Online-Backup.dk v9

OneDrive Backup & Restore Guide for Windows

Ahsay Systems Corporation Limited

4 May 2022

Copyright Notice

Trademarks

Disclaimer

Revision History

Date	Descriptions	Version
25 January 2022	▪ Ch. 4 – added Migrate Data	9.1.0.0

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.

AhsayCBS Replication Server

Replication from AhsayCBS Backup Server to AhsayCBS Replication Server

Cloud Destination

AhsayCBS Backup Server

Back up from AhsayOBM to AhsayCBS

Back up from AhsayOBM to Predefined Destination

Internet

Data are compressed, encrypted, and divided into individual data block size of 16 or 32MB

Back up from AhsayOBM to Local Destination

AhsayOBM

AhsayOBM Remote Backup Machine

Local Destination

Data are downloaded from Cloud Storage

Restore from AhsayCBS

Internet

Restore from Predefined Destination

Restore from Local Destination

Cloud Storage (Backup Source)

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.
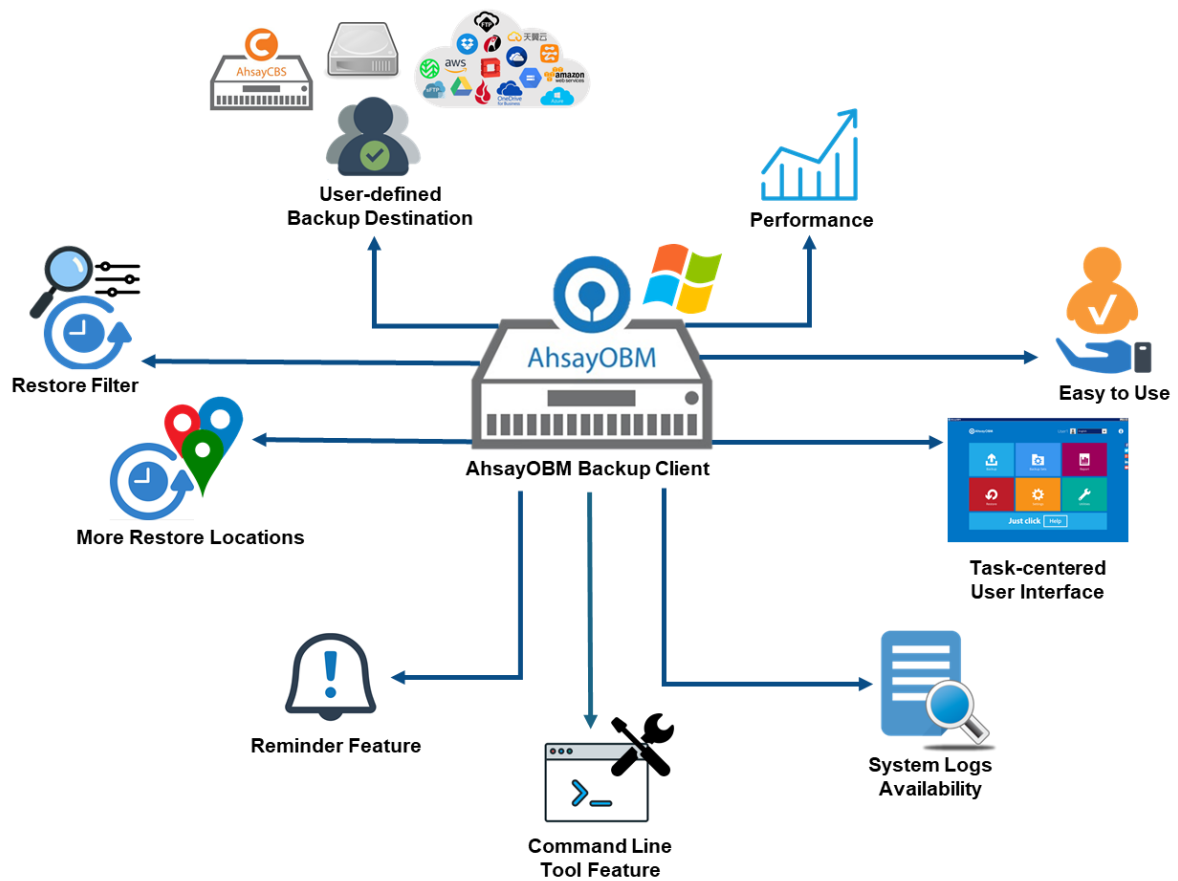
User-defined Backup Destination

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.

Command Line Tool

Agent-based backup solution has a feature that allows user to configure a pre and/or post-backup command which can be an operating system level command, script or batch file, or third-party utilities that will run before and/or after a backup job.

Reminder Feature

With the agent-based backup, a reminder feature is provided which will display a backup confirmation dialog box that will prompt user to run a backup job during machine log off, restart or shut down when enabled.

More Restore Locations

Agent-based backup offers you three (3) restore locations such as the local machine, original location (or the cloud storage where your backed up files are located) 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* – a last resort 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		**Microsoft Azure**
	CTYun		**Microsoft OneDrive**
	Amazon S3		**Microsoft OneDrive for Business**
	AWS S3 Compatible Cloud Storage		**Rackspace**
	Wasabi		**OpenStack**
	Backblaze		**Dropbox**
	Google Cloud Storage		**FTP**
	Google Drive		**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	✓	✖
Deduplication	AhsayOBM	AhsayOBM
Retention Policy	✓	AhsayOBM
Command Line Tool	AhsayOBM	✖
Reminder	AhsayOBM / AhsayACB for Windows only	✖
Restore Filter	✓	✖
Bandwidth Control	✓	AhsayOBM
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 guide:
AhsayCBS v9 User Guide – Cloud File Run on Server (Agentless) Backup and Restore Guide

---

1.3 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 9.1 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 9.1 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 for the list of processes and directory paths that should be added to all antivirus software white-list / exclusion list.
[FAQ: Suggestion on antivirus exclusions to improve performance of Ahsay software on Windows](#)

2.4 Upgrade VMware Tools Requirement

To avoid unexpected java crash, if the Windows machine is a guest VM hosted on a VMware Host, then it is highly recommended that the VMware Tools version installed on the guest VM is 10.3.5 or higher.

Below is the warning message that will be displayed if the version of the VMware Tools is earlier than 10.3.5.
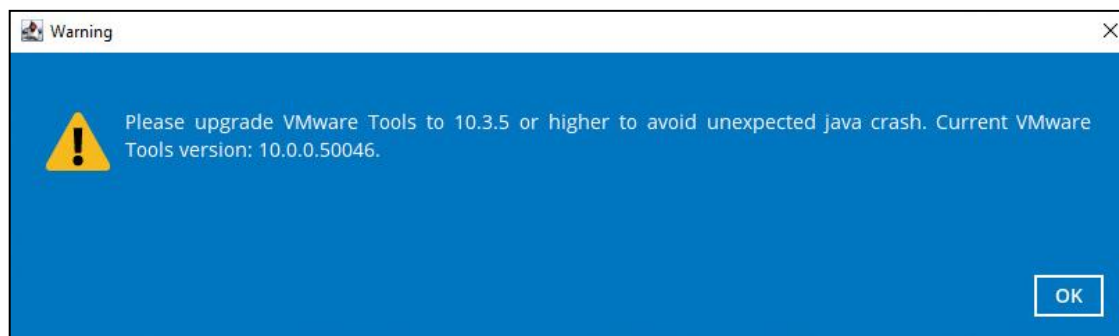
For more information about the upgrade of VMware Tools, refer to the following article.
[ISSUE: AhsayOBM / ACB crash when performing backup or restore on a VMware virtual machine with VMware Tools pre-10.3.5 installed](#)

2.5 Internet / Network Connection

In order to allow access to the cloud storage, an internet connection must be available on the computer where the AhsayOBM is installed.

2.6 Valid AhsayOBM User Account

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

2.7 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.

2.8 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. This only applies to backup sets created using AhsayOBM v8 or before.

NOTE

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

For AhsayOBM user account

2.9 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.

2.10 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		**Microsoft Azure**
	CTYun		**Microsoft OneDrive**
	Amazon S3		**Microsoft OneDrive for Business**
	AWS S3 Compatible Cloud Storage		**Rackspace**
	Wasabi		**OpenStack**
	Backblaze		**Dropbox**
	Google Cloud Storage		**FTP**
	Google Drive		**SFTP**

2.11 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.

2.12 Network Bandwidth

10 Mbps or above connection speed.

2.13 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.

- Perform test restores periodically to ensure your backup is set up 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.

⦿ **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.

2.14 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.
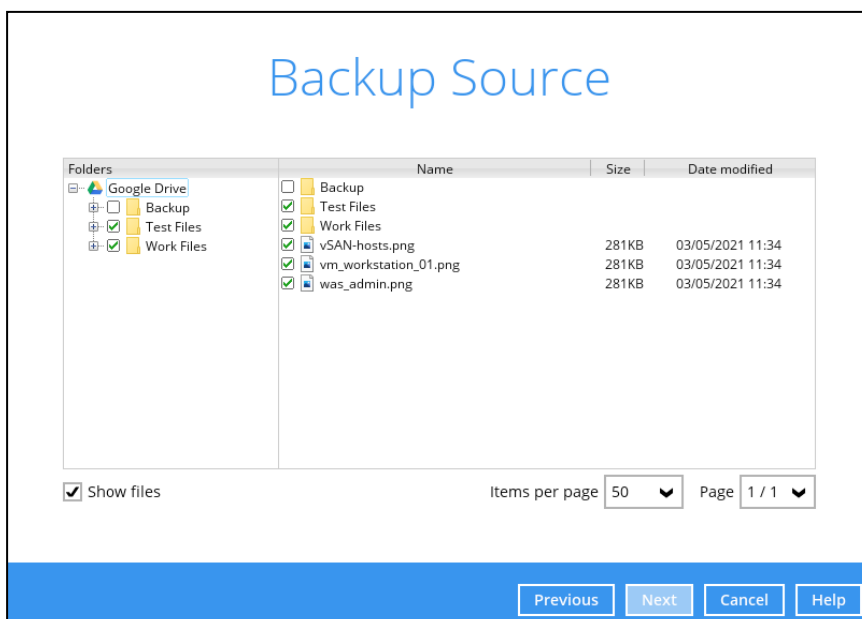
2. If there are any top level folders and/or files added to the Cloud drive after the backup set is created, they will not be added in the backup source automatically. The backup set will have to be manually updated to include the new top level folders and/or files before they can be backed up.

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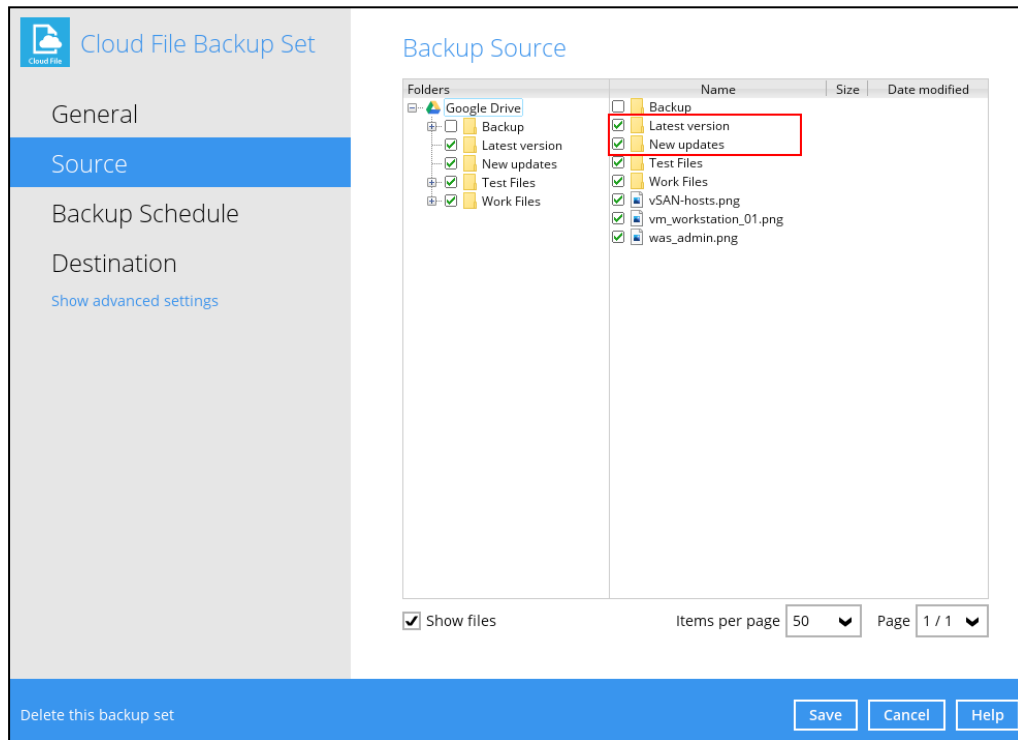 be removed from the backup source automatically. The backup set will have to be manually updated to unselect the deleted top level folders and/or files. Otherwise, the backup job will be completed with warnings.

