

Ahsay Online Backup Manager v7

Cloud File Backup & Restore Guide for Mac OS X

Ahsay Systems Corporation Limited

10 April 2017

Copyright Notice

© 2017 Ahsay Systems Corporation Limited. All rights reserved.

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

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

Trademarks

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

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

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

Dropbox is registered trademark of Dropbox Inc.

Google Cloud Storage and Google Drive are registered trademarks of Google Inc.

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

Microsoft, Windows, Microsoft Exchange Server, Microsoft SQL Server, Microsoft Hyper-V, Microsoft Azure, One Drive and One Drive for Business are registered trademarks of Microsoft Corporation.

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

Oracle, Oracle 10g, Oracle 11g and MySQL are registered trademarks of Oracle Corporation.

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

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

ShadowProtect is registered trademark of StorageCraft Technology Corporation.

VMware, ESX, ESXi, vCenter are registered trademarks of VMware, Inc.

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

Disclaimer

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

Revision History

Date	Descriptions	Type of modification
18 Sept 2016	First Draft	New
3 Feb 2017	Added instructions and screen shots for Encryption key handling in Ch. 4.1	New
28 Feb 2017	Added Encryption Type option in Ch. 4 Creating a Cloud File Backup Set section	New
10 Apr 2017	Added Backup Destination for Run-on-Server Backup Set related info; Added new Encryption Type option in Create a Backup Set section	New

Table of Contents

1	Overview.....	1
1.1	About This Document.....	7
2	Preparing for Backup and Restore	8
2.1	Hardware Requirement.....	8
2.2	Software Requirement	8
2.3	Other Requirement and Recommendation	8
2.4	Best Practices and Recommendations	8
3	Login to AhsayOBM / AhsayCBS User Web Console	10
3.1	Login to AhsayOBM	10
3.2	Login to the AhsayCBS User Web Console	11
4	Creating a Cloud File Backup Set	12
4.1	Create a Cloud File Backup Set in AhsayOBM	12
4.2	Create a Cloud File Backup Set on the Web Console	23
5	Overview of Cloud File Backup	28
6	Running a Backup	30
6.1	Start a Manual Backup in AhsayOBM.....	30
6.2	Start a Manual Backup on the Web Console	31
6.3	Configure Backup Schedule for Automated Backup in AhsayOBM	32
6.4	Configure Backup Schedule for Automated Backup on the User Web Console	34
7	Restoring with a Cloud File Backup Set.....	36
7.1	Restore with AhsayOBM.....	36
7.2	Restore with the AhsayCBS User Web Console	41
8	Technical Assistance.....	43
9	Documentation	44
	Appendix	45
Appendix A	Setting Backup Destination on AhsayOBM for Backup Created on User Web Console	45

1 Overview

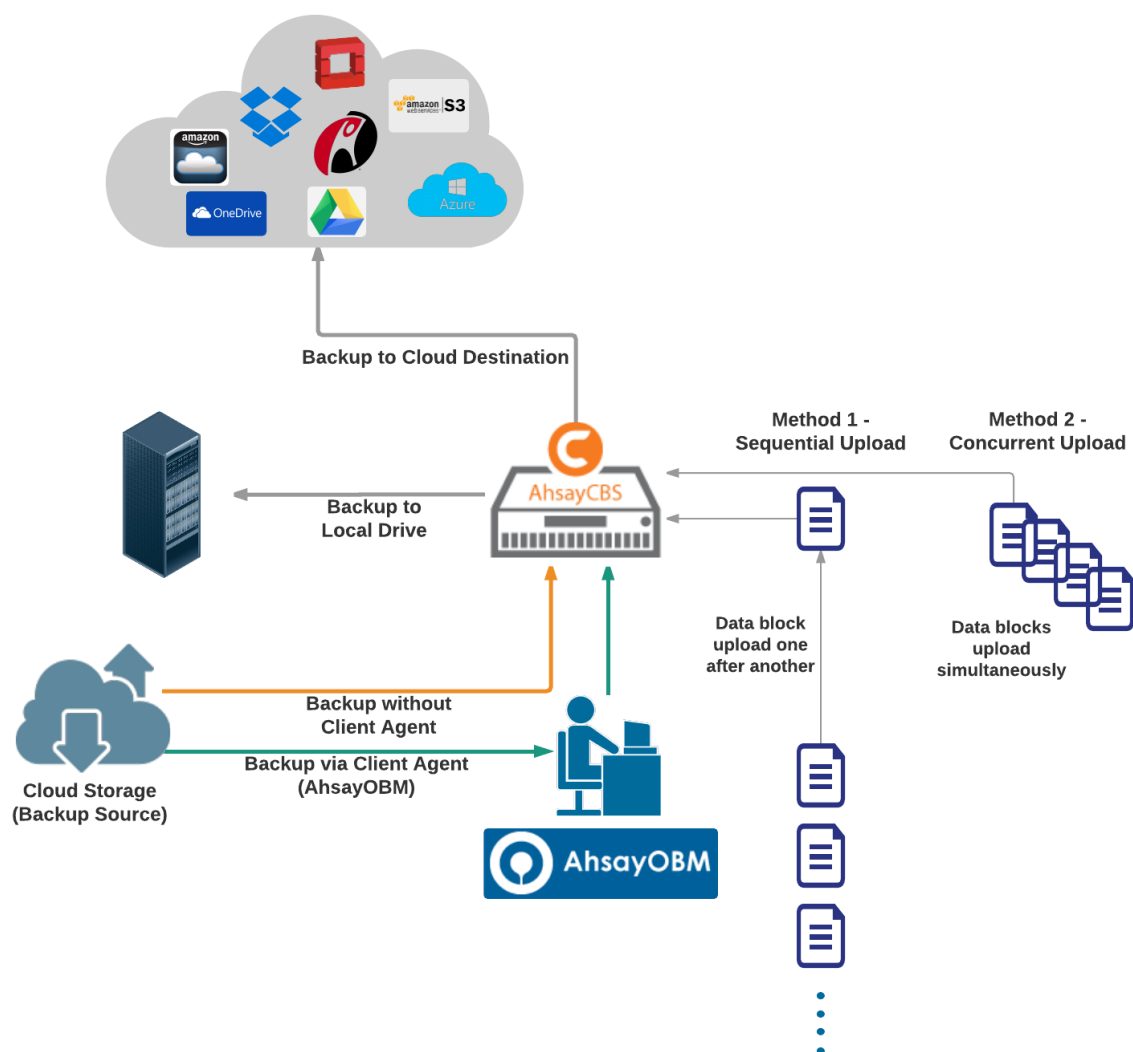
What is this software?

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

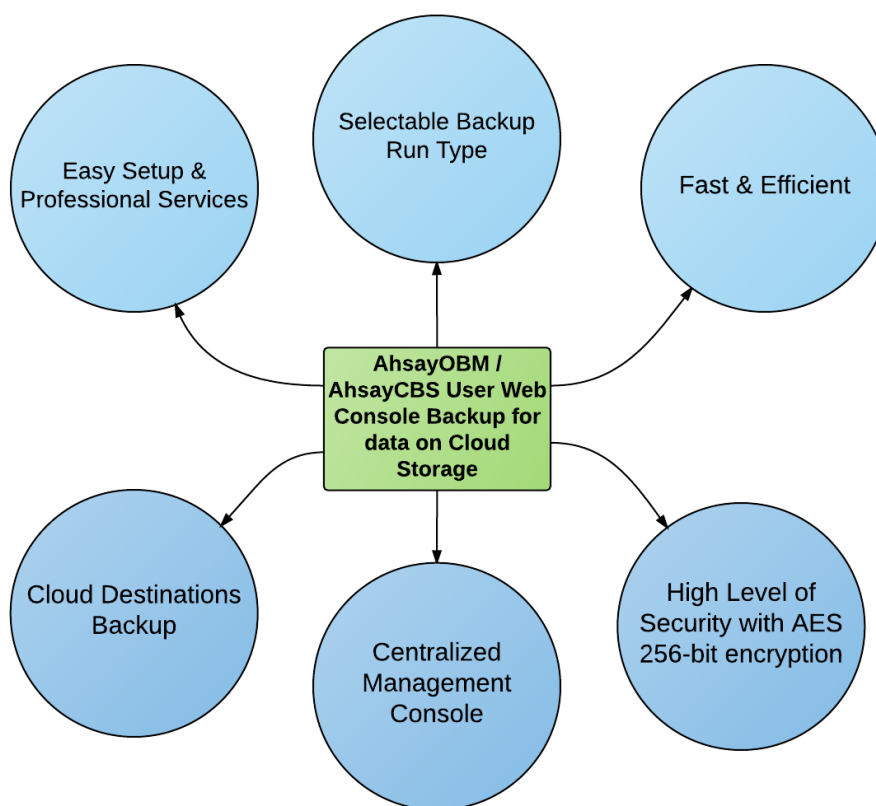
Below is the system architecture diagram illustrating the major elements involved in the backup process among the Cloud Storage, AhsayOBM and AhsayCBS.

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 v7 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	Yes (Restricted to AhsayCBS only)	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 / AhsayCBS
To Run a Restore	AhsayCBS User Web Console Only	AhsayOBM / AhsayCBS



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.

- ❶ **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.
- ❷ **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.

- ❶ Create backup set
- ❷ Restore backup
- ❸ Configure user settings
- ❹ Configure backup settings
- ❺ View and download backup and restore reports
- ❻ 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.

Amazon S3	Amazon Cloud Drive	AWS S3 Cloud Storage	Google Cloud Storage
Google Drive	OneDrive	Microsoft OneDrive / OneDrive for Business	Rackspace
OpenStack	Microsoft Azure	Dropbox	FTP
SFTP			

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.

Note

Cloud destination backup applies only to agent-based backup sets. The backup destination is restricted to AhsayCBS for all agentless backup sets.



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

Configuring an Automated Backup

Configure backup schedule for automated backup

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 7.3 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 7.3 or above](#)

2.3 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.

2.4 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

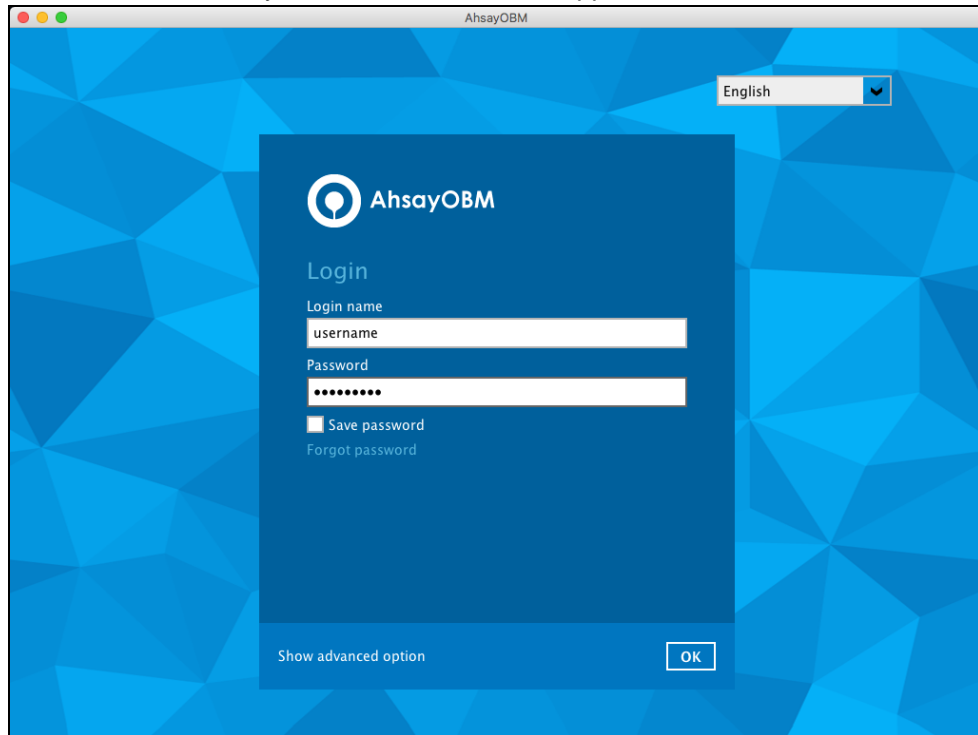
in your recovery plan. It's important that you do not try to make the test easier, as the objective of a successful test is not to demonstrate that everything is flawless. There might be flaws identified in the plan throughout the test and it is important to identify those flaws.

