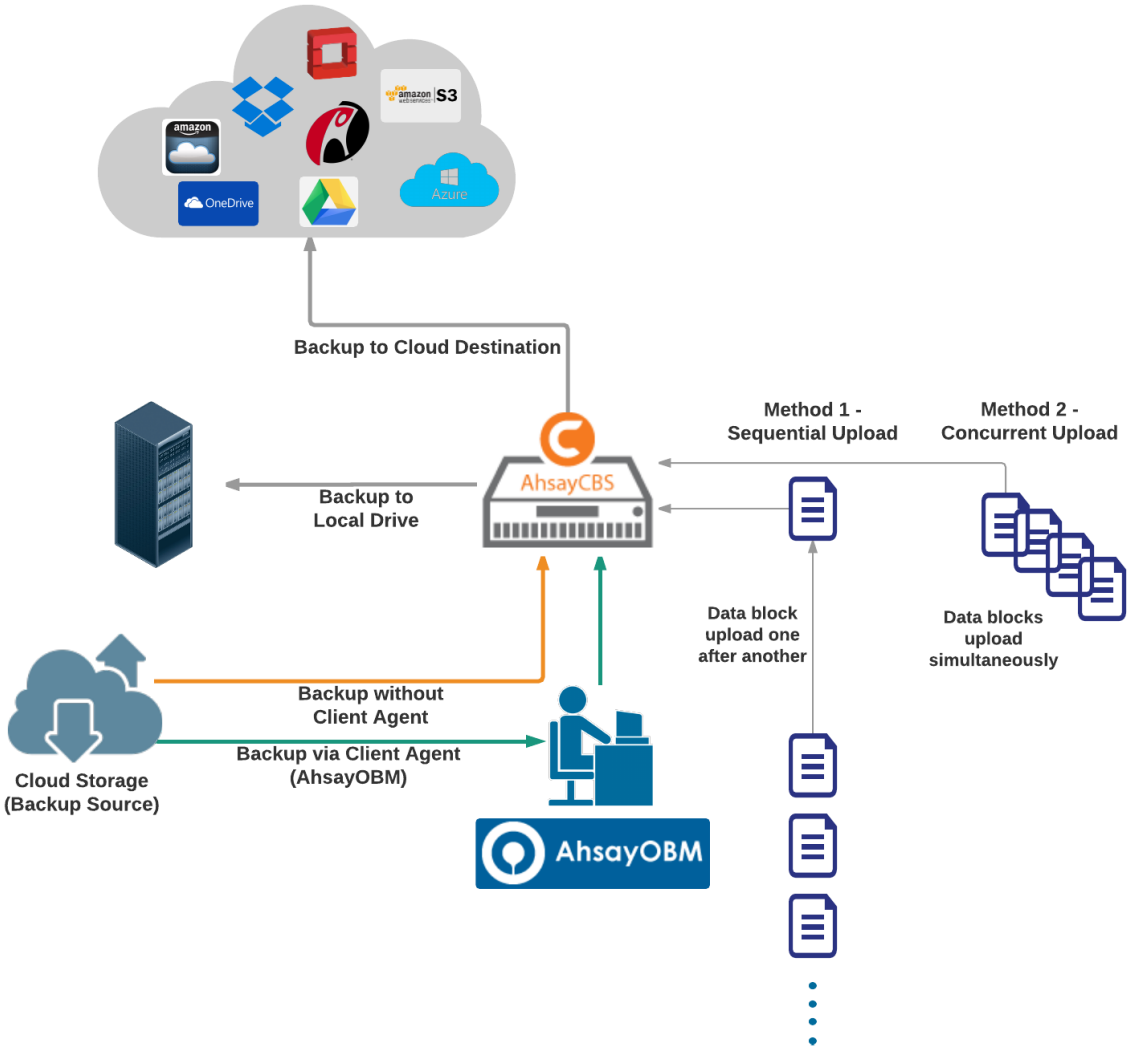
What is this software?

Ahsay brings you specialized client backup software, namely AhsayOBM, to provide a set of tools to protect your data on cloud storage. This includes backup and recovery of individual files with versioning and retention policy to protect your data on cloud storages.

System Architecture

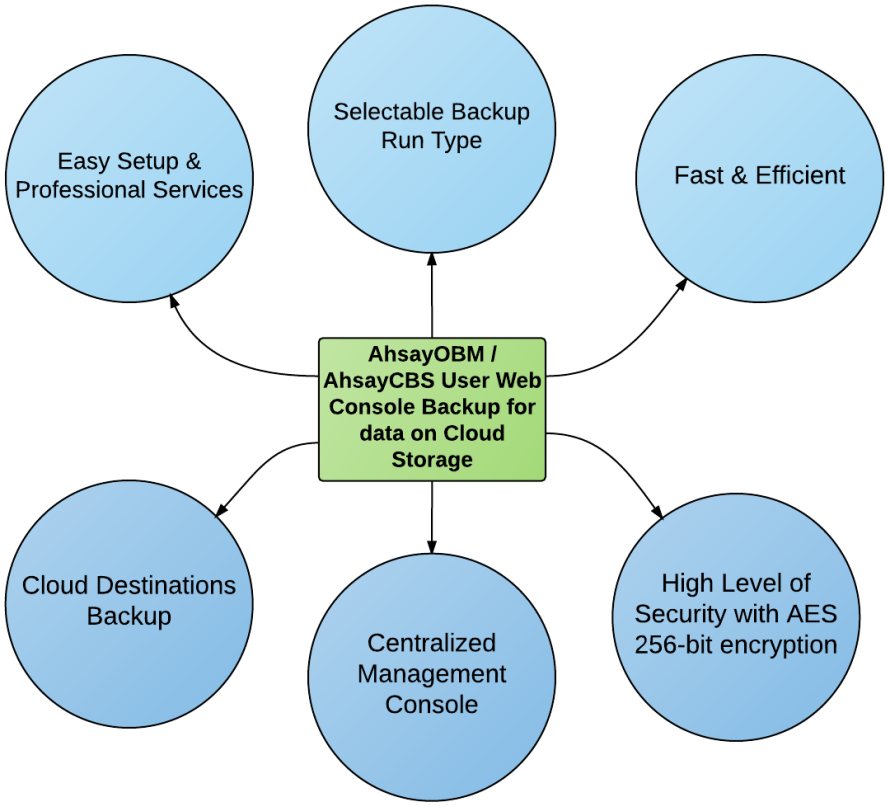
Below is the system architecture diagram illustrating the major elements involved in the backup process among the Cloud Storage, AhsayOBM and AhsayCBS.

In this user guide, we will focus on the software installation, as well as the end-to-end backup and restore process using both the AhsayOBM (Client Agent) and AhsayCBS User Web Console (Agentless).



Why should I use AhsayOBM or AhsayCBS User Web Console to back up my data on Cloud Storage?

We are committed to bringing you a comprehensive cloud storage backup solution with AhsayOBM. Below are some key areas we can help making your backup experience a better one.



Easy Setup & Professional Services

Setup is a few clicks away - our enhanced AhsayOBM v8 can be easily downloaded and installed in just a few clicks. The refined user interface also provides user-friendly instructions to guide you through installation, configuration, backup and restore. The intuitive setup procedures together with instructions in this user guide makes the software installation and operations easy even for layman users. That being said, if you do run into any problems during setup, we are here to help out. Visit the URL below for details on technical assistance.
https://www.ahsay.com/jsp/en/contact/kbQuestion.jsp

Professional Services

AhsayOBM Installation and Configuration Service

If you would like to save the time of reading through this document for setup, we have introduced this service to take care of all the installation and setup for you. On top of the installation and setup services, we also have a whole series of premium after-sales services to provide you with the best user experiences possible.

Valid Maintenance

Our Valid Maintenance provides you with professional and timely customer support along the way. You are entitled to the Valid Maintenance for free during the first year of your service subscription, and recurring annual fee at 20% of your annual subscription fee.

Refer to our Professional Services webpage for further details and subscription.

Selectable Backup Run Type

You can choose to either run the backup set you created on **Server** (AhsayCBS) or **Client** (AhsayOBM).

The run type of a cloud file backup set can only be set if you create a backup set via the AhsayCBS Admin / User Web Console. For backup set created via the backup client application (i.e. AhsayOBM), the run type is set to Run on Client by default.

Run on Server

A Run on Server cloud file backup set provides you with an agentless backup solution. Manual or scheduled backup job is performed on the backup server (i.e. AhsayCBS); you do not need to install a backup agent on your personal computer in order to backup your data on cloud storages.

What are the benefits?

- **Physical Machine not Required**

  Since the whole backup and restore process is done over the CBS server and therefore you do not need a physical machine at all.

- **Simplified Installation**

  Unlike agent-based backup, you do not need to install the client backup agent on your computer or upgrade it when a newer version becomes available.

- **Simplified Administration**

  With one software to manage (AhsayCBS, the backup server application), this allows administrator / user to manage backup and restore operations from a centralized console with lower time investment.

- **Compliance**

  Some organizations cannot install client agents due to regulatory requirements. An agentless solution allows for compliance during backup or restore.

- **Consistency and Recoverability**

  Backup client agent could interfere with the processing power of core applications of the machines that it is installed on. Run on Server cloud file backup job is performed on the backup server, which does not consume resources on client computer during a backup job.

The advantages of agentless backup technology make it a good option for administrators / users who want to simplify the backup and restore management.

Run on Client

A Run on Client cloud file backup set provides you with an agent-based backup solution. Manual or scheduled backup job is performed on the client computer (i.e. AhsayOBM); you need to install a backup agent on your personal computer in order to back up your data on cloud storages.

What are the benefits?

- **Robustness**

  In the event of a failure to a single backup agent, it fails in isolation to other users' environment.

- **Industry standard requires minimal learning curve**

  Agent-based backup is the traditional backup approach that is well understood by most administrators and end users whom would only need minimal effort and time to understand the backup and restore process and operations.

- **Performance**

  Unlike an agentless backup, where backup / restore operations of all users are performed on the backup server which may have multiple jobs to run at the same time, resulting in slower performance. Agent-based backup is performed on your computer with resources that is dedicated for your own backup and restores.

  The advantages of agent-based backup technology make it a good option for users who want to have more control on individual backup / restore and resources management.

With both **Run on Server** (agentless) and **Run on Client** (agent-based) backup options available and the freedom to use different setting on different backup sets according to your needs, our backup solution offers you with high level of flexibility and efficiency for cloud file backup and restore.

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

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

	Run on Server Cloud File Backup Set	Run on Client Cloud File Backup Set
General Settings	Yes	Yes
Backup Source	Yes	Yes
Backup Schedule	Yes	Yes
Continuous Backup	Yes	Yes
Destination	AhsayCBS and Predefined Destinations	Yes
In-File Delta	Yes	Yes
Retention Policy	Yes	Yes
Command Line Tool	N/A	Yes
Reminder	N/A	Yes
Bandwidth Control	Yes	Yes
IP Allowed for Restore	N/A	Yes
Other	Yes	Yes
To Run a Backup	AhsayCBS User Web Console Only	AhsayOBM
To Run a Restore	AhsayCBS User Web Console Only	AhsayOBM / AhsayOBR

Refer to this link for AhsayOBR guide: [AhsayOBR v8 User Guide for Windows]

Fast and Efficient

We understand that backup could be a time and resources consuming process, which is why AhsayOBM is designed with advanced technologies to make backup a fast and efficient process.

We also understand that you may wish to run backup at a specified time interval of your choice, that's why we also allow you to set your own backup schedules so that you can take full control of the time when to perform backup.

- ***Multi-threading*** – this technology utilizes the computing power of multiple CPU cores for creating multiple backup and restore threads to produce fast backup and restore performance.
- ***Block Level Incremental Backup*** – this technology breaks down the backup files into multiple blocks and only the changed blocks will be backed up each time.

Centralized Management Console

Our enriched features on the centralized web console offers you a one-stop location for monitoring and managing your backup and restore, whether you are a system administrator or backup user. Below is an overview of what you can do with it.

- Create backup set
- Restore backup
- Configure user settings
- Configure backup settings
- View and download backup and restore reports
- Monitor backup and restore live activities

Cloud Destinations Backup

To offer you with the highest flexibility of backup destination, you can now back up mail objects to a wide range of cloud storage destinations. Below is a list of supported cloud destinations.

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

Cloud backup gives you **two major advantages**:

- ***Cloud to Cloud Backup*** – you can back up your data on cloud storage to another cloud destination of your choice. This gives you an extra layer of protection in the event of a local drive corruption, where you will still be able to retrieve data from the cloud destination.
- ***Eliminate Hardware Investment*** – with the increasingly affordable cloud storage cost, you can deploy on cloud platform and utilize cloud storage as your centralized data repository, or simply expand your cloud storage as a backup destination without having to invest on hardware.

High Level of Security

We understand the data on your cloud storage may contain sensitive information that requires to be protected, that is why 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, you can turn on the encryption feature which will be default encrypt the backup data locally with AES 256-bit truly 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.

1.1 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 Cloud File backup and restore, followed by step-by-step instructions on creating backup set, running backup job and restoring backed up data, using both the AhsayOBM and AhsayCBS Web User Console.

The document can be divided into 3 main parts.

Part 1: Preparing for Cloud File Backup & Restore

Requirements
Requirements on hardware & software for installation

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

Part 2: Performing Cloud File Backup

Logging in to Client Agent or User Web Console
Log in to AhsayOBM or User Web Console

Creating a Backup Set
Create a backup set using AhsayOBM and User Web Console

Running a Backup Set
Run a backup set using the AhsayOBM and User Web Console

Part 3: Restoring Cloud File Backup

Restoring a Backup Set using AhsayOBM & User Web Console
Restore a backup using the AhsayOBM and User Web Console

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 AhsayOBM and User Web Console, 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 AhsayOBM is running 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 versions.
FAQ: Ahsay Software Compatibility List (SCL) for version 8.1 or above

2.3 Antivirus Exclusion Requirement

To optimize performance of AhsayOBM on Windows, and to avoid conflict with your antivirus software, refer to the following KB article the list of processes and directory paths that should be added to all antivirus software white-list / exclusion list:
http://wiki.ahsay.com/doku.php?id=public:5352_suggestion_on_antivirus_exclusions

2.4 Other Requirement and Recommendation

Ensure that the following requirements are met:

- **AhsayOBM Installation**

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

- **Access for AhsayCBS User Web Console**

  It is now possible to perform agentless backup and restore, which can be done via the AhsayCBS User Web Console without using the AhsayOBM client agent. In order to access the User Web Console, make sure you have Internet connection and a web browser installed on your computer or mobile device.

- **Backup Quota Requirement**

  Make sure that your AhsayOBM user account has sufficient quota assigned to accommodate the storage for the Cloud File backup. Contact your backup service provider for details.

2.5 Best Practices and Recommendations

The following are some best practices or recommendations we strongly recommend you to follow before you start any Cloud File backup and restore.

- **Temporary Directory Folder Location (For backup and restore running on AhsayOBM only)**

  Temporary directory folder is used by 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

Consider the following best practices for optimized performance of the backup operations:

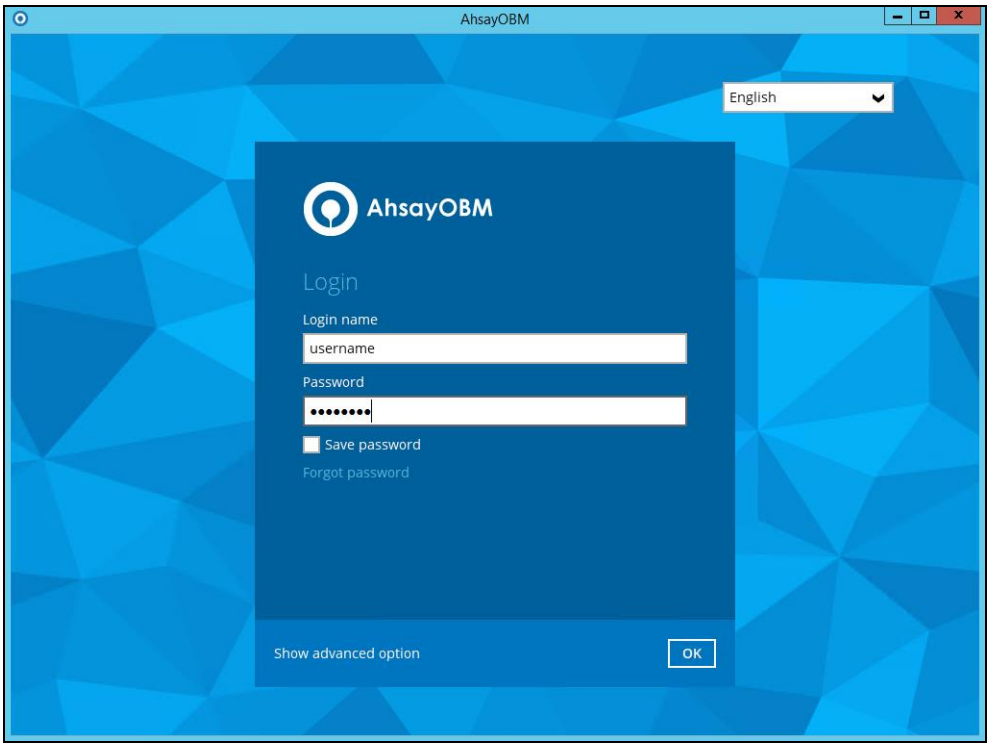
- Schedule backup jobs when system activity is low to achieve the best possible performance.
- Perform test restores periodically to ensure your backup is set up and performed properly. Performing recovery test can also help identify potential issues or gaps in your recovery plan. It's important that you do not try to make the test easier, as the objective of a successful test is not to demonstrate that everything is flawless. There might be flaws identified in the plan throughout the test and it is important to identify those flaws.

3 Login to AhsayOBM / AhsayCBS User Web Console

3.1 Login to AhsayOBM

1. Login to the AhsayOBM application user interface.

   For client installation on Windows, double click the AhsayOBM desktop icon to launch the application.



2. Enter the **Login name** and **Password** of your AhsayOBM account.

3. Click **Show advanced option** to configure the **Backup Server** and **Proxy** details if necessary.

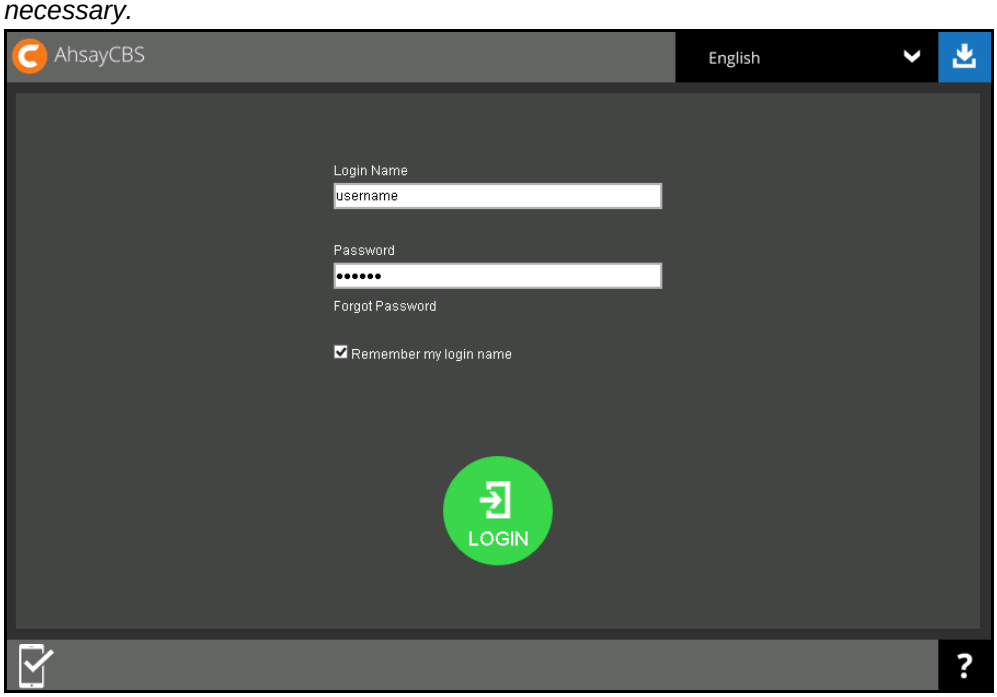
4. Click **OK** afterward to login to AhsayOBM.

3.2 Login to the AhsayCBS User Web Console

1. Login to the AhsayCBS web console at

   `https://backup_server_hostname:port`

   Note: *Contact your service provider for the URL to connect to the web console if necessary.*



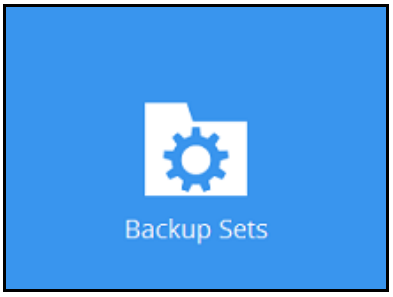
2. Enter the **Login Name** and **Password** of your AhsayOBM account.

3. Click **Login** afterward to login to the web console.

4 Creating a Cloud File Backup Set

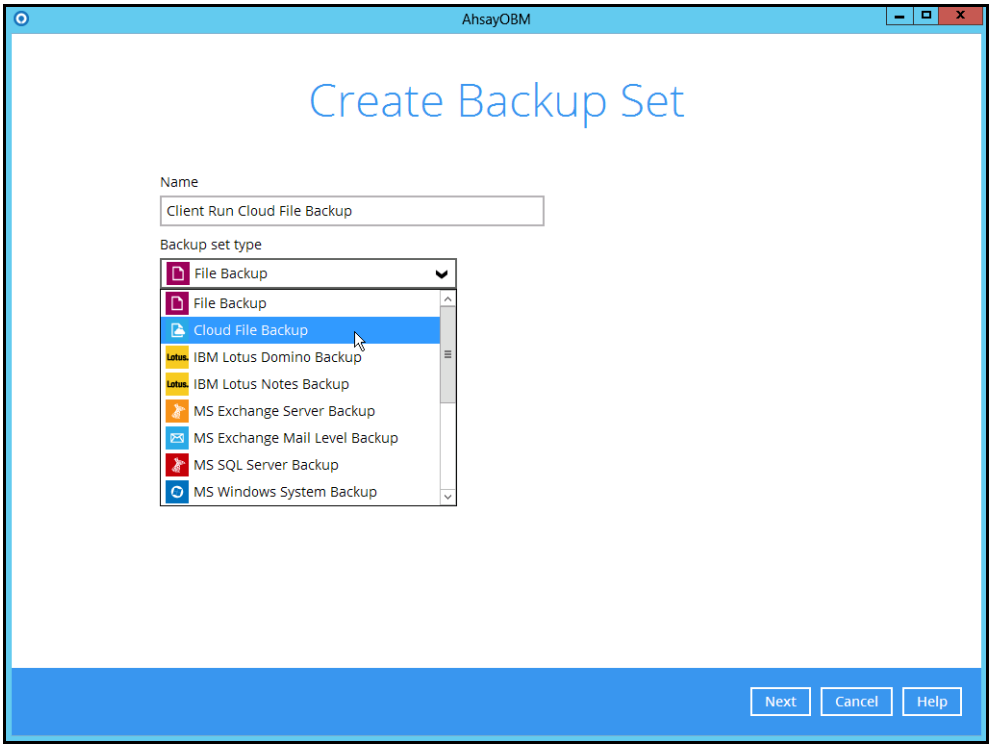
4.1 Create a Cloud File Backup Set in AhsayOBM

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

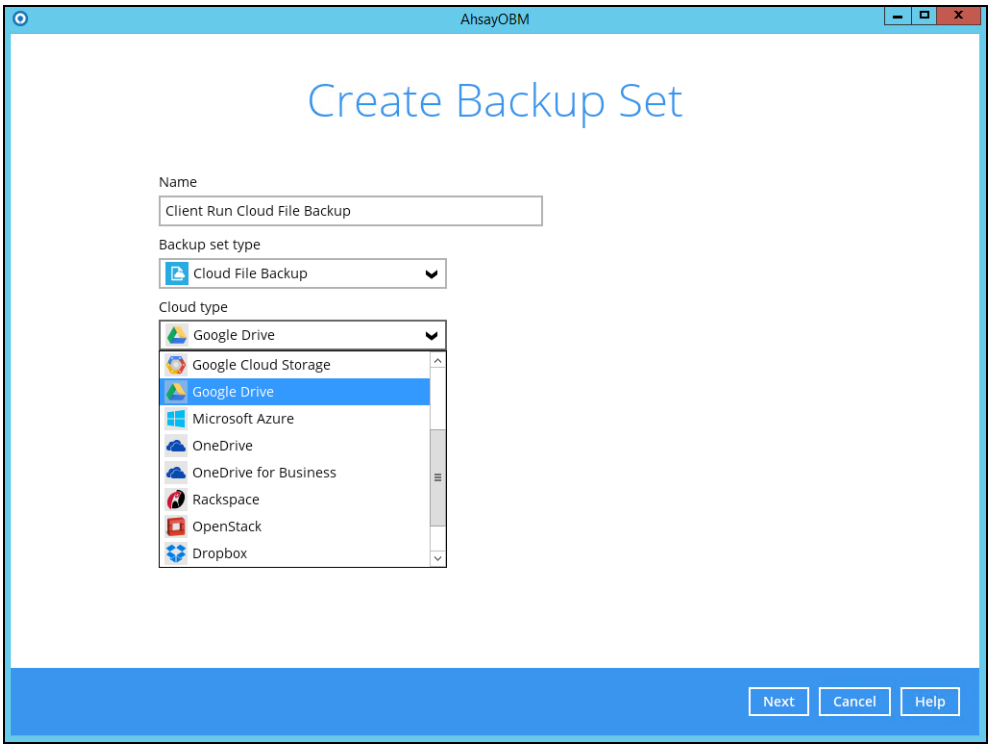


2. Create a Cloud File backup set by clicking the "+" icon next to **Add new backup set**.

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

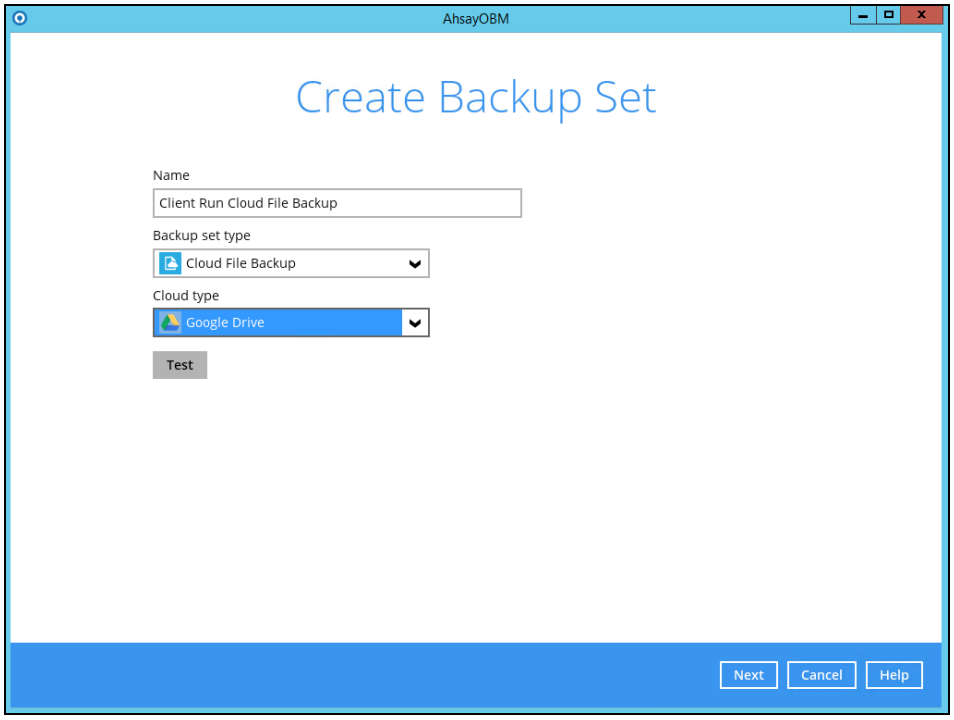


4. Select the **Cloud type** of the cloud storage that contain the data that you want to backup. For example, Google Drive.