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.
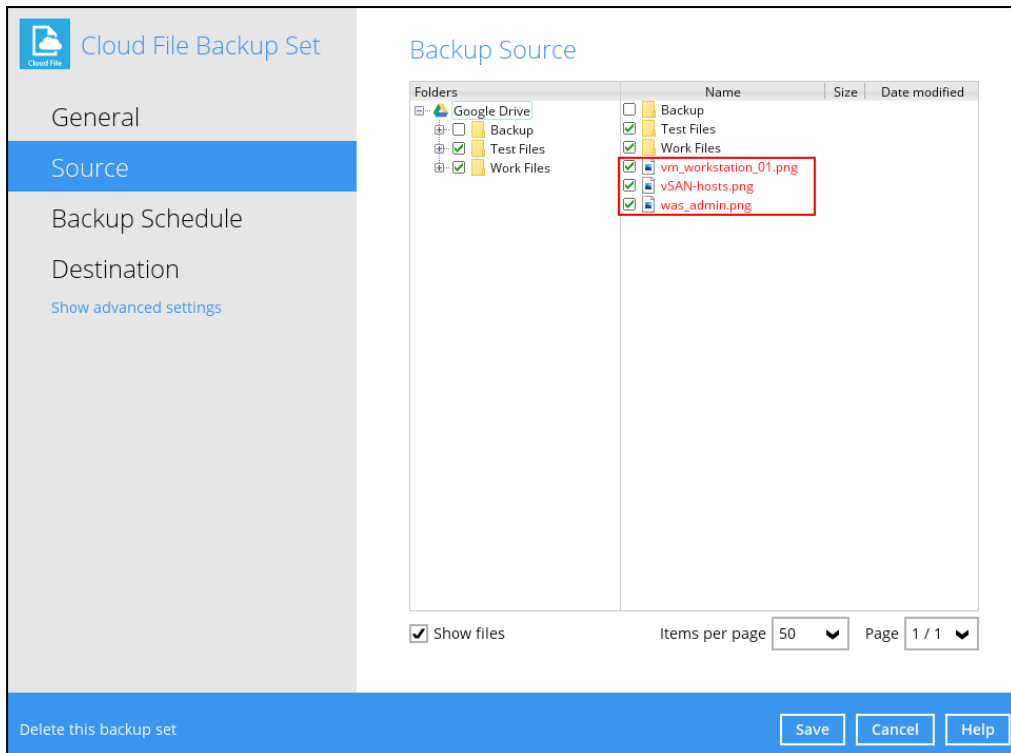
Backup log

```
[2021/05/07 17:38:00] [warn] [1619158570719] Backup source
"was_admin.png" does not exist !

[2021/05/07 17:38:00] [cbs] [1619158570719] warn,"Backup
source \"was_admin.png\" does not exist !",0,0,0,,,

[2021/05/07 17:38:00] [warn] [1619158570719] Backup source
"vm_workstation_01.png" does not exist !

[2021/05/07 17:38:00] [cbs] [1619158570719] warn,"Backup
source \"vm_workstation_01.png\" does not exist !",0,0,0,,,

[2021/05/07 17:38:00] [warn] [1619158570719] Backup source
"vSAN-hosts.png" does not exist !

[2021/05/07 17:38:00] [cbs] [1619158570719] warn,"Backup
source \"vSAN-hosts.png\" does not exist !",0,0,0,,,
```

3   Creating a Cloud File Backup Set

1.   Log in to AhsayOBM.

     For instructions on how to do this please refer to Chapter 8 of the AhsayOBM v9 Quick Start
     Guide for Windows.

2.   In the AhsayOBM main interface, click the following icon.

3.   Create a Cloud File backup set by clicking the "+" icon next to **Add new backup set**.
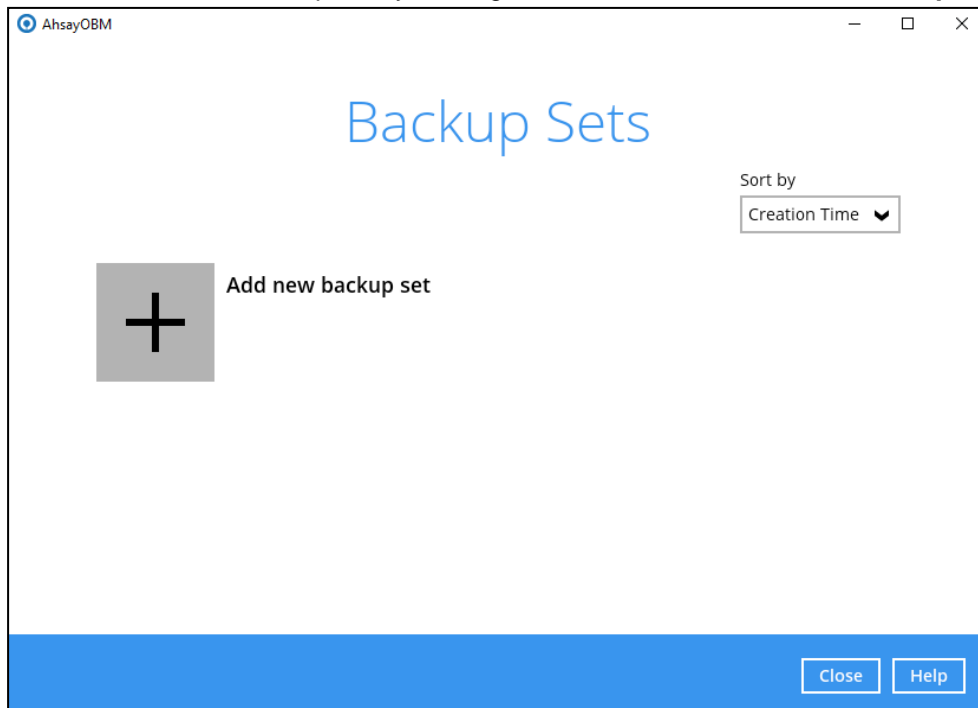
4. Enter a **Name** for your backup set and select **Cloud File Backup** as the **Backup set type**.
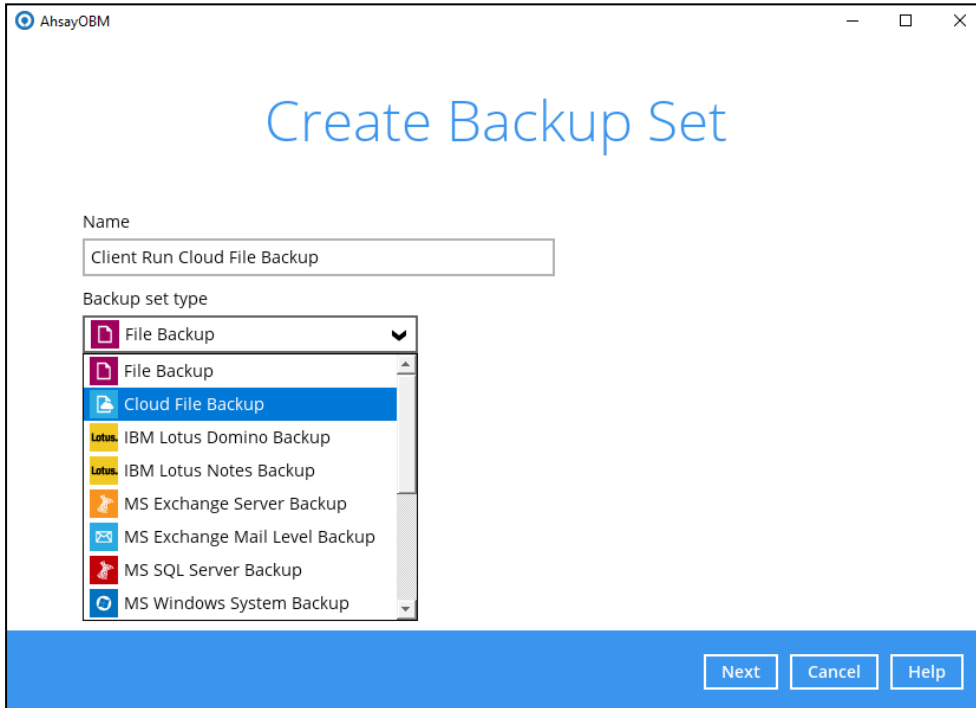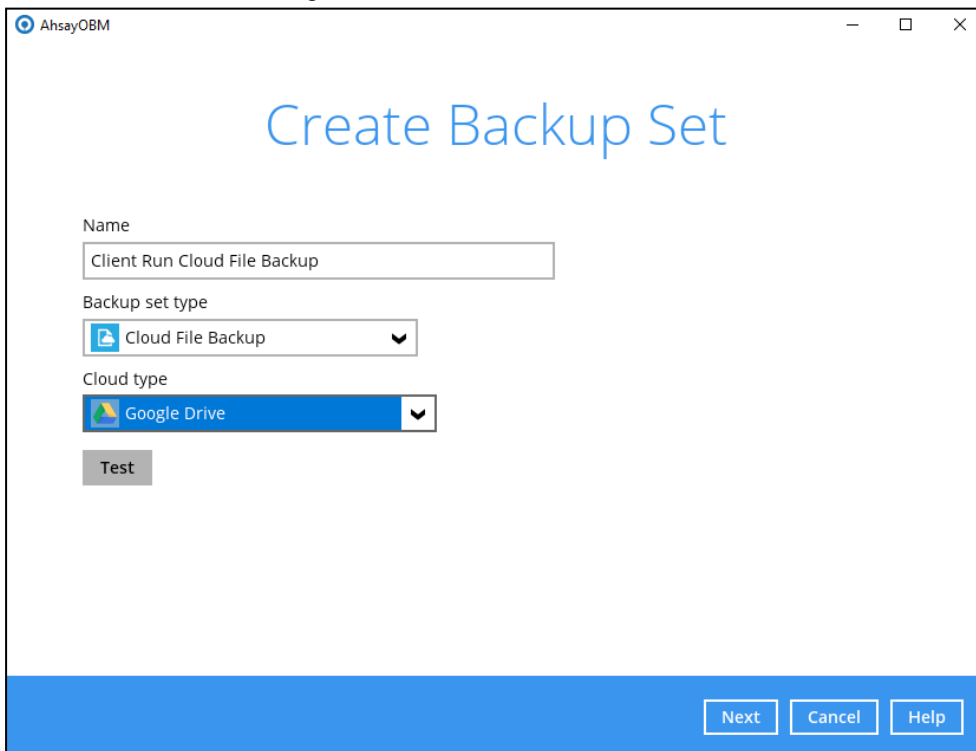
5. Select the **Cloud type** of the cloud storage that contains the data that you want to back up. For example, Google Drive.
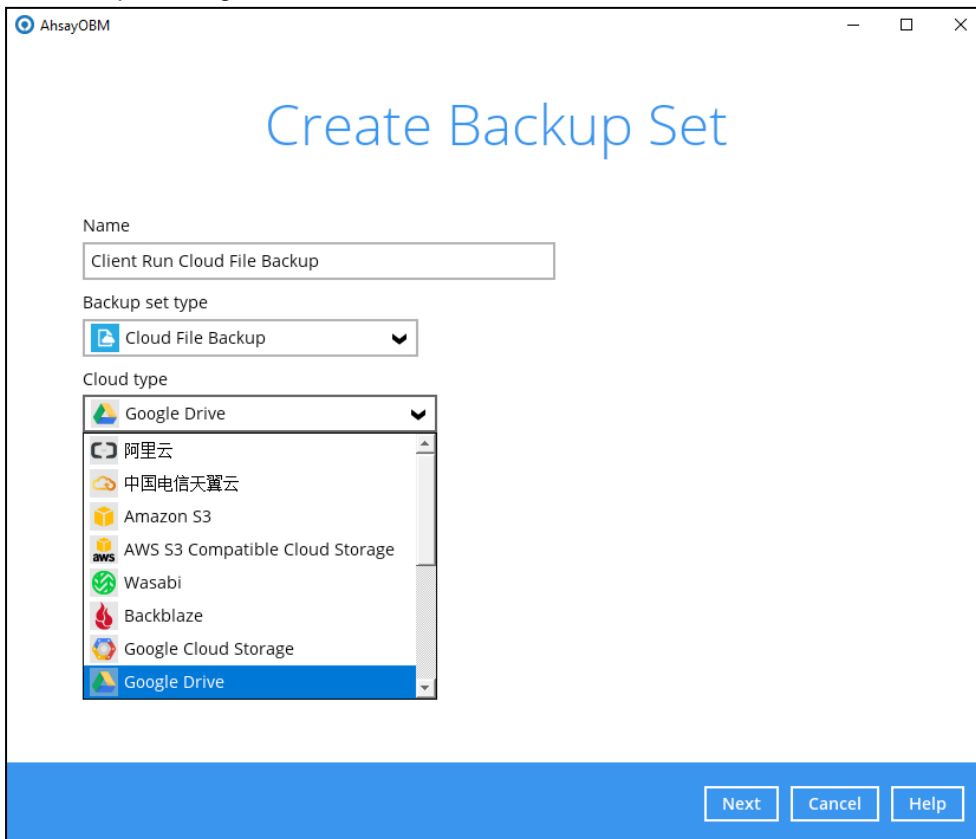
6. Depending on the cloud type you have selected, you will be prompted to enter the cloud service login details.

7.   Click **Test** to get redirected to the login page of the cloud service provider on your default
      browser, then enter the login details there.
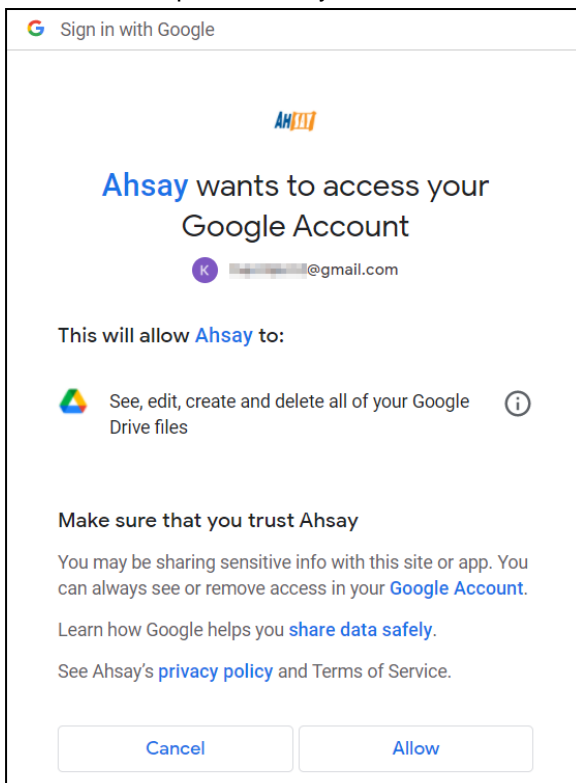
NOTE
The authentication request will be opened in a new tab or window. Ensure that the pop-up window is not blocked, and pop-up blocker is disabled in your browser.