3 Login to AhsayOBM / AhsayCBS User Web Console

3.1 Login to AhsayOBM

1. Login to the AhsayOBM application user interface.

Double click the AhsayOBM icon to launch the application.



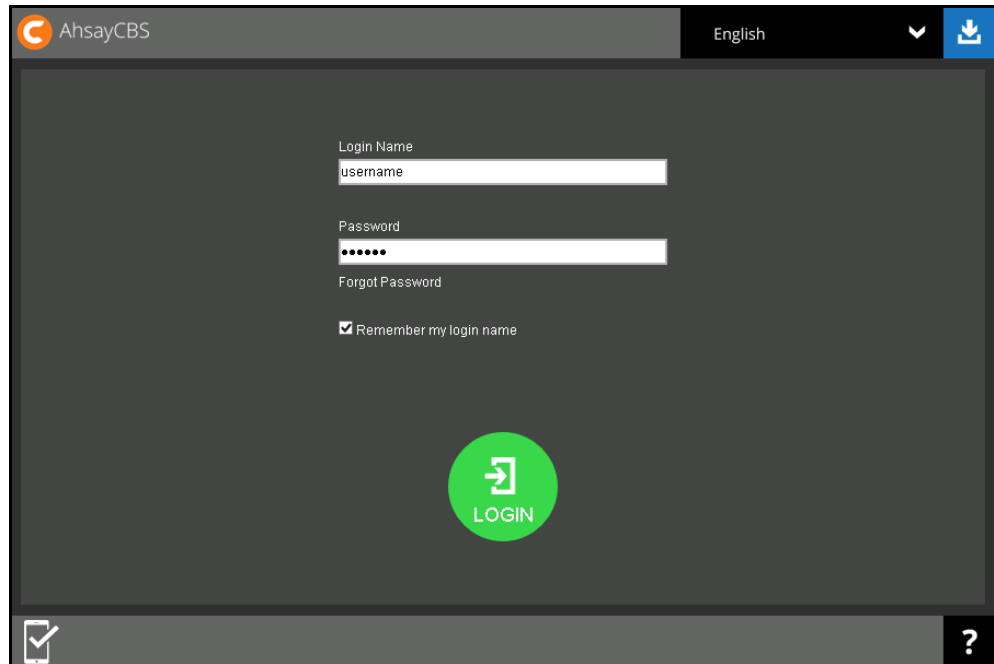
2. Enter the **Login name** and **Password** of your AhsayOBM account.
3. Click **Show advanced option** to configure the **Backup Server** and **Proxy** details if necessary.
4. Click **OK** afterward to login to AhsayOBM.

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.

The screenshot shows the AhsayCBS login web console. At the top, there is a header bar with the AhsayCBS logo on the left, the word "English" in the center, and a download icon on the right. The main content area is dark gray and contains a login form. The form has two input fields: "Login Name" with the placeholder text "username" and "Password" with placeholder dots. Below the password field is a link for "Forgot Password". There is a checkbox labeled "Remember my login name" which is checked. A large green circular button with a white right-pointing arrow and the word "LOGIN" is centered below the form. At the bottom of the page, there is a footer bar with a mobile app icon on the left and a question mark icon on the right.

2. Enter the **Login Name** and **Password** of your AhsayOBM account.
3. Click **Login** afterward to login to the web console.

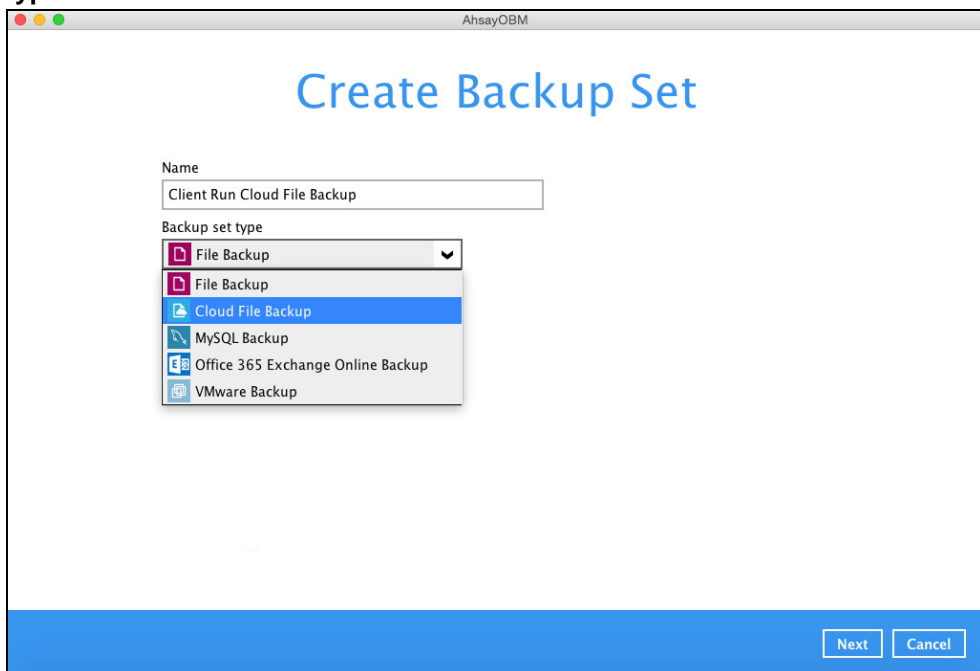
4 Creating a Cloud File Backup Set

4.1 Create a Cloud File Backup Set in AhsayOBM

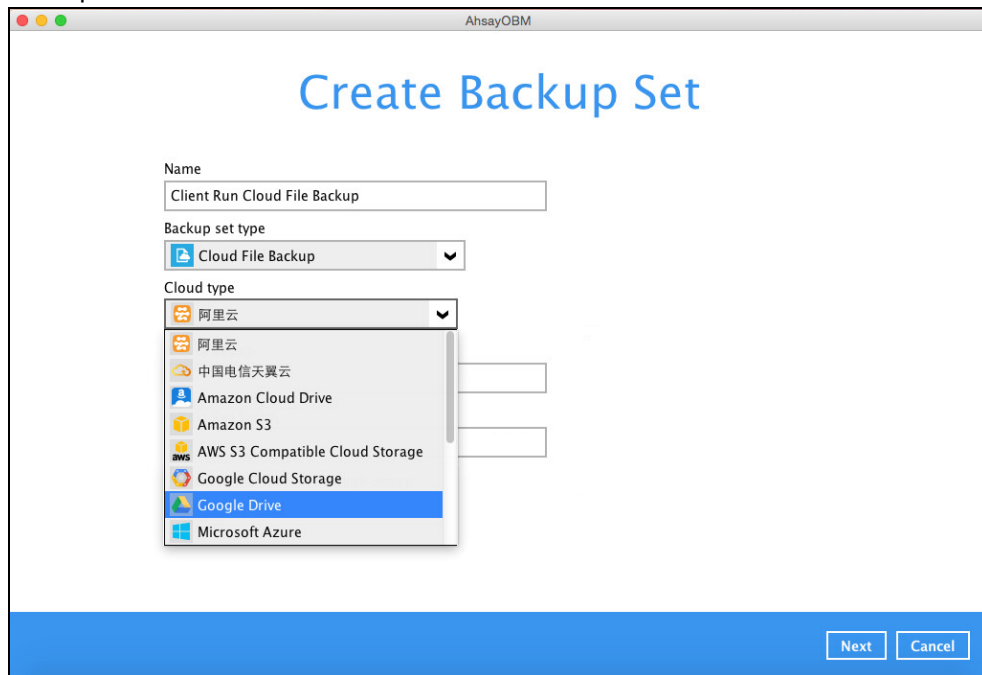
1. In the AhsayOBM main interface, click **Backup Sets**.



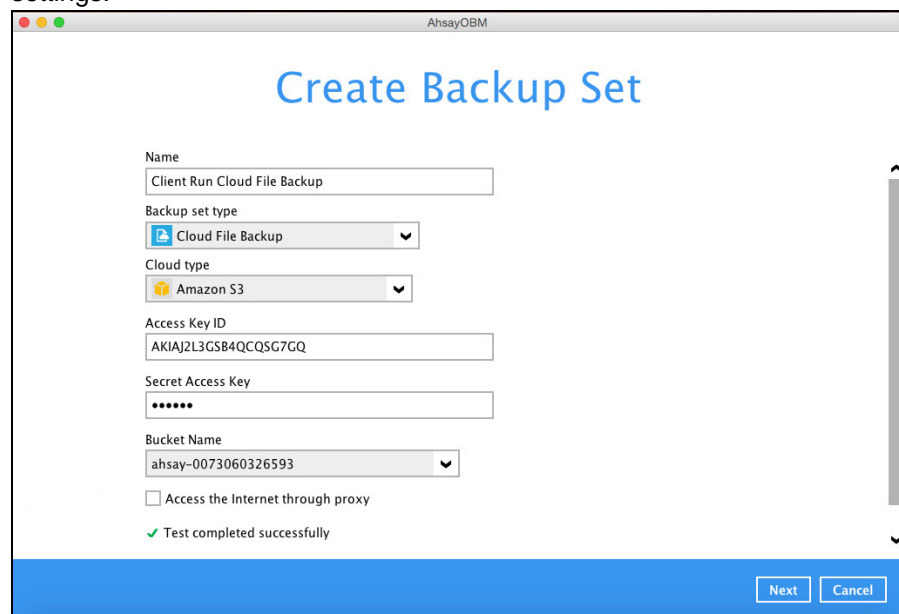
2. Create a Cloud File backup set by clicking the "+" icon next to **Add new backup set**.
3. Enter a **Name** for your backup set and select **Cloud File Backup** as the **Backup set type**.



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



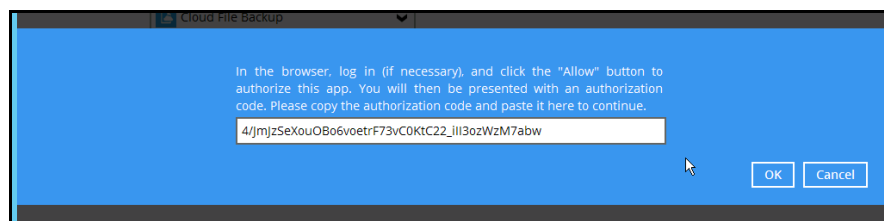
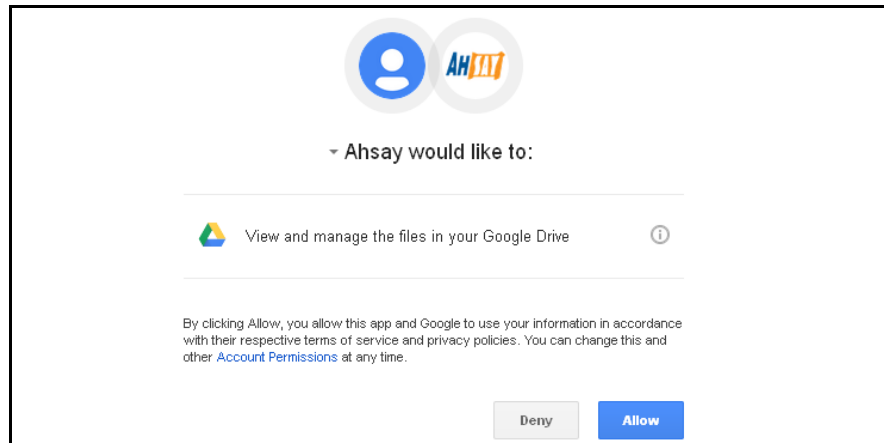
5. Depending on the cloud type you have selected, you will be prompted to enter the cloud service login details in either way below.
- Enter the login details on the current page in AhsayOBM, then click **Test** to validate your account information. A confirmation text **Test completed successfully** shows when AhsayOBM is connected to the cloud service successfully. If you need to route through proxy server to access the Internet, enable the **Access the Internet through proxy** checkbox to configure the settings.