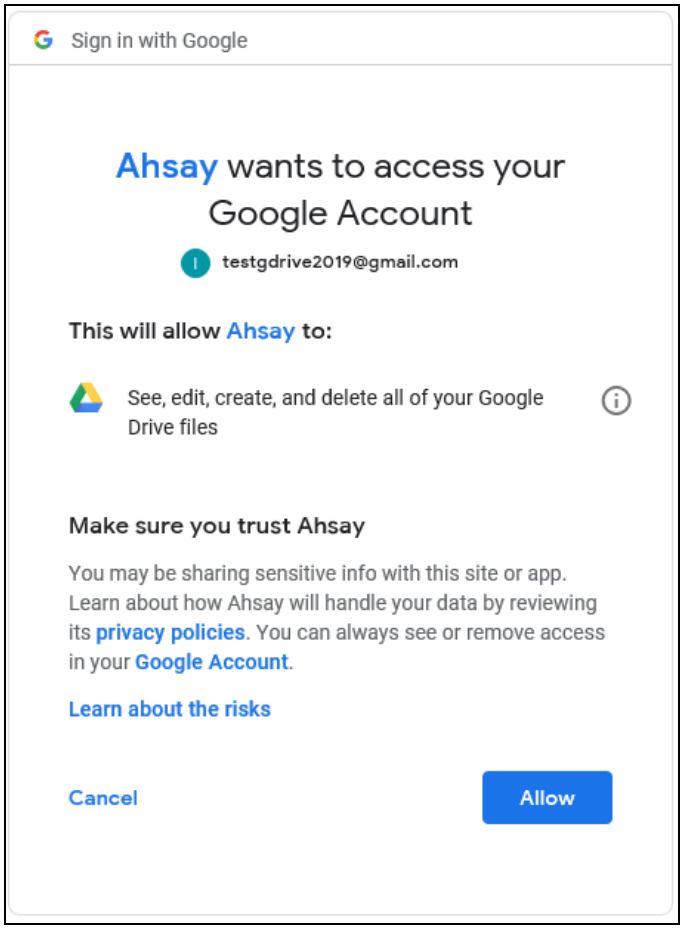


5. Depending on the cloud type you have selected, you will be prompted to enter the cloud service login details.

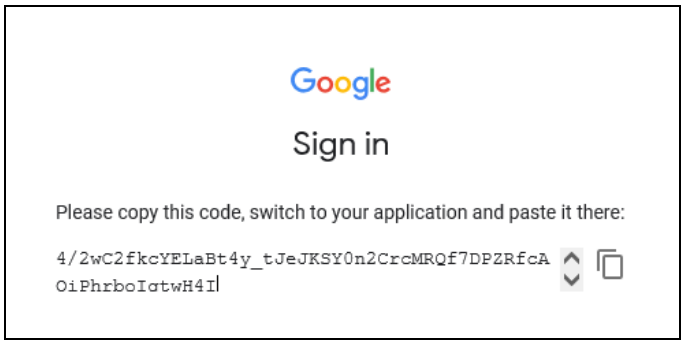
   - Click **Test** to get redirected to the login page of the cloud service provider on your default browser, then enter the login details there.

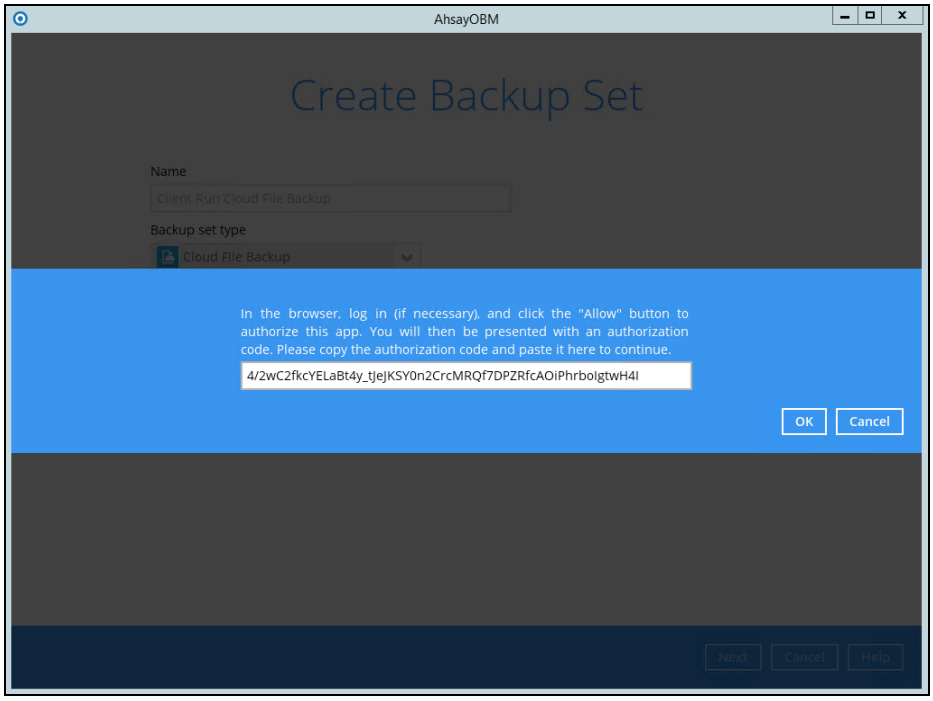


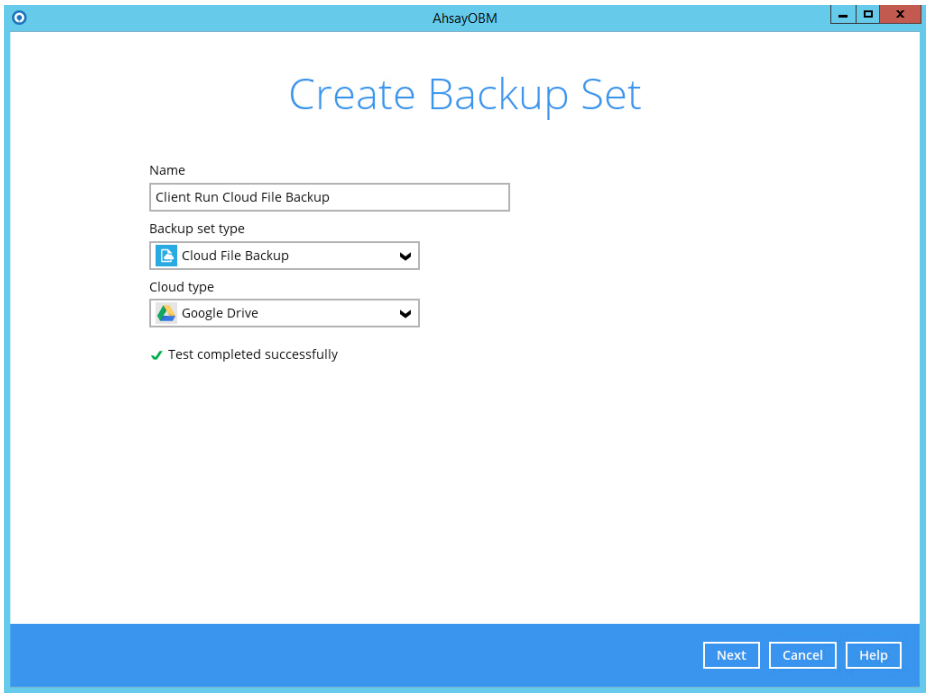
➢ Click **Allow** to permit AhsayOBM to access the cloud storage.



➢ 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.



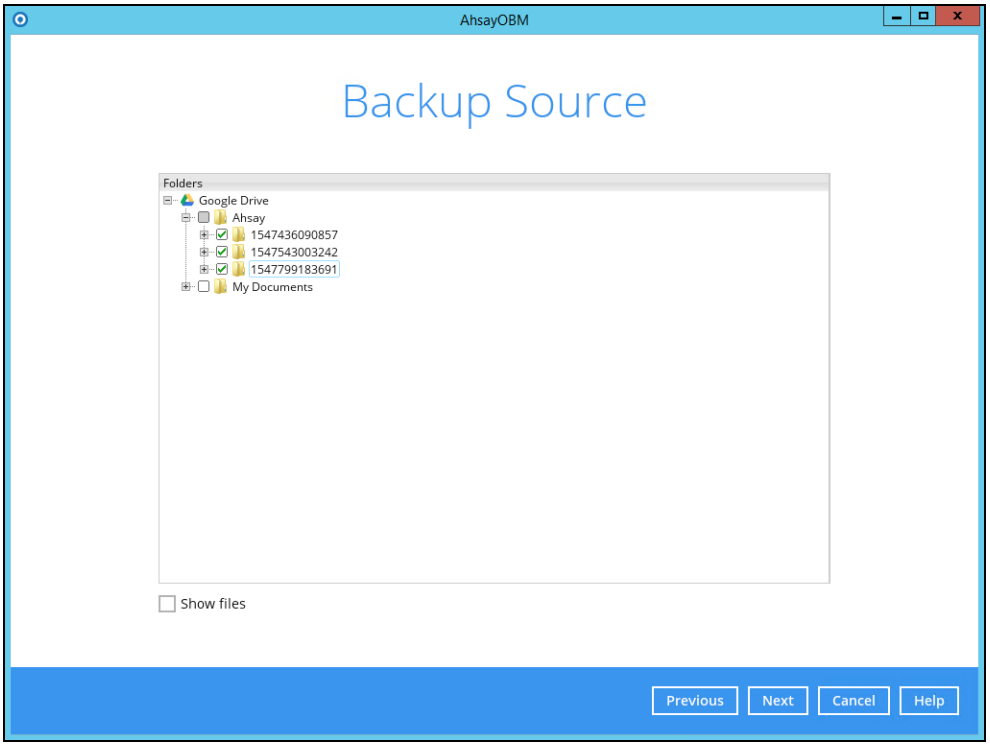




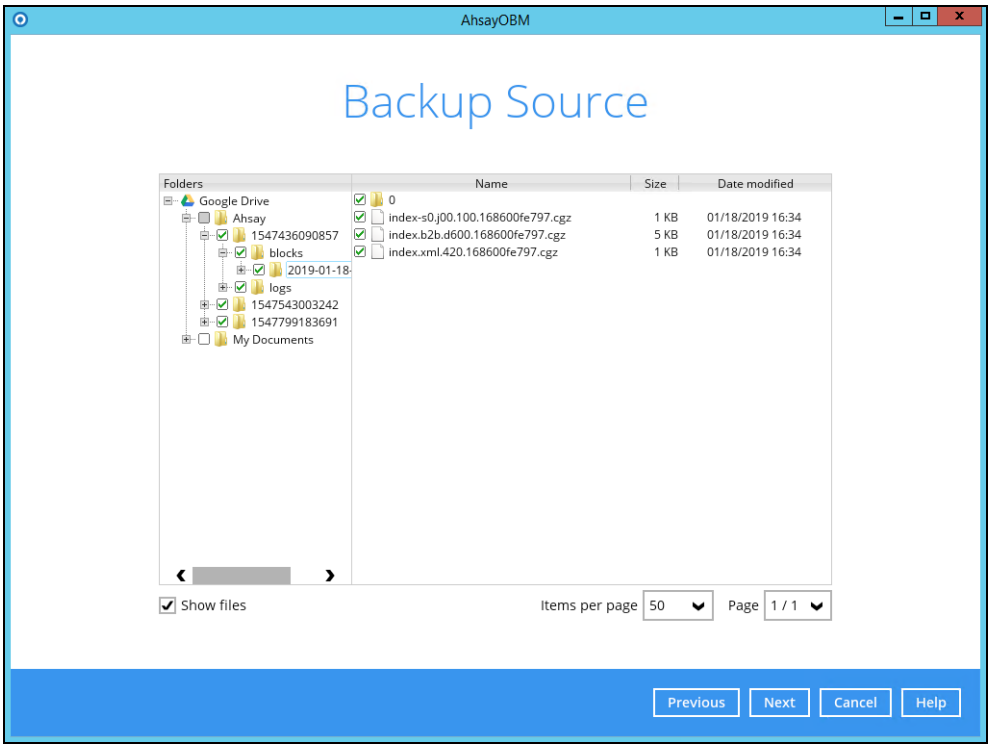
IMPORTANT

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

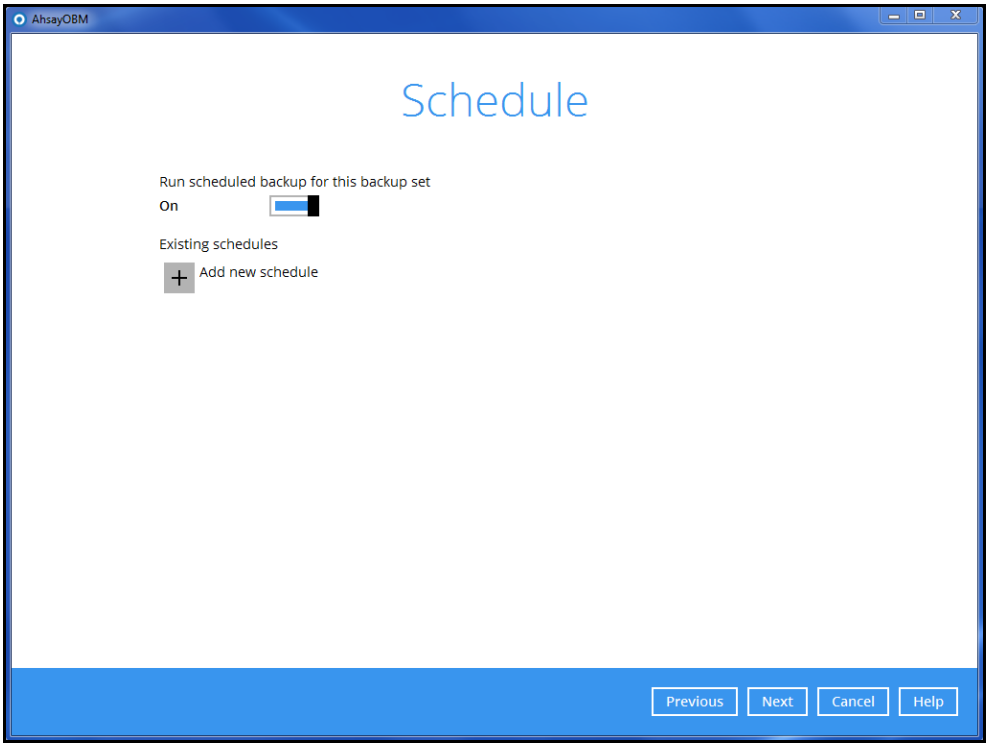
6. In the **Backup Source** menu, select the folder / files that you would like to backup.



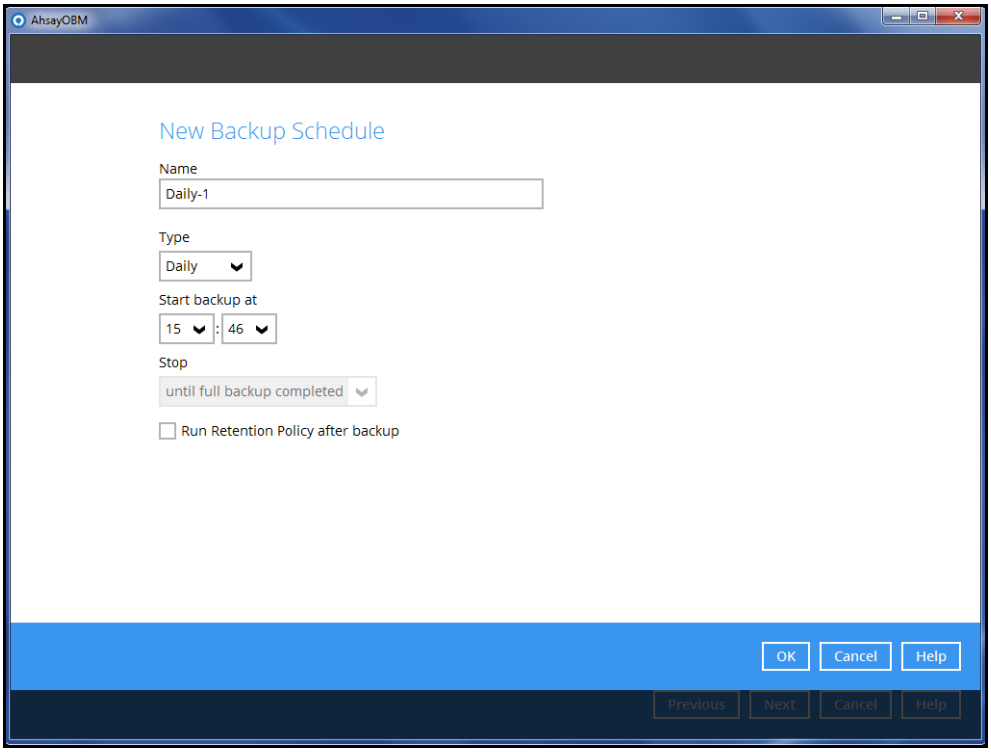
Enable the **Show files** checkbox at the bottom left corner if you would like to choose individual file for backup. Click **Next** to proceed when you are done with the selection.



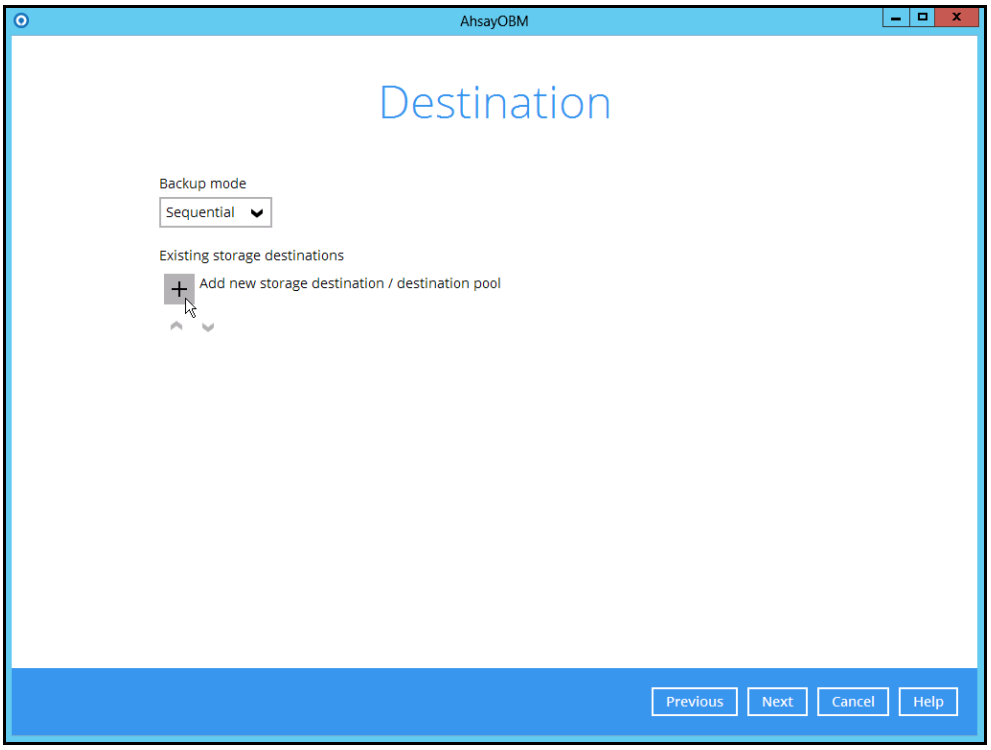
7. In the **Schedule** menu, configure a backup schedule for backup job to run automatically at your specified time interval. Click **Add new schedule** to add a new schedule, then click **Next** to proceed afterward.



Configure the backup schedule settings on this page, then click **OK** when you are done with the settings, then 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**.

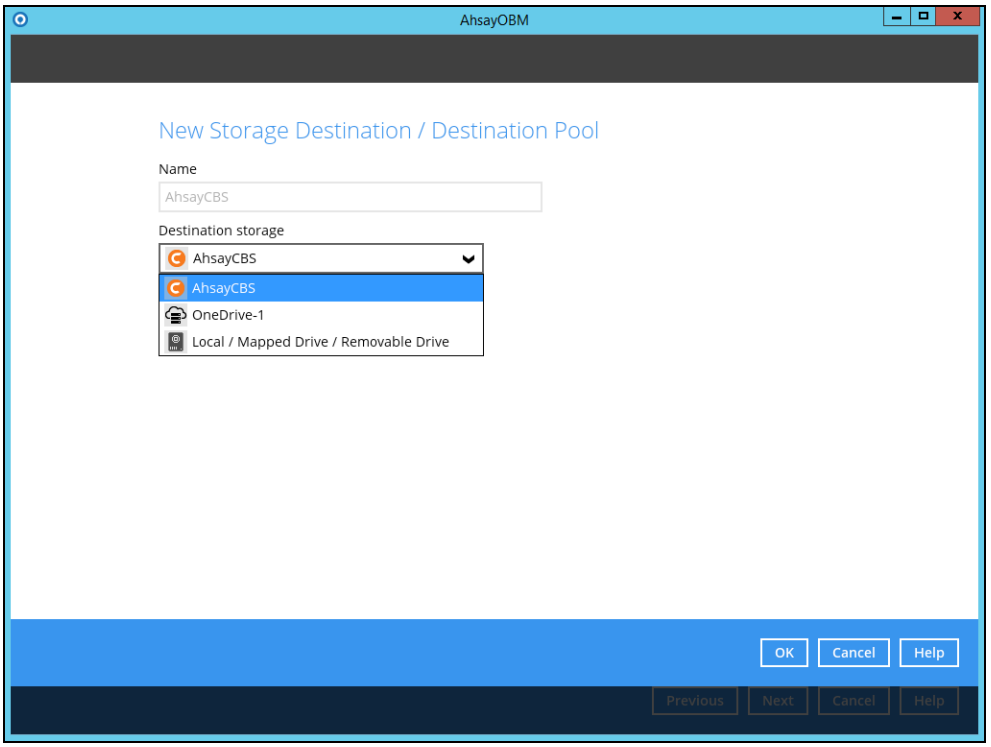


Note

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

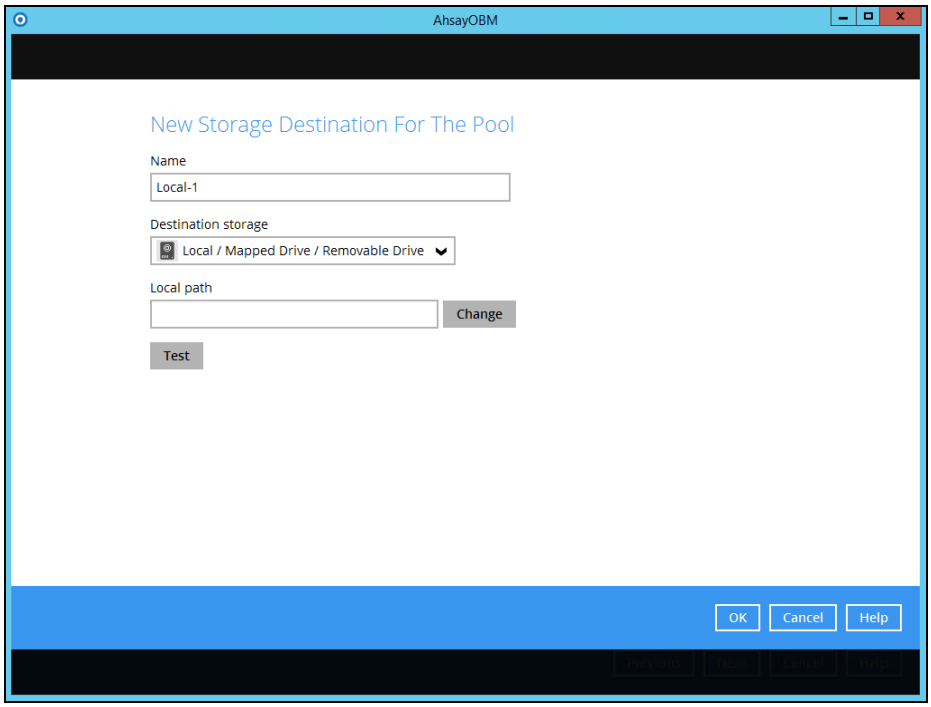
FAQ: Frequently Asked Questions on Backup Destination

9. Select the Destination storage.

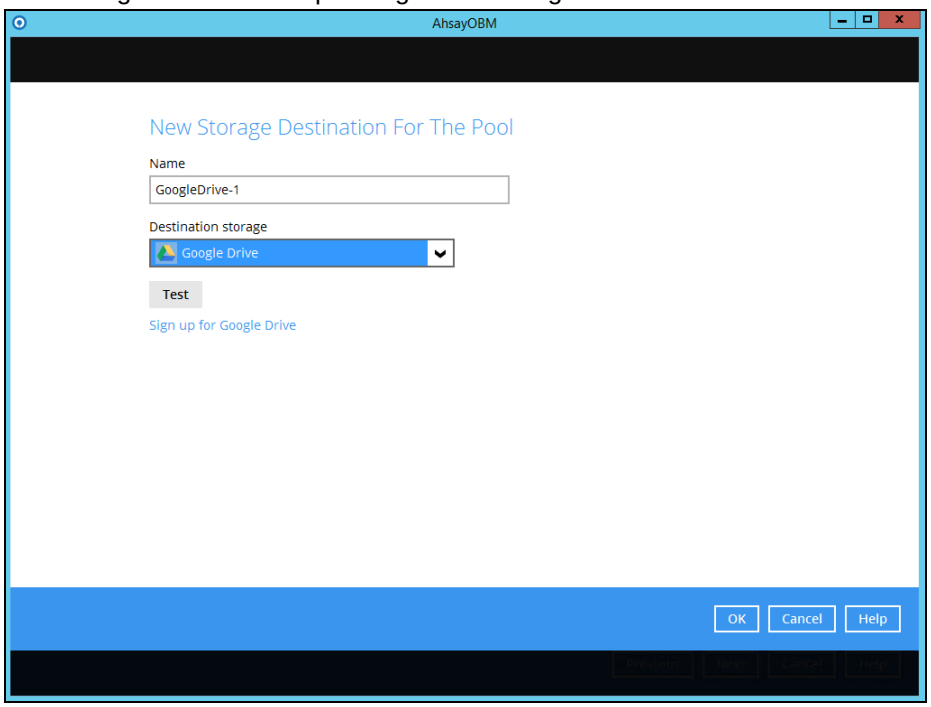


You can choose a storage combination of the Local/Mapped drive/Removable Drive, Cloud storage or FTP. Click **OK** to proceed when you are done with the settings.