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

9. Copy and paste the code generated by the cloud service provider to AhsayOBM, then click **OK** to confirm.
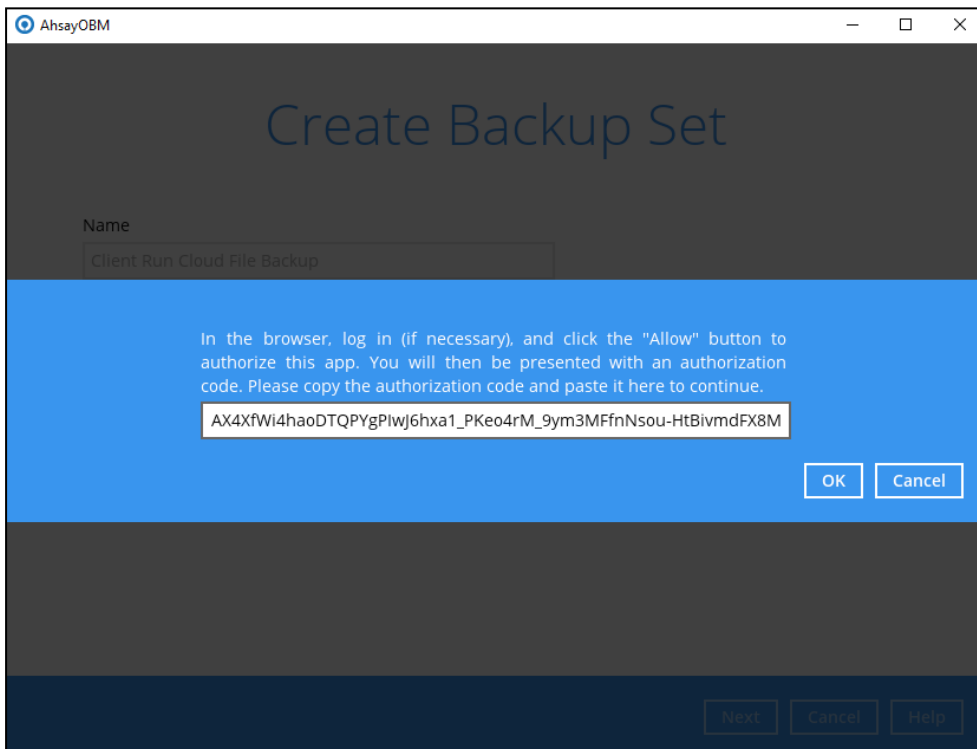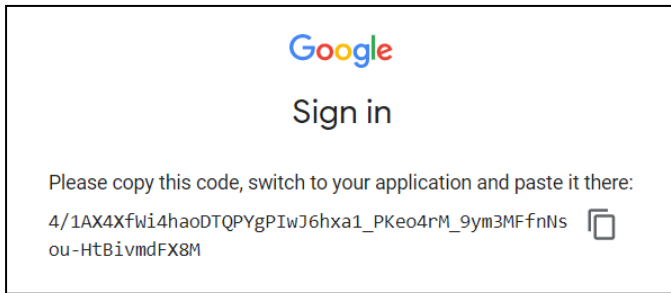
10. Click **Next** to proceed.
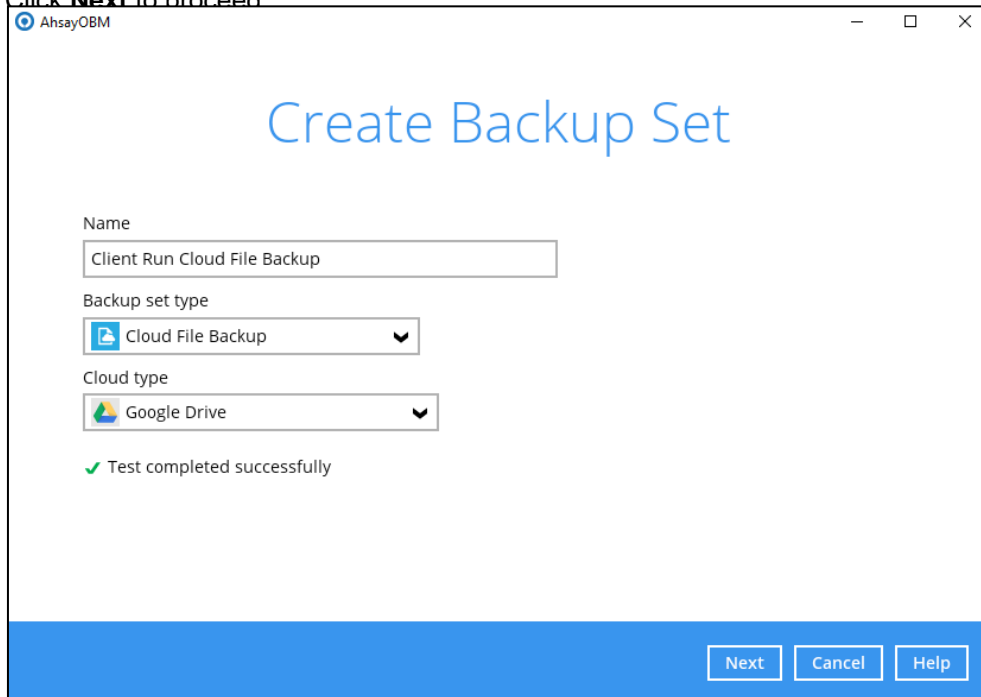
11. In the **Backup Source** window, select the files and/or folders that you would like to back up.
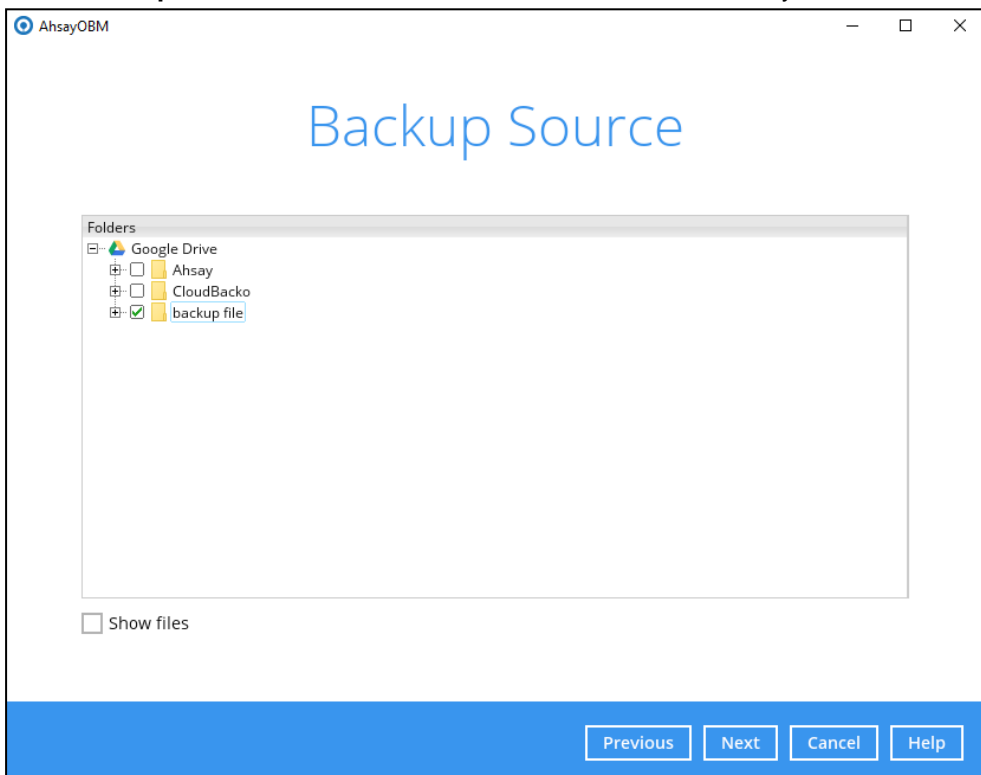
NOTE
There are limitations in selecting files and/or folders in the backup source menu. For further details, please refer to Ch. 2.14 Limitations.

Tick the **Show files** checkbox at the bottom left corner if you would like to choose individual file(s) for backup. Click **Next** to proceed when you are done with the selection.
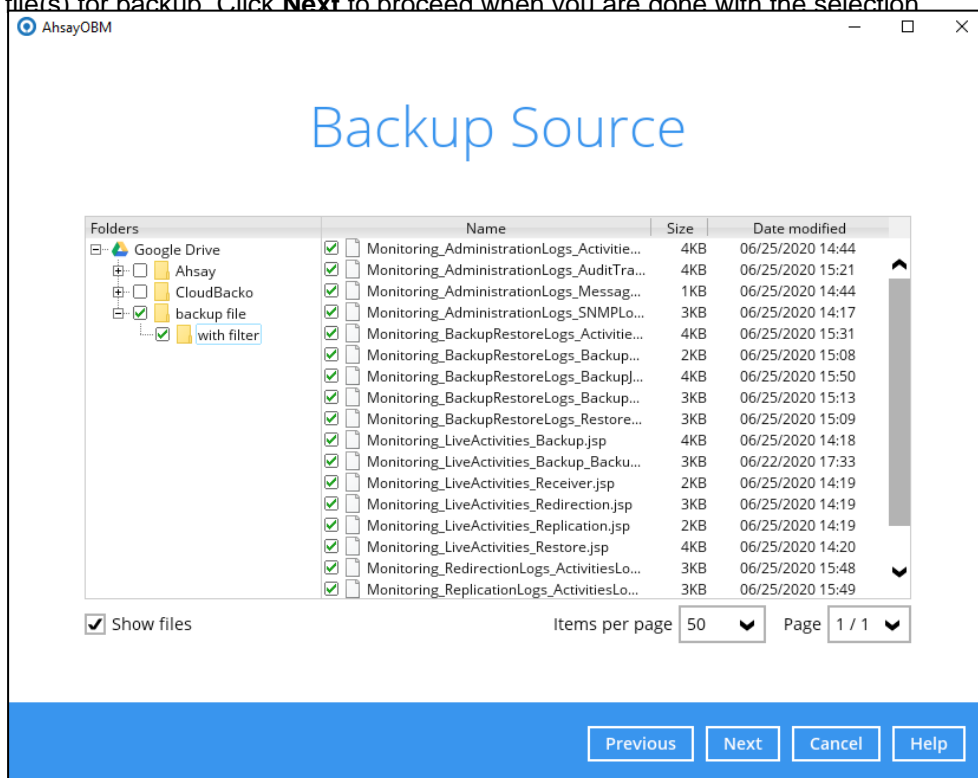
12. In the **Schedule** window, configure a backup schedule for backup job to run automatically at your specified time interval. If enabled, click **Add new schedule** to add a new schedule, then click **Next** to proceed.
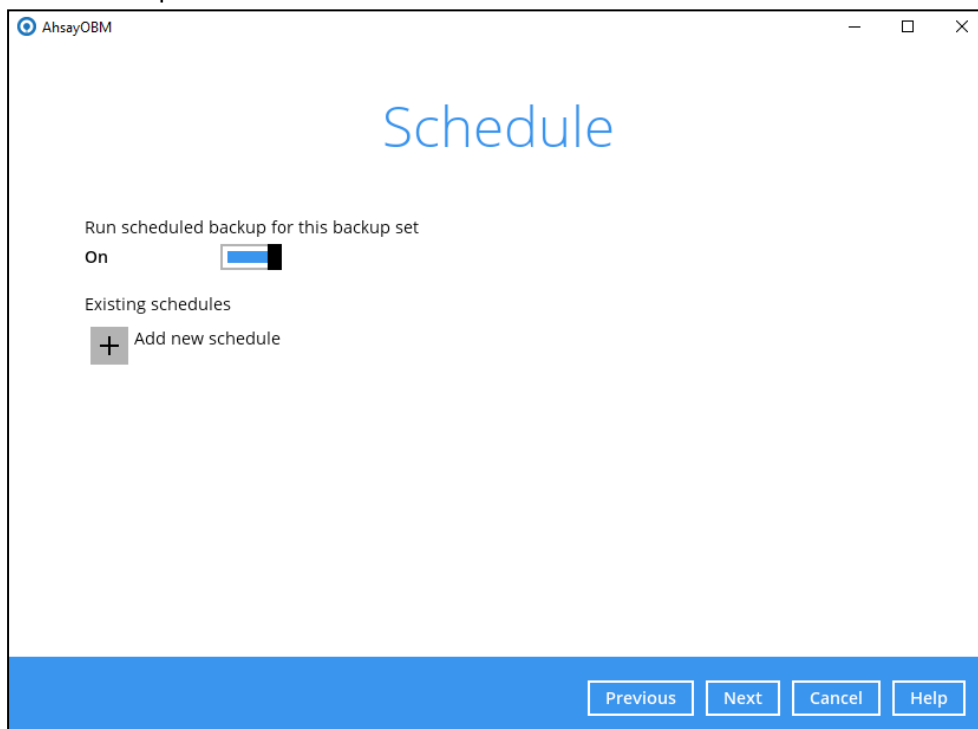
13. Configure the backup schedule settings on this page, then click **OK** when you are done with the settings. Click **Next** to proceed.

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.