-OR-

- 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

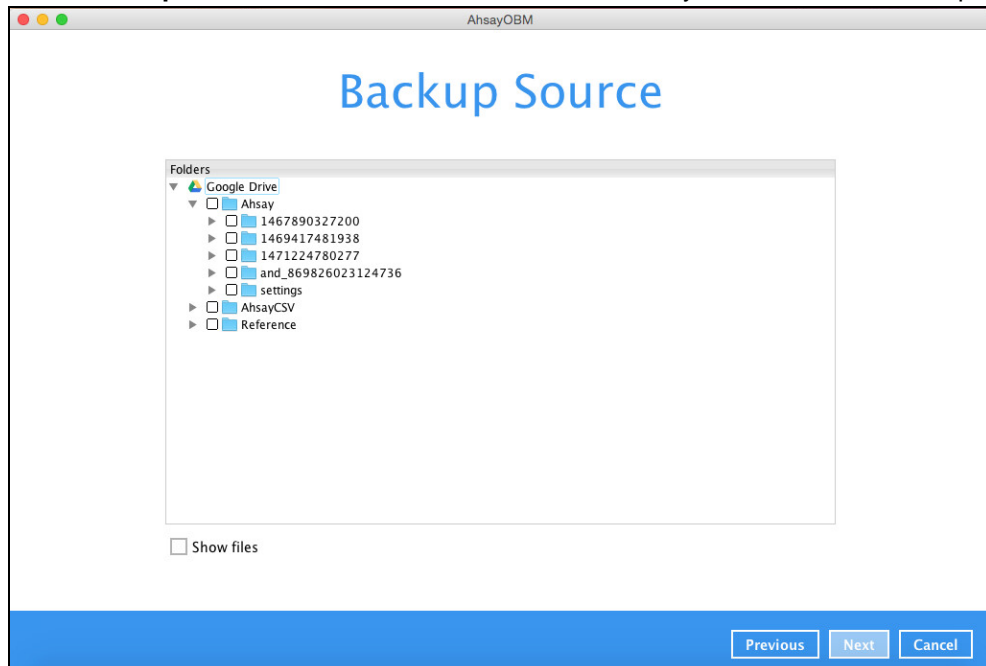
AhsayOBM to access the cloud storage. Copy and paste the code generated by the cloud service provider to AhsayOBM where you will be prompted to enter, then click **OK** to confirm.



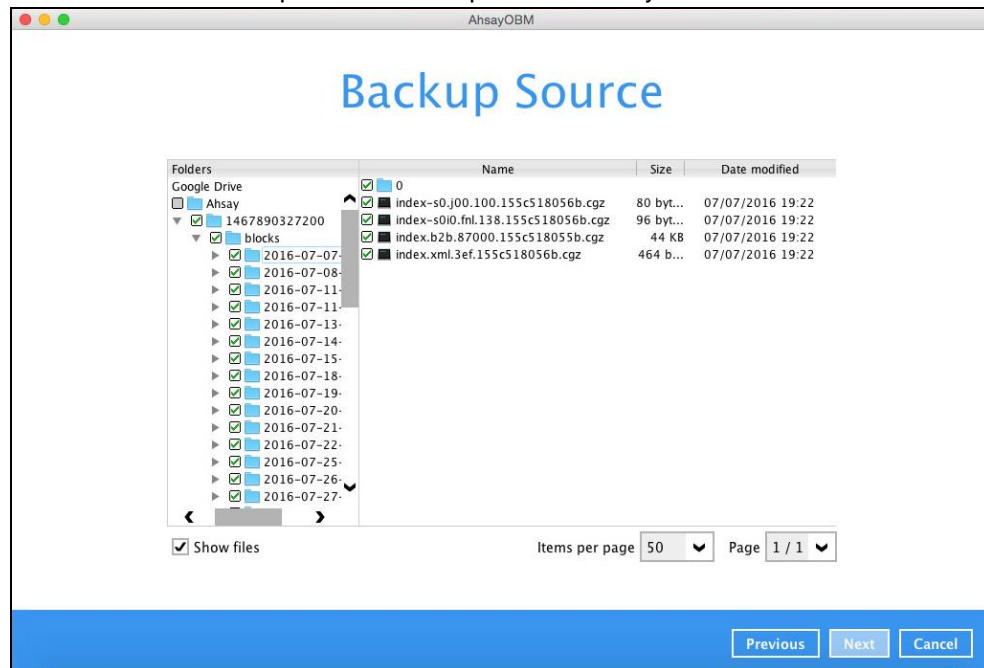
IMPORTANT

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).

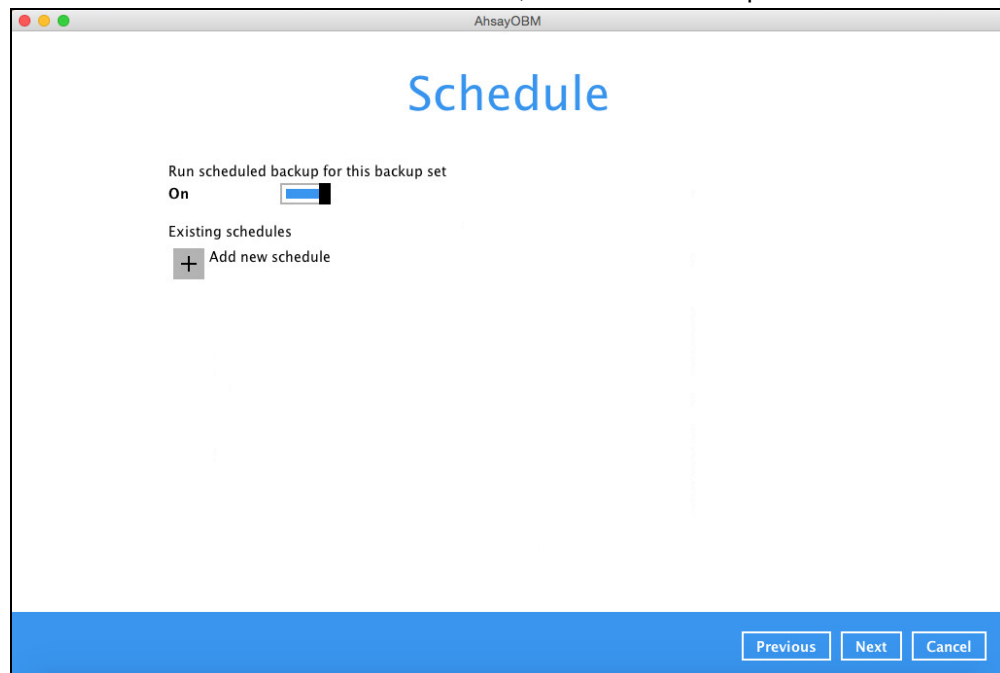
6. In the **Backup Source** menu, select the folder / files that you would like to backup.



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. Slide the on/off button to turn on this feature, then click **Add new schedule** to add a new schedule, then click **Next** to proceed afterward.



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

The screenshot shows the 'New Backup Schedule' dialog box in the AhsayOBM application. The dialog has a title bar with standard window controls and the text 'AhsayOBM'. The main content area is titled 'New Backup Schedule' in blue. Below the title, there are several input fields: 'Name' with the value 'Daily-2', 'Type' with a dropdown menu set to 'Daily', 'Start backup at' with a time picker set to '18:07', and 'Stop' with a dropdown menu set to 'until full backup completed'. There is also an unchecked checkbox labeled 'Run Retention Policy after backup'. At the bottom right, there are two buttons: 'OK' and 'Cancel'. Below the dialog box, there are three buttons: 'Previous', 'Next', and 'Cancel'.

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**.

The screenshot shows the 'Destination' dialog box in the AhsayOBM application. The dialog has a title bar with standard window controls and the text 'AhsayOBM'. The main content area is titled 'Destination' in blue. Below the title, there are several input fields: 'Backup mode' with a dropdown menu set to 'Sequential', and 'Existing storage destinations' with a '+' icon and the text 'Add new storage destination / destination pool'. At the bottom right, there are three buttons: 'Previous', 'Next', and 'Cancel'.

Note

For more details on Backup Destination, refer to the following KB article for details:
<https://forum.ahsay.com/viewtopic.php?f=186&t=14049>

9. Select the storage type.

- **Single storage destination** – the entire backup will be uploaded to one single destination you selected under the **Destination storage** drop-down list. By default, the destination storage is selected as **CBS**.

AhsayOBM

New Storage Destination / Destination Pool

Name
CBS

Type
☒ Single storage destination
☐ Destination pool

Destination storage
CBS

OK Cancel

Previous Next Cancel

- **Destination pool** – the backup will be spread over on the destinations you have selected. Enter a **Name** for the destination pool and then click **Add new storage destination to the pool** to select the desired storage destinations.

AhsayOBM

New Storage Destination / Destination Pool

Name
DestinationPool-1

Type
☐ Single storage destination
☒ Destination pool

Add the cloud (e.g. Google Drive or Dropbox) or local storage that you would like to pool together for backup. You can always add more storage to this pool in the future.

Existing storage destinations in the pool

+ Add new storage destination to the pool

OK Cancel

Previous Next Cancel

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.

AhsayOBM

New Storage Destination For The Pool

Name
Local-1

Destination storage
Local / Mapped Drive / Removable Drive ▼

Local path
 Change

Test

OK Cancel

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

AhsayOBM

New Storage Destination For The Pool

Name
GoogleDrive-1

Destination storage
Google Drive ▼

Test

[Sign up for Google Drive](#)

OK Cancel

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

The screenshot shows a dialog box titled "New Storage Destination For The Pool" from the AhsayOBM application. It contains the following fields and options:

- Name:** A text input field containing "FTP-1".
- Destination storage:** A dropdown menu with "FTP" selected.
- Host:** A text input field.
- Port:** A text input field.
- Username:** A text input field.
- Password:** A text input field.
- (optional) FTP directory to store backup data (default to ~/AhsayCSV):** A text input field.
- Connect with SSL/TLS (explicit only):** An unchecked checkbox.
- Access the Internet through proxy:** An unchecked checkbox.
- Buttons:** "OK" and "Cancel" buttons at the bottom right.

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.

The screenshot shows the "Destination" screen in the AhsayOBM application. It displays the following information:

- Backup mode:** A dropdown menu with "Sequential" selected.
- Existing storage destinations:** A list showing two destinations:
 - CBS**
Host: 10.23.6.69:60080
 - DestinationPool-1**
- Buttons:** An "Add" button below the list, and "Previous", "Next", and "Cancel" buttons at the bottom right.

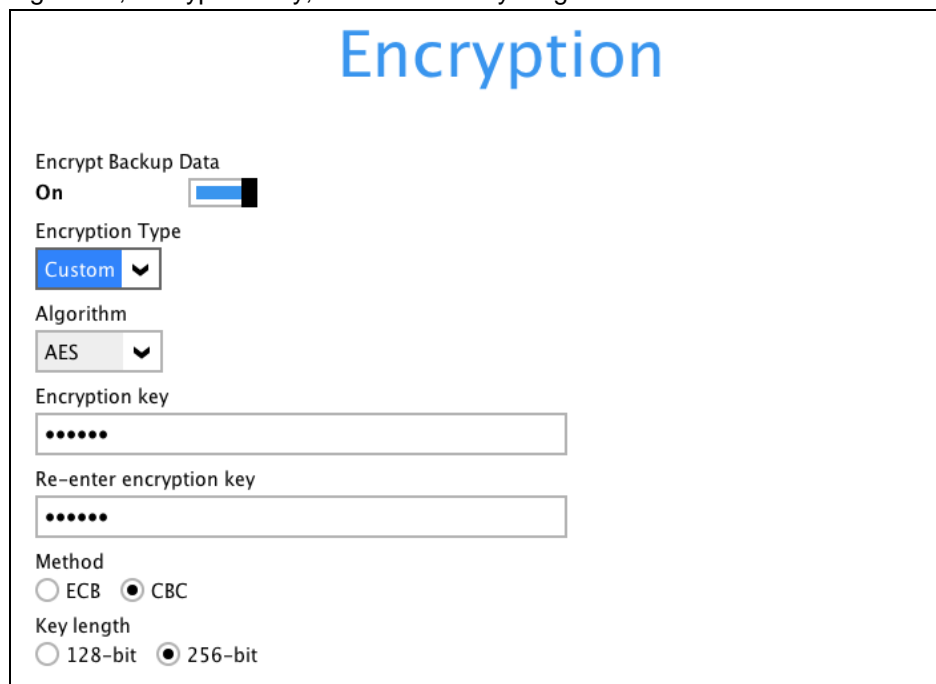
11. In the Encryption window, the default **Encrypt Backup Data** option is enabled with an encryption key preset by the system which provides the most secure protection.