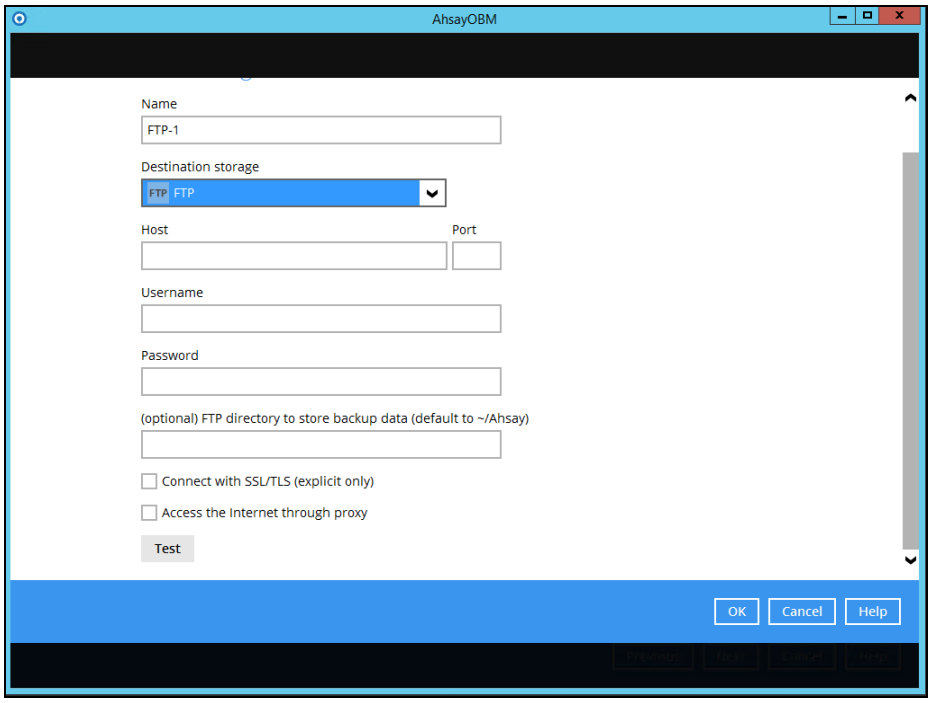
- If you have chosen the Local/Mapped Drive/Removable Drive option, click **Change** to browse to a directory path where backup data will be stored, then click **Test** to validate the path. **Test completed successfully** shows when the validation is done.



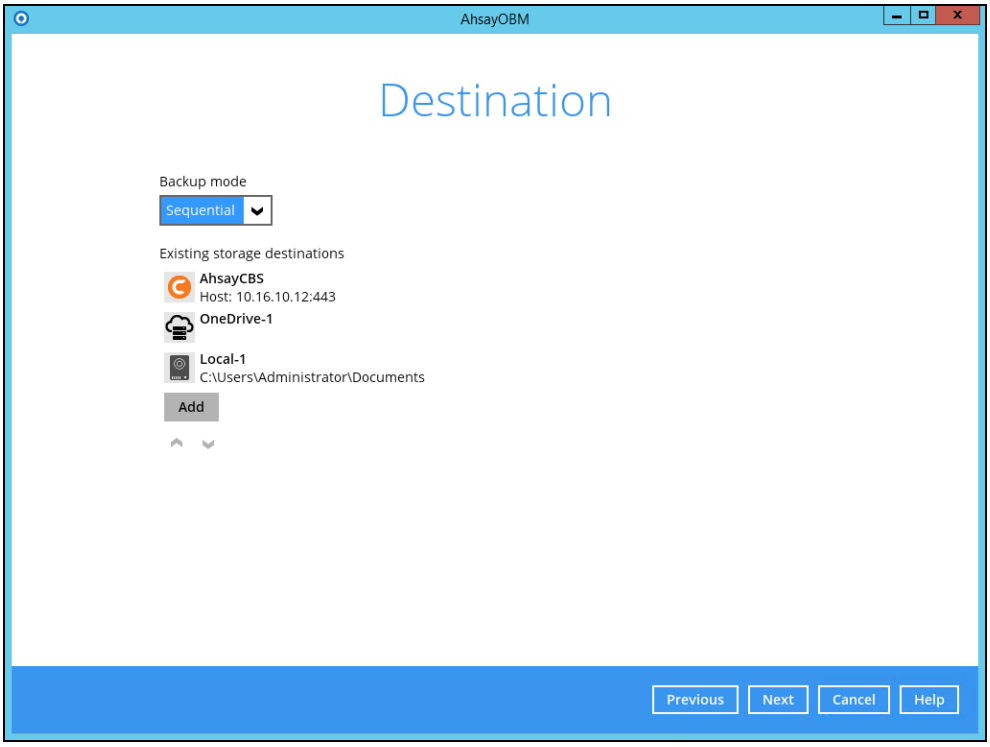
- If you have chosen to store the backup files in another Cloud Storage, click **Test** to log in to the corresponding cloud storage service.



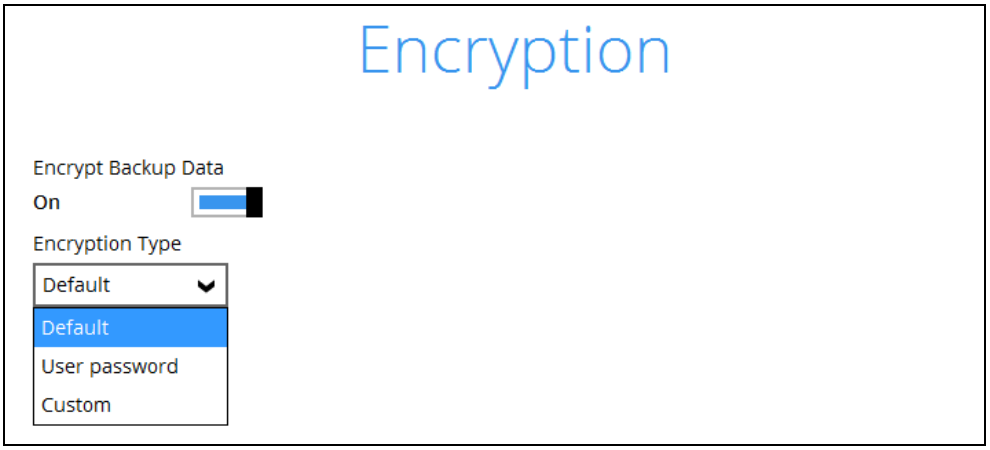
- If you have chosen the FTP as the destination, enter the the Host, Username and Password details.



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.

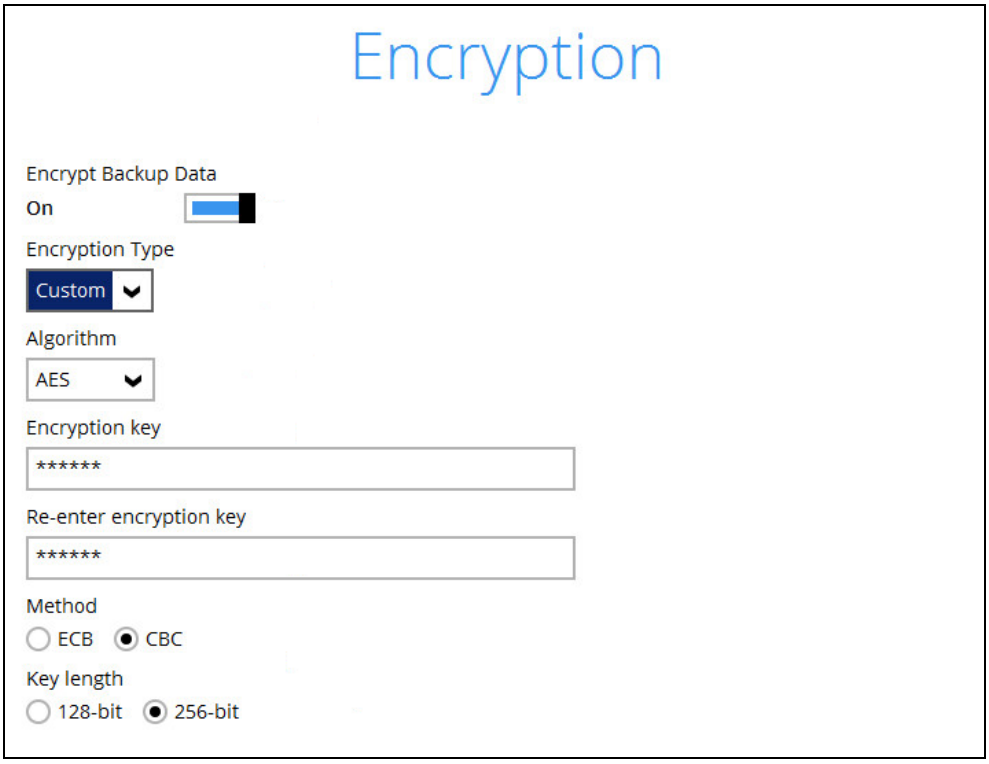


11. In the Encryption window, the default **Encrypt Backup Data** option is enabled with an encryption key preset by the system which provides the most secure protection.



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.



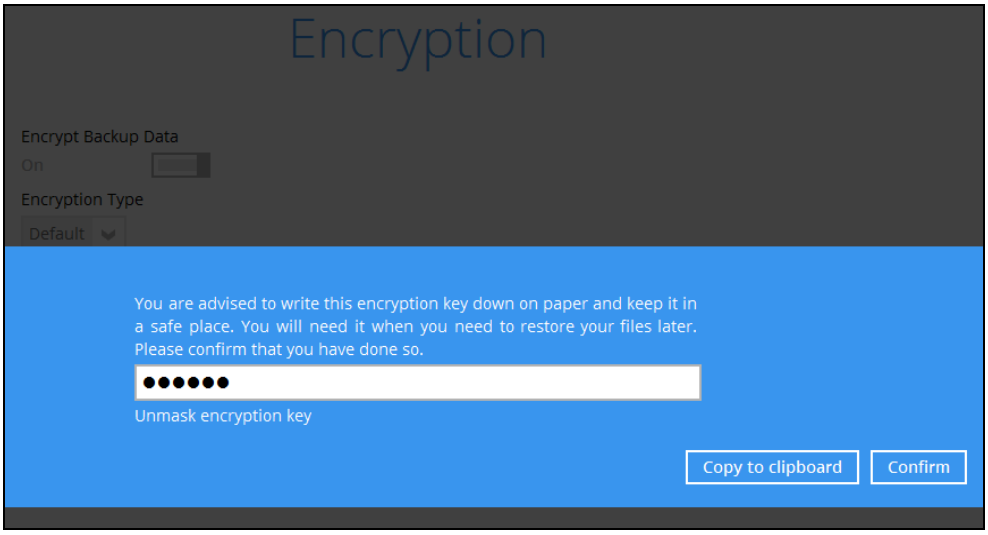
Note

For more details on managing your encryption key, refer to this article:

FAQ: Best practices for managing encryption key for AhsayOBM or AhsayACB

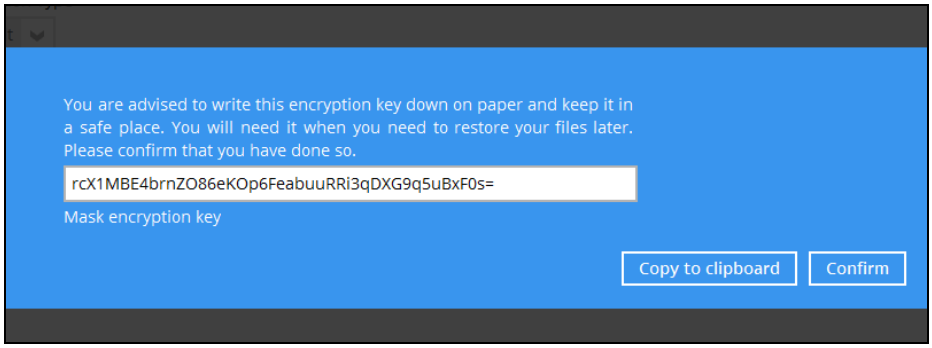
Click **Next** when you are done setting.

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:

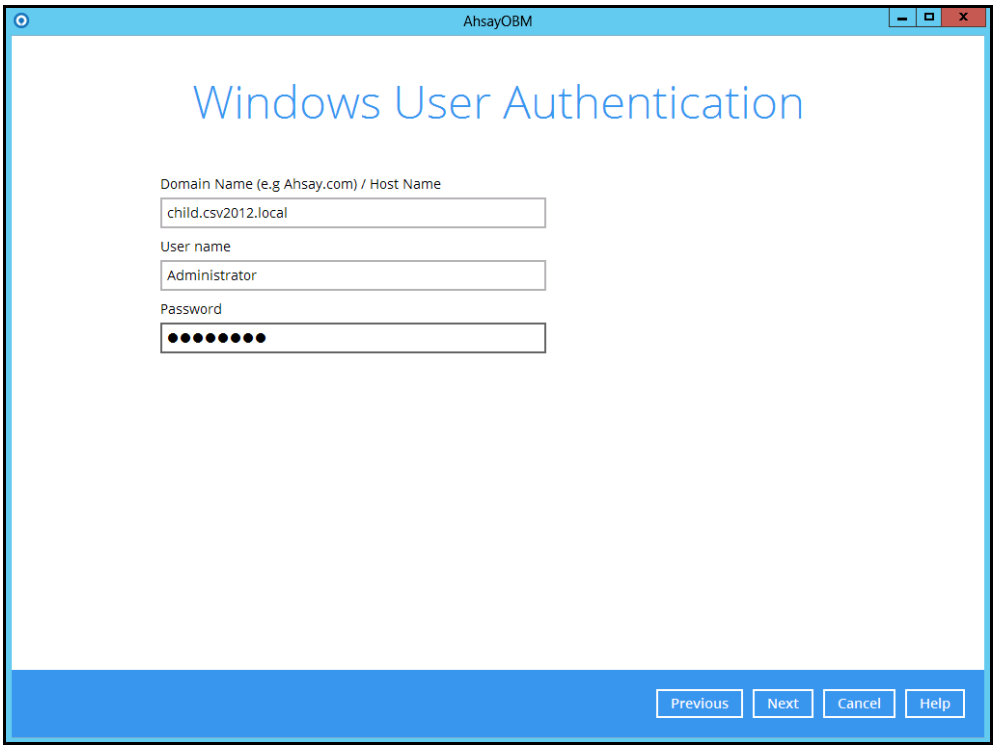
- **Unmask encryption key** – The encryption key is masked by default. Click this option to show the encryption key.



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

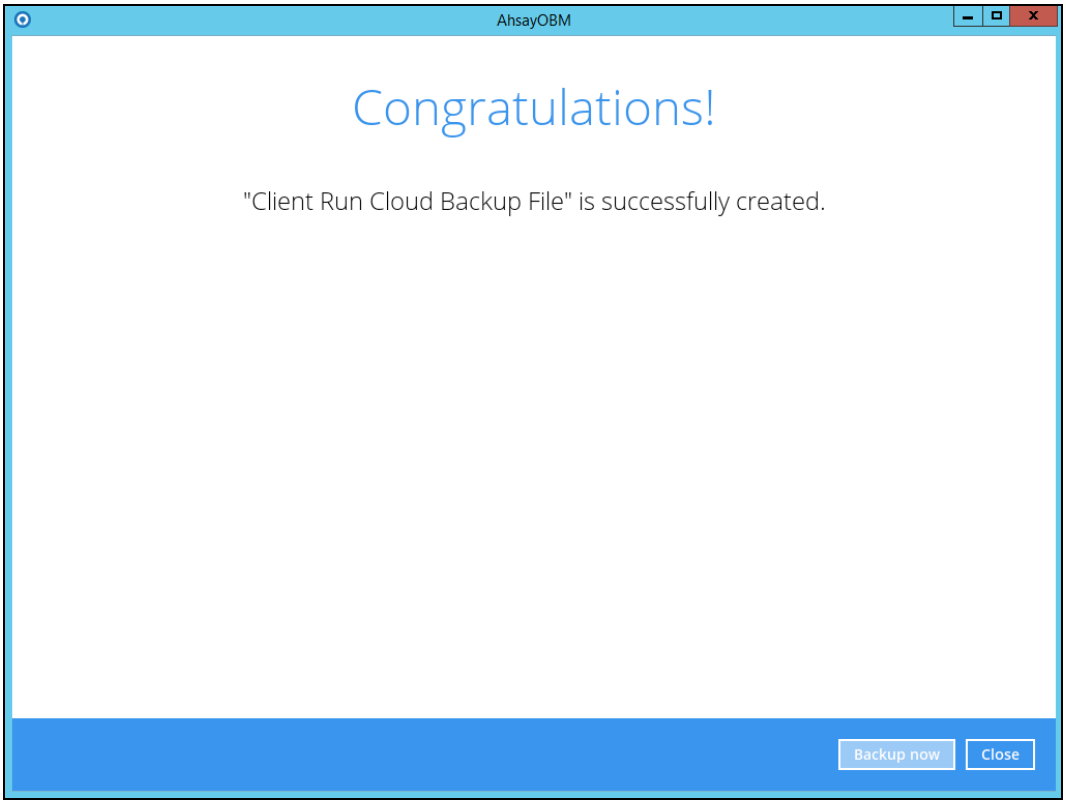
- **Confirm** – Click to exit this pop-up window and proceed to the next step

13. Enter the **Domain Name / Host Name**, **User Name** and **Password** of the Windows account that will be running the backup.



Note: *This menu will only be displayed for backup set with backup schedule configured (for installation on Windows).*

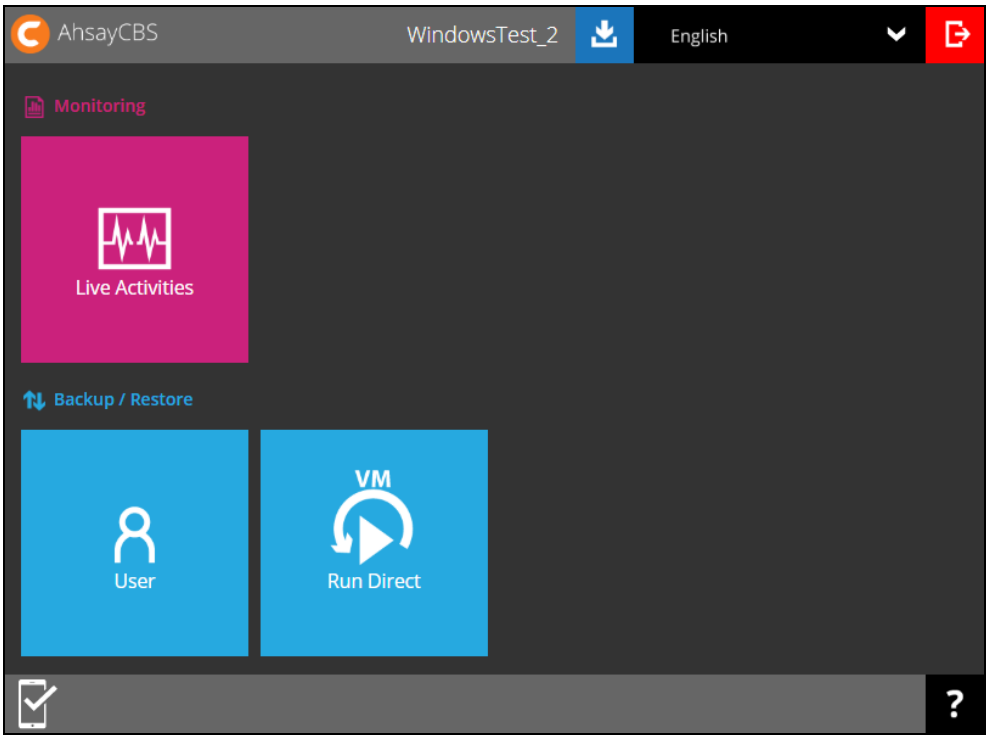
14. The backup set has been successfully created.



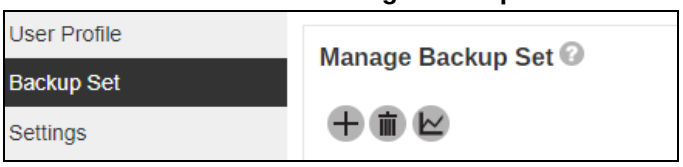
4.2 Create a Cloud File Backup Set on the AhsayCBS User Web Console

1. Log in to the User Web Console according to the instructions in Login to the AhsayCBS User Web Console.

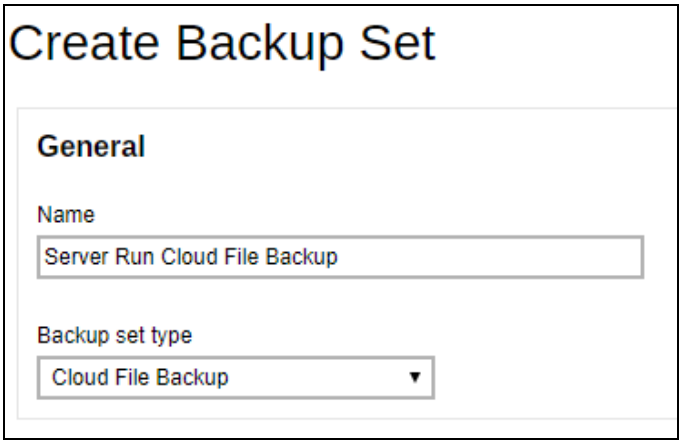
2. Click the **User** icon on the User Web Console landing page.



3. Select **Backup Set** from the left panel, then create a Cloud File backup set by clicking the circular "+" icon under **Manage Backup Set**.



4. Select **Cloud File Backup** as the **Type**, and enter a **Name** for the backup set.



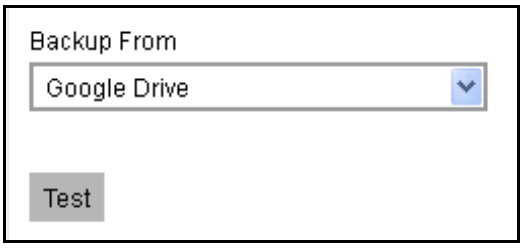
5. On the same menu under **Run on**, select **Server** to create a run on server (agentless backup) backup set or **Client** to create a run on client (agent-based backup) backup set.

- **Server** - If you choose to run the backup set on the CBS server, you won't be able to back up, restore or manage your backups on the AhsayOBM once the backup set is created.
- **Client** - If you choose to run the backup set on the AhsayOBM, you won't be able to back up, restore or manage your backups on the AhsayCBS Web Management Console once the backup is created.

Notes

This setting **CANNOT** be altered once the backup set is created. If you wish to change the backup method later, you will have to create a new backup set and start over the configurations again.

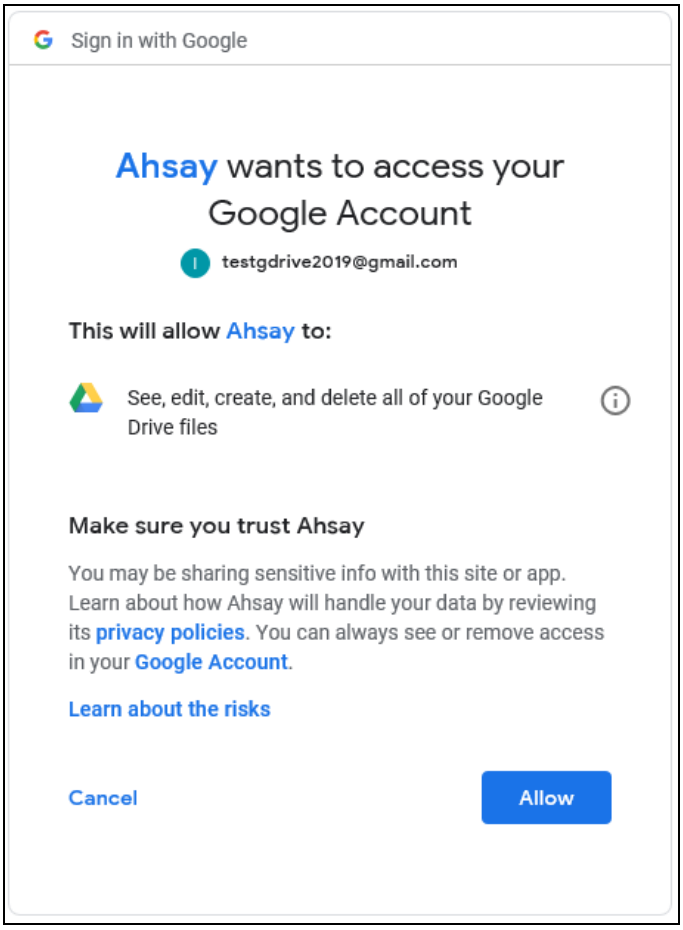
6. Select the cloud storage that contains the data that you want to backup under **Backup From**. Click **Test** afterward to authenticate AhsayCBS / AhsayOBM to access the cloud storage.