New Backup Schedule

Name

Weekly-1

Type

Weekly ▾

Backup on these days of the week

☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☑ Sat

Start backup

at ▾ 23 ▾ : 00 ▾

Stop

until full backup completed ▾

☑ Run Retention Policy after backup

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

New Backup Schedule

Name

Monthly-1

Type

Monthly ▾

Backup on the following day every month

◉ Day Last ▾

○ First ▾ Sunday ▾

Start backup at

23 ▾ : 00 ▾ on the selected days

Stop

until full backup completed ▾

☑ Run Retention Policy after backup

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

New Backup Schedule

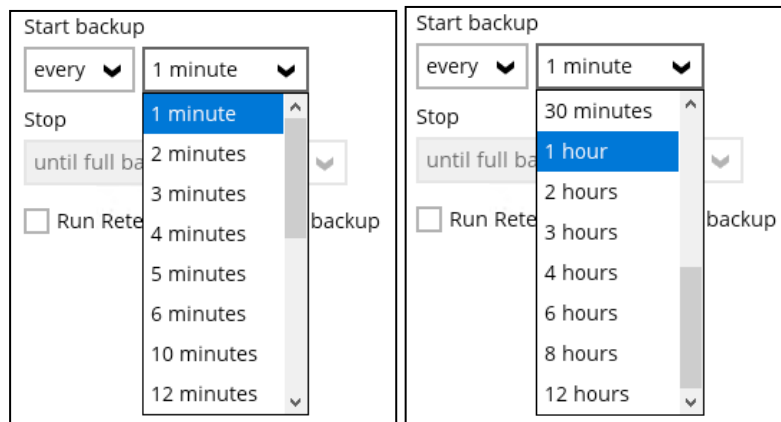Name

Custom-1

Type

Custom ▾

Backup on the following day once

2021 December ▾ 31 ▾

Start backup at

23 ▾ : 59 ▾

Stop

until full backup completed ▾

☑ Run Retention Policy after backup

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

  - ⊙ **at** – this option will start a backup job <u>at a specific time</u>.

  - ⊙ **every** – this option will start a backup job <u>in intervals of minutes or hours</u>.

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

| *Figure 1.1* | *Figure 1.2* |

Figure 1.1 – Periodic schedule every 4 hours Monday - Friday during business hours

Figure 1.2 – Normal schedule run at 21:00 or 9:00 PM on Saturday & Sunday during 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 AhsayACB 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.
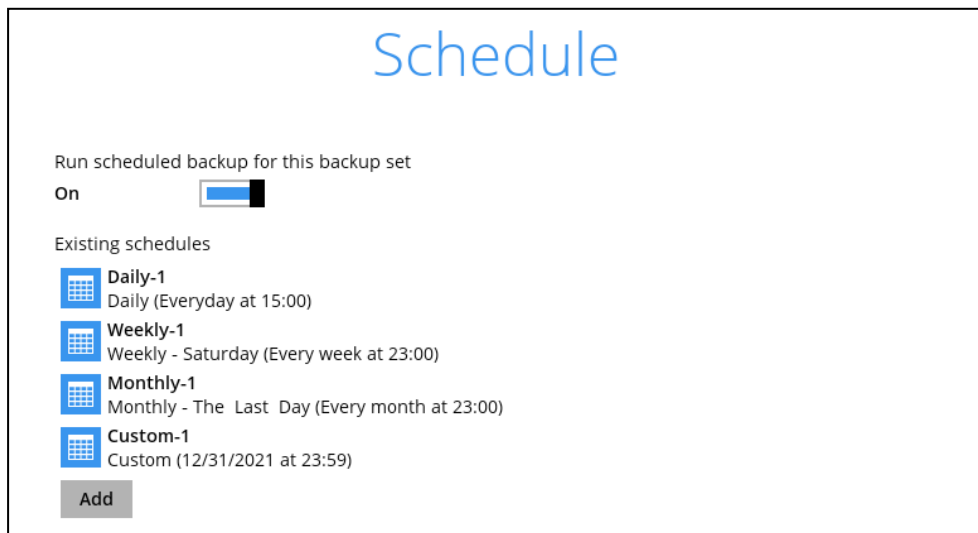
Click **Next** to proceed.

14. 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**
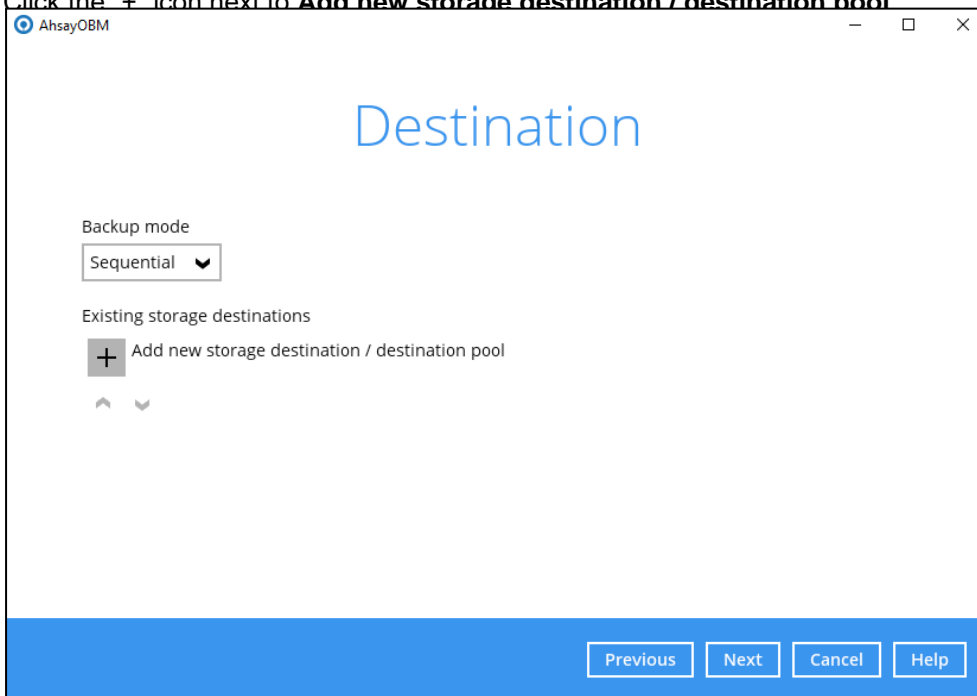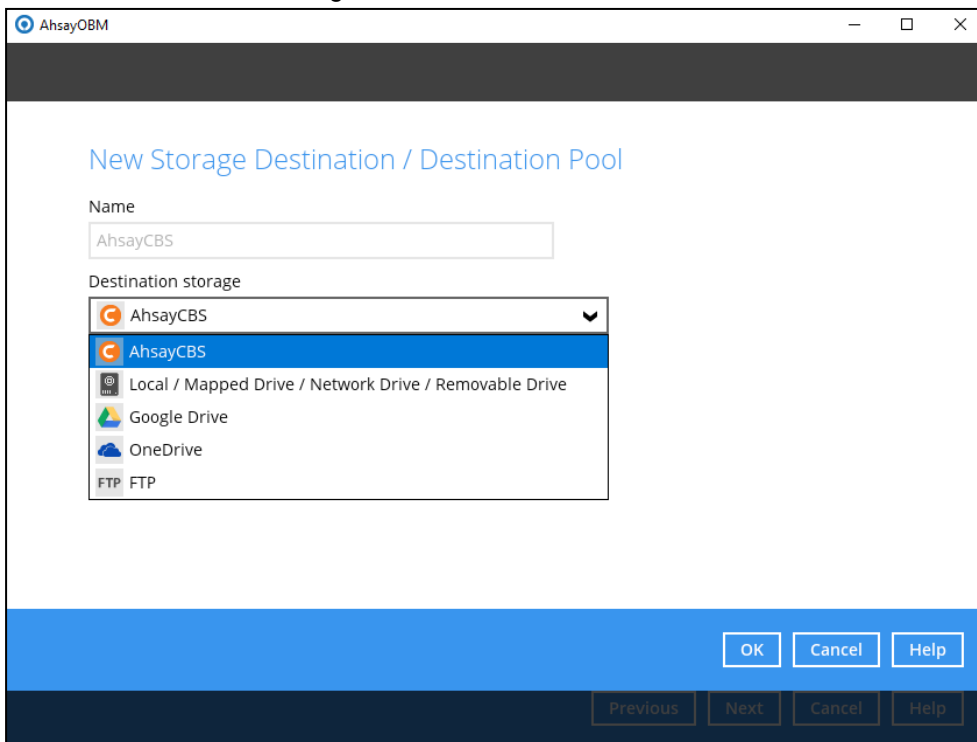

15. Select the Destination storage.

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 / Network Drive / Removable Drive option, click **Change** to browse to a directory path where backup data will be stored. Check "This share requires access credentials" if credentials are needed to access the directory path. 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.

16. You can add multiple storage destinations here. 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.
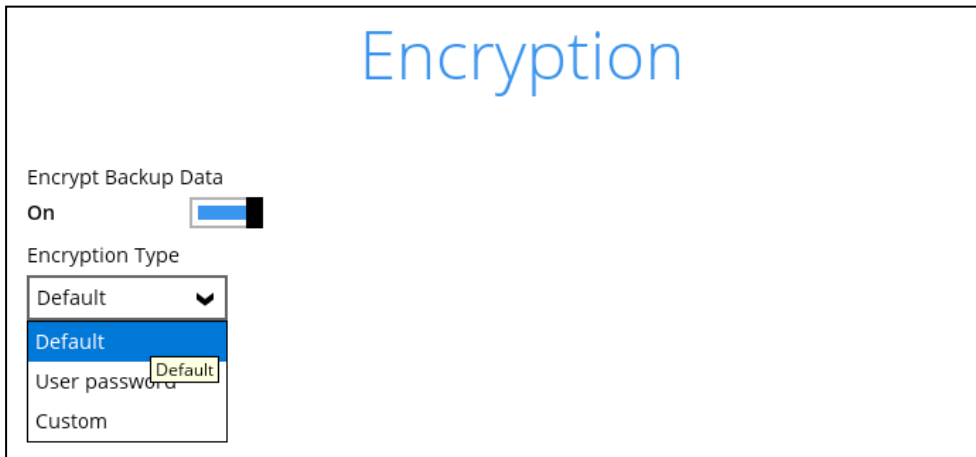
17. In the Encryption window, the default **Encrypt Backup Data** option is enabled with an encryption key preset by the system which provides the most secure protection.

You can choose from one of the following three (3) 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 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.

18.   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.
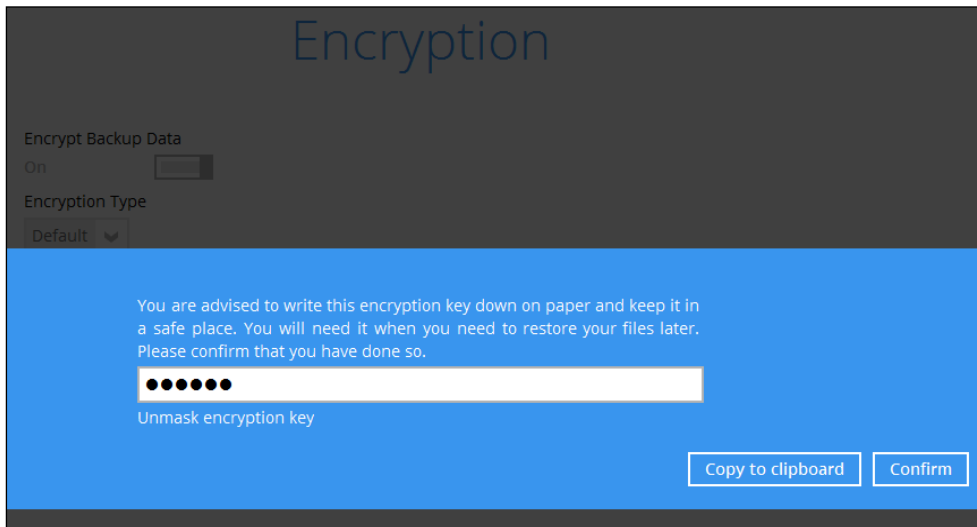
The pop-up window has the following three options to choose from:

- **Unmask encryption key** – The encryption key is masked by default. Click this option to show the encryption key.
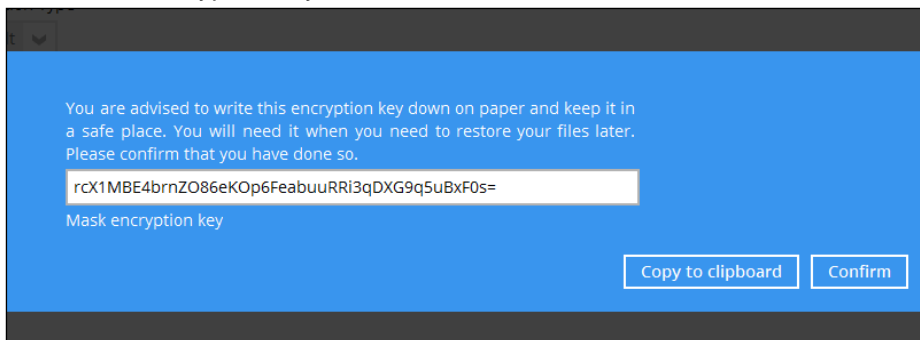
- **Copy to clipboard** – Click this to copy the encryption key, then you can paste it on another location of your choice for your reference (e.g. notepad).

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

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

20. The cloud file backup set is created succesfully.

21. 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 Drive C.