The screenshot shows the 'Encryption' window. At the top, the title 'Encryption' is displayed in blue. Below it, the 'Encrypt Backup Data' option is set to 'On' with a toggle switch. Underneath, the 'Encryption Type' dropdown menu is open, showing three options: 'Default' (highlighted), 'User password', and 'Custom'.

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.

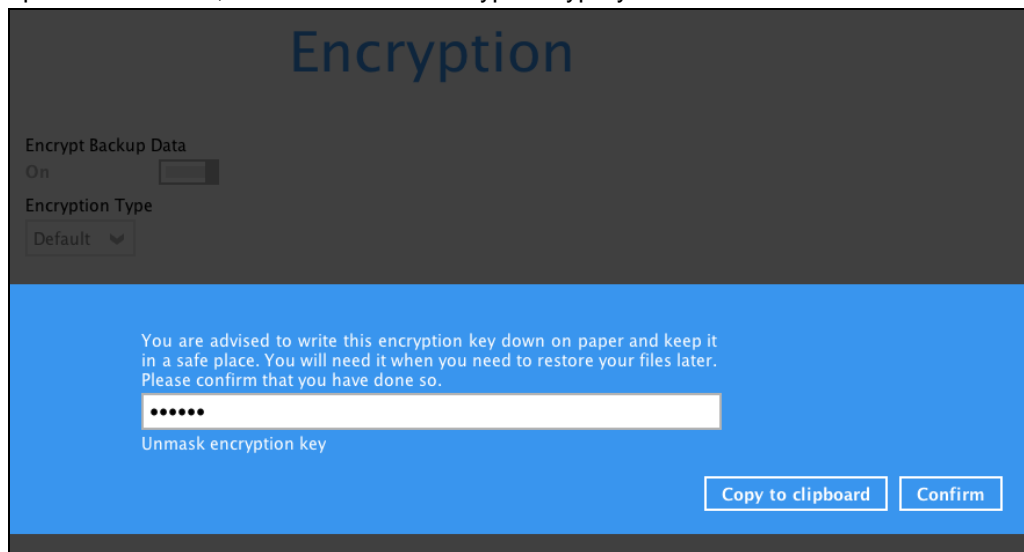


The screenshot shows the 'Encryption' window with the 'Custom' encryption type selected. The 'Algorithm' dropdown is set to 'AES'. There are two input fields for the 'Encryption key' and 'Re-enter encryption key', both containing six dots. The 'Method' section has two radio buttons: 'ECB' and 'CBC' (selected). The 'Key length' section has two radio buttons: '128-bit' and '256-bit' (selected).

Note: For best practice on managing your encryption key, refer to the following KB article. <https://forum.ahsay.com/viewtopic.php?f=169&t=14090>

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

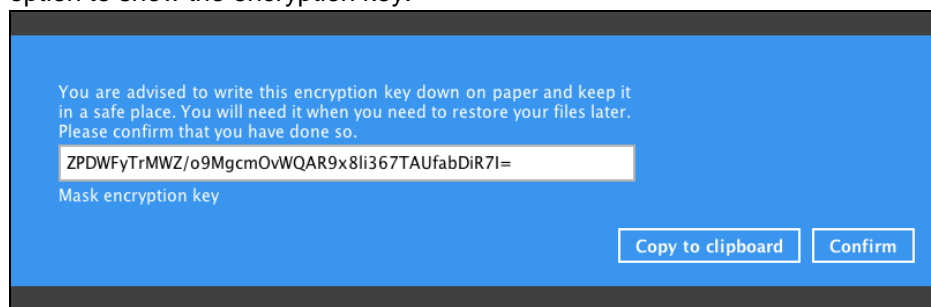
12. If you have enabled the Encryption Key feature in the previous step, the following pop-up window shows, no matter which encryption type you have selected.



The screenshot shows a dark-themed window titled "Encryption". At the top, there is a toggle for "Encrypt Backup Data" which is turned "On", and a dropdown for "Encryption Type" set to "Default". The main area has a blue background with white text: "You are advised to write this encryption key down on paper and keep it in a safe place. You will need it when you need to restore your files later. Please confirm that you have done so." Below this is a text input field containing six dots, representing a masked key. Under the field is the label "Unmask encryption key". At the bottom right are two buttons: "Copy to clipboard" and "Confirm".

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.

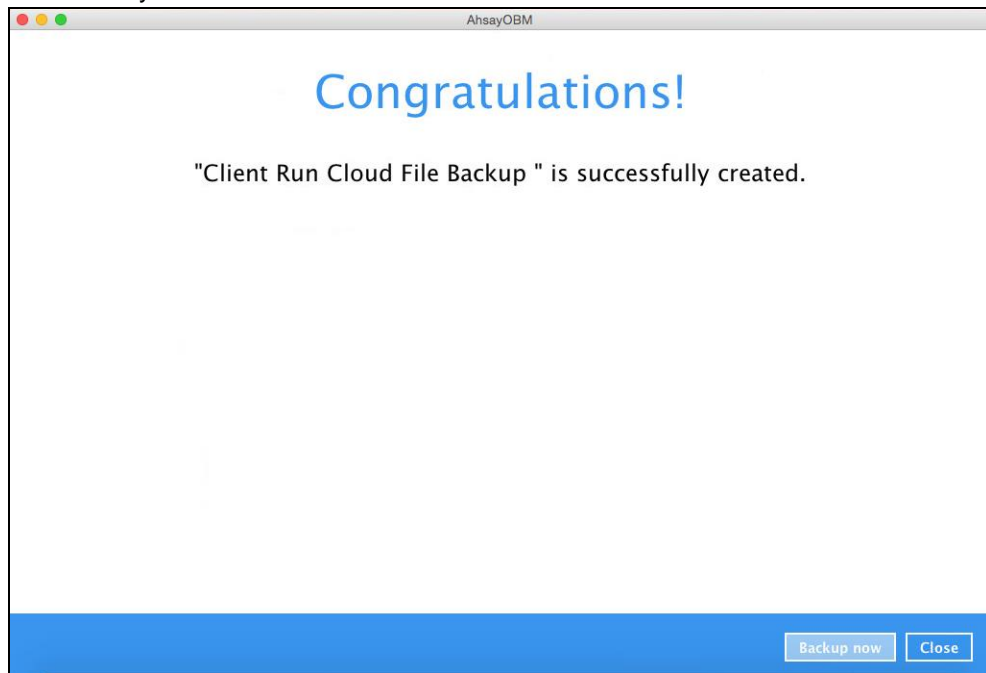


This screenshot shows the same "Encryption" window, but the text input field now displays the actual encryption key: "ZPDWFyTrMWZ/o9MgcmOvWQAR9x8li367TAUfabDiR7I=". Below the field is the label "Mask encryption key". The "Copy to clipboard" and "Confirm" buttons remain at the bottom right.

- **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.

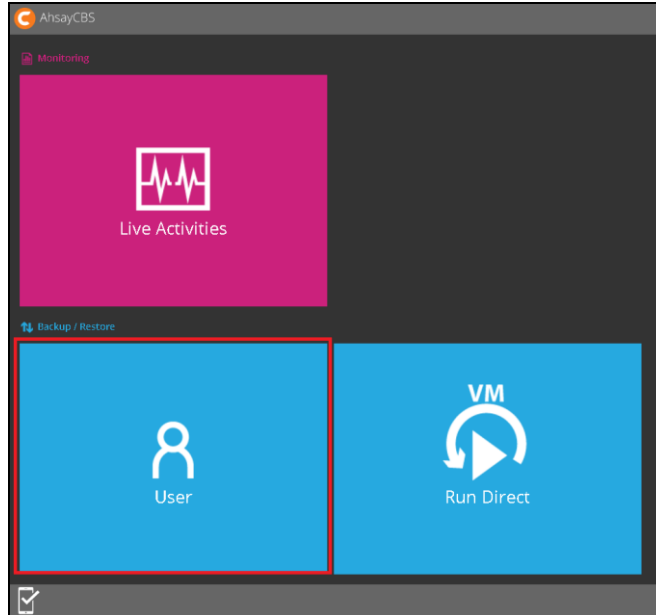
13. Click **Next** to create the backup set.

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

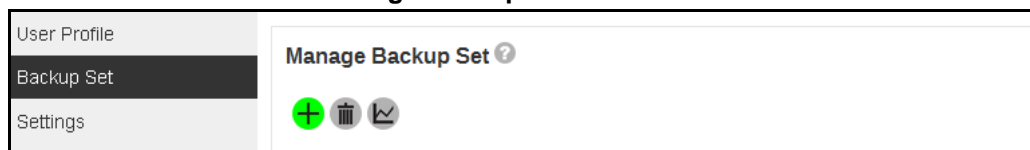


4.2 Create a Cloud File Backup Set on the Web Console

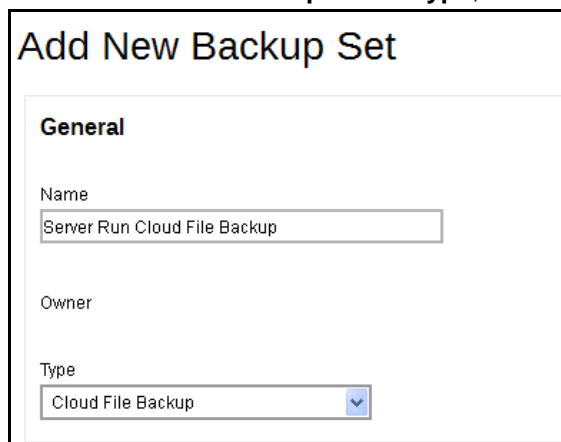
1. Log in to the User Web Console according to the instructions in [Login to the AhsayCBS User Web Console](#).
2. Click the **User** icon on the User Web Console landing page.



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.



Add New Backup Set

General

Name
Server Run Cloud File Backup

Owner

Type
Cloud File Backup

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.

Run on
☒ Server ☐ Client

Notes

1. 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.
2. For backup sets created in **Run-on-Server** backup type, the backup destination is restricted to AhsayCBS by default and cannot be altered. If you wish to back up to other destinations, backup sets should be created in **Run-on-Client** backup type instead.

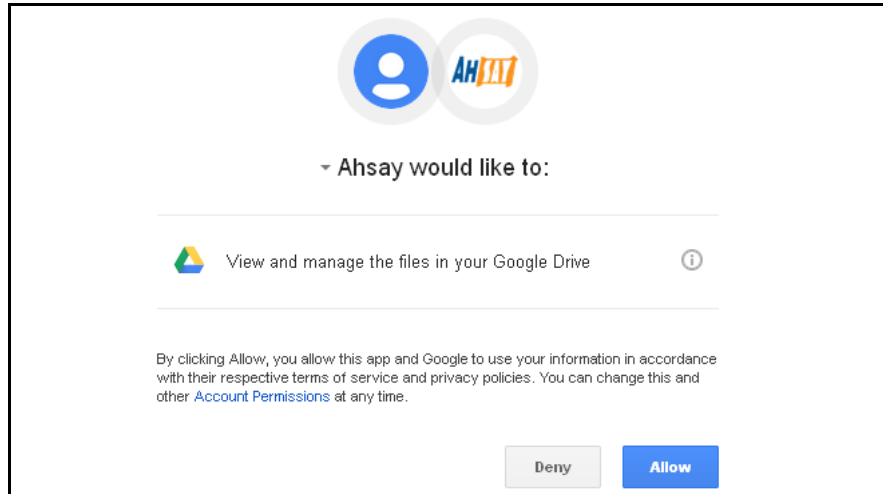
6. Select the cloud storage that contains the data that you want to backup under **Backup From**. Click **Test** afterward to authenticate AhsayCBS / AhsayOBM to access the cloud storage.