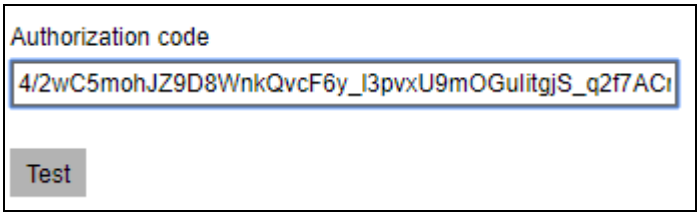
IMPORTANT

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

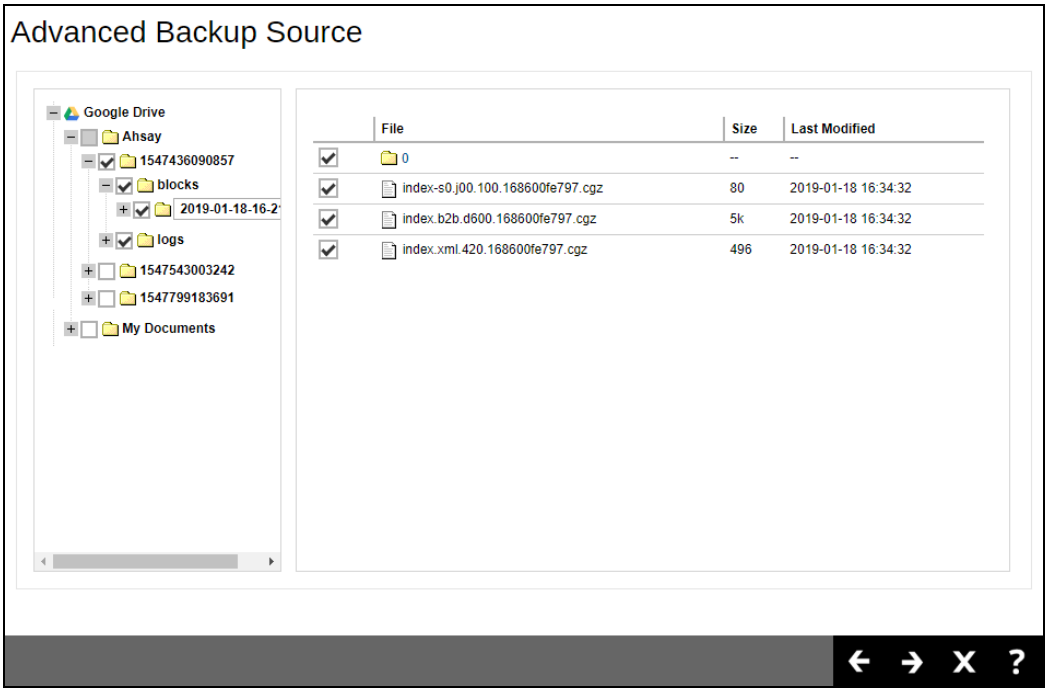
7. Click **Allow** to permit access the cloud storage.



Enter the **Authentication code** returned on the web console to complete the authentication setup.

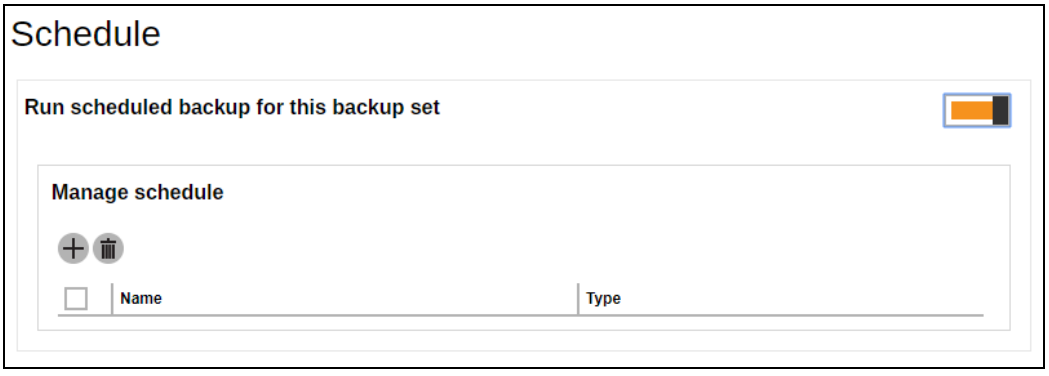


8. In the **Backup Source** menu, select the folder / files that you would like to backup.



9. 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.

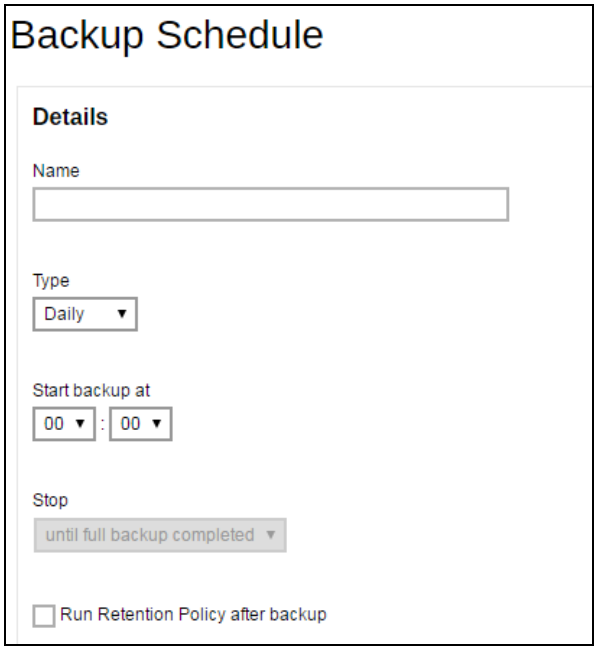
Click the **+** icon under **Manage Schedule** to add a new schedule.



You may configure the following items for the schedule.

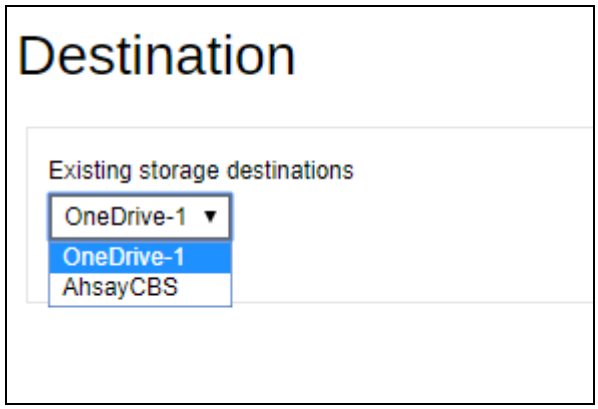
- Name of the scheduled backup
- Backup schedule type
  - Daily
  - Weekly
  - Monthly
  - Custom
- Backup start time

- Run Retention Policy after backup



Click the + icon and then click Next to proceed.

10. To add a destination, select from the existing storage destinations listed on the dropdown list.



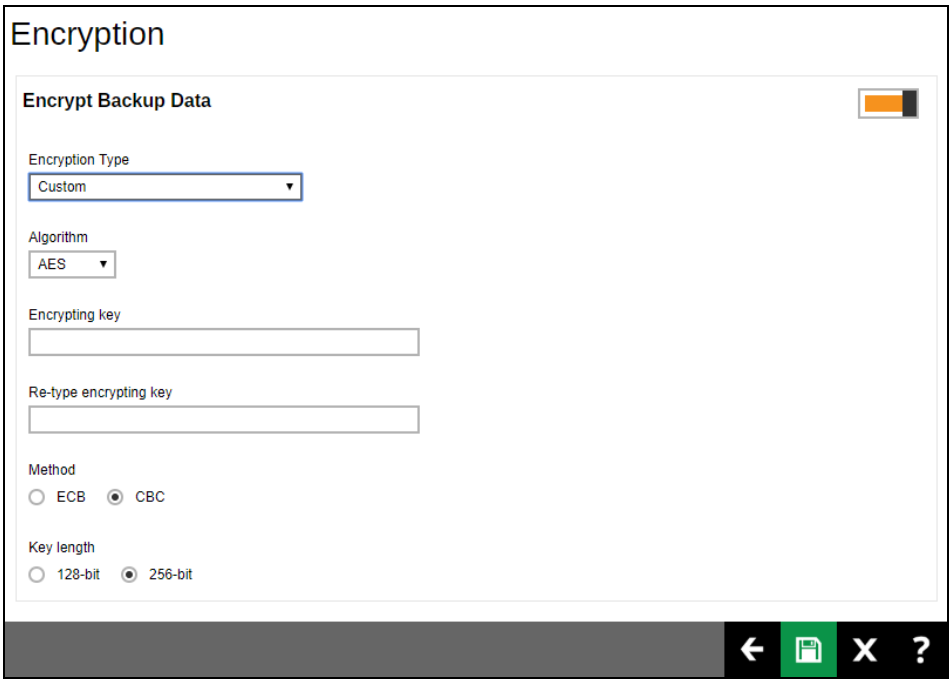
In the sample screen shot above, you have two (2) available destinations, OneDrive-1 and AhsayCBS.

If you would like to choose other backup destination other than the Predefined Destination, proceed to the next step without making any setting here. You will have to compelete this backup set creation first

11. By default, the **Encrypt Backup Data** option is enabled with the Encryption Type preset as **Default** which provides the most secure protection.

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

- **Default (Machine Generated Random)** – 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 AhsayACB at the time when this backup set is created. Please be reminded that if you change the AhsayACB 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.



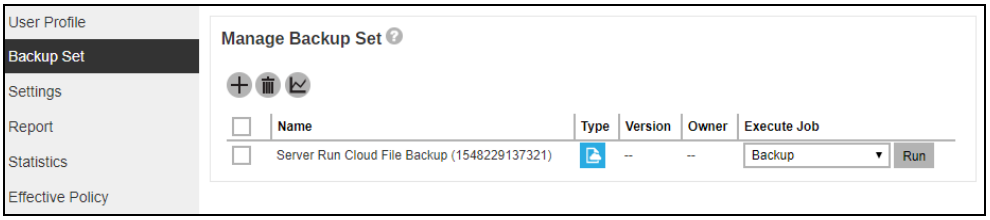
Note

For more details on managing your encryption key, refer to this article:

FAQ: Best practices for managing encryption key for AhsayOBM or AhsayACB

12. Click the  icon at the bottom right corner to confirm creating this backup set.

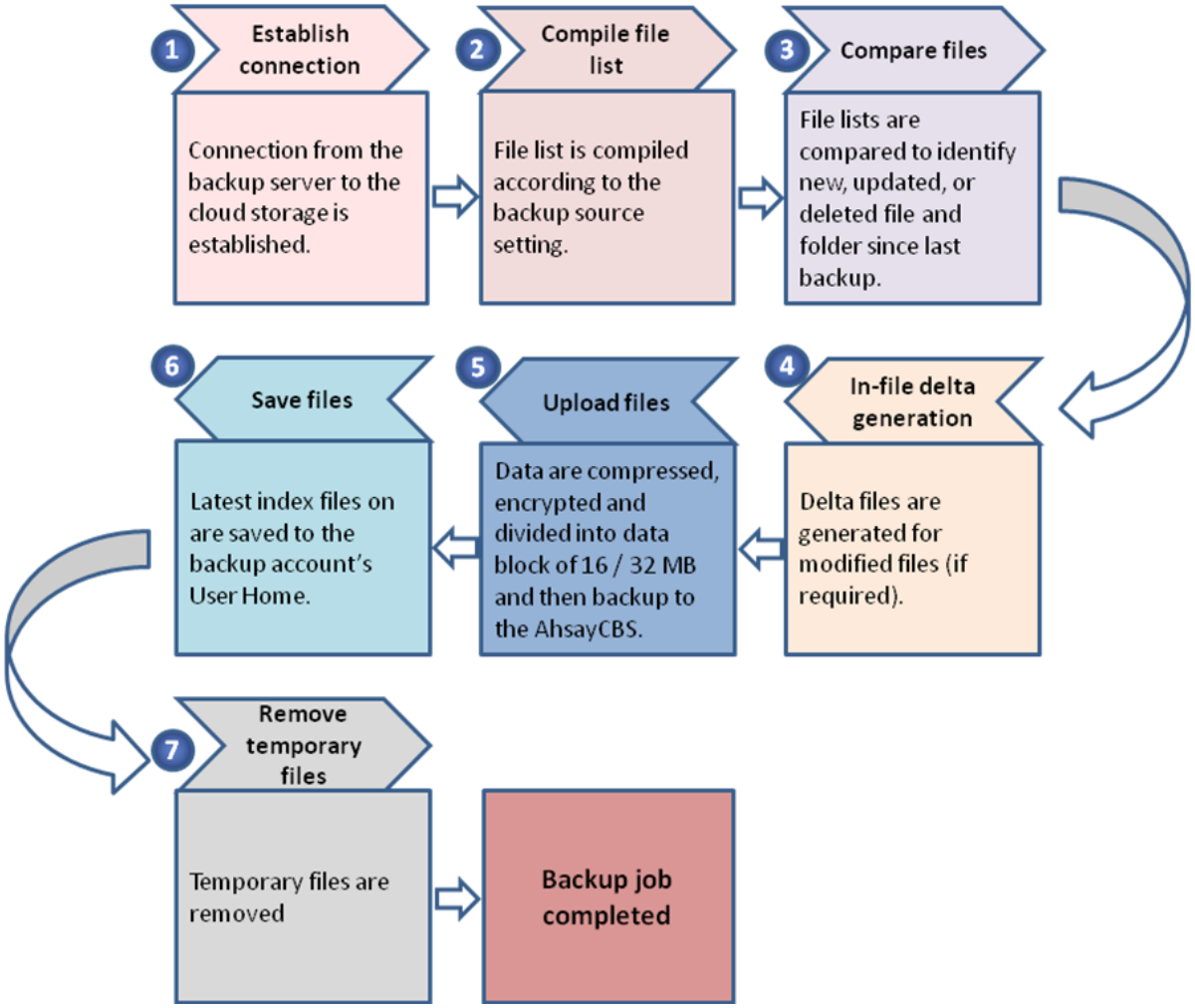
13. The backup set has been succesfully created.



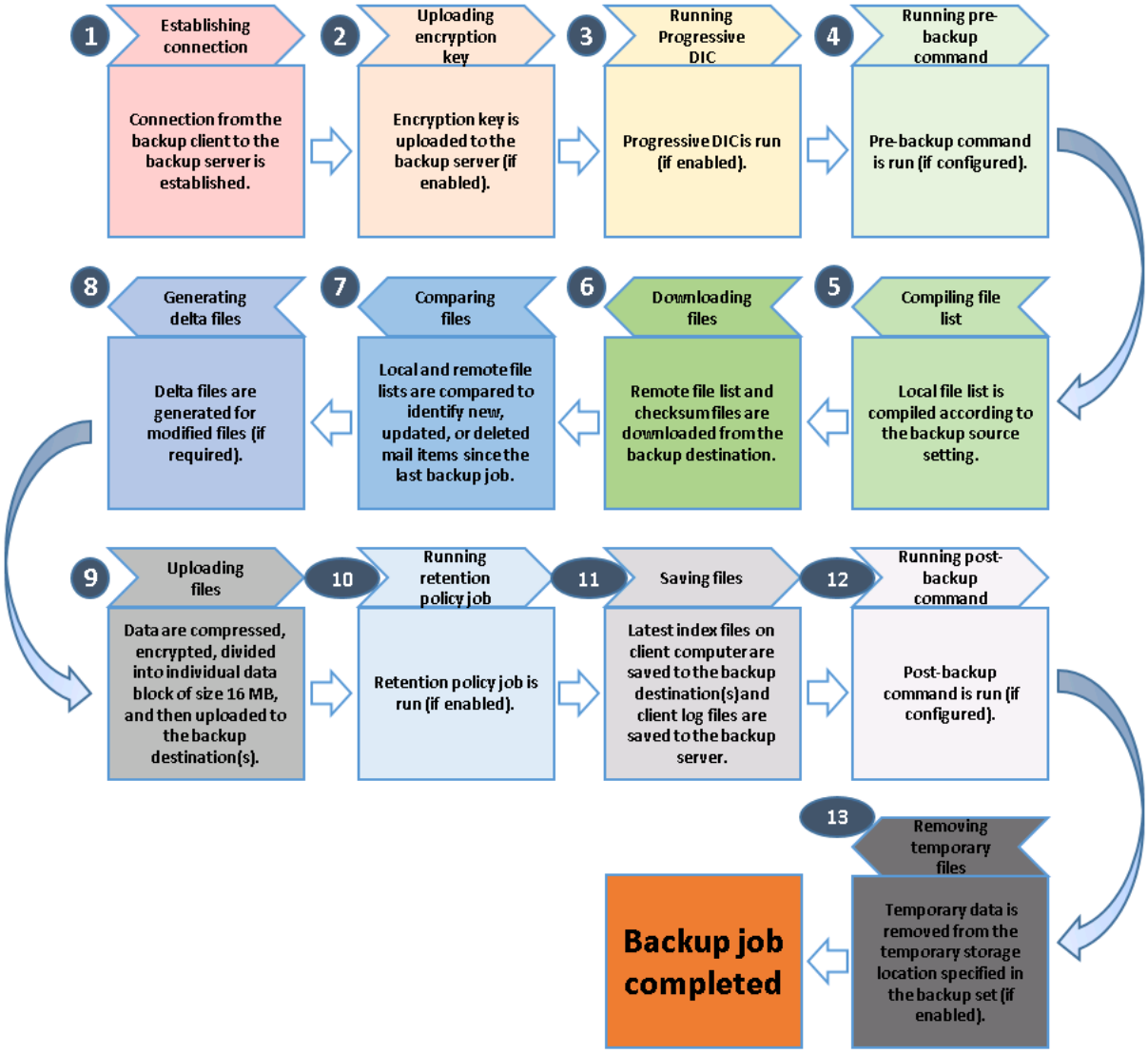
5 Overview of Cloud File Backup

The following steps are performed during a cloud file backup job:

Run on Server Cloud File Backup



Run on Client Cloud File Backup

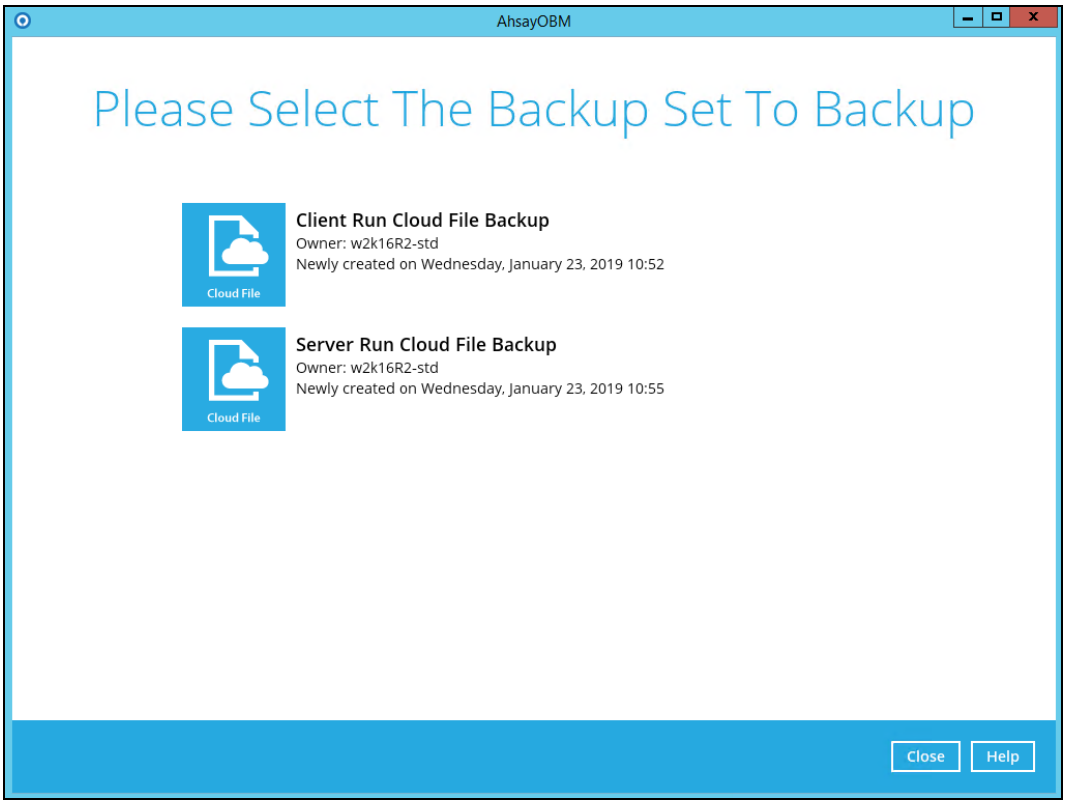


6 Running a Backup

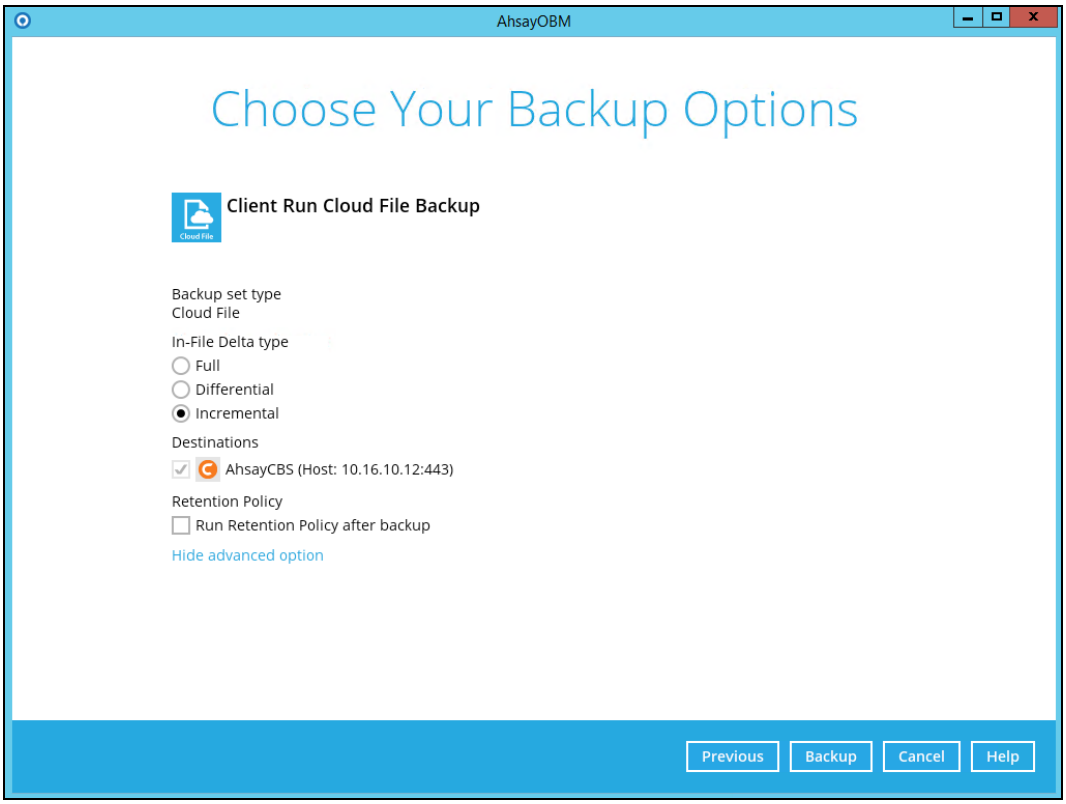
6.1 Start a Manual Backup in AhsayOBM

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

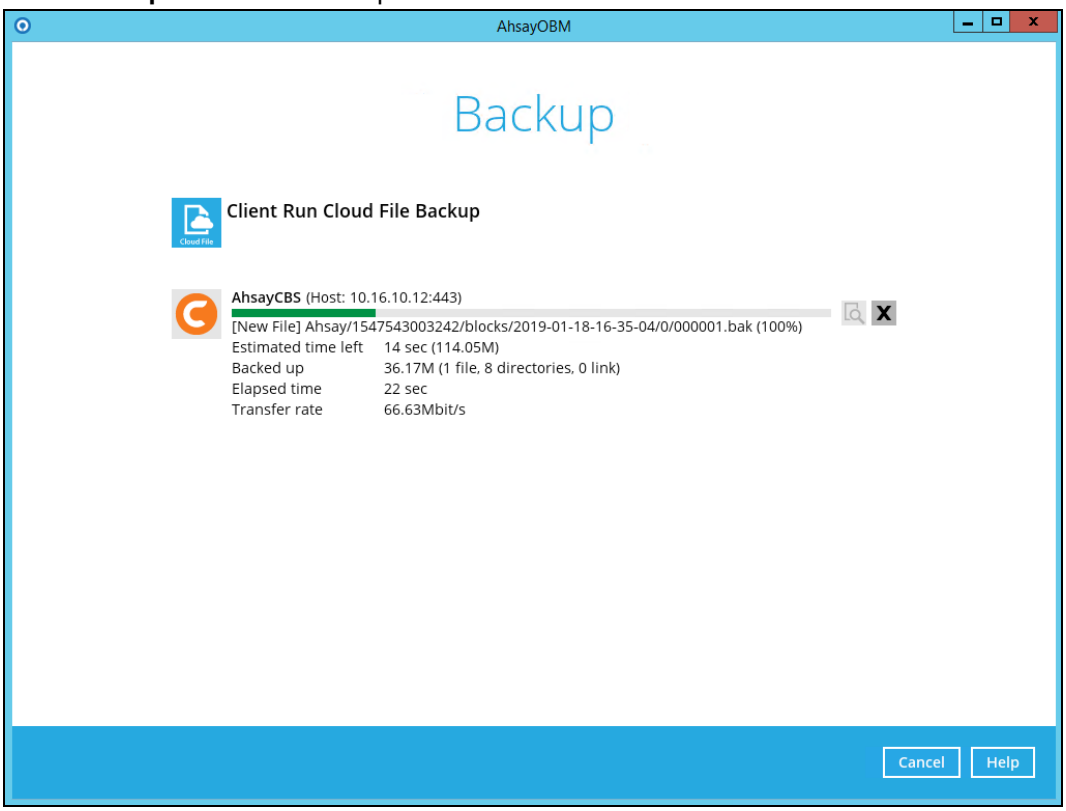
2. Select the backup set which you would like to start a backup for.