Go to **Others > Temporary Directory**. Click **Change** to browse for another location.
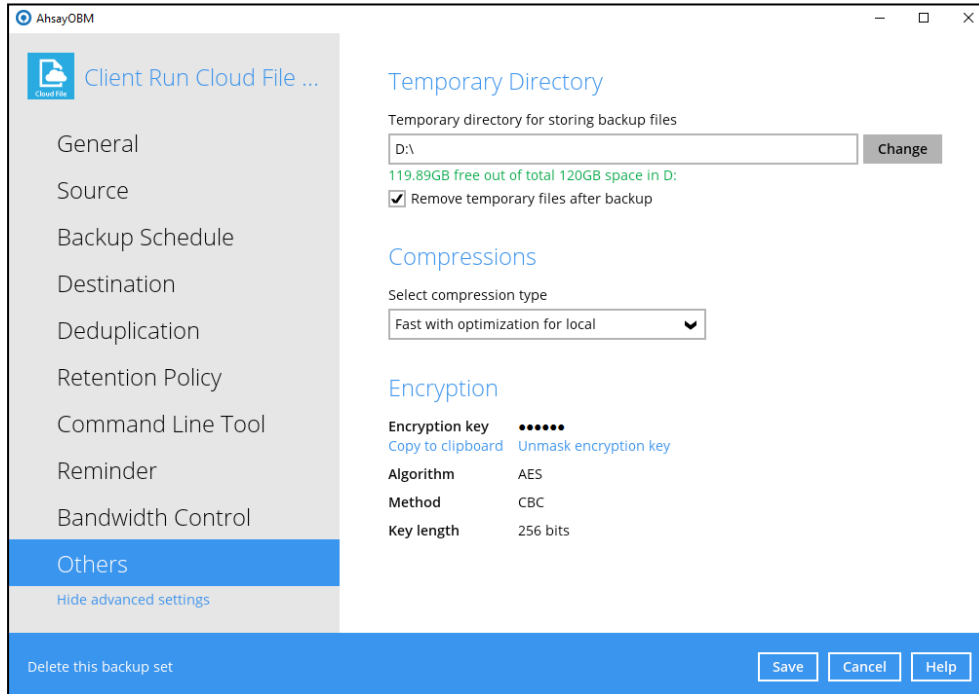
22. Optional: Select your preferred **Compression** type. By default, the compression is Fast with optimization for local.

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

- No Compression

- Normal

- Fast (Compressed size larger than normal)

- Fast with optimization for local
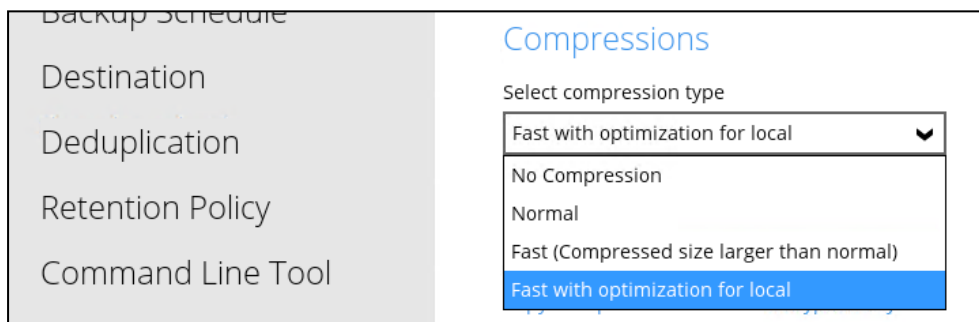
4 Running a Backup Job

For an overview of the backup process, please refer to [Chapter 12](#) in the AhsayOBM v9 Quick Start Guide for Windows.

To start a backup, follow the steps below:

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

2. Select the backup set which you would like to start a backup on.
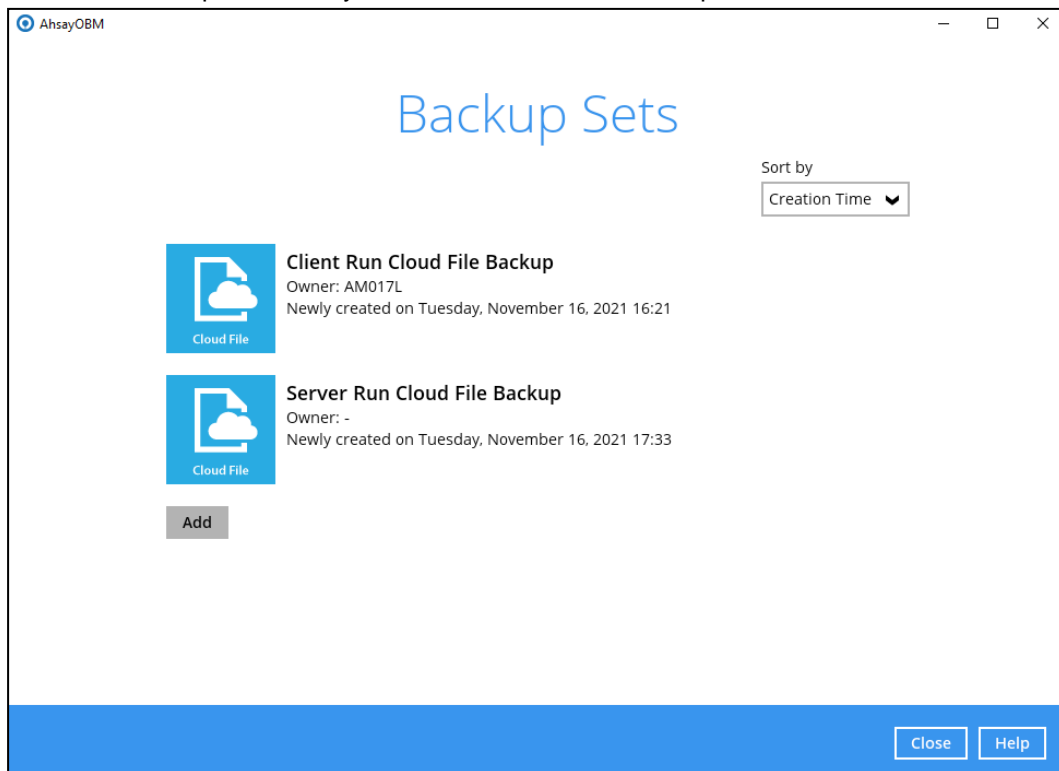
3. If you would like to modify the Destinations, Migrate Data and Retention Policy settings, click **Show advanced option**.
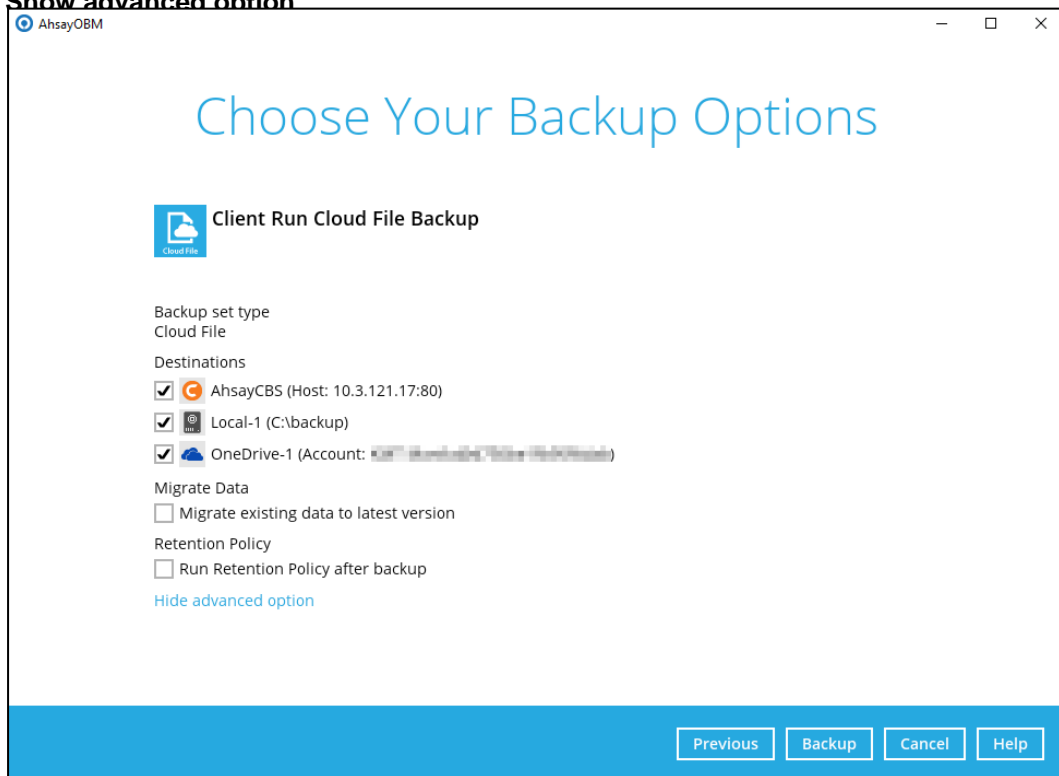
NOTE

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

After configuring the settings, click **Backup** to start the backup job and wait until it is finished.
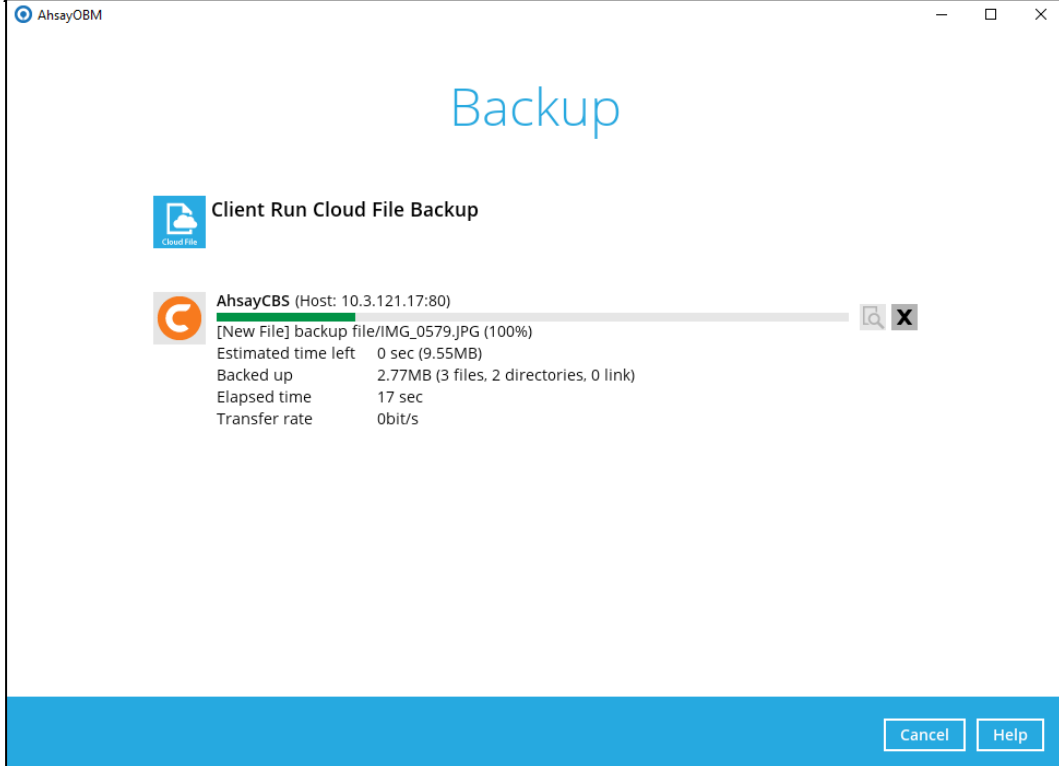
4. The backup job through AhsayOBM completed successfully.
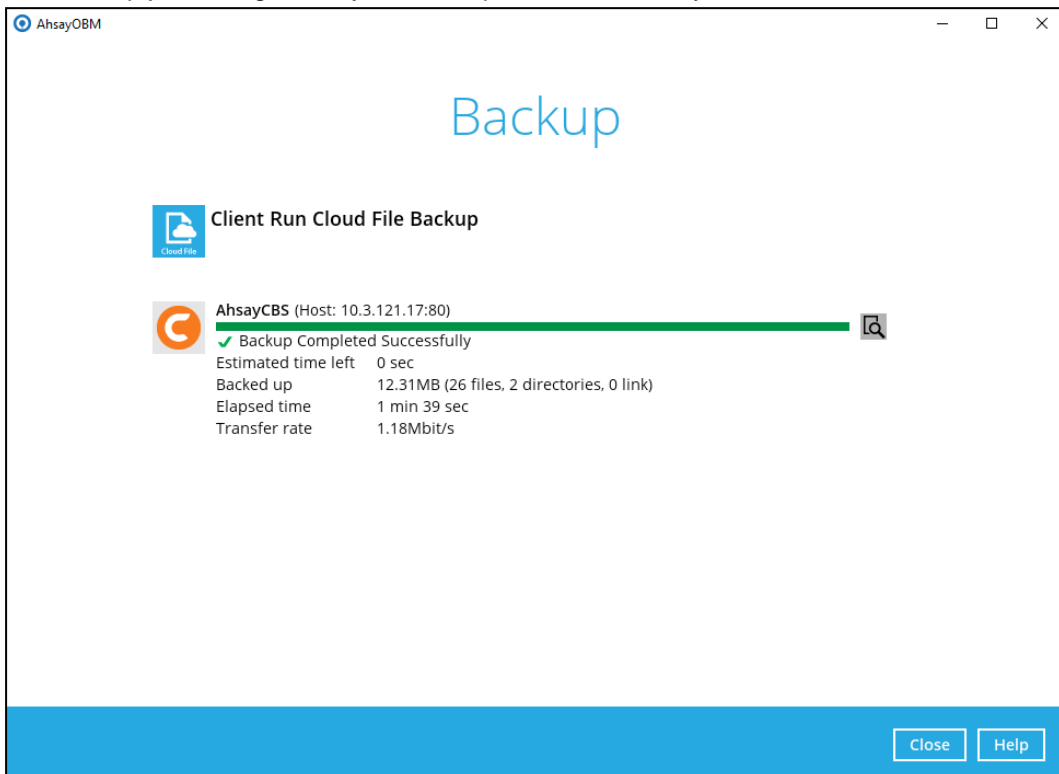
5. To view the backup logs, click the 🔍 button. This will display the backup job process with corresponding date and time.