Backup From

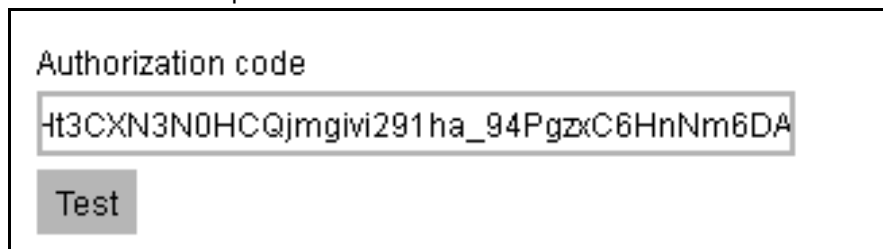
IMPORTANT

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).

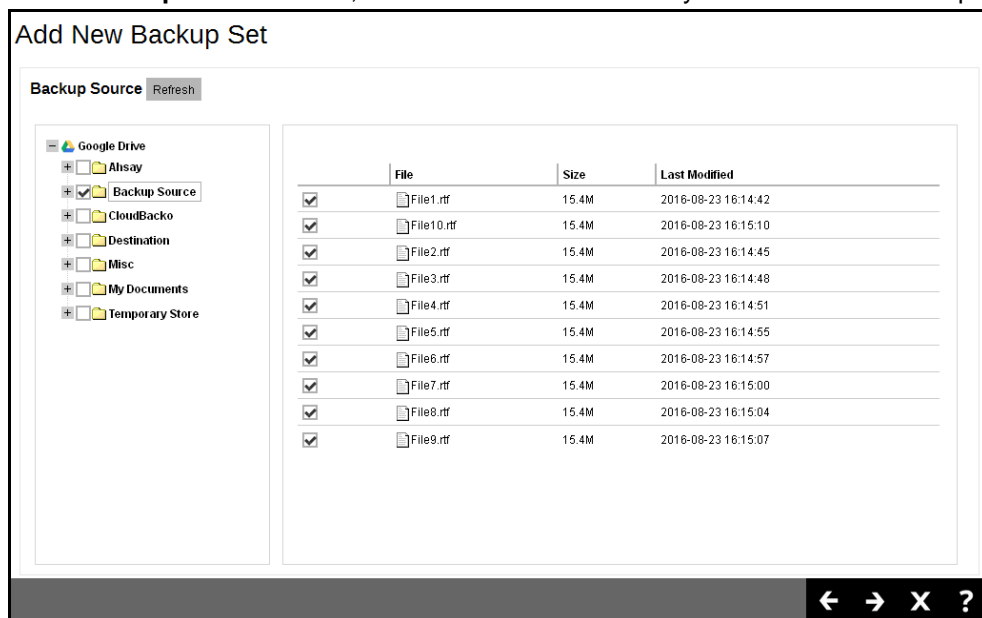
7. Click **Allow** to permit access the cloud storage.



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, then click **Next** to proceed afterward
10. For **Run on Client** Cloud File backup set, select a predefined backup destination where the backup data will be stored. Click the **+** icon under **Predefined Destination**.

IMPORTANT

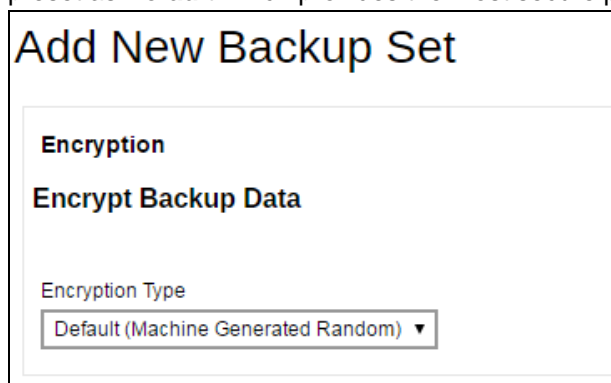
The **Destination** menu will only be displayed for **Run on Client** Cloud File backup set. For **Run on Server** Cloud File backup set, the destination will automatically be set to the backup server (AhsayCBS), the destination is not configurable.

If you would like to create a **Run on Client** Cloud File backup set with a standard backup destination, please create the backup set via the AhsayOBM user interface instead.

Select the corresponding predefined destination, and then click **Add**. Click **Next** to proceed afterward.

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 complete this backup set creation first, then log in to the AhsayOBM and configure the backup destination from there. For further details, refer to [Appendix A Setting Backup Destination on AhsayOBM for Backup Created on User Web Console](#).

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



The screenshot shows a web form titled "Add New Backup Set". Inside the form, there is a section labeled "Encryption". Under this section, the option "Encrypt Backup Data" is checked. Below this, there is a label "Encryption Type" followed by a dropdown menu. The dropdown menu is currently set to "Default (Machine Generated Random)".

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 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.

Add New Backup Set

Encryption
Encrypt Backup Data

Encryption Type

Custom

Algorithm

AES

Encrypting key

Re-type encrypting key


Method


☐ ECB ☒ CBC

Key length

☐ 128-bit ☒ 256-bit

Note: For best practice on managing your encryption key, refer to the following KB article: <https://forum.ahsay.com/viewtopic.php?f=169&t=14090>

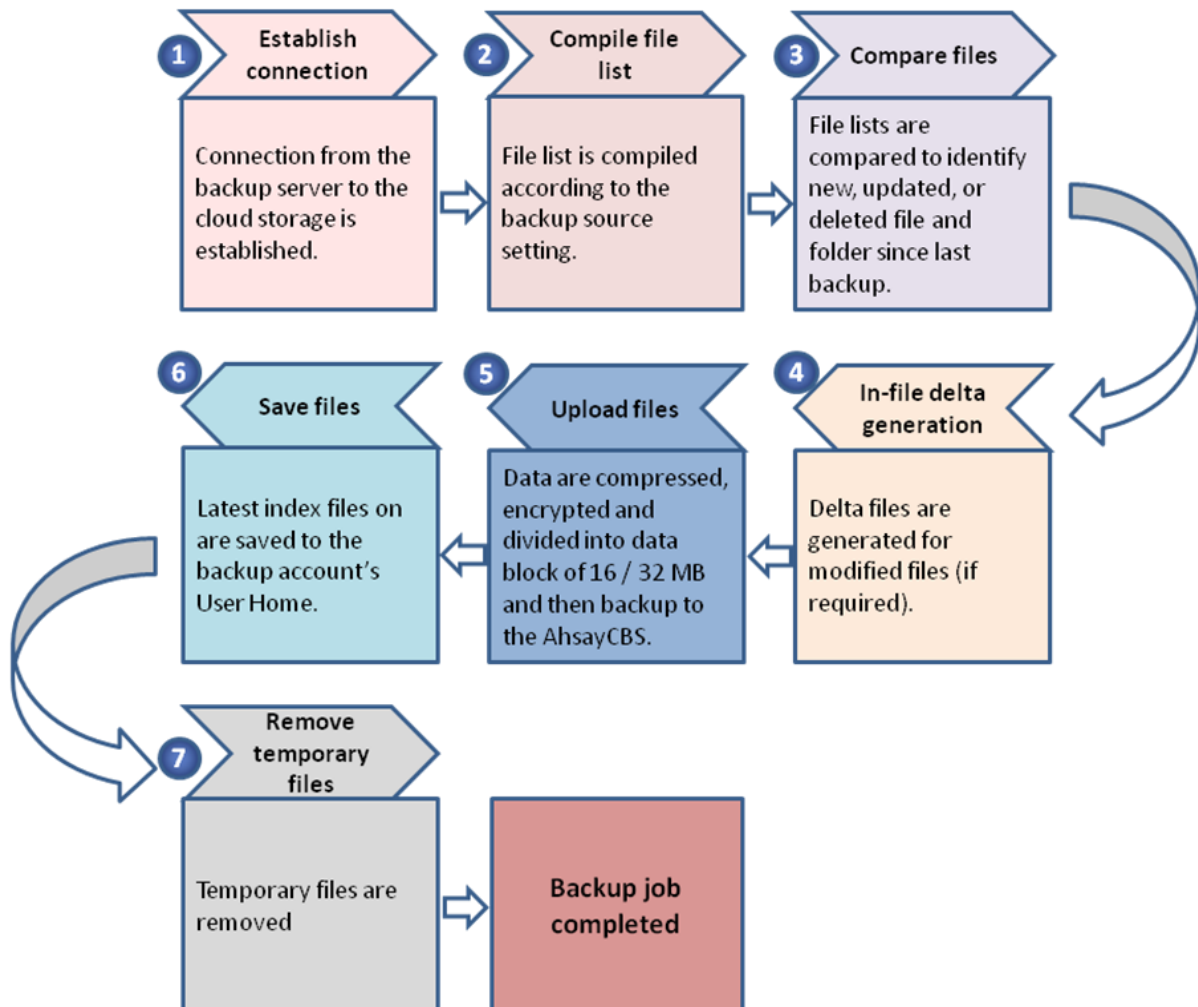
Click the green  icon at the bottom right corner to confirm the backup schedule once you finish setting.