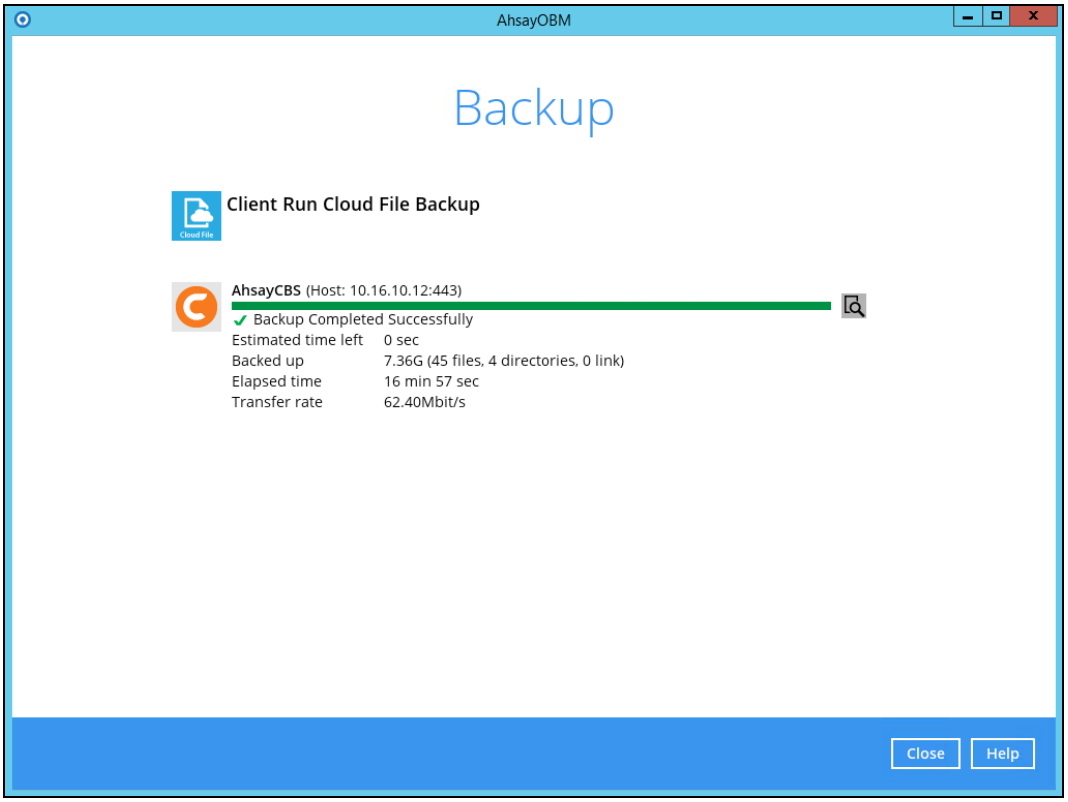
If you would like to modify the In-File Delta type, Destinations and Retention Policy Settings, click **Show advanced option**.



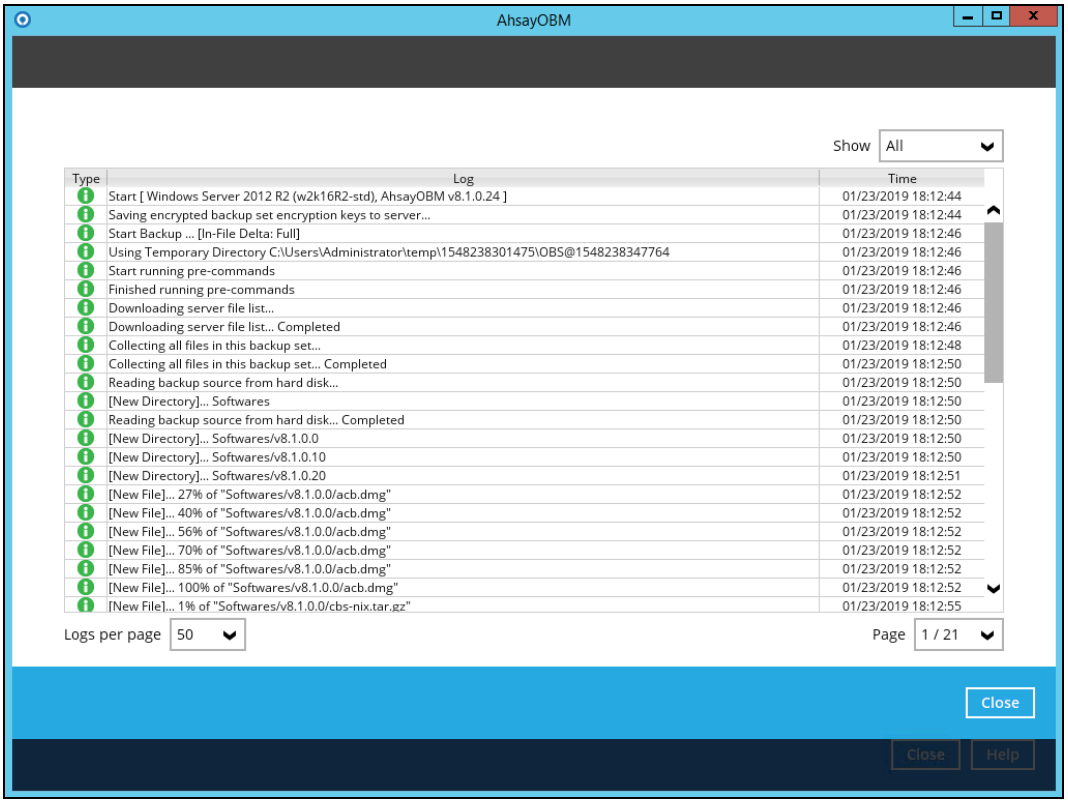
3. Click **Backup** to start the backup and wait until it is finish.



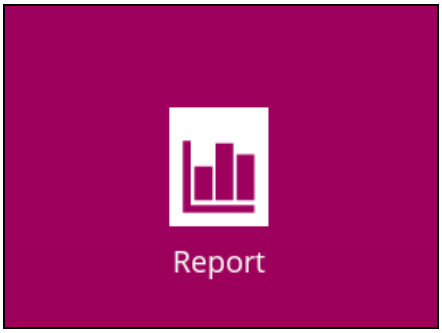
4. The backup through AhsayOBM has been successful.



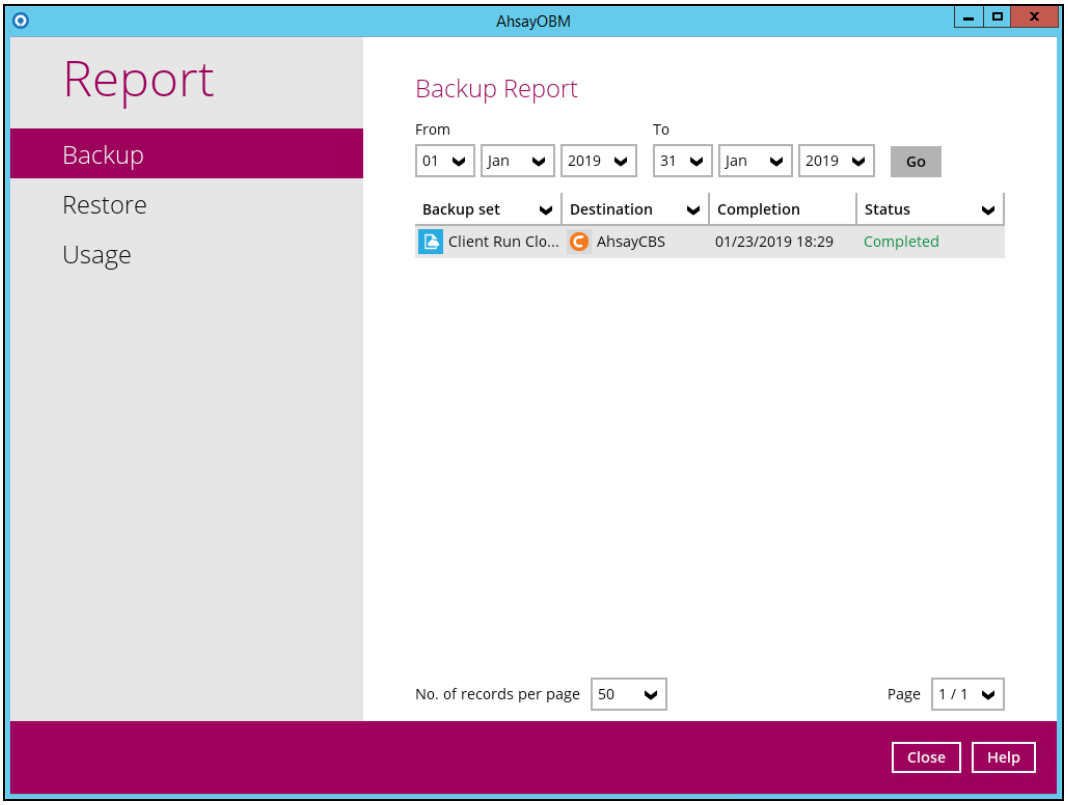
5. Check the log of your backup by clicking this icon  . It will show you the log of your backup with corresponding date and time.



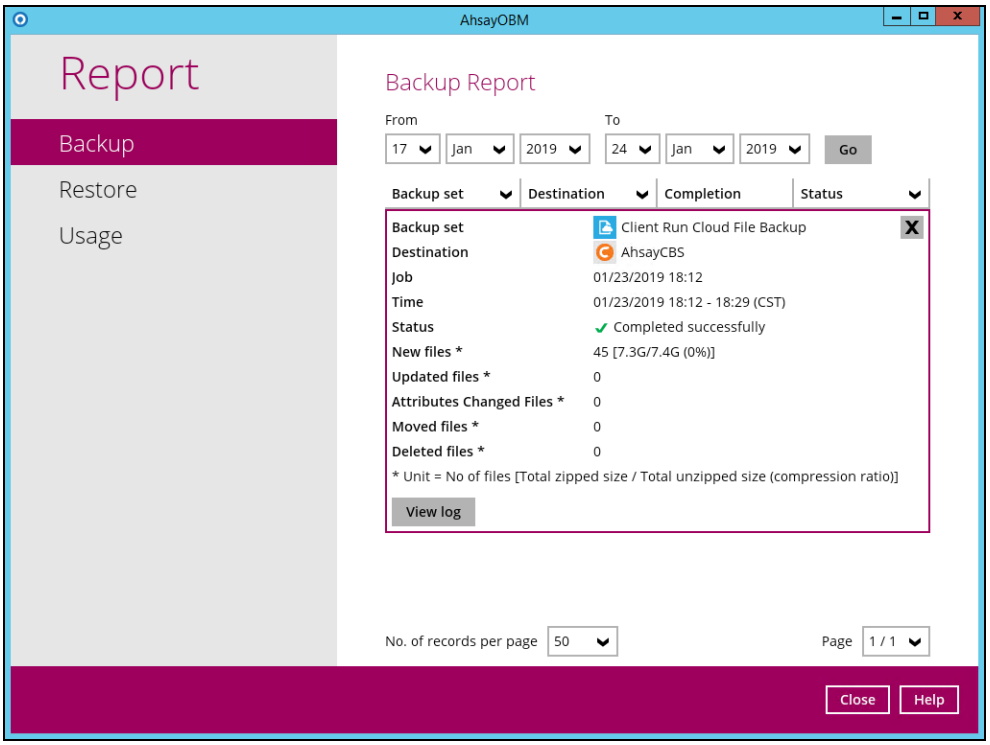
To view the report, go to the **Report > Backup**

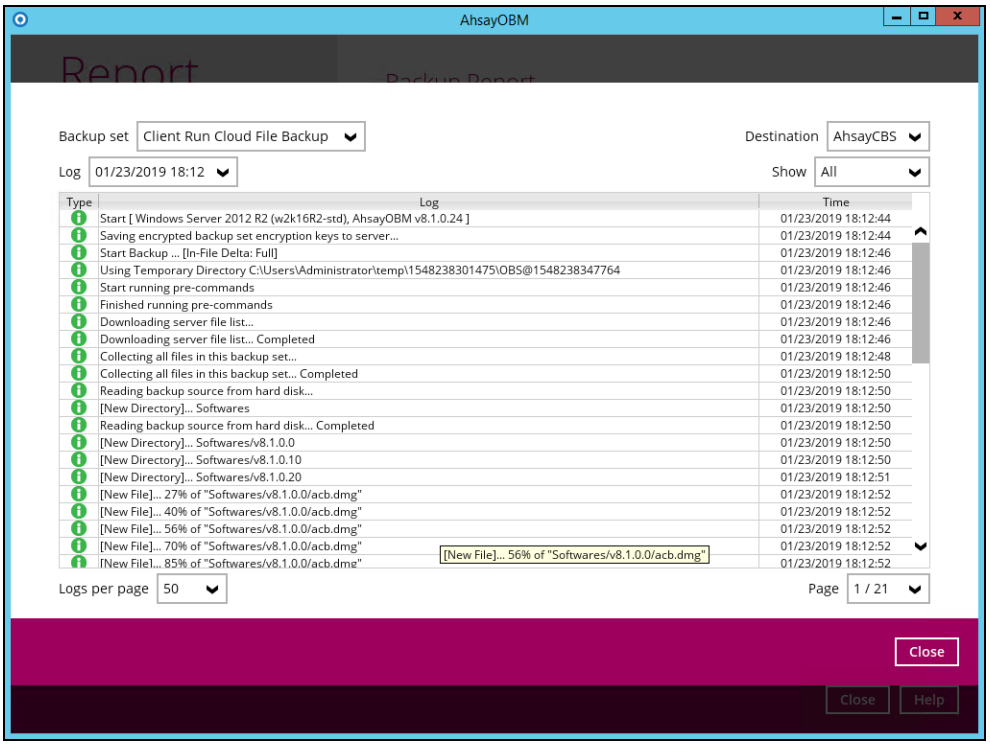


In this Backup Report screen, you can see the backup set with corresponding destination, completion date and time, and status.



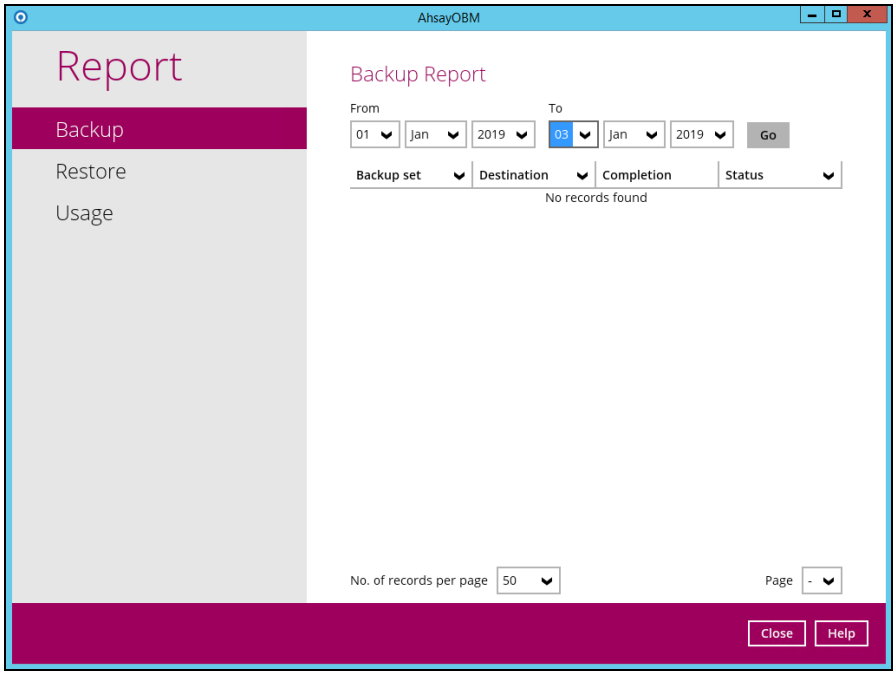
Click the backup report and the summary of the backup will be displayed. You can also click the **View Log**, this will redirect you to the log summary of your backup.





You can also search for backup reports from a specific period of date. For example, we have the **From** date which is, **01 Jan 2019** and the To date which is, **23 Jan 2019**. Then click the Go button to generate the available reports.

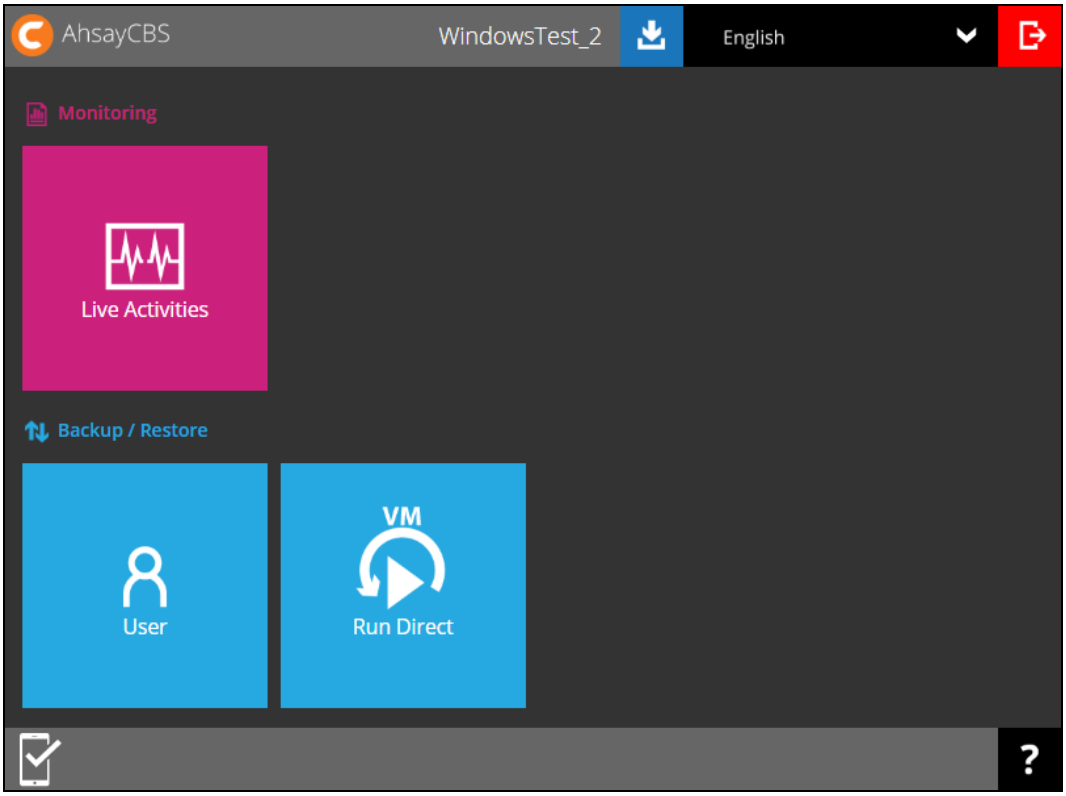
If this is a valid range of dates then backup reports will be displayed unless there were no backup running on the specified dates. A message of **No records found** will also be displayed.



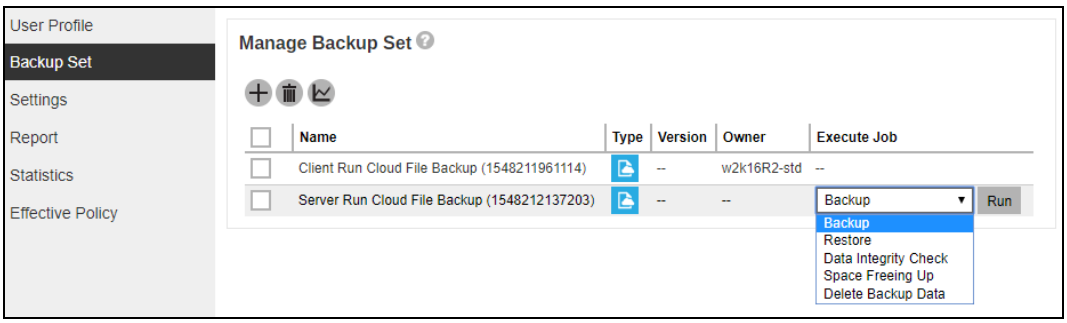
6.2 Start a Manual Backup on the AhsayCBS User Web Console

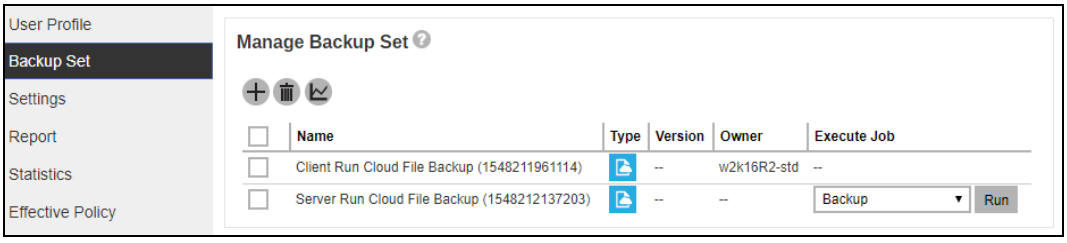
1. Log in to the User Web Console according to the instructions in Login to the AhsayCBS User Web Console.

2. Click on the **User** icon.

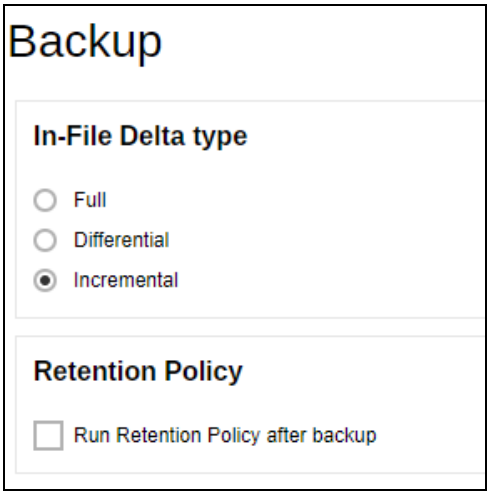


3. Select **Backup Set** from the left panel, then select **Backup** under **Execute Job** drop down menu.



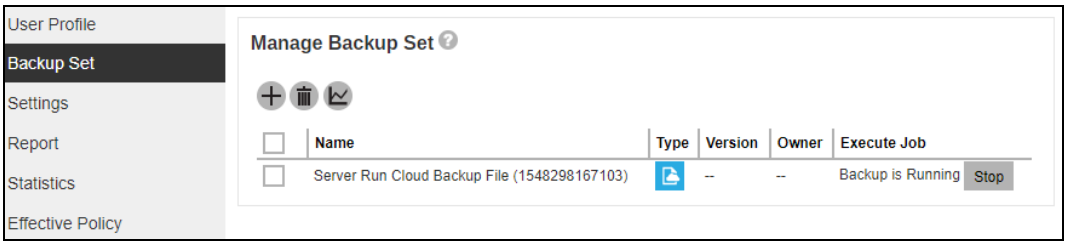


4. Modify the **In-File Delta type** and **Retention Policy** setting if necessary.

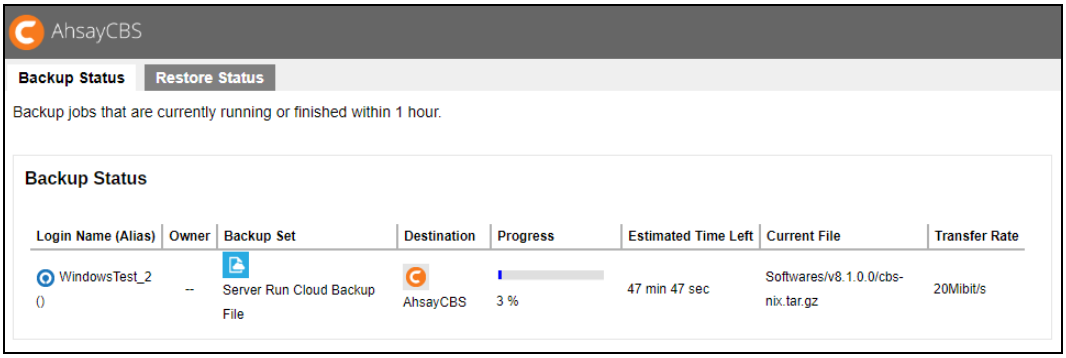


5. Click **Run Backup**  to start the backup job and wait until the backup is finished.

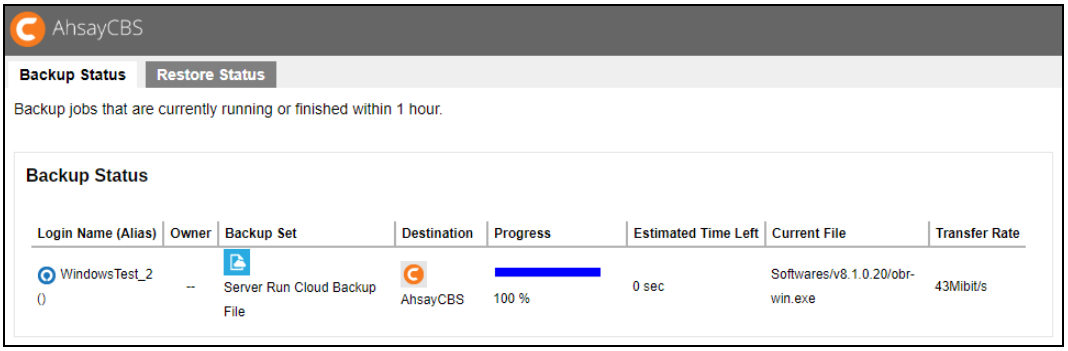
6. When a backup job is running, the status **Backup is Running** will be displayed. Click **Stop** to stop the backup job if necessary.



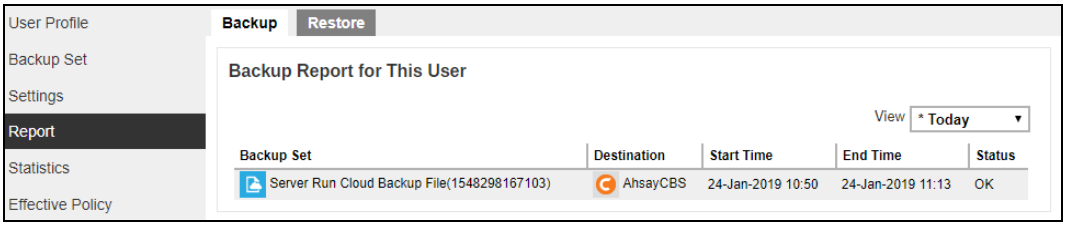
You can also check the status of your backup by going to the **Monitoring > Live Activities.**



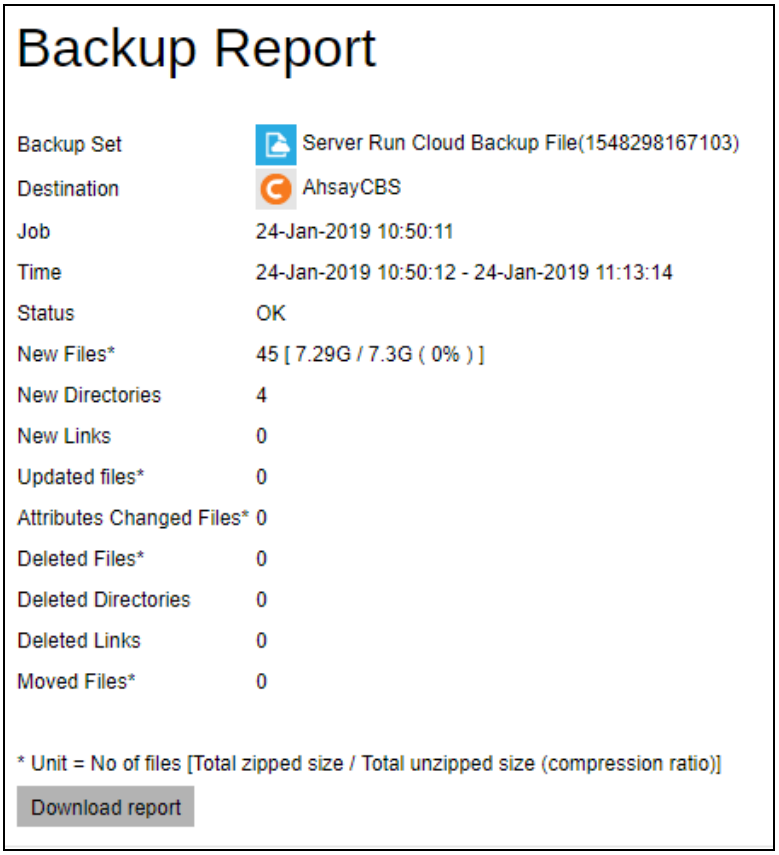
7. The backup through AhsayCBS User Web Console has been successful.