| Type	Log	Time
ℹ	Start [AhsayOBM v9.0.0.46]	11/16/2021 17:39:54
ℹ	Saving encrypted backup set encryption keys to server...	11/16/2021 17:39:55
ℹ	Start Backup ... [Migrate Delta: Incremental]	11/16/2021 17:39:57
ℹ	Using Temporary Directory C:\Users\admin\.obm\temp\1637050903813\OBS@1637051254368	11/16/2021 17:39:57
ℹ	Start running pre-commands	11/16/2021 17:40:01
ℹ	Finished running pre-commands	11/16/2021 17:40:01
ℹ	Downloading server file list...	11/16/2021 17:40:01
ℹ	Downloading server file list... Completed	11/16/2021 17:40:02
ℹ	Reading backup source from hard disk...	11/16/2021 17:40:04
ℹ	[New Directory]... backup file	11/16/2021 17:40:05
ℹ	[New Directory]... backup file/with filter	11/16/2021 17:40:05
ℹ	Reading backup source from hard disk... Completed	11/16/2021 17:40:05
ℹ	[New File]... 10% of "backup file/Best Practices and Recommendations_draft_03162020-updated-ivy.doc"	11/16/2021 17:40:06
ℹ	[New File]... 20% of "backup file/Best Practices and Recommendations_draft_03162020-updated-ivy.doc"	11/16/2021 17:40:06
ℹ	[New File]... 31% of "backup file/Best Practices and Recommendations_draft_03162020-updated-ivy.doc"	11/16/2021 17:40:06
ℹ	[New File]... 42% of "backup file/Best Practices and Recommendations_draft_03162020-updated-ivy.doc"	11/16/2021 17:40:06
ℹ	[New File]... 53% of "backup file/Best Practices and Recommendations_draft_03162020-updated-ivy.doc"	11/16/2021 17:40:06
ℹ	[New File]... 64% of "backup file/Best Practices and Recommendations_draft_03162020-updated-ivy.doc"	11/16/2021 17:40:06
ℹ	[New File]... 75% of "backup file/Best Practices and Recommendations_draft_03162020-updated-ivy.doc"	11/16/2021 17:40:06
ℹ	[New File]... 85% of "backup file/Best Practices and Recommendations_draft_03162020-updated-ivy.doc"	11/16/2021 17:40:06

Show: All

Logs per page: 50   Page: 1 / 5

Close

In order to view the backup report, go back to the main interface and click the following icon.
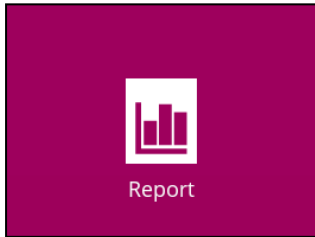
In the Backup Report screen, you can see the backup set with corresponding destination, completion date and time, and status.

Click the backup report to display the summary of the backup job. You can also click the **View Log** button that will redirect you to the log summary of your backup.

You can also search for backup reports from a specific period of date using the **From** and **To** date filter. Set this and available backup report will be displayed.

5   Restoring a Cloud File Backup Set

AhsayOBM provided three (3) options in restoring a backup such as through the **Local machine**, **Original location**, and **Alternate location**. 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, you can also restore your data to your original location, on the cloud storage, where you backed up them.

- **Alternate location**

    Besides the two (2) options above, you can also restore your data to an alternate location which is through the same cloud storage but on a different folder.

1.   On the main interface, click the following icon.
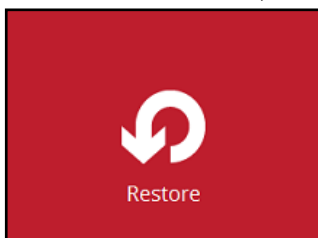
2.   Select the backup set that you would like to restore.
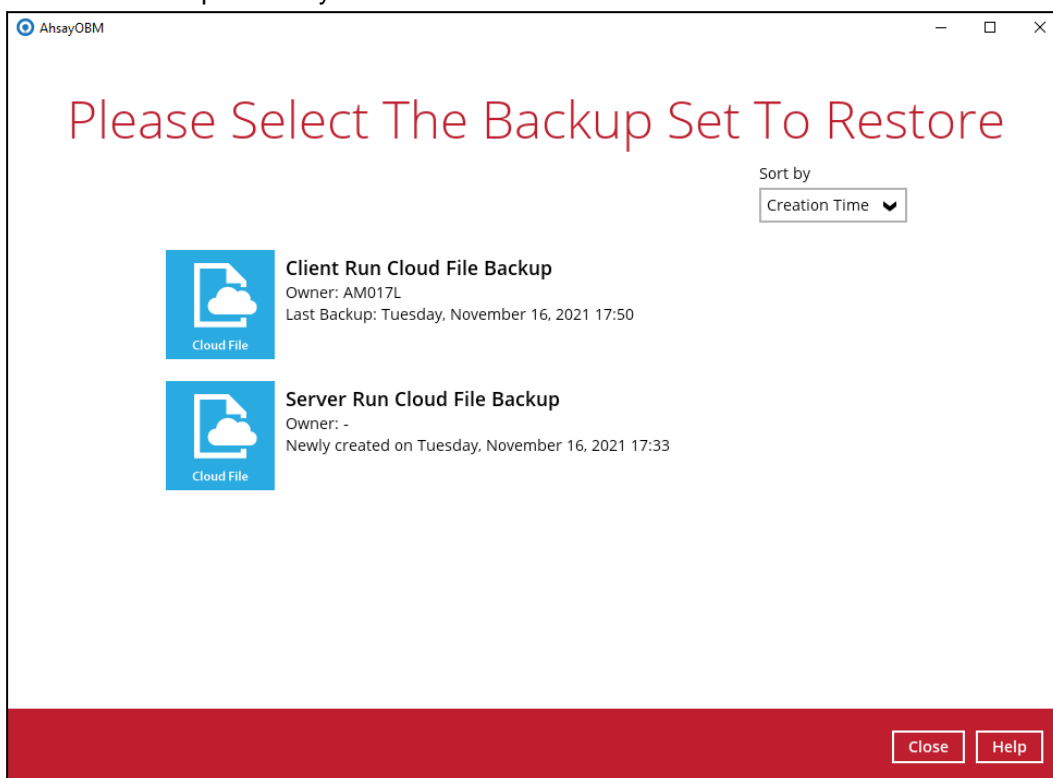
3. Select the backup destination that contains the data that you would like to restore.
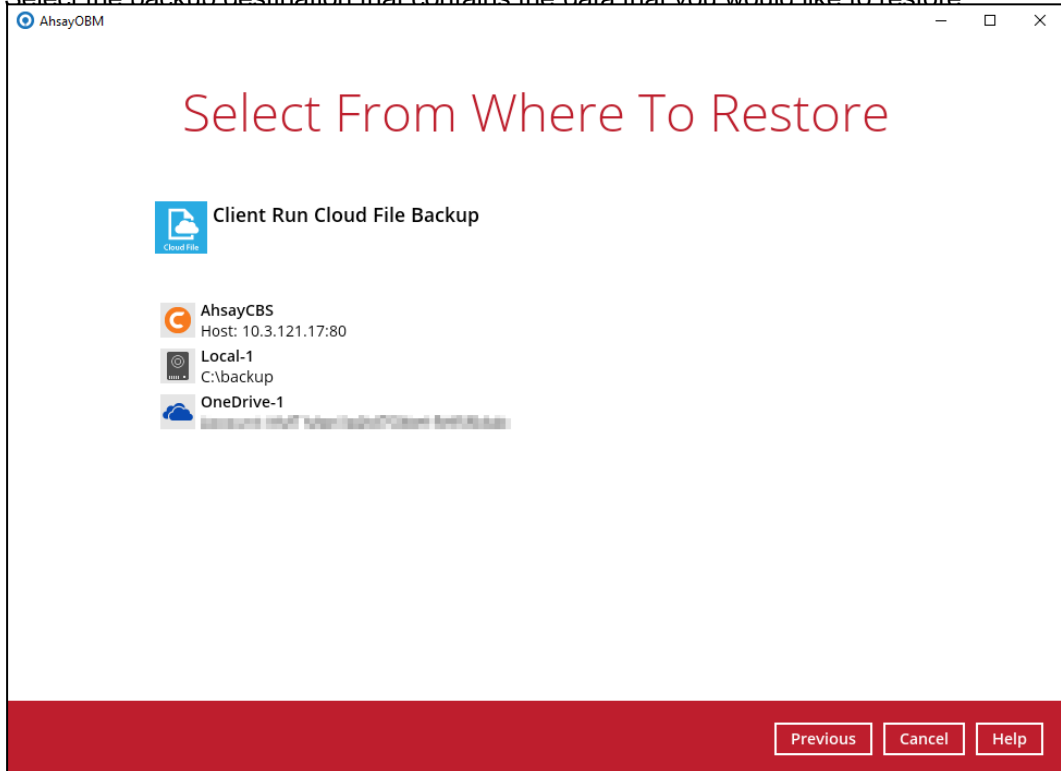
4. Select to restore from a specific backup job, or the latest job available from the **Select what to restore** drop-down menu.
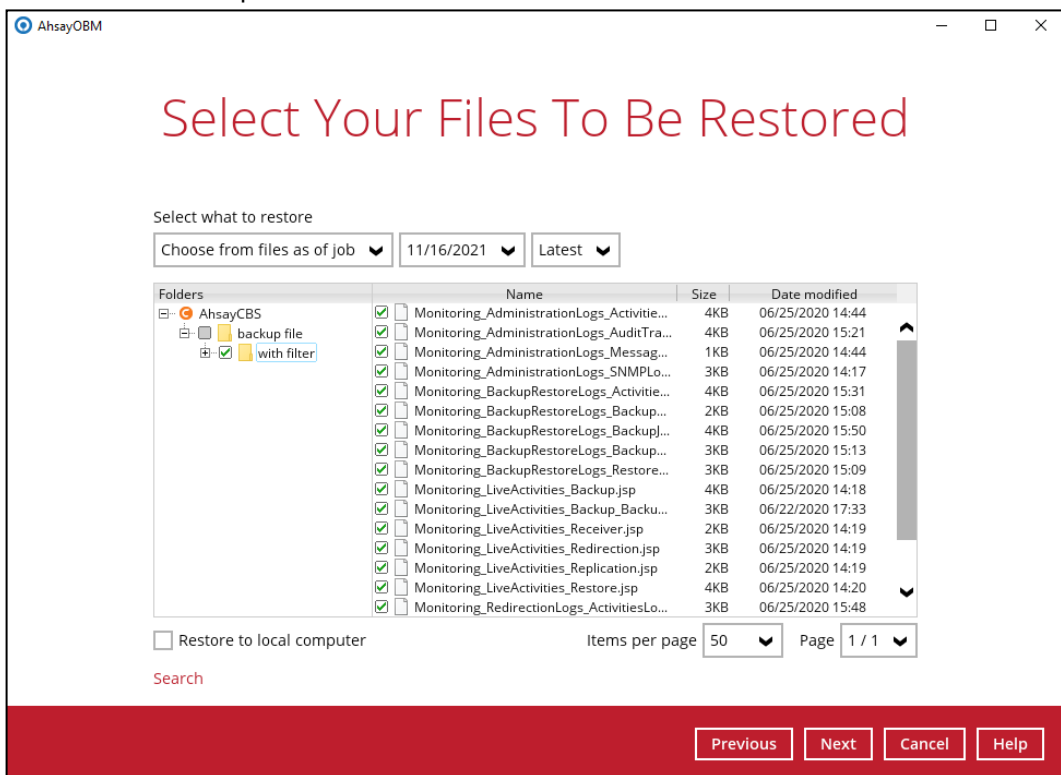
Tick **Restore to local computer** if you want to restore the backup data to the local drive.
Once done selecting the files and/or folders to restore, click **Next** to proceed.
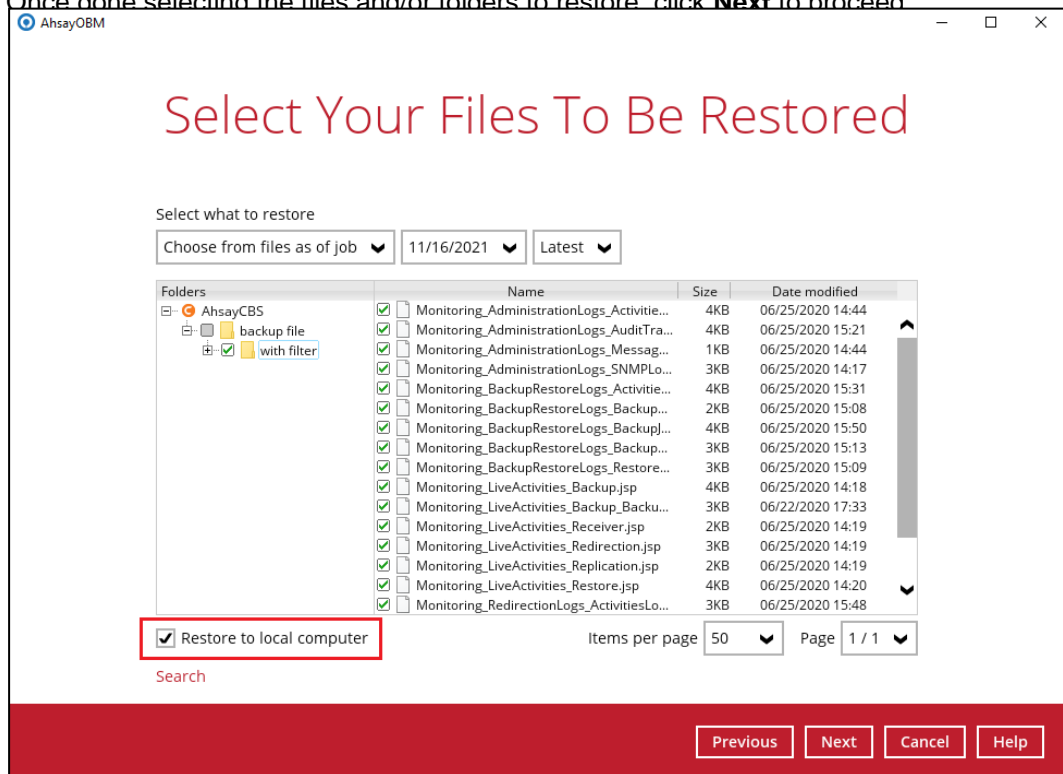
If you want to search for directories, files and folders to be restored, click **Search** to use the restore filter.