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

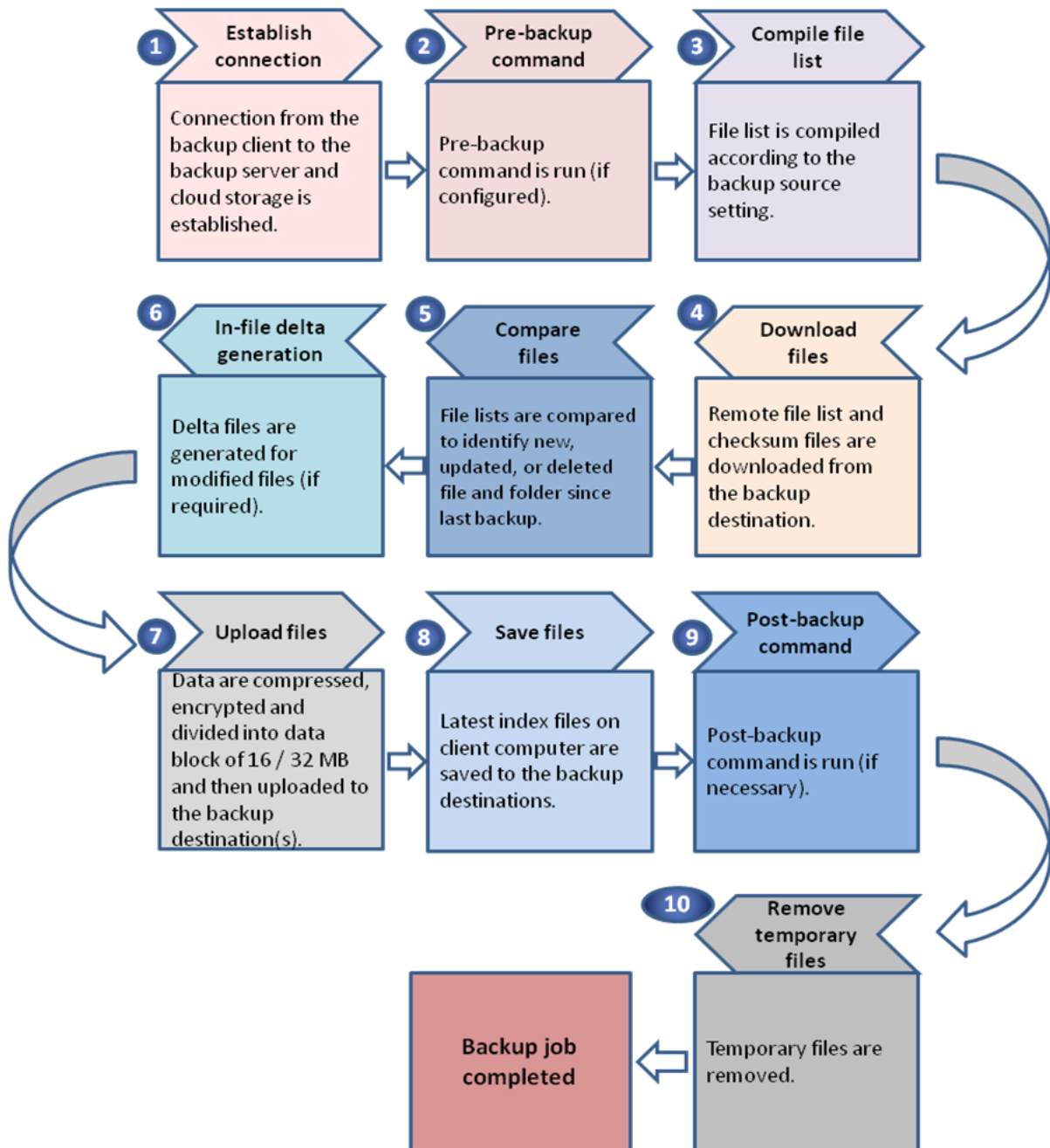
5 Overview of Cloud File Backup

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

Run on Server Cloud File Backup



Run on Client Cloud File Backup



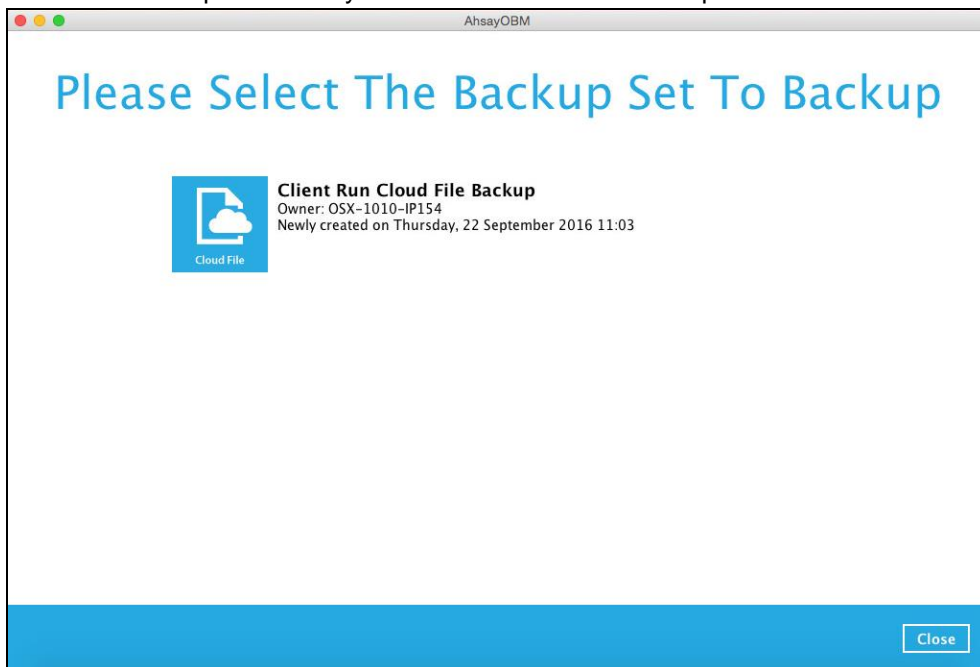
6 Running a Backup

6.1 Start a Manual Backup in AhsayOBM

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



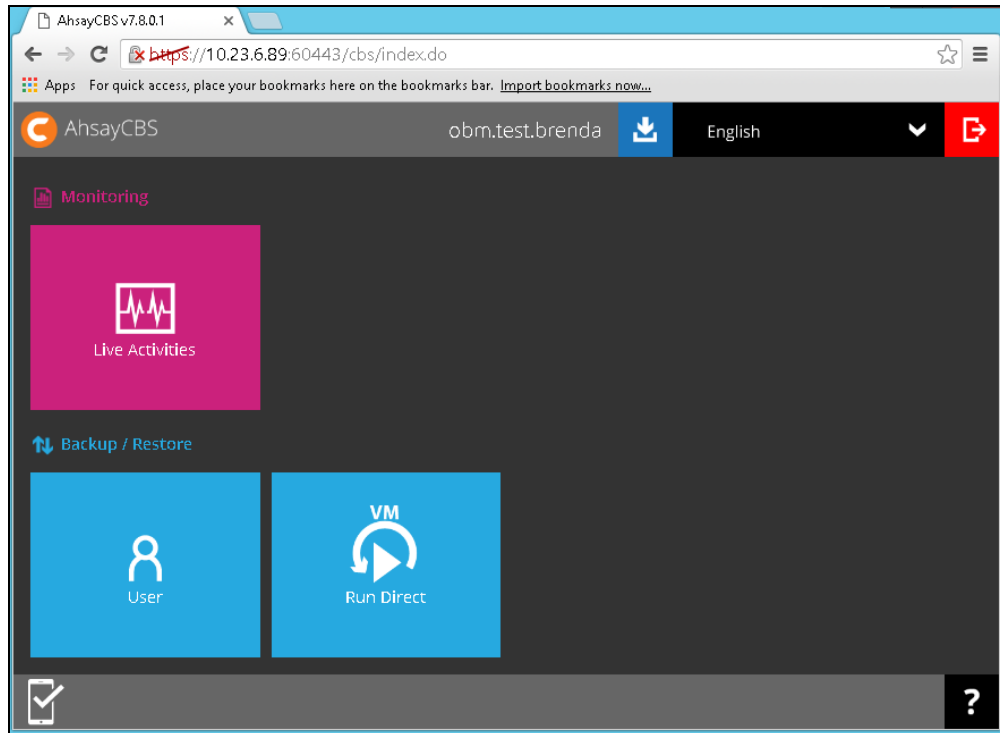
2. Select the backup set which you would like to start a backup for.



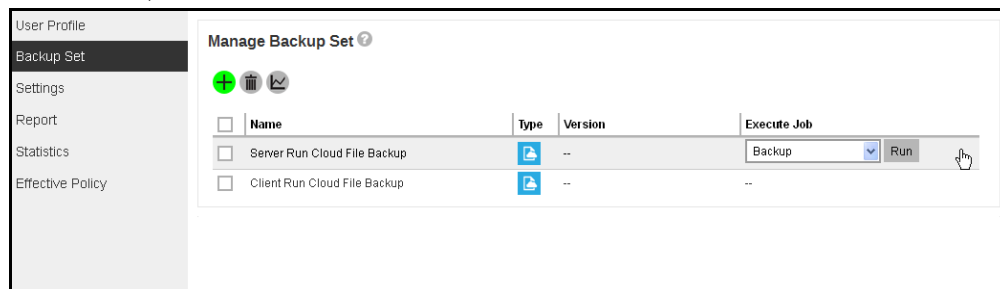
3. If you would like to modify the In-File Delta type, Destinations and Retention Policy Settings, click **Show advanced option**.
4. Click **Backup** to start the backup.

6.2 Start a Manual Backup on the Web Console

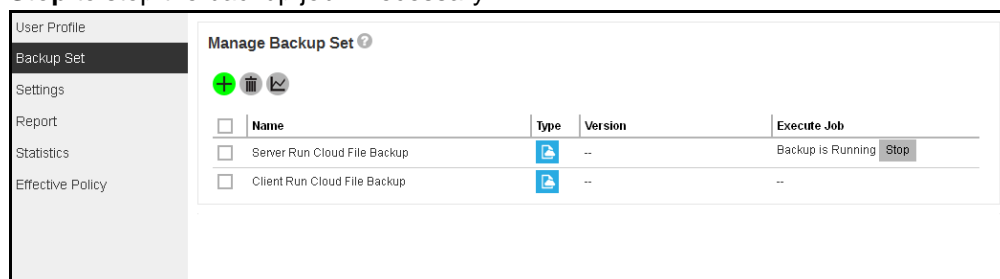
1. Log in to the User Web Console according to the instructions in [Login to the AhsayCBS User Web Console](#).
2. Click on the **User** icon.



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

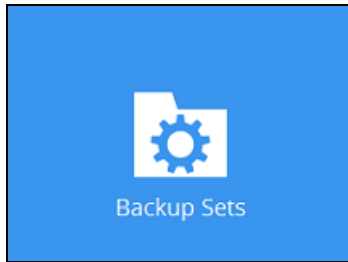


4. Modify the **In-File Delta** type and **Retention Policy** setting if necessary.
5. Click **Run Backup** to start the backup job.
6. When a backup job is running, the status **Backup is Running** will be displayed. Click **Stop** to stop the backup job if necessary.

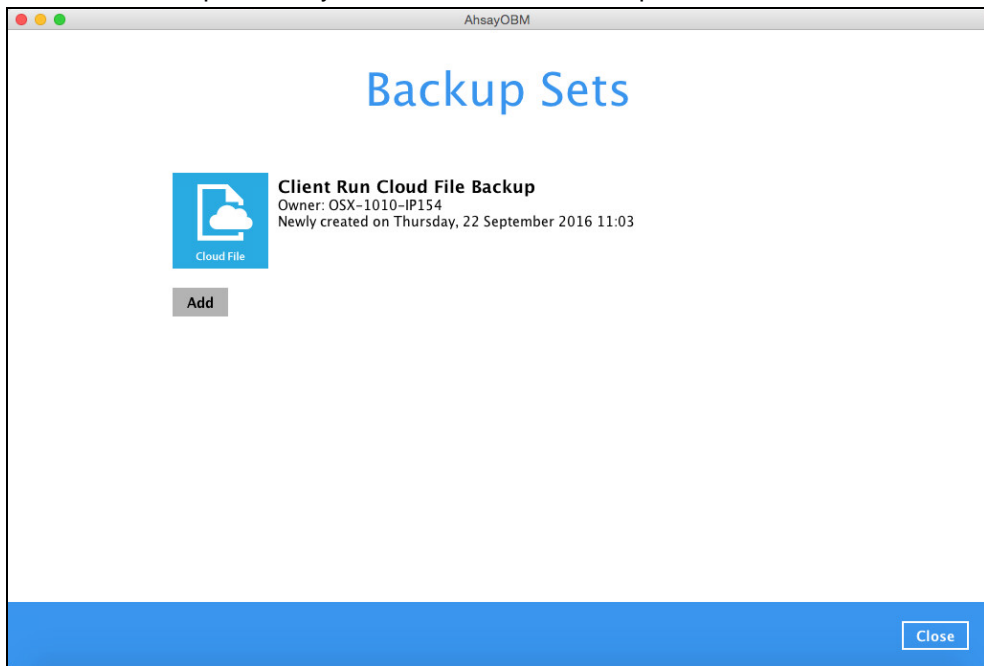


6.3 Configure Backup Schedule for Automated Backup in AhsayOBM

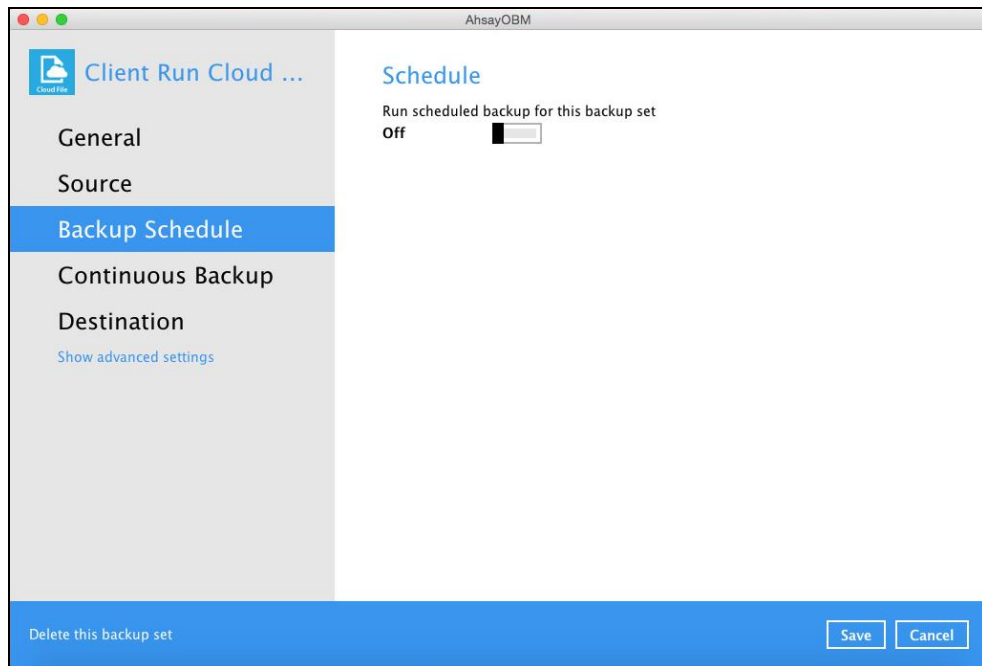
1. Click the **Backup Sets** icon on the AhsayOBM main interface.