To view the report, go to the **Report > Backup.** In this Backup Report screen, you can see the backup set with corresponding destination, completion start and end date with time, and status.



Click the backup set and this screen will be displayed. It shows the summary of the backup and you can download the backup report by clicking the Download Report.



AhsayCBS

Full Backup report

Backup Job Summary

User	WindowsTest_2
Backup Set	Server Run Cloud Backup File (1548298167103)
Destination	AhsayCBS (AhsayCBS)
Data Size	7.34G
Retention Size	0
Backup Quota	100G
Remaining Quota	92.66G
Backup Job	2019-01-24-10-50-11
Job Status	OK
Start - End	01/24/2019 10:50:12 - 01/24/2019 11:13:14
IP Address	172.16.10.12
New Files *	45 (7.3G)
New Directories	4
New Links	0
Updated Files *	0 (0)
Attributes Changed Files *	0 (0)
Deleted Files *	0 (0)
Deleted Directories	0
Deleted Links	0
Moved Files *	0 (0)

* No. of files (size)

Backup Set Settings

Field	Value
Backup Source	[Softwares]
Filter	[Enabled: false]
Backup Schedule	[Computer Name: *][Daily:][Weekly:][Monthly:][Custom:]
Continuous Data Protection	[Enabled: No]
In-File Delta	[Enabled: Yes, Default Type: I, Block Size: -1, Minimum Size = 26214400, Maximum No. of Delta = 100, Delta Ratio = 50, Weekly: [], Monthly: [, Day: 0, Criteria: Friday, Day of selected months in yearly variations: First]
Retention Policy	[Type: Simple, Period: 7, Unit: Day(s)]
Command Line Tool	
Reminder	Logout Backup Reminder: *, Off-line Backup Reminder: , Off-line Notification Day: 1 Days 0 hours
Bandwidth Control	[Enabled: No, Mode: Independent, Bandwidth Control:]
Others	Remove temporary files after backup: Yes, Follow Link: Yes, Volume Shadow Copy: Yes, File Permissions: Yes, Compression Type: Fast (Compressed size larger than normal)

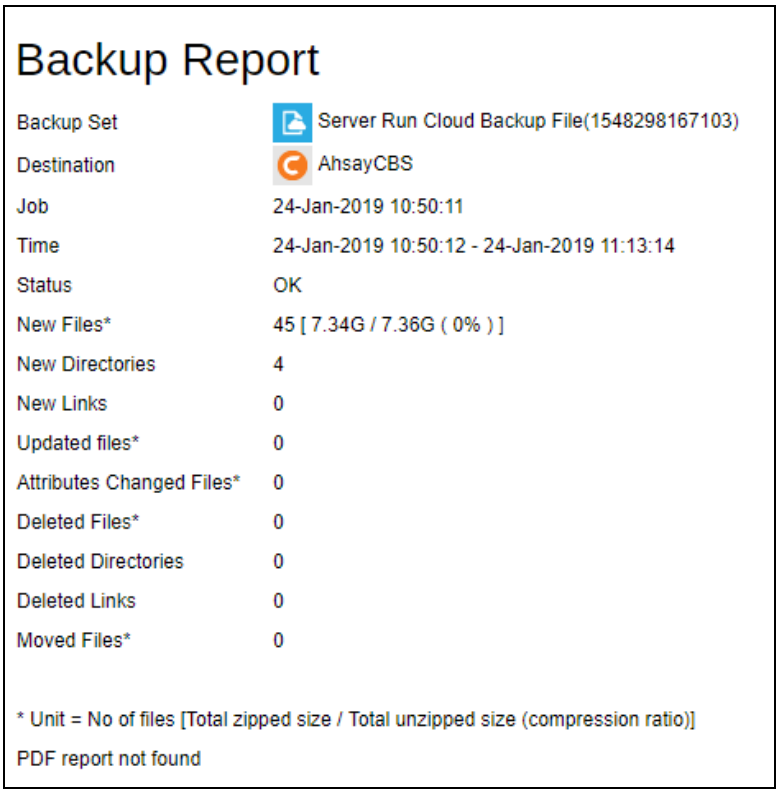
Backup Logs

No.	Type	Timestamp	Log
1	start	2019/01/24 10:50:12	Start [Windows Server 2012 R2 (w2k16R2-std), Ahsay Cloud Backup Suite v8.1.0.24]
2	info	2019/01/24 10:50:14	Using Temporary Directory C:\Program Files\AhsayCBS\temp\1548298167103\Local@1548298202136

Backup Files

No.	Type	Dirs/Files	Size	Last Modified
1	new	Softwares	0 / 0 (0%)	
2	new	Softwares/v8.1.0.0	0 / 0 (0%)	
3	new	Softwares/v8.1.0.10	0 / 0 (0%)	
4	new	Softwares/v8.1.0.20	0 / 0 (0%)	

Make sure to wait 15 to 20 minutes after the backup to be able to download the report file otherwise the report will not be displayed.



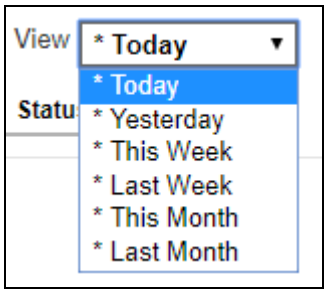
Backup Report

Backup Set	Server Run Cloud Backup File(1548298167103)
Destination	AhsayCBS
Job	24-Jan-2019 10:50:11
Time	24-Jan-2019 10:50:12 - 24-Jan-2019 11:13:14
Status	OK
New Files*	45 [7.34G / 7.36G (0%)]
New Directories	4
New Links	0
Updated files*	0
Attributes Changed Files*	0
Deleted Files*	0
Deleted Directories	0
Deleted Links	0
Moved Files*	0

* Unit = No of files [Total zipped size / Total unzipped size (compression ratio)]

PDF report not found

You can also view the reports for Today, Yesterday, This Week, Last Week, This Month, and Last Month. Pick any of the following choices and the available reports will be displayed.



7 Restoring with a Cloud File Backup Set

7.1 Restore with AhsayOBM

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**

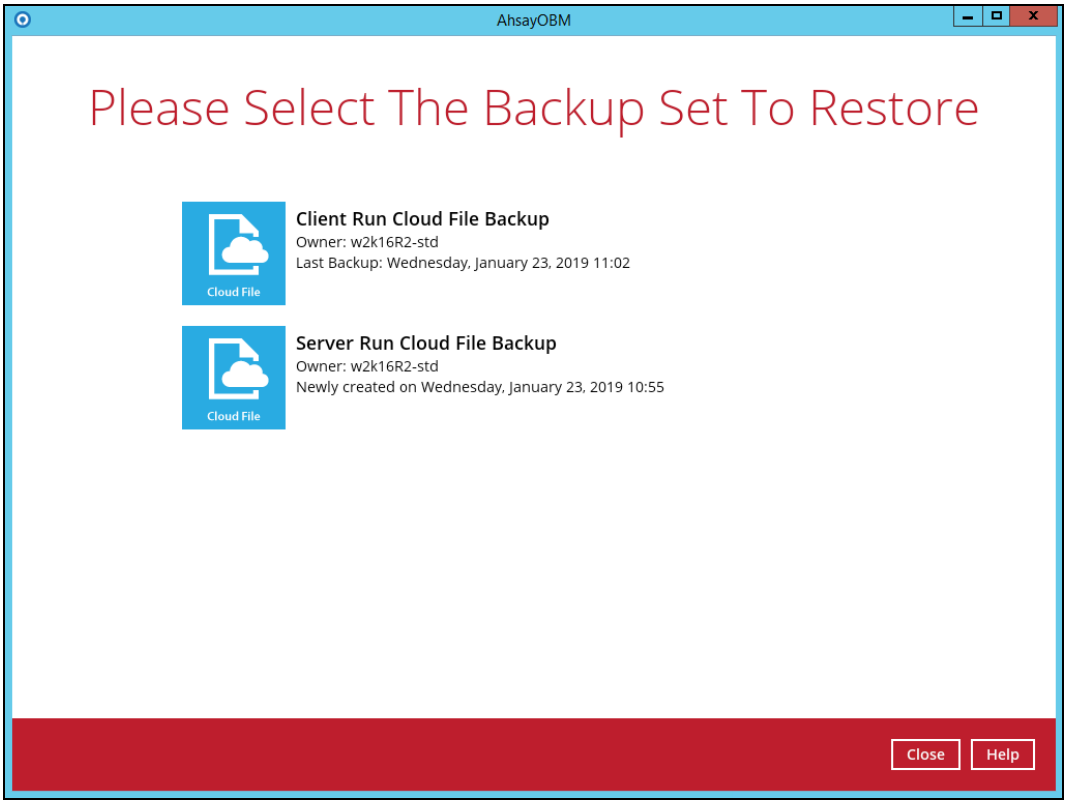
  Besides the two options above, you can also restore your data to an alternate location which is through the same cloud storage but on a different folder.

Note

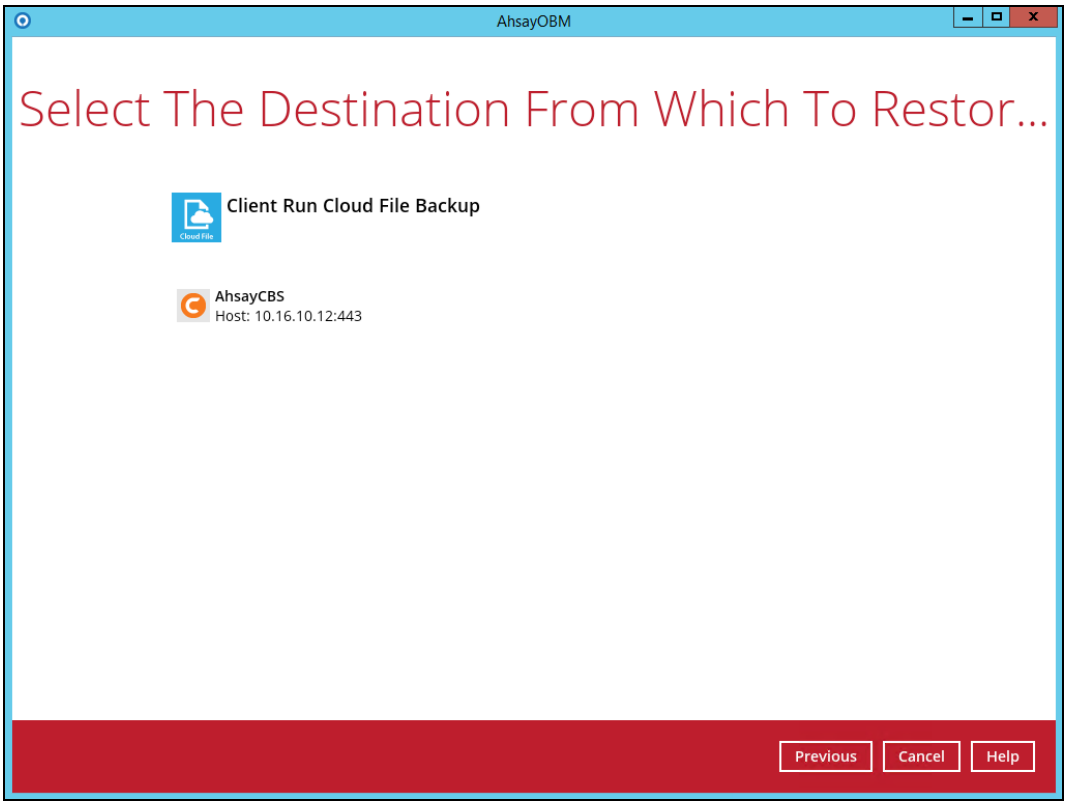
Login to the AhsayOBM application according to the instruction provided in the chapter on Login to AhsayOBM.

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

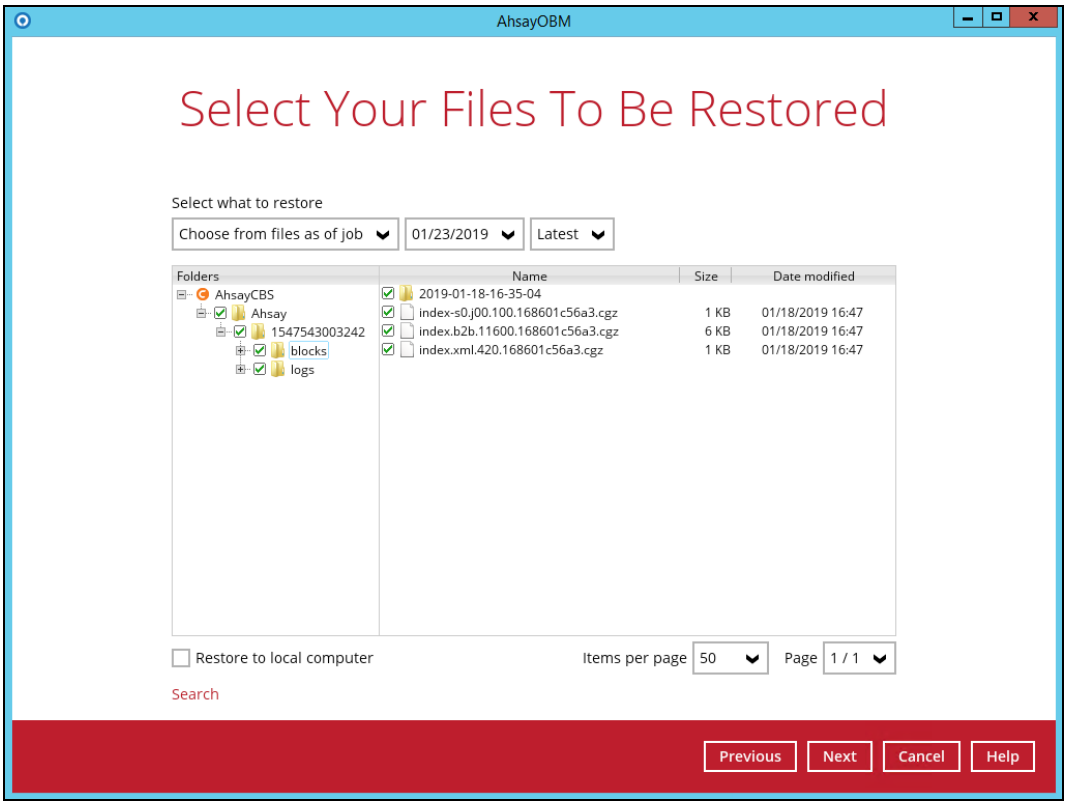
2. Select the backup set that you would like to restore from.



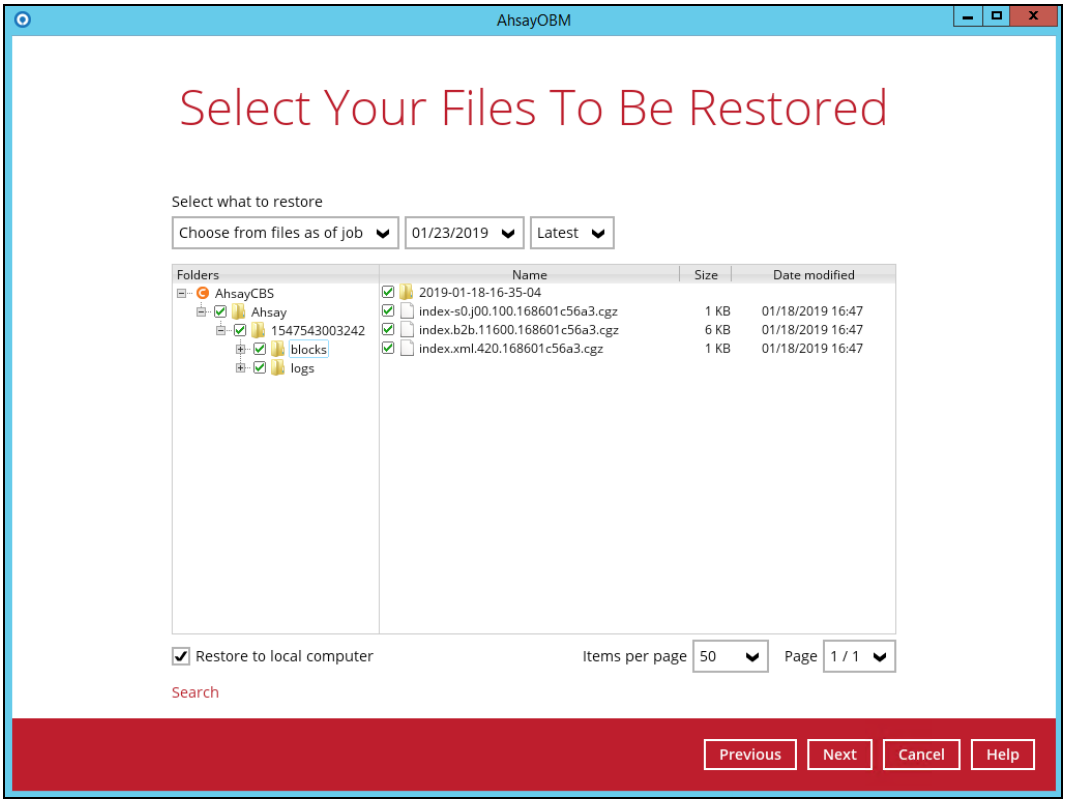
3. Select the backup destination that contains the data that you would like to restore.



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

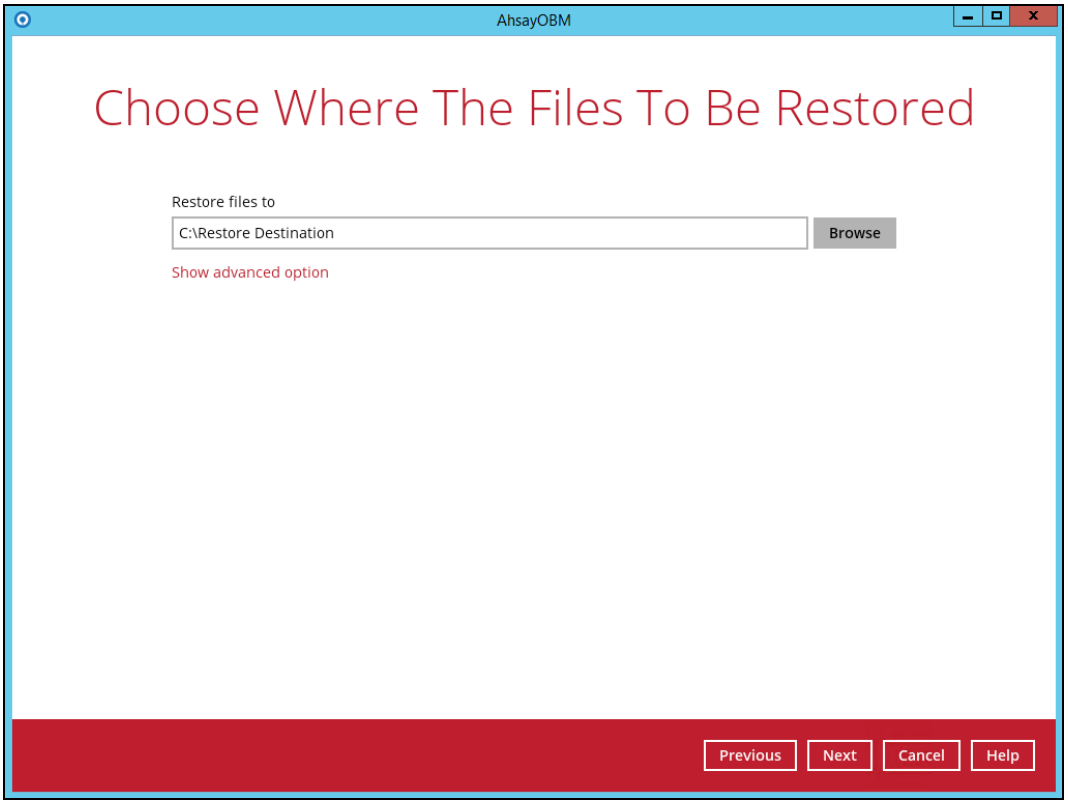


5. Select **Restore to local computer** if you want to restore the backed up data to the location computer.

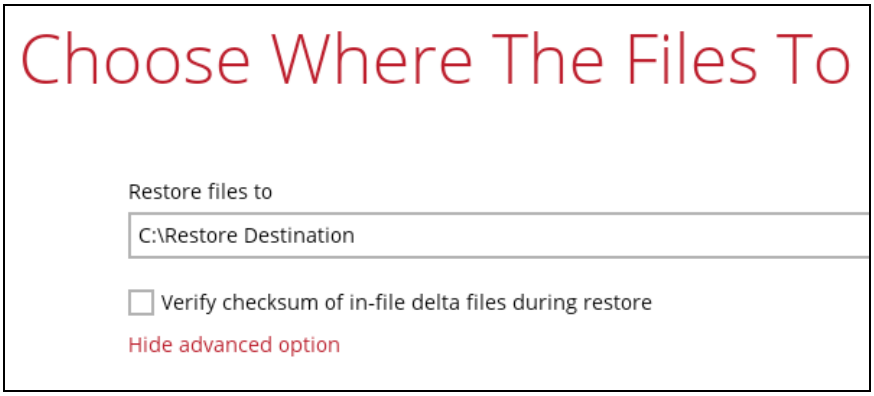


Click **Next** to continue.

6. If you want to restore on your local computer, browse to the corresponding directory path on the local computer that you want the data to be restored to.



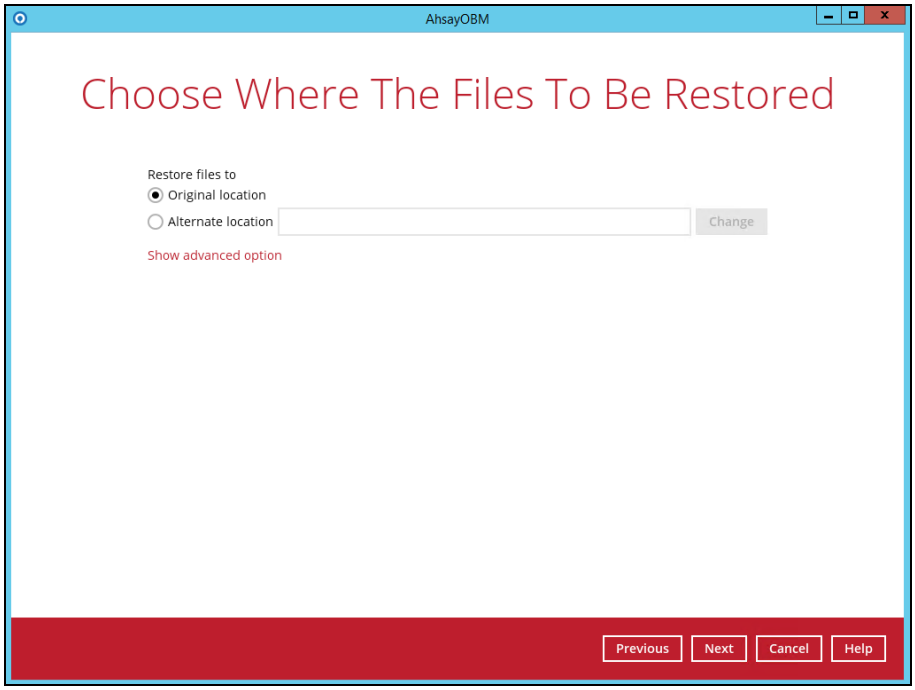
Click **Show advanced option** to configure other restore settings.



- **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.

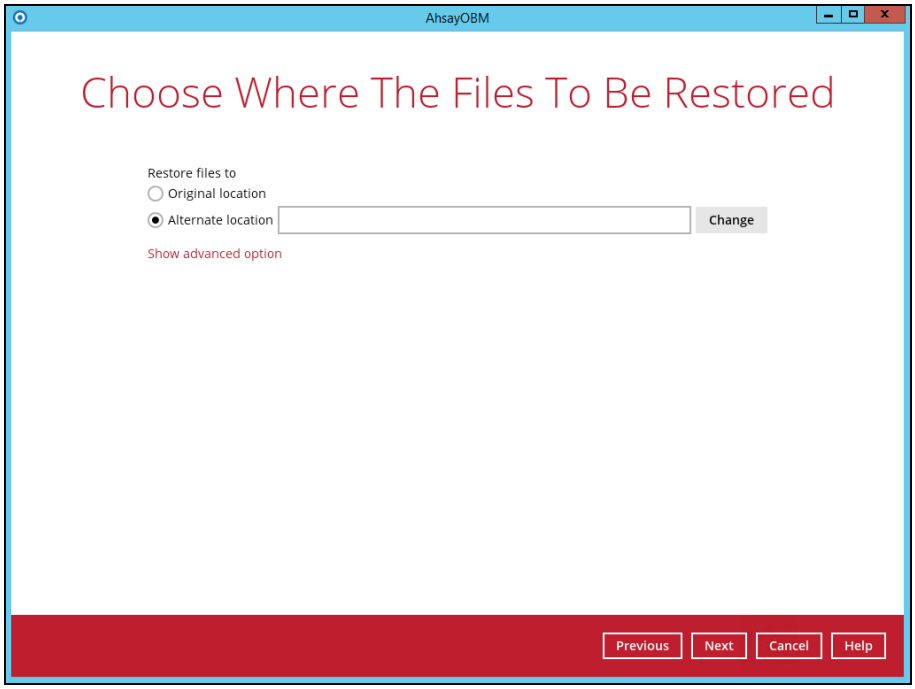
- **Original location** – The backed-up date will be restored to the computer running the AhsayOBM under the same directory path as on the machine storing the backup source.