For more information on how to use the restore filter please refer to Chapter 14.2 of the AhsayOBM v9 Quick Start Guide for Windows.

For more detailed examples using the restore filter, refer to Appendix A: Example Scenarios for Restore Filter.

5. The window that will be displayed will depend on the restore destination selected. Here are the three options:

- **Local computer**

   If you want to restore on your local computer, browse the corresponding directory path on the local drive where you want the backup data to be restored.
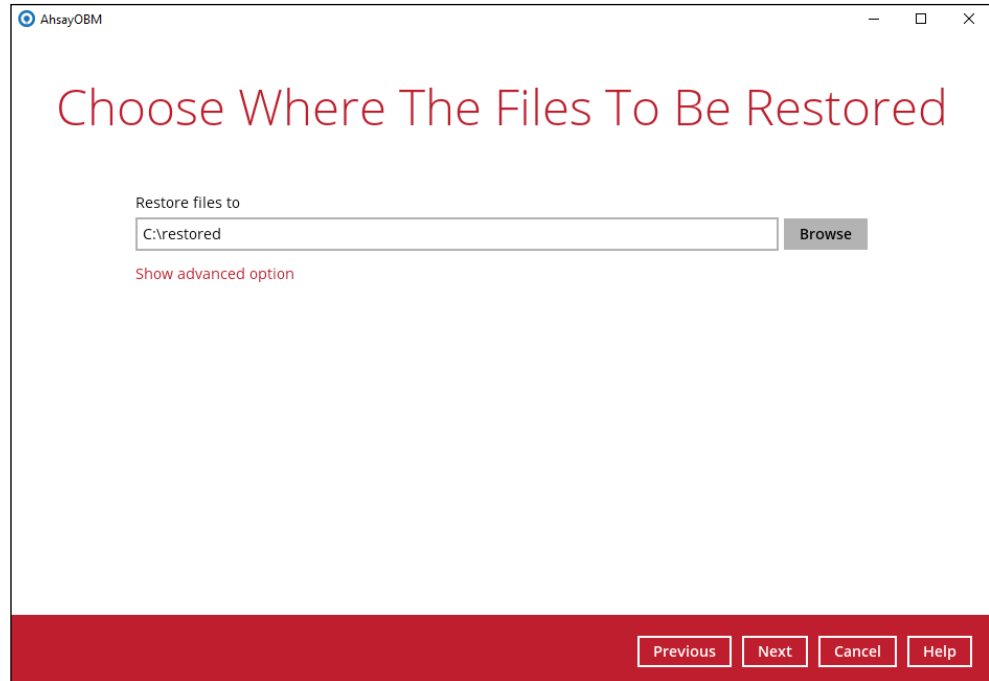
   Click **Show advanced option** to configure other restore settings.
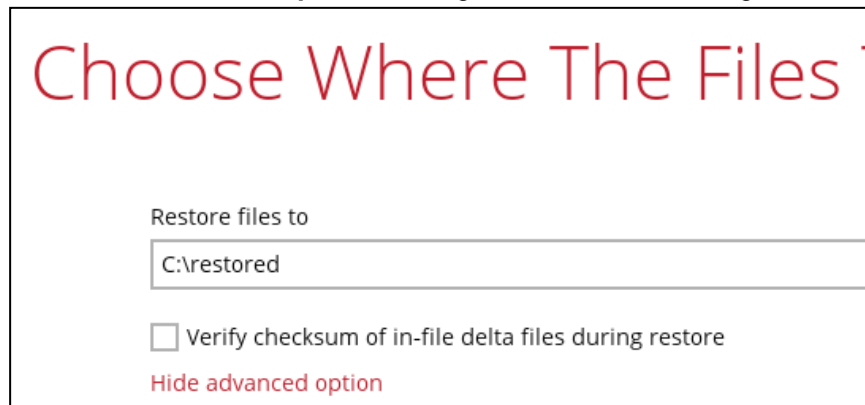
   Verify checksum of in-file delta files during restore

   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 will create a data summary of the in-file delta files which will be included in the report.

- **Original location**

  If you have chosen this option, the backup data will be restored to the computer running the AhsayOBM under the same directory path.
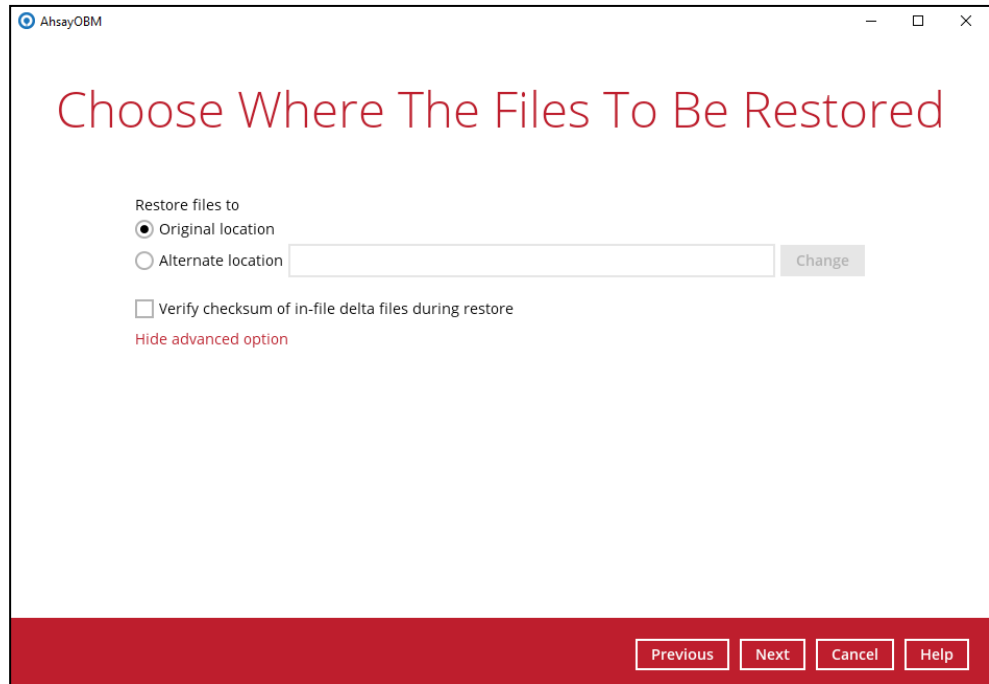
- **Alternate location**

  If you have chosen this option, backup data will be restored to another location of your choice. Click **Change** to select the alternate path on the cloud storage.
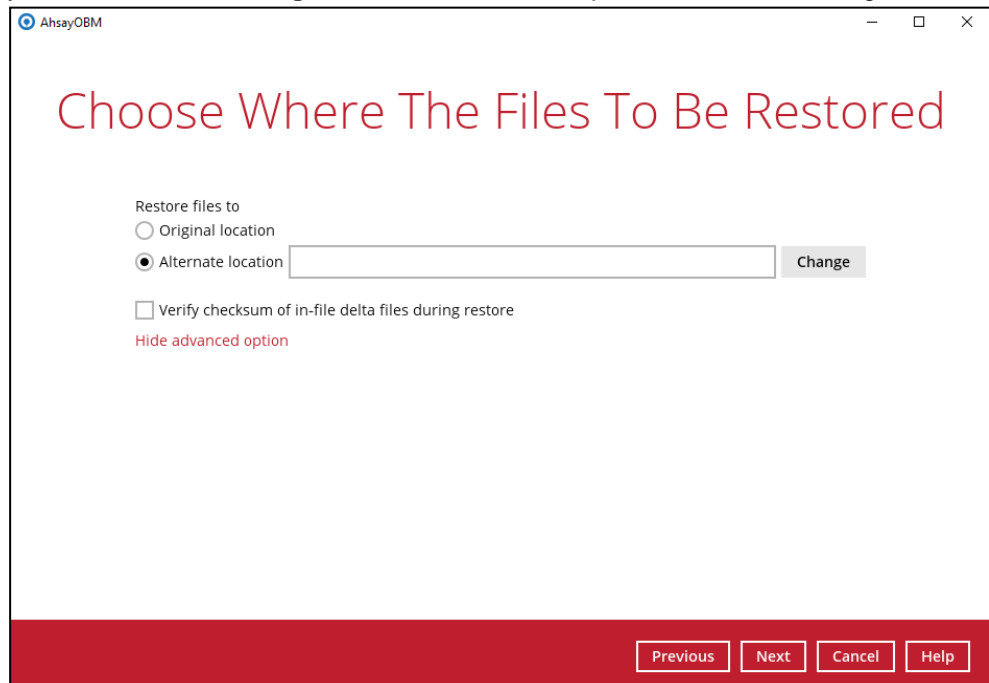
Select the path where the data will be restored then click **OK**.
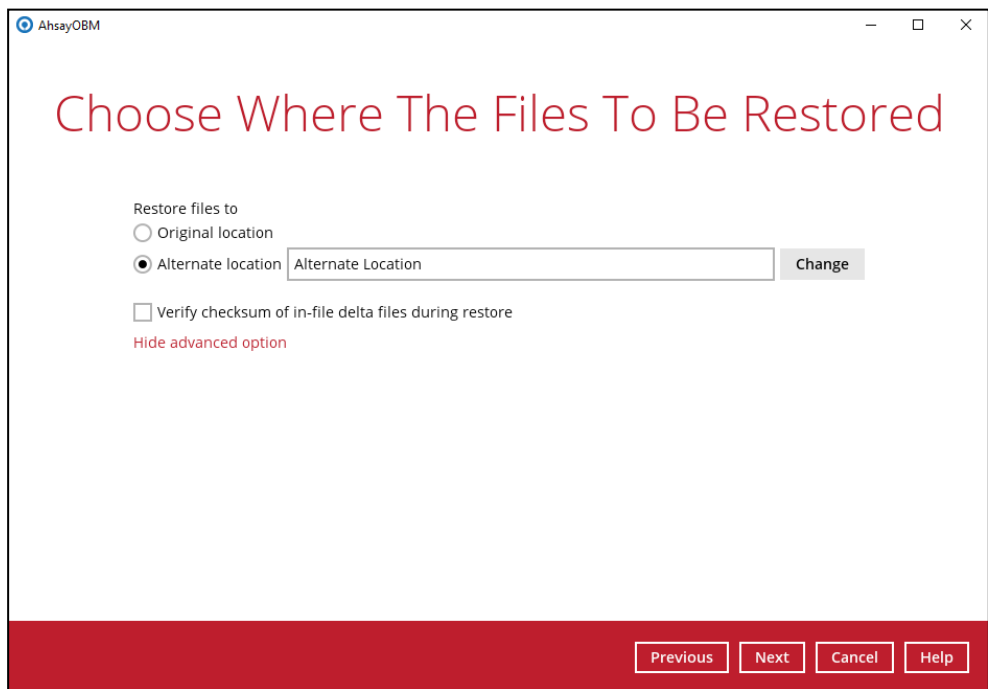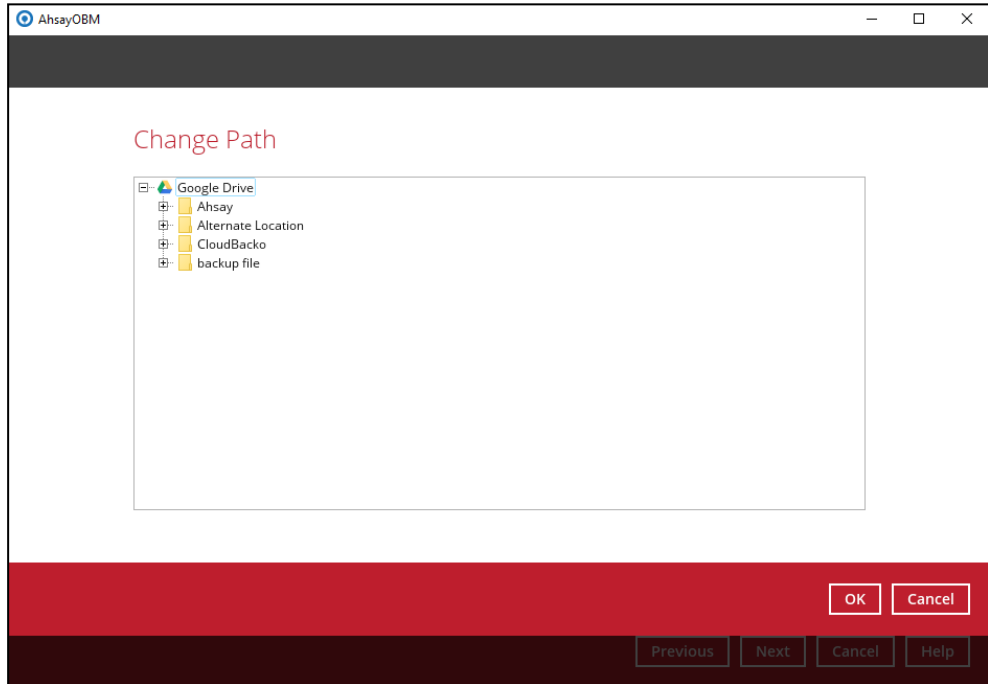
Click **Next** to proceed.

NOTE

Data can only be restored to the local computer or to the original cloud storage where the data was backed up from (i.e. same cloud storage provider and same account). Restoring backup data to a different cloud storage provider or different account is **NOT** possible.