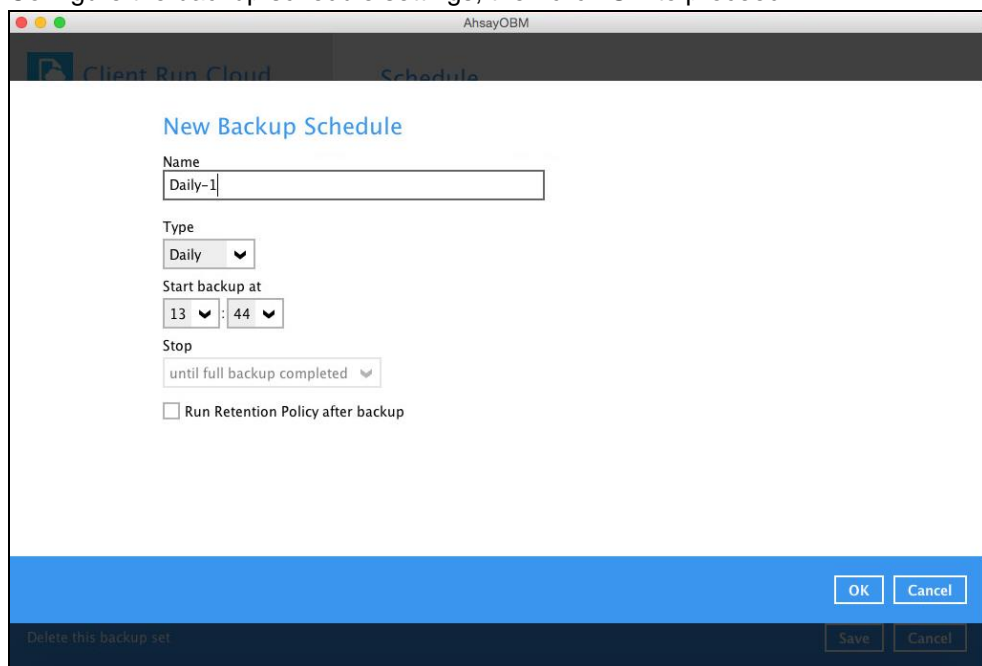
2. Select the backup set that you want to create a backup schedule for.



3. Click **Backup Schedule**, switch on the **Run scheduled backup for this backup set** button and click **Add new schedule**.



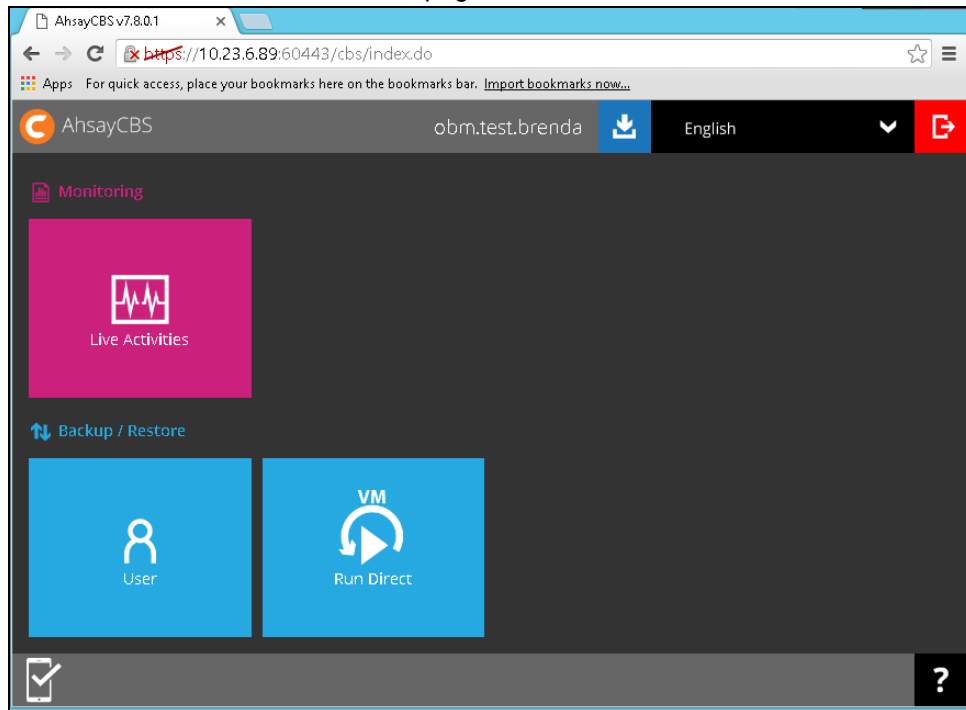
4. Configure the backup schedule settings, then click **OK** to proceed.



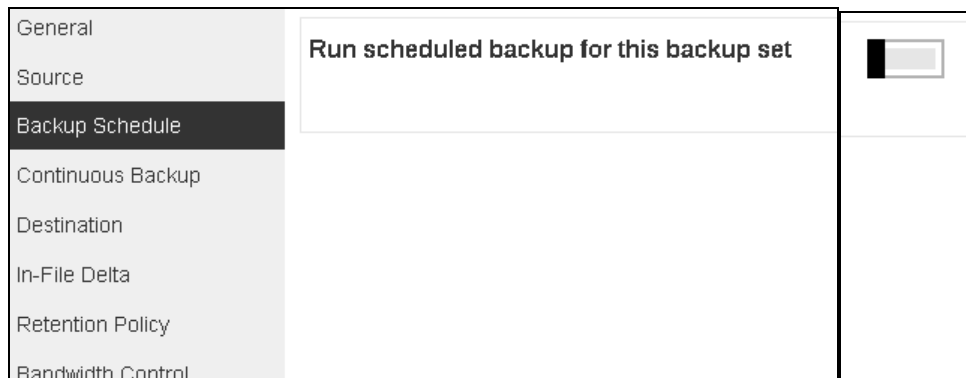
5. Click **Save** to confirm your settings.

6.4 Configure Backup Schedule for Automated Backup on the User Web Console

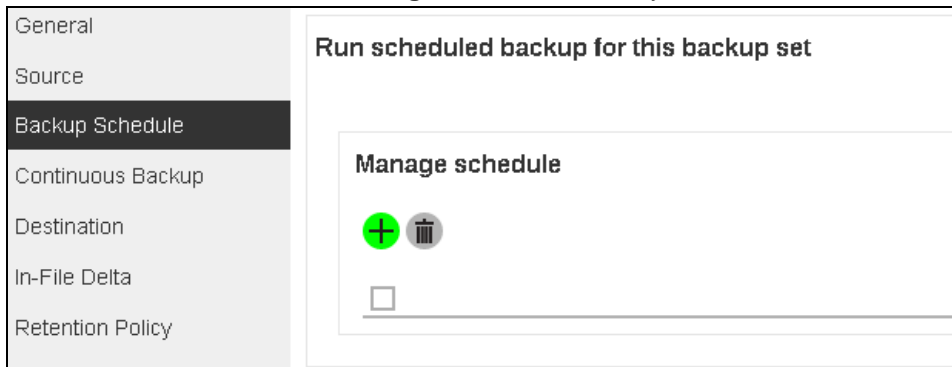
1. Click on the **User** icon on the main page of the User Web Console.



2. Select **Backup Set** from the left panel, then click on the corresponding backup set.
3. Go to the Backup **Schedule** menu, slide the on/off switch at the right to turn this feature on.

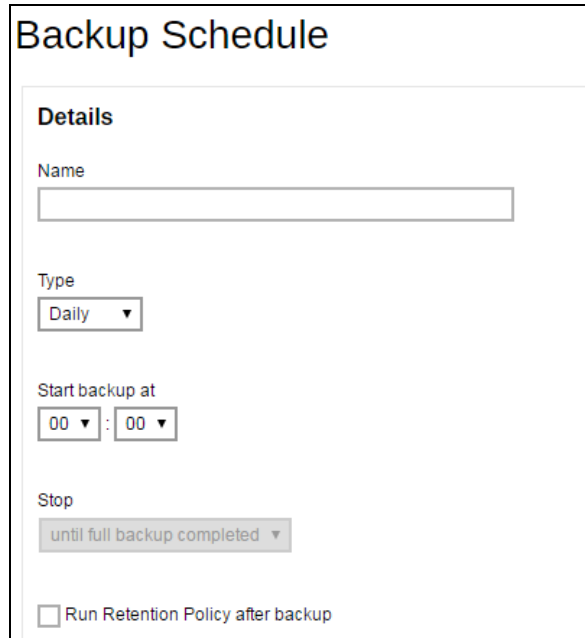


4. Click the  icon under the **Manage schedule** to add your desired schedule.



5. You may configure the following items for the schedule.

- Name of the scheduled backup
- Backup schedule type
- Backup start time
- Run Retention Policy after backup



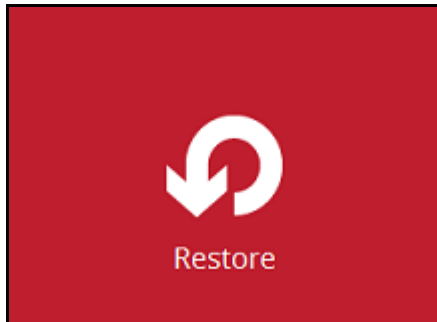
6. Click the  icon and then the  icon to confirm the setting.

7 Restoring with a Cloud File Backup Set

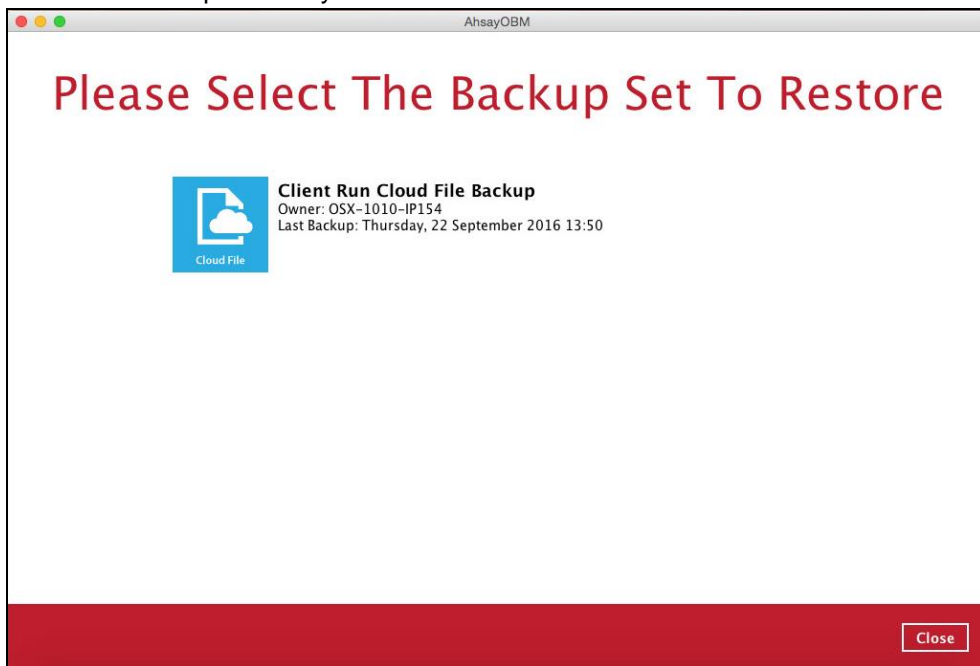
7.1 Restore with AhsayOBM

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.