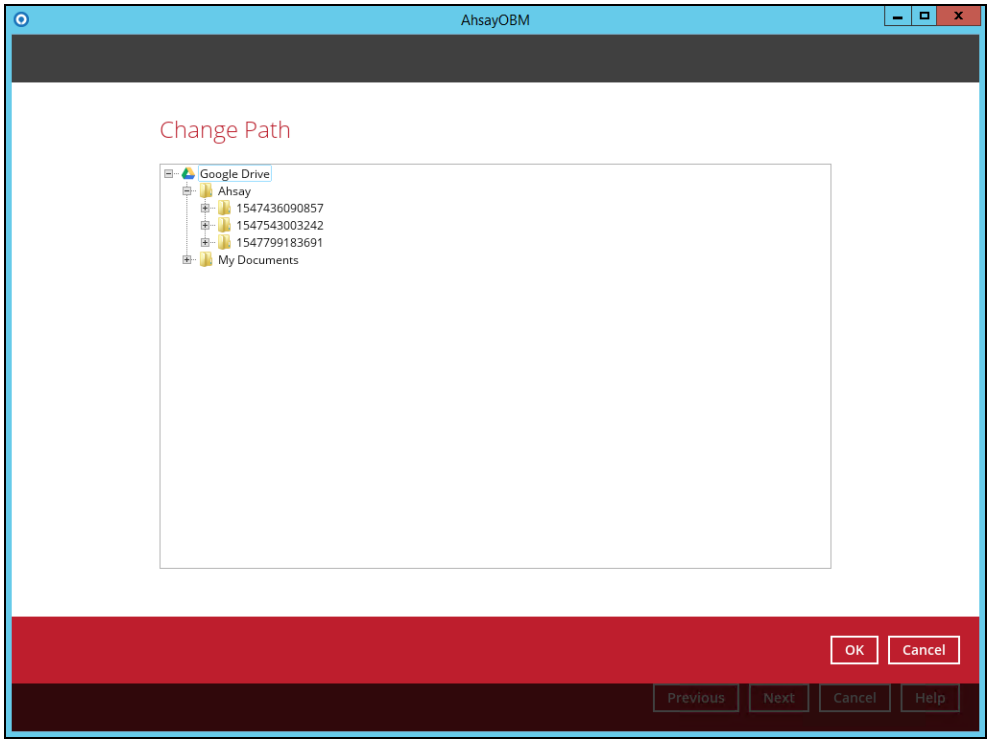


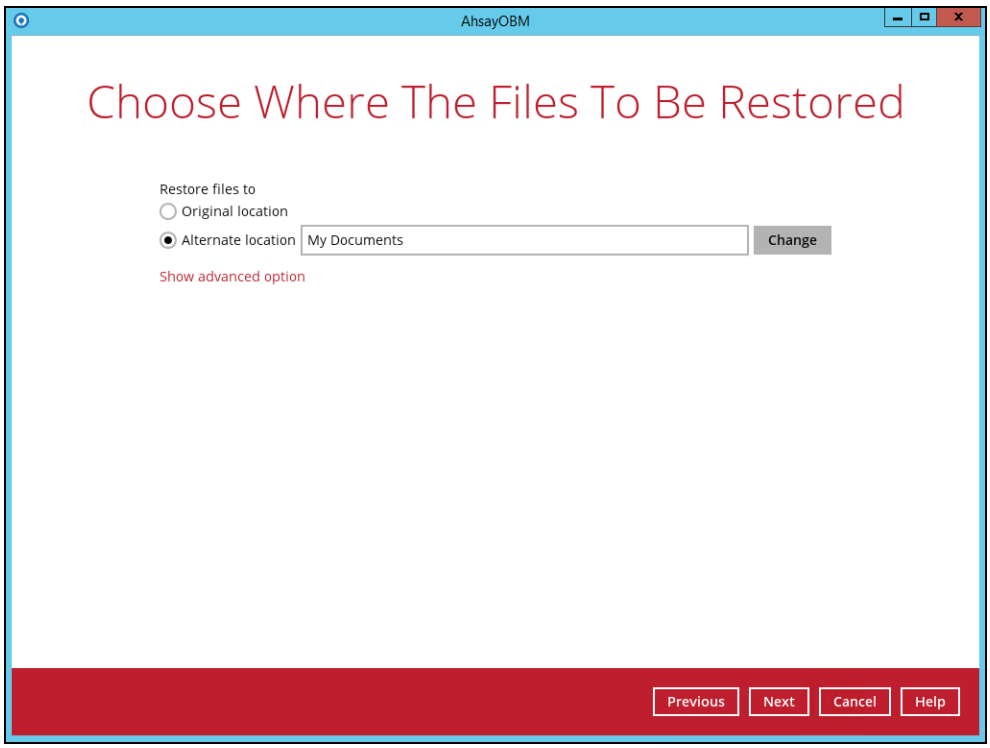
- **Alternate location –** You can choose to restore the data to a location of your choice. Click **Change** to browse to the alternate path on the cloud storage.

Important: *Data can only be restored to a local computer, or to the original cloud storage that the data was backed up from (e.g. same cloud storage provider and same account). You cannot restore the data to a different cloud storage (e.g. a different cloud storage provider or different account)*

In this example, we have chosen the **My Documents** folder as the alternate location on the cloud storage.

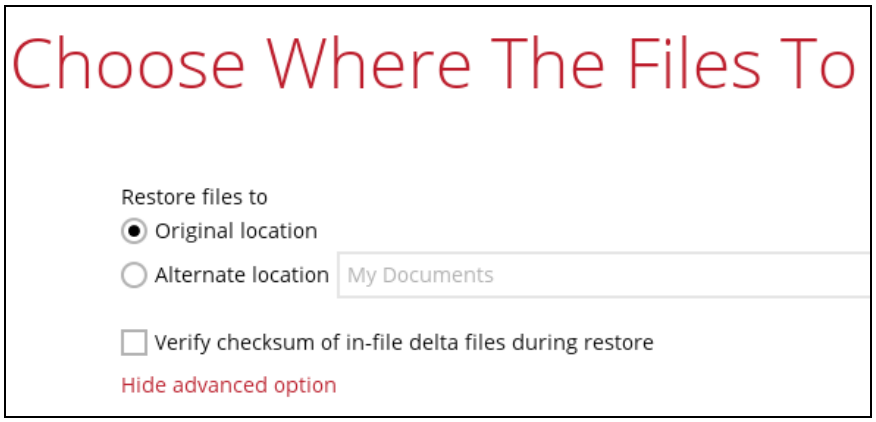



AhsayOBM
Change Path
Google Drive
Ahsay
1547436090857
1547543003242
1547799183691
My Documents
OK
Cancel
Previous
Next
Cancel
Help

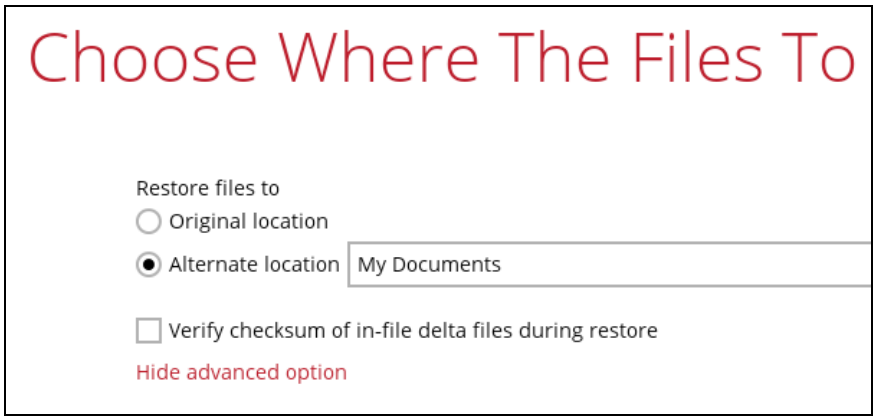

AhsayOBM
Choose Where The Files To Be Restored
Restore files to
Original location
Alternate location
My Documents
Change
Show advanced option
Previous
Next
Cancel
Help

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

- **Original location**



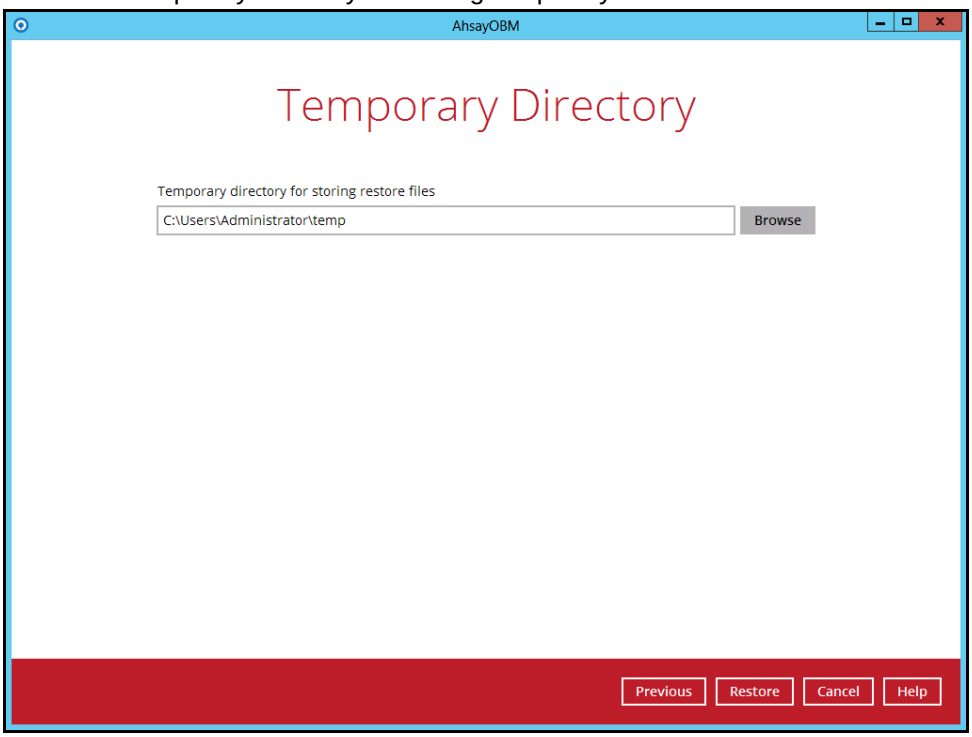
- **Alternate location**



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

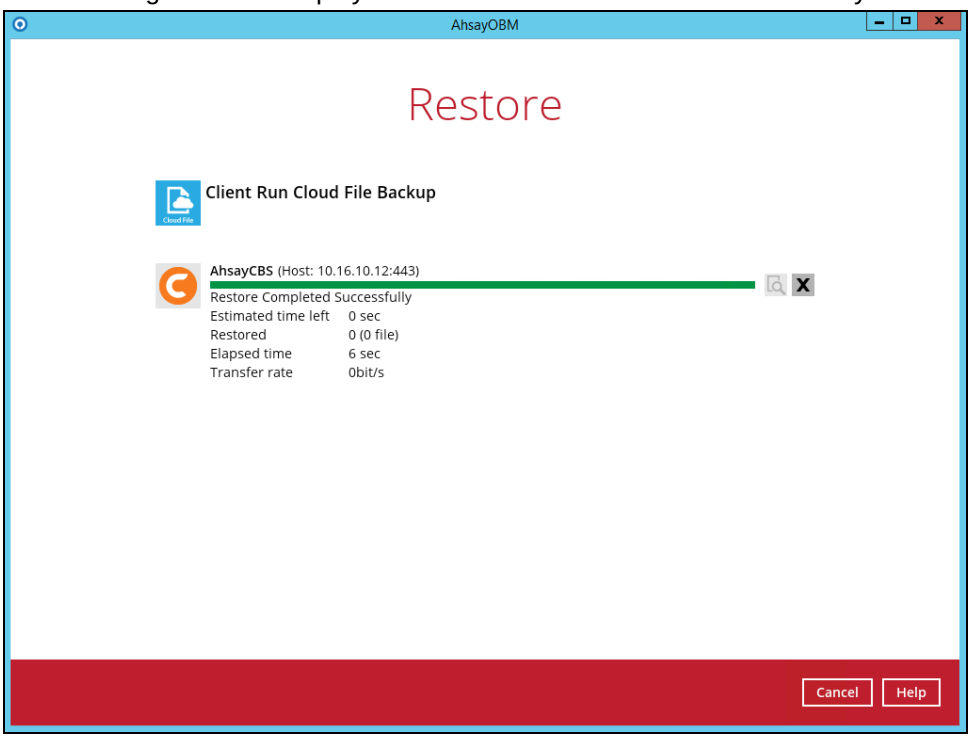
  By enabling this option, the checksum of in-file delta files will be verified during the restore process. This will check the data for errors during the restore process and create a data summary of the in-file delta files which will be included in the report.

7. Select the temporary directory for storing temporary files.

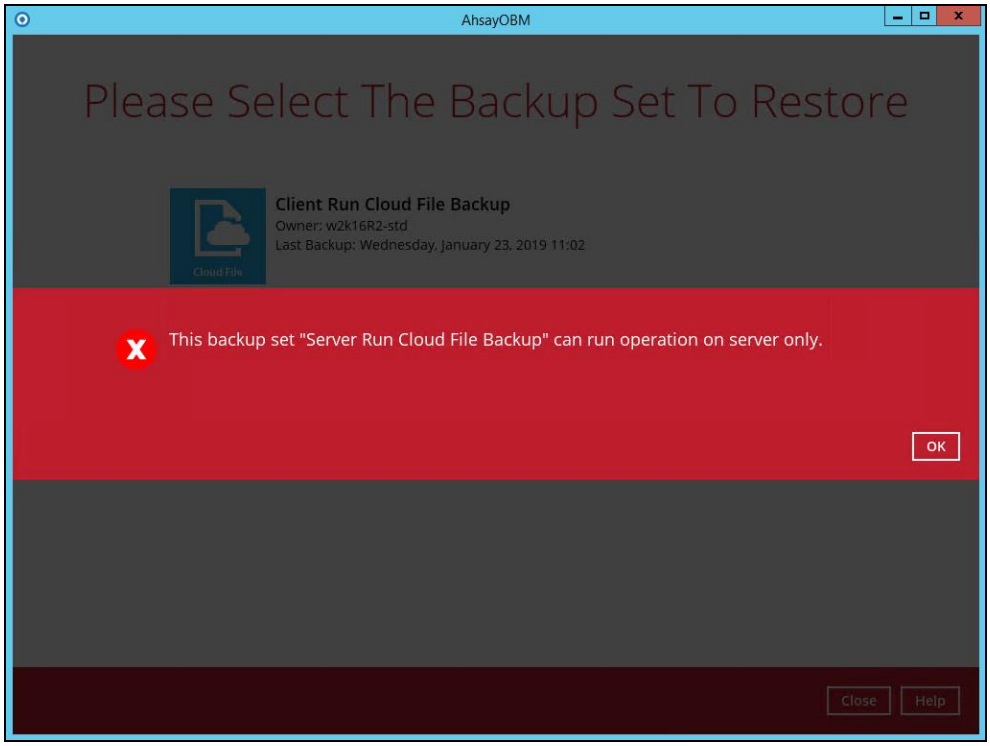


8. Click **Restore** to start the restoration.

9. 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.*



*Refer to the chapter on [Restore with the AhsayCBS Web Console] for instruction on how to restore data for a **Run on Server** Cloud File backup set.*

7.2 Restore with the AhsayCBS User Web Console

Using AhsayCBS Web Console to do the restoration has two (2) options unlike using the AhsayOBM which has 3 options. It is through Original 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.

- **Original location**

  Restore your data to your original location, on the cloud storage, where you backed them up.

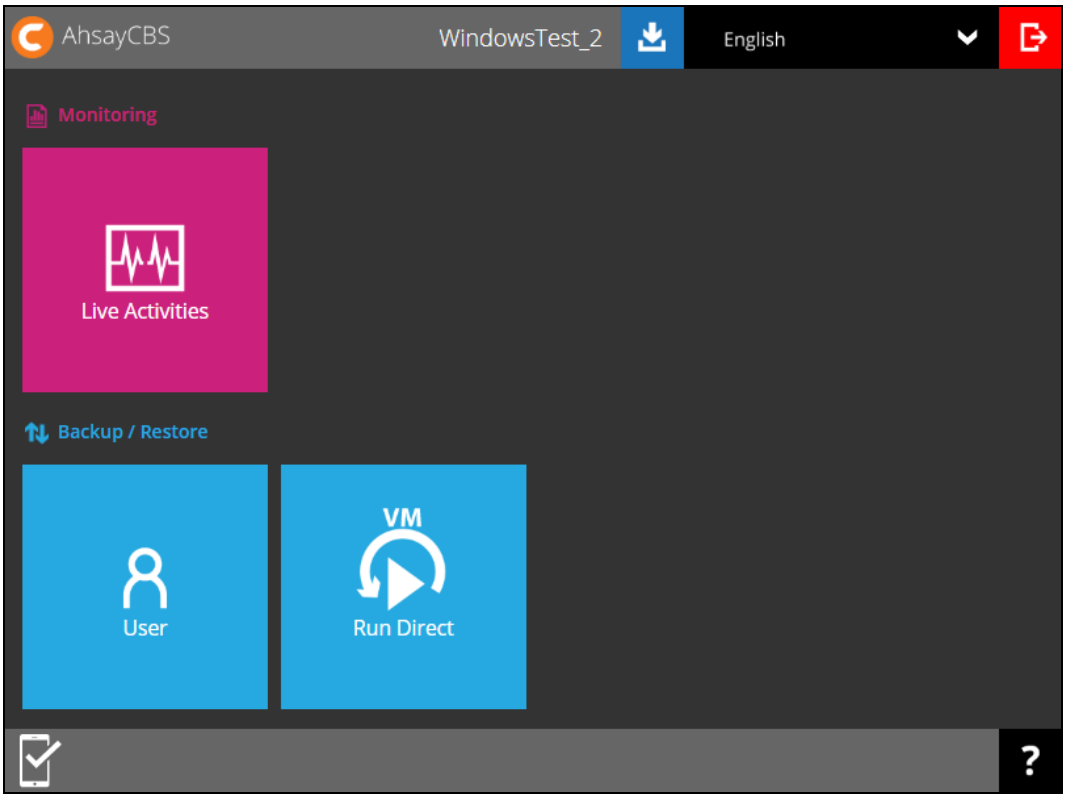
- **Alternate location**

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

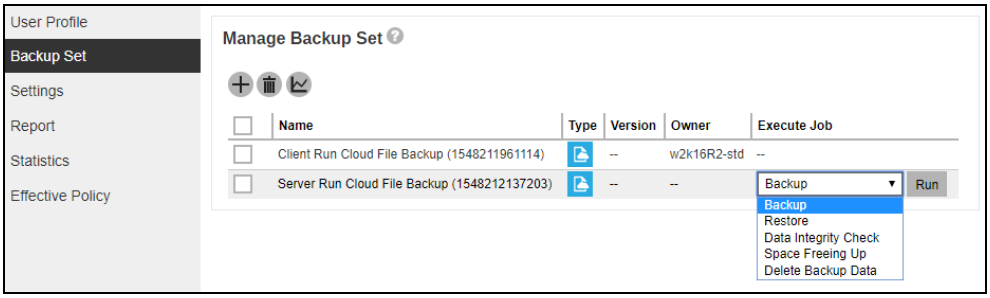
Notes

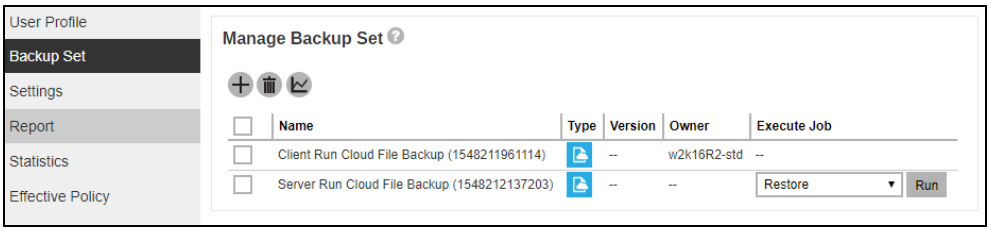
- Login to the AhsayOBM application according to the instruction provided in the chapter on Login to AhsayOBM.
- Data of a Run on Server Cloud File backup set can only be restored via the AhsayCBS web console

1. Click on the **User** icon.

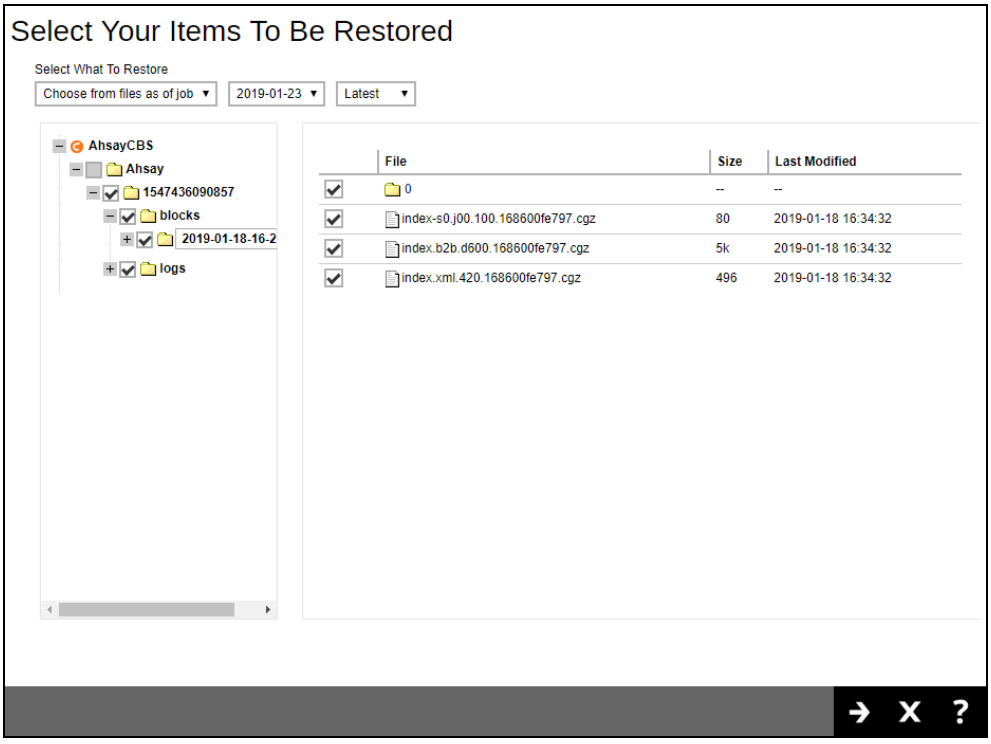


2. Select **Backup Set** from the left panel, then select **Restore** under **Execute Job** drop down menu.



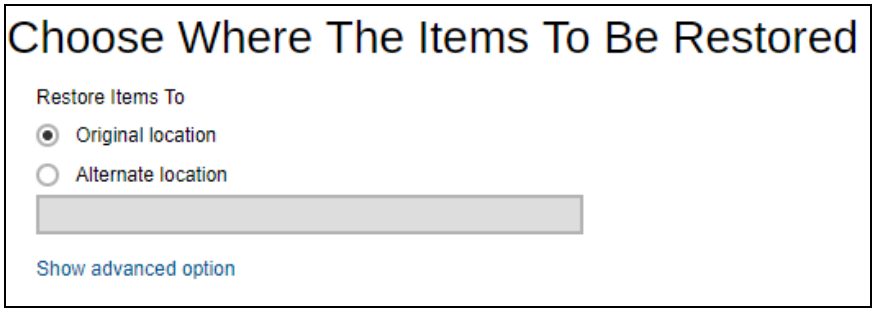


3. Select to restore from a specific backup job, or the latest job available from the Select **What To Restore** drop down menu. Click **Next** to proceed.

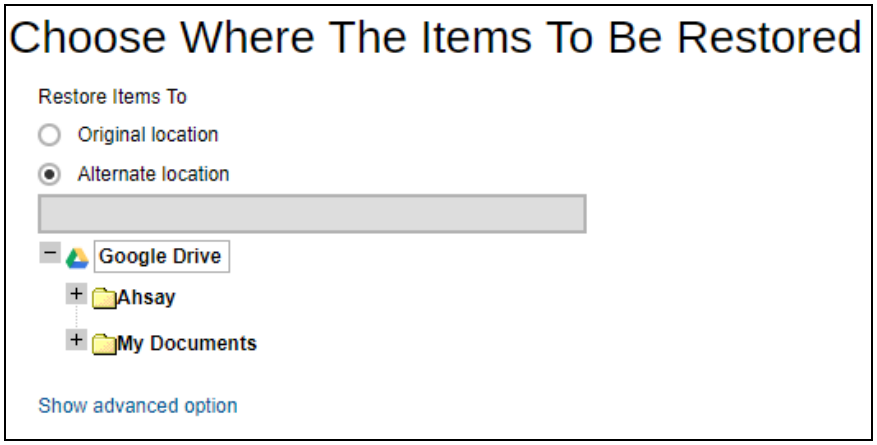


4. Select **Original location** to restore the data to the original directory path on the cloud storage, or **Alternate location** to restore to the data to an alternate path on the cloud storage.

- **Original Location**



- **Alternate Location**

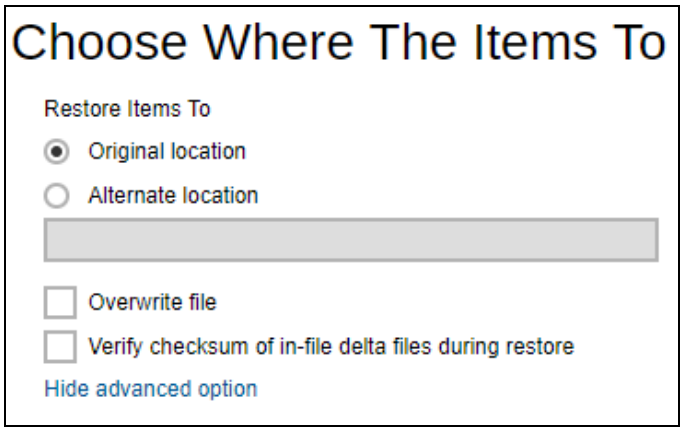


Expand the directory path to browse to the alternate location on the cloud storage. In this example we have two (2) available folders, Ahsay and My Documents for Google Drive.