---

6. Select the temporary directory for storing temporary files. Then click the **Restore** button to start the restoration process.
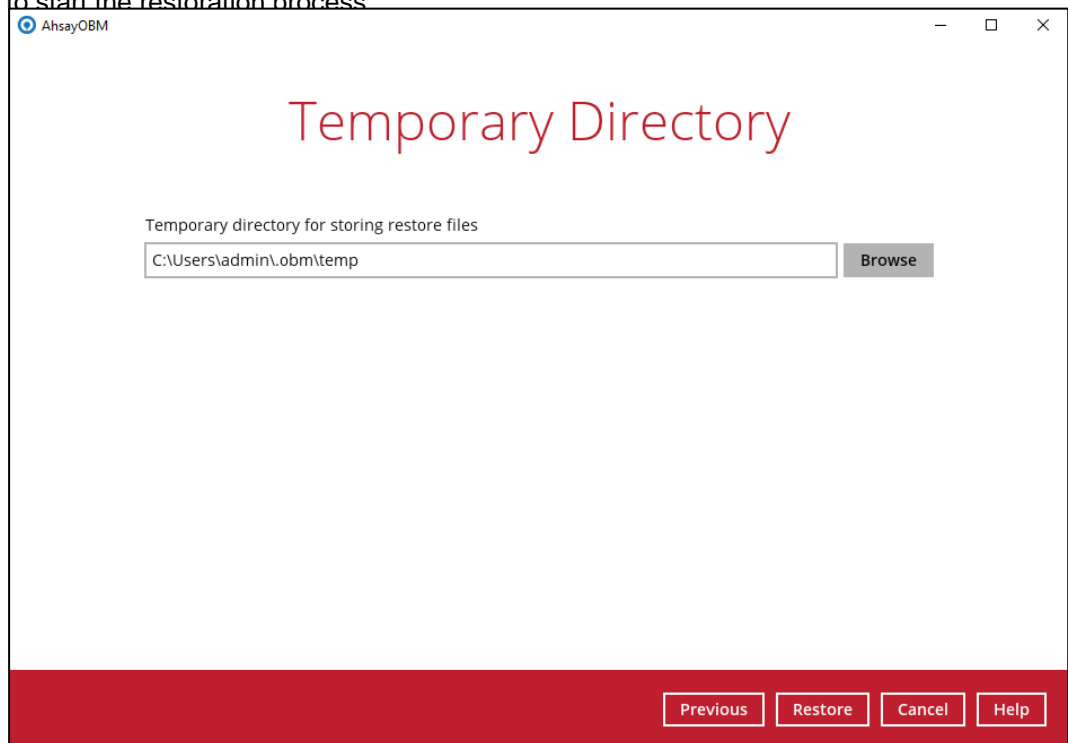
7. The following screen will be displayed after the restore process is complete.
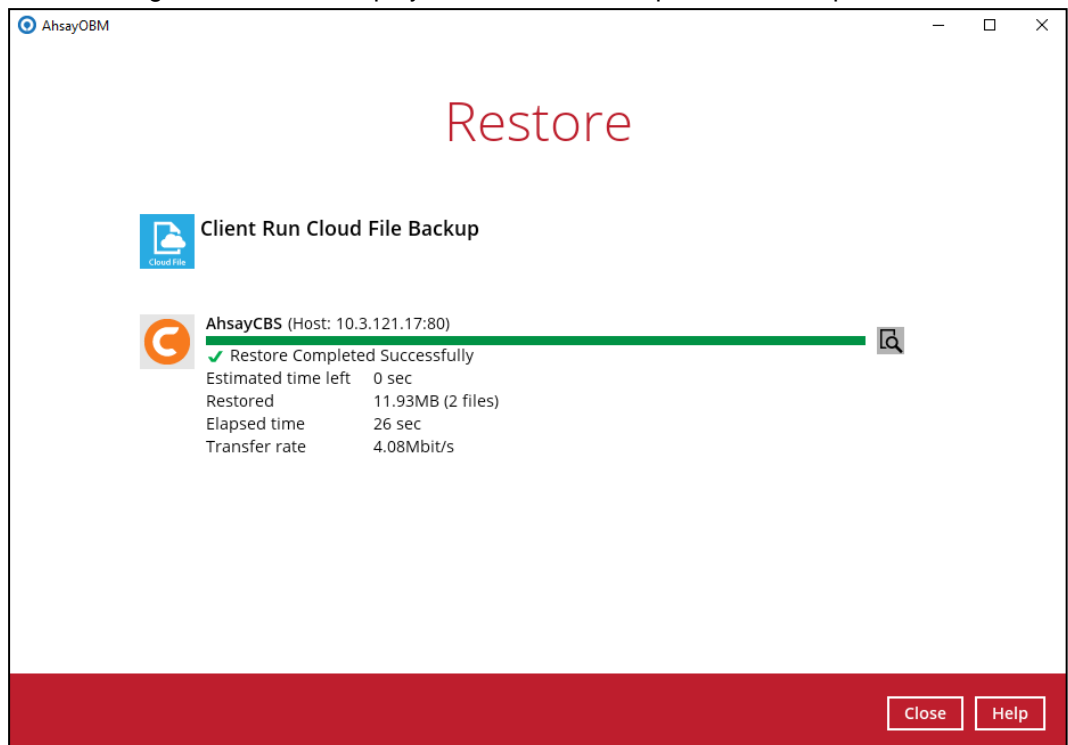
6   Contacting Ahsay

6.1   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/

6.2   Documentation

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

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

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

Appendix

Appendix A   Example Scenarios for Restore Filter

Example No. 1: Restore filter setting - Files and Directories

Location:	Photos/TestFiles/Photos
Search subfolders:	True
Kind:	Files and Directories
Type:	Contains
Pattern:	Test
Match Case:	True

Search

Look in

Photos/TestFiles/Photos   [Change]

☑ Search subfolders

Kind	Type	Pattern	
Files and Directories ⌄	contains ⌄	Test	☑ Match case

Searching ...   [**Stop**]

Name	In Folder	Size	Date modified
☑ TestJPG-1.jpg	Photos/TestFiles/Photos	517 KB	10/16/2019 03:02
☑ TestJPG-2.jpg	Photos/TestFiles/Photos	517 KB	10/16/2019 03:02
☑ TestJPG-3.jpg	Photos/TestFiles/Photos	517 KB	10/16/2019 03:03
☑ TestJPG-4.jpg	Photos/TestFiles/Photos	517 KB	10/16/2019 03:04
☑ TestJPG-5.jpg	Photos/TestFiles/Photos	517 KB	10/16/2019 03:04
☑ TestPNG-1.png	Photos/TestFiles/Photos	517 KB	10/16/2019 03:05
☑ TestPNG-2.png	Photos/TestFiles/Photos	517 KB	10/16/2019 03:05
☑ TestPNG-3.png	Photos/TestFiles/Photos	517 KB	10/16/2019 03:06
☑ TestPNG-4.png	Photos/TestFiles/Photos	517 KB	10/16/2019 03:06
☑ TestPNG-5.png	Photos/TestFiles/Photos	517 KB	10/16/2019 03:07

Items per page   50 ⌄   Page   1 / 1 ⌄

[OK]   [Cancel]   [Help]

[Previous]   [Next]   [Cancel]   [Help]

Search

Look in

Photos/TestFiles/Photos   [Change]

☑ Search subfolders

Kind	Type	Pattern	
Files and Directories ⌄	contains ⌄	Test	☑ Match case

[Search]

Name	In Folder	Size	Date modified
☑ TestJPG-1.jpg	Photos/TestFiles/Photos	517 KB	10/16/2019 03:02
☑ TestJPG-2.jpg	Photos/TestFiles/Photos	517 KB	10/16/2019 03:02
☑ TestJPG-3.jpg	Photos/TestFiles/Photos	517 KB	10/16/2019 03:03
☑ TestJPG-4.jpg	Photos/TestFiles/Photos	517 KB	10/16/2019 03:04
☑ TestJPG-5.jpg	Photos/TestFiles/Photos	517 KB	10/16/2019 03:04
☑ TestPNG-1.png	Photos/TestFiles/Photos	517 KB	10/16/2019 03:05
☑ TestPNG-2.png	Photos/TestFiles/Photos	517 KB	10/16/2019 03:05
☑ TestPNG-3.png	Photos/TestFiles/Photos	517 KB	10/16/2019 03:06
☑ TestPNG-4.png	Photos/TestFiles/Photos	517 KB	10/16/2019 03:06
☑ TestPNG-5.png	Photos/TestFiles/Photos	517 KB	10/16/2019 03:07

Items per page   50 ⌄   Page   1 / 1 ⌄

[OK]   [Cancel]   [Help]

[Previous]   [Next]   [Cancel]   [Help]

Explanation:

All files and directories under /Photos/TestFiles/Photos that has the exact pattern of 'Test" with match-case set to true will be included upon performing search.

As you can see on the screenshot above, the result panel contains the Name of the Files and/or Directories, Directory of the files and/or directories which are indicated in Folder column, Size of each files and/or directories, and Date Modified.

The restore filter setting includes the Search subfolder and Match case set to true. Meaning the filter will include all available subfolders in /Photos folder upon searching. And it will strictly search only the specified pattern and case which contains with 'Test'.

Example No. 2: Restore filter setting - Files only

Location:	Photos/TestFiles/Photos
Search subfolders:	True
Kind:	Files only
Type:	Starts with
Pattern:	T
Match Case:	True

Search

Look in

Photos/TestFiles/Photos | Change

☑ Search subfolders

Kind	Type	Pattern	
Files only ⌄	starts with ⌄	T	☑ Match case

�█████_____ **Stop**

Searching ...

Name	In Folder	Size	Date modified	
☑ 🖼 TestJPG-1.jpg	Photos/TestFiles/Photos	517 KB	10/16/2019 03:02	⌃
☑ 🖼 TestJPG-2.jpg	Photos/TestFiles/Photos	517 KB	10/16/2019 03:02	
☑ 🖼 TestJPG-3.jpg	Photos/TestFiles/Photos	517 KB	10/16/2019 03:03	
☑ 🖼 TestJPG-4.jpg	Photos/TestFiles/Photos	517 KB	10/16/2019 03:04	
☑ 🖼 TestJPG-5.jpg	Photos/TestFiles/Photos	517 KB	10/16/2019 03:04	
☑ 🖼 TestPNG-1.png	Photos/TestFiles/Photos	517 KB	10/16/2019 03:05	
☑ 🖼 TestPNG-2.png	Photos/TestFiles/Photos	517 KB	10/16/2019 03:05	
☑ 🖼 TestPNG-3.png	Photos/TestFiles/Photos	517 KB	10/16/2019 03:06	
☑ 🖼 TestPNG-4.png	Photos/TestFiles/Photos	517 KB	10/16/2019 03:06	⌄
☑ 🖼 TestPNG-5.png	Photos/TestFiles/Photos	517 KB	10/16/2019 03:07	

Items per page 50 ⌄   Page 1 / 1 ⌄

OK | Cancel | Help

Previous | Next | Cancel | Help

Search

Look in

Photos/TestFiles/Photos | Change

☑ Search subfolders

Kind	Type	Pattern	
Files only ⌄	starts with ⌄	T	☑ Match case

Search

Name	In Folder	Size	Date modified	
☑ 🖼 TestJPG-1.jpg	Photos/TestFiles/Photos	517 KB	10/16/2019 03:02	
☑ 🖼 TestJPG-2.jpg	Photos/TestFiles/Photos	517 KB	10/16/2019 03:02	⌃
☑ 🖼 TestJPG-3.jpg	Photos/TestFiles/Photos	517 KB	10/16/2019 03:03	
☑ 🖼 TestJPG-4.jpg	Photos/TestFiles/Photos	517 KB	10/16/2019 03:04	
☑ 🖼 TestJPG-5.jpg	Photos/TestFiles/Photos	517 KB	10/16/2019 03:04	
☑ 🖼 TestPNG-1.png	Photos/TestFiles/Photos	517 KB	10/16/2019 03:05	
☑ 🖼 TestPNG-2.png	Photos/TestFiles/Photos	517 KB	10/16/2019 03:05	
☑ 🖼 TestPNG-3.png	Photos/TestFiles/Photos	517 KB	10/16/2019 03:06	
☑ 🖼 TestPNG-4.png	Photos/TestFiles/Photos	517 KB	10/16/2019 03:06	⌄
☑ 🖼 TestPNG-5.png	Photos/TestFiles/Photos	517 KB	10/16/2019 03:07	

Items per page 50 ⌄   Page 1 / 1 ⌄

OK | Cancel | Help

Previous | Next | Cancel | Help

Explanation:

All files only under /Photos/TestFiles/Photos that has the exact pattern of 'T" with match-case set to true will be included upon performing search.

As you can see on the screenshot above, the result panel contains the Name of the files, Directory of the files which are indicated in Folder column, Size of each files, and Date Modified.

The restore filter setting includes the Search subfolder and Match case set to true. Meaning the filter will include all available subfolders in /Photos folder upon searching. And it will strictly search only the specified pattern and case which starts with 'T'.

Example No. 3: Restore filter setting - Directories only

Location:	Photos/TestFiles
Search subfolders:	True
Kind:	Directories only
Type:	Ends with
Pattern:	s
Match Case:	True

Search

Look in

Photos/TestFiles   [Change]

☑ Search subfolders

Kind	Type	Pattern	
Directories only ▼	ends with ▼	s	☑ Match case

▰▰▱▱▱▱   [Stop]

Searching ...

Name	In Folder	Size	Date modified
☑ 📁 Photos	Photos/TestFiles		

Items per page [50 ▼]   Page [1 / 1 ▼]

[OK] [Cancel] [Help]

[Previous] [Next] [Cancel] [Help]

Search

Look in

Photos/TestFiles   [Change]

☑ Search subfolders

Kind	Type	Pattern	
Directories only ▼	ends with ▼	s	☑ Match case

[Search]

Name	In Folder	Size	Date modified
☑ 📁 Photos	Photos/TestFiles		

Items per page [50 ▼]   Page [1 / 1 ▼]

[OK] [Cancel] [Help]

[Previous] [Next] [Cancel] [Help]

Explanation:

All directories only under /Photos/TestFiles that has the exact pattern of 's" with match-case set to true will be included upon performing search.

As you can see on the screenshot above, the result panel contains the Name of the directories, Directory which are indicated in Folder column, Size of each directories, and Date Modified.

The restore filter setting includes the Search subfolder and Match case set to true. Meaning the filter will include all available subfolders in /TestFiles folder upon searching. And it will strictly search only the specified pattern and case which ends with 's'.