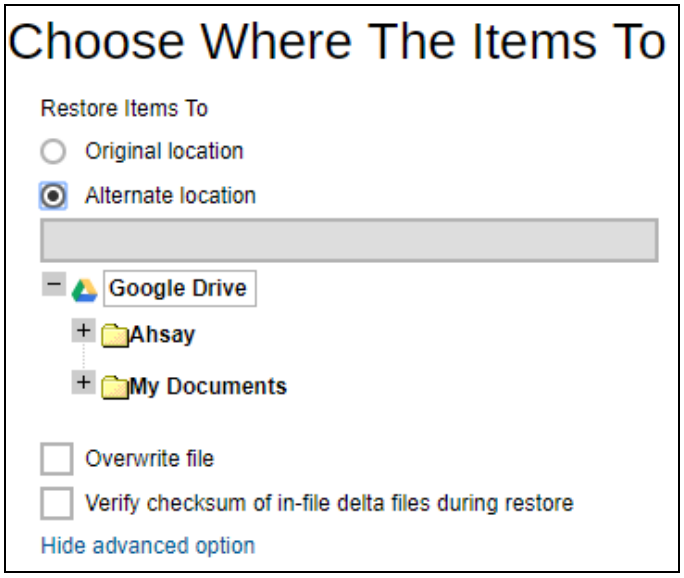
Important: *Data can only be restored to the original cloud storage that the data was backed up from (e.g. same cloud storage provider and same account).*

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

- **Original location**



- **Alternate location**



- **Overwrite file**

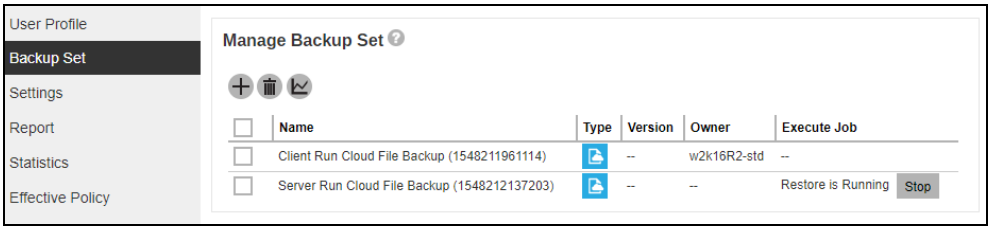
  By enabling this option, this will overwrite your existing files. For example, if the files/folders you are going to restore are already available in your chosen alternate location then during the restore process your existing files will be overwritten.

- **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.

5. Click the  icon to start the restoration.

6. You will see the status showing **Restore is Running** when the restore is in progress. Click **Stop** to stop the restore job if necessary.



8 Technical Assistance

To contact Ahsay support representatives for technical assistance, visit the following website:
https://www.ahsay.com/jsp/en/contact/kbQuestion.jsp

Also use the Ahsay Knowledge Base for resource such as Hardware Compatibility List, Software Compatibility List, and other product information:
http://wiki.ahsay.com/doku.php?id=public:home

9 Documentation

Documentations for all Ahsay products are available at:
https://www.ahsay.com/jsp/en/home/index.jsp?pageContentKey=ahsay_downloads_documentation_guides

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

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

Appendix

Appendix A Setting Backup Destination on AhsayOBM for Backup Set Created on AhsayCBS User Web Console

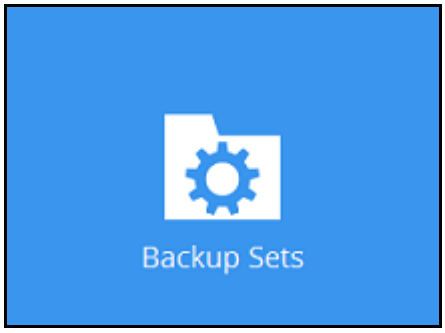
You need to read the instructions below only if you:

- Have created a backup set on AhsayCBS User Web Console; **AND**
- Selected the backup set to Run on Client; **AND**
- Have not selected any Predefined Destination in the backup creation process on the User Web Console

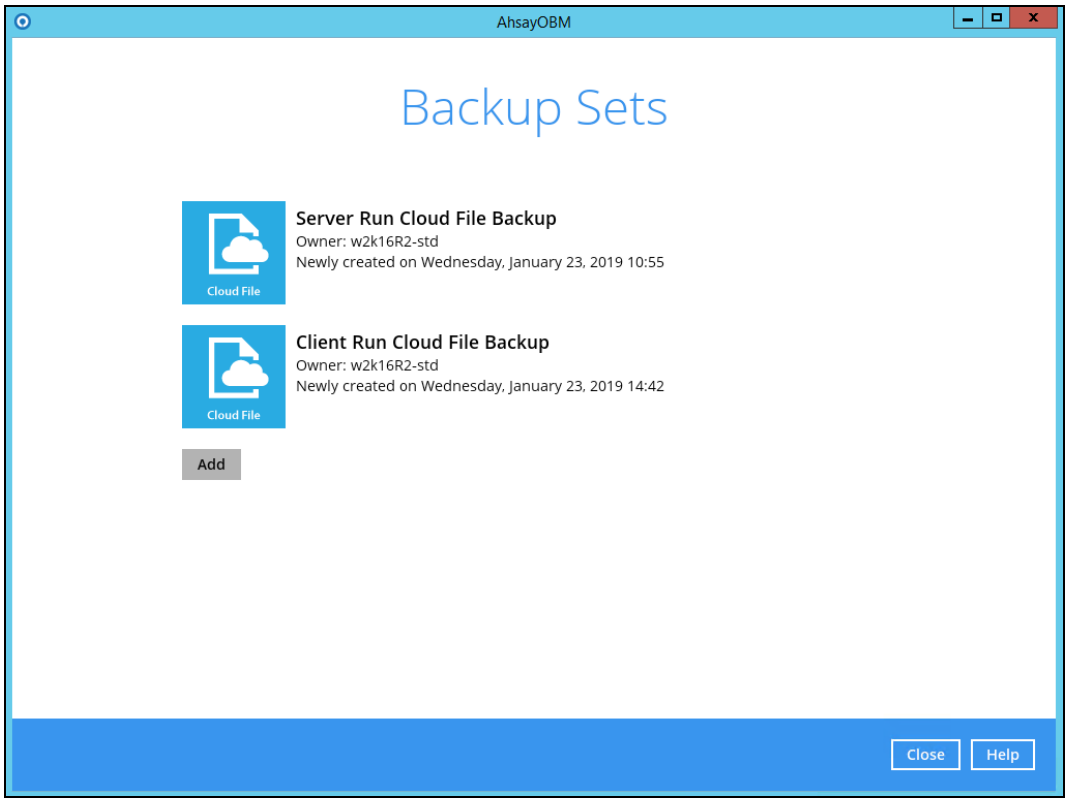
  -**OR-**

  Have selected a Predefined Destination in the backup creation process on User Web Console but wish to add additional backup destination other than the predefined destination

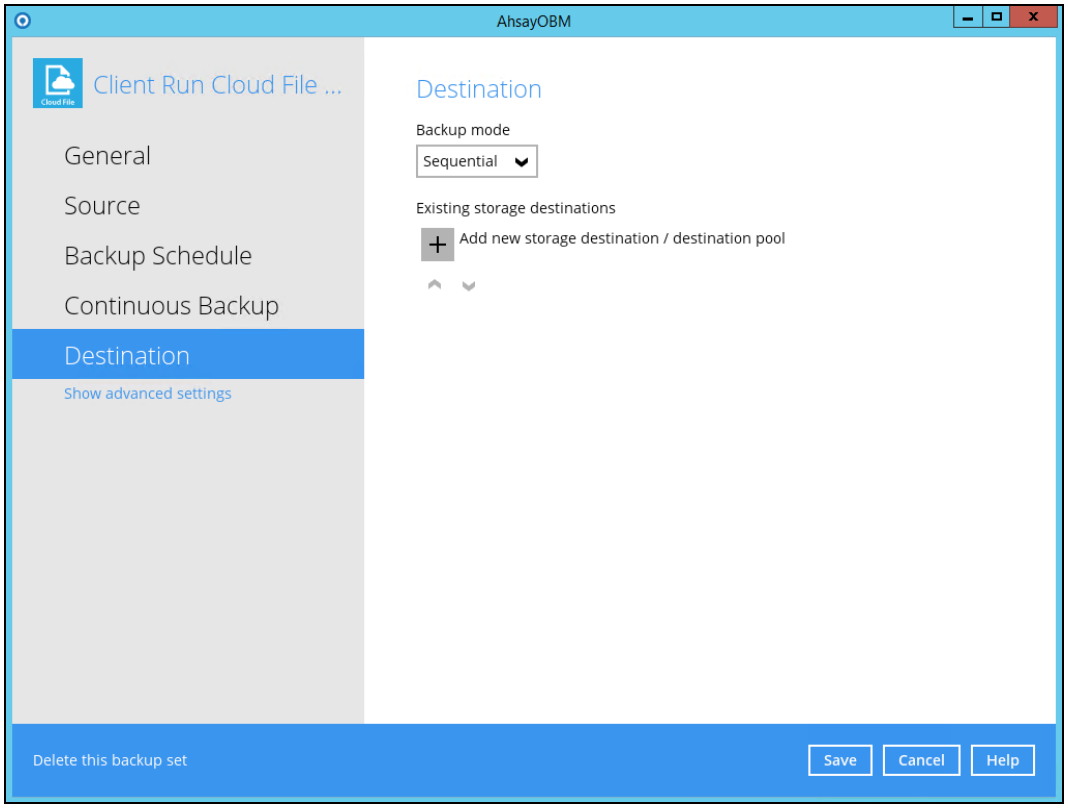
1. Log in to AhsayOBM according to the instructions in Login to AhsayOBM.
2. In the AhsayOBM main interface, click **Backup Sets**.



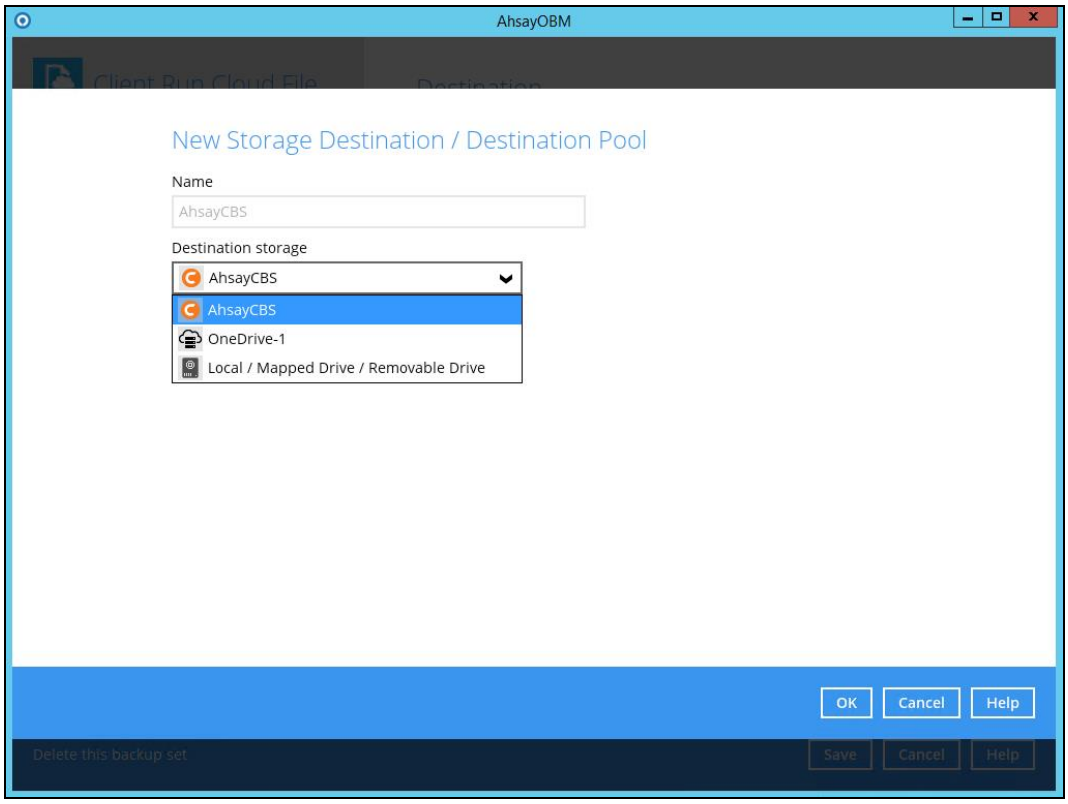
3. Click the backup set which you wish to add backup destination to.



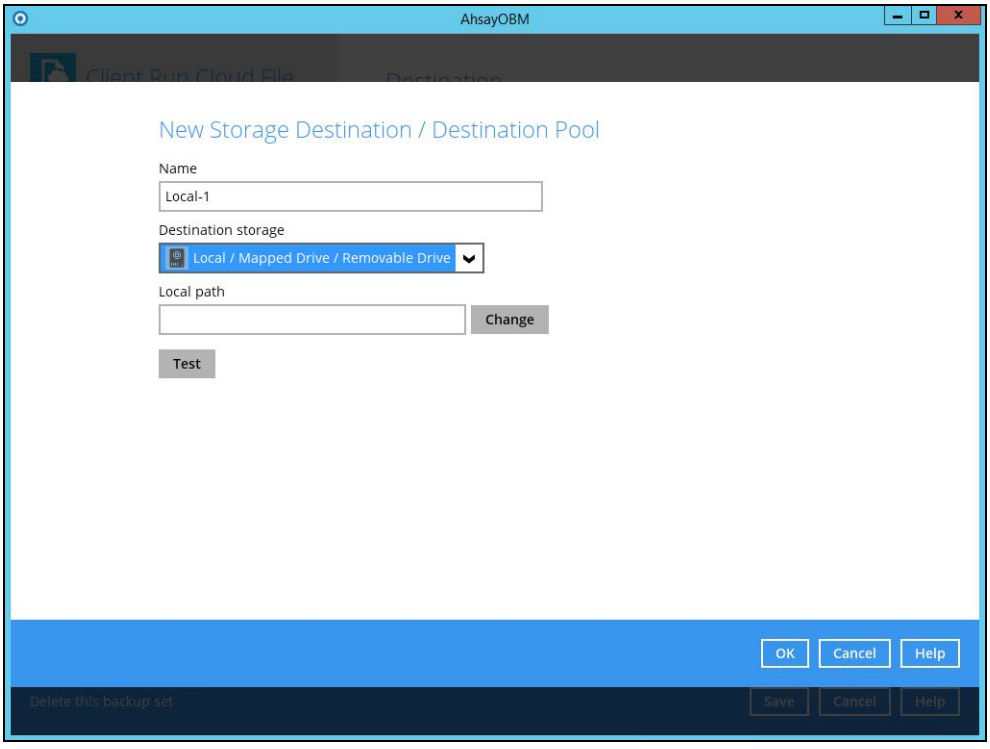
4. Click the **Destination** menu on the left side, then click the plus button  on the right to add storage destination.

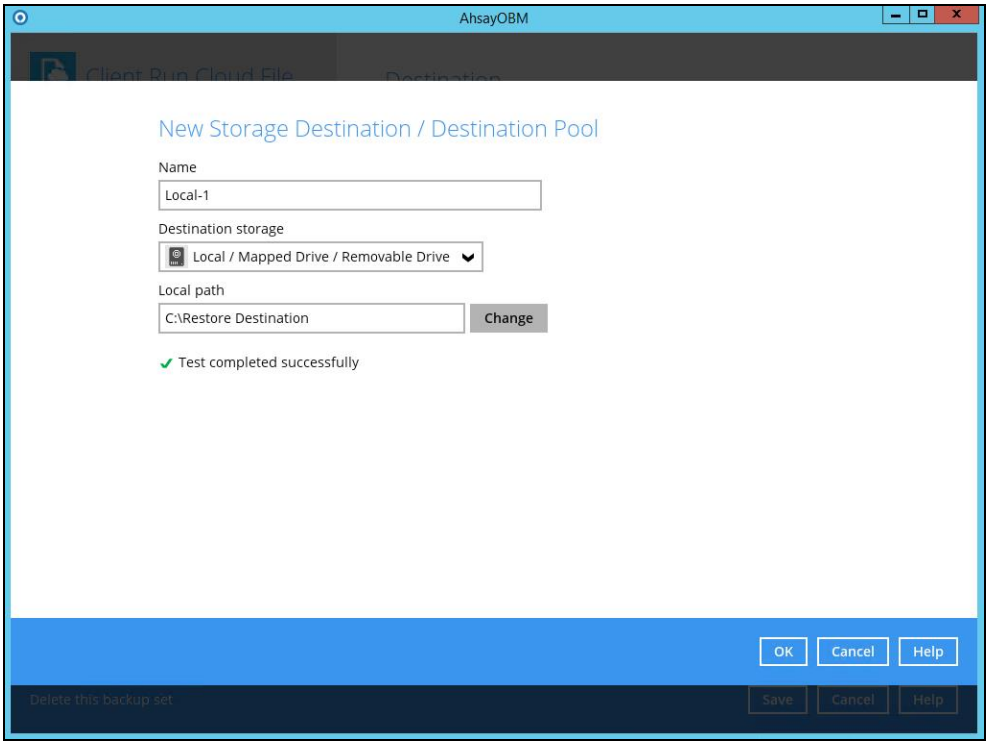


5. Select the storage destination

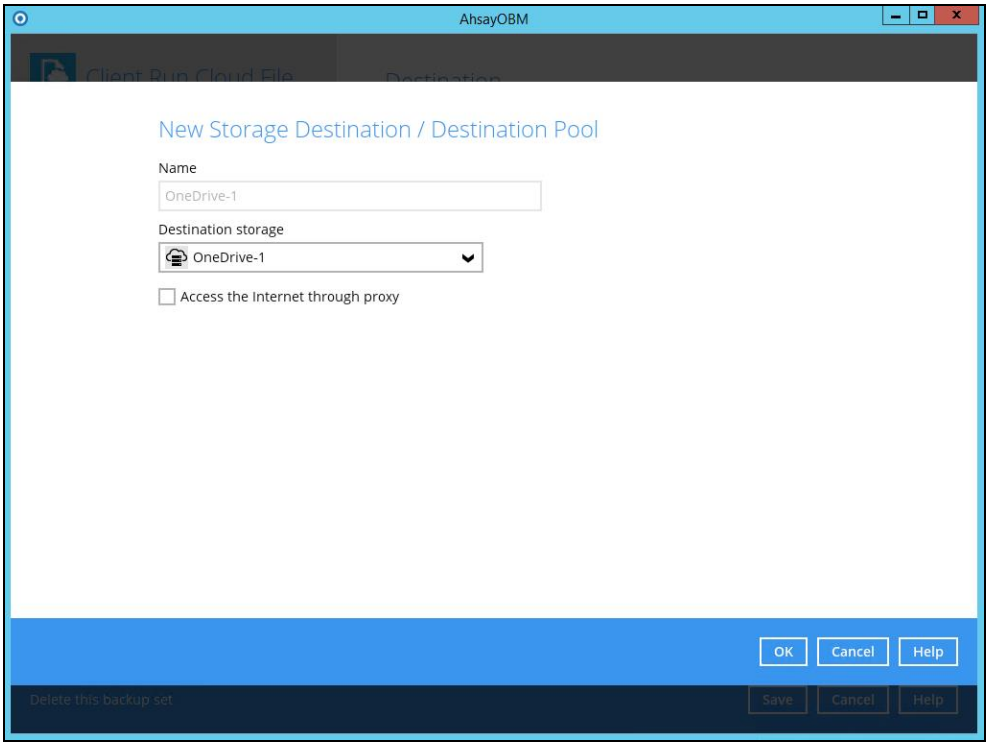


- If you have chosen the Local/Mapped Drive/Removable Drive option, click **Change** to browse to a directory path where backup data will be stored, then click **Test** to validate the path. **Test completed successfully** shows when the validation is done.

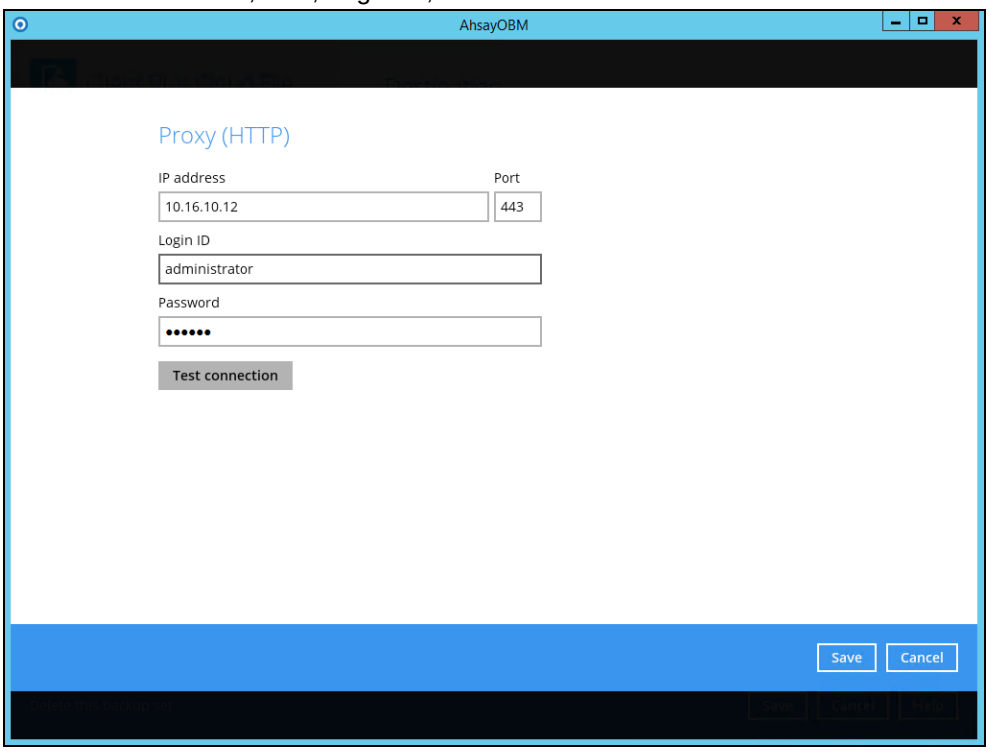


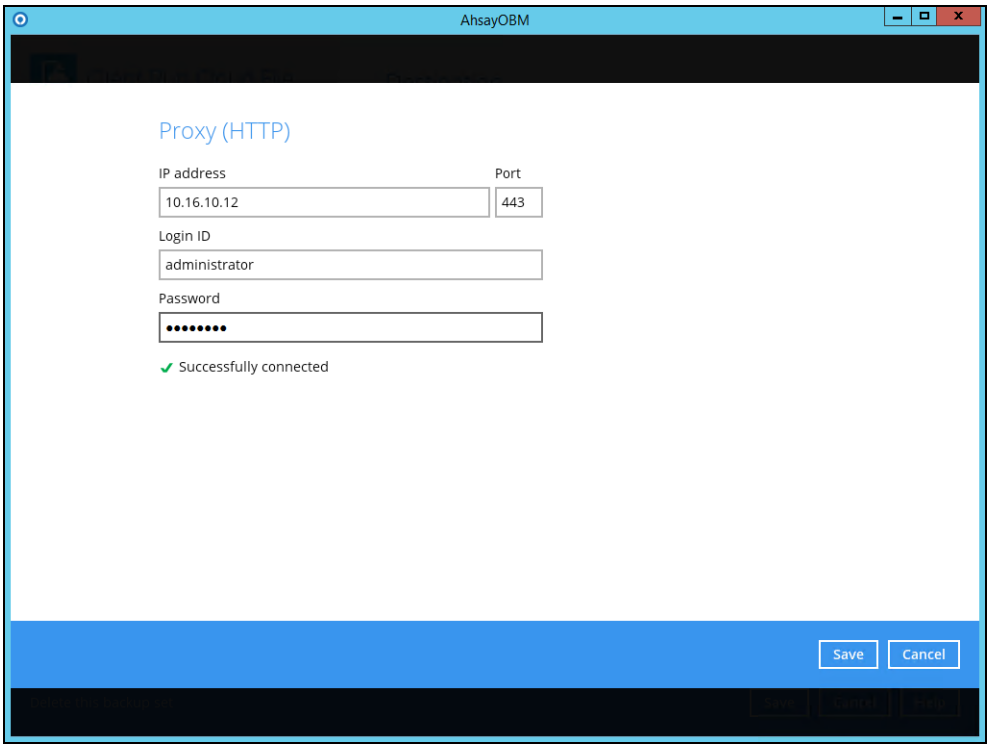


- If you have chosen the Cloud Storage, tick the checkbox **Access the Internet through proxy**.

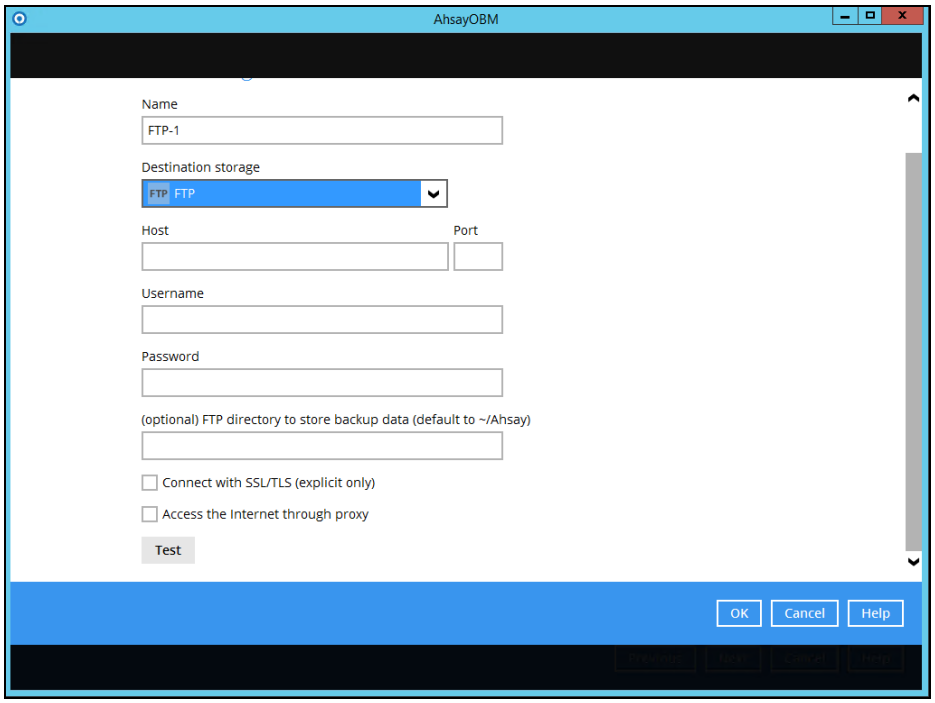


Enter the IP Address, Port, Login ID, and Password then click the **Test connection**.





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



6. 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 **Save** to proceed when you are done with the selection.