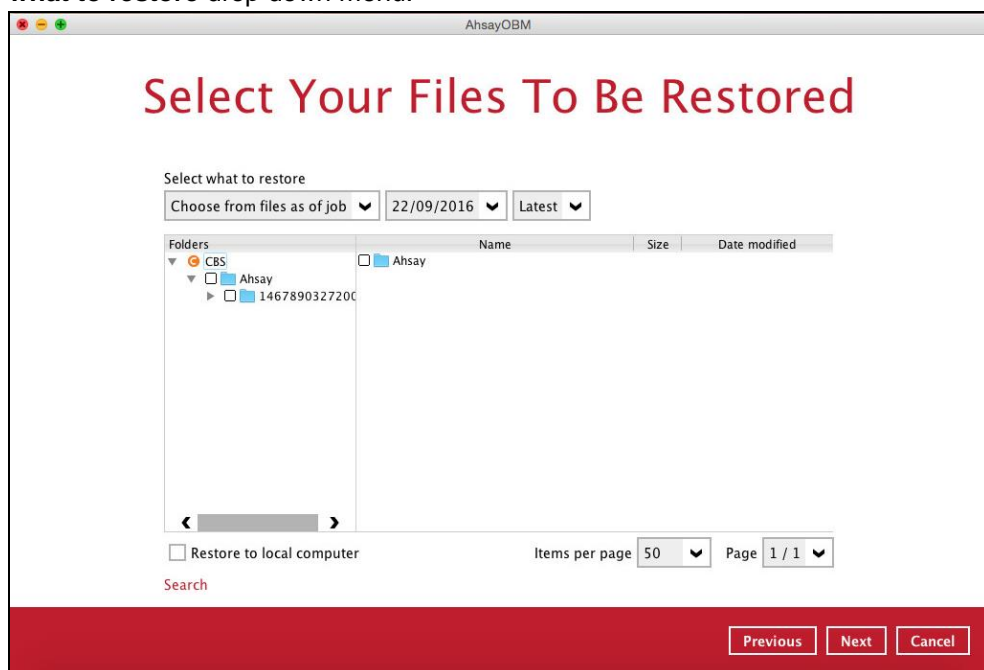
2. Select the backup set that you would like to restore from.



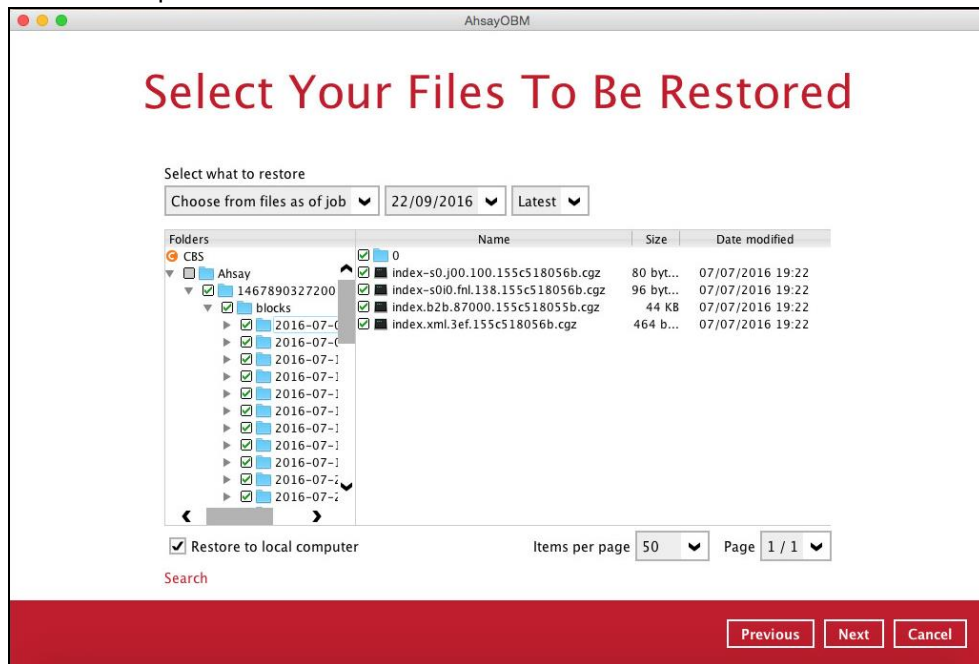
3. Select the backup destination that contains the data that you would like to restore.



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

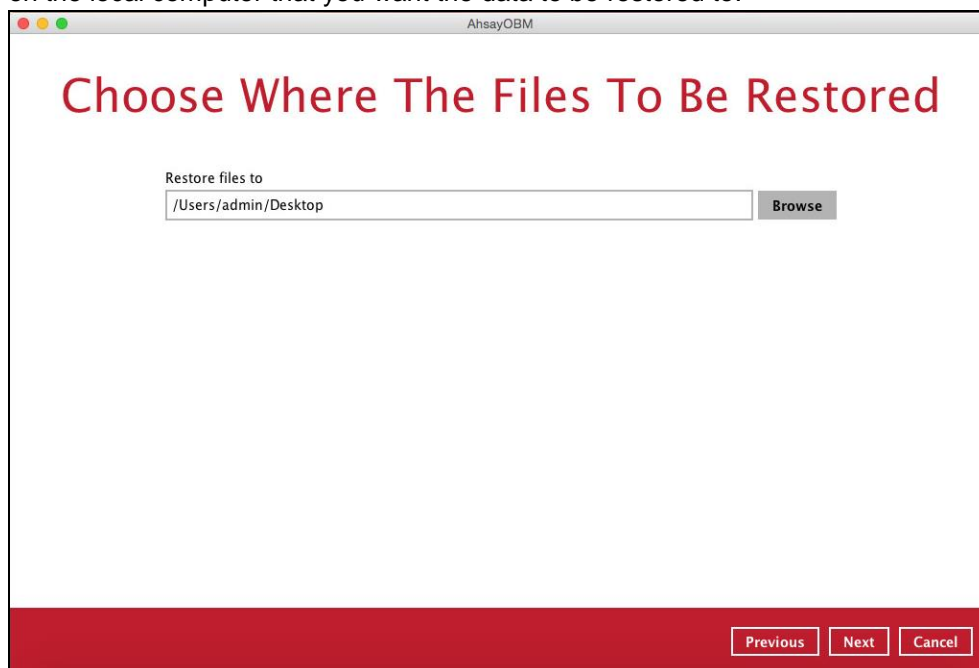


5. Select **Restore to local computer** if you want to restore the backed up data to the location computer.



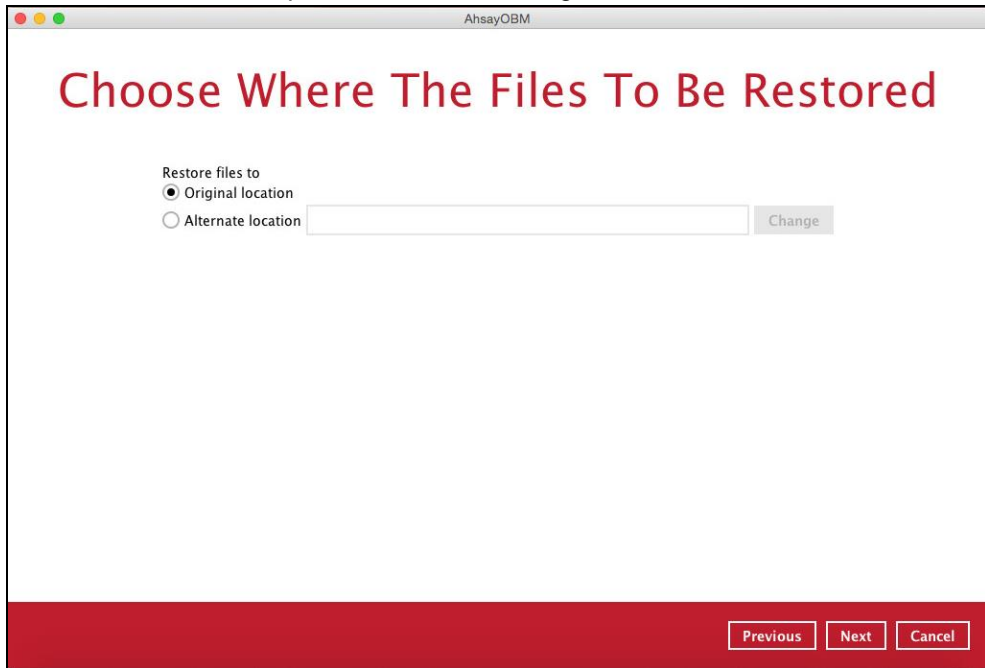
Click **Next** to continue.

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



-OR-

If **Restore to local computer** is disabled, select **Original location** to restore the data to the original directory path on the cloud storage, or **Alternate location** to restore the data to an alternate path on the cloud storage.

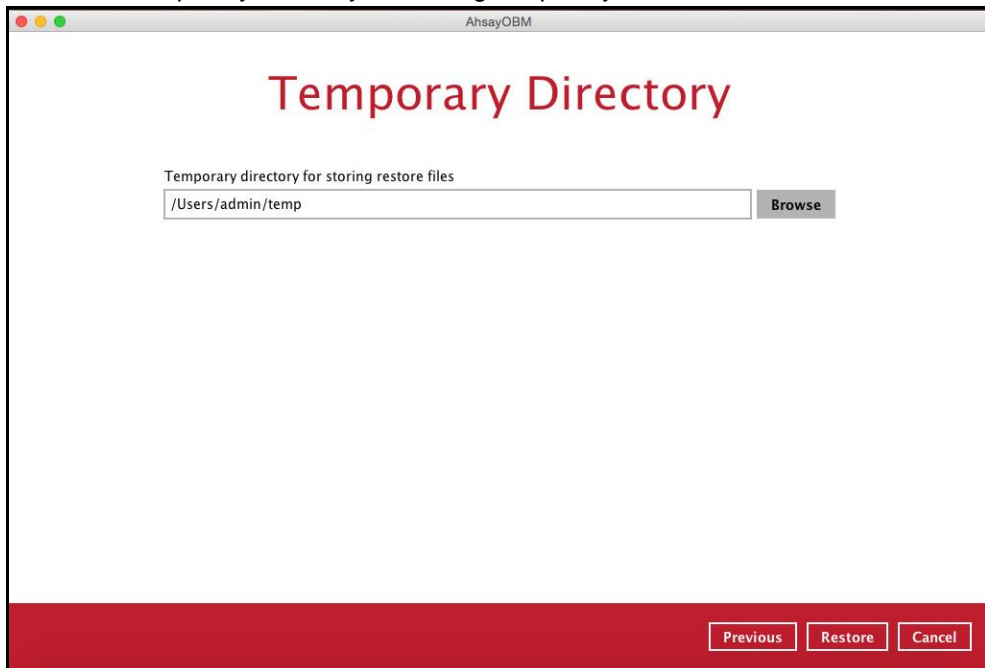


The screenshot shows a window titled "AhsayOBM" with the heading "Choose Where The Files To Be Restored". Below the heading, there is a section "Restore files to" with two radio button options: "Original location" (which is selected) and "Alternate location". To the right of the "Alternate location" option is a text input field and a "Change" button. At the bottom of the window, there is a red bar containing three buttons: "Previous", "Next", and "Cancel".

Click **Change** to browse to the alternate path on the cloud storage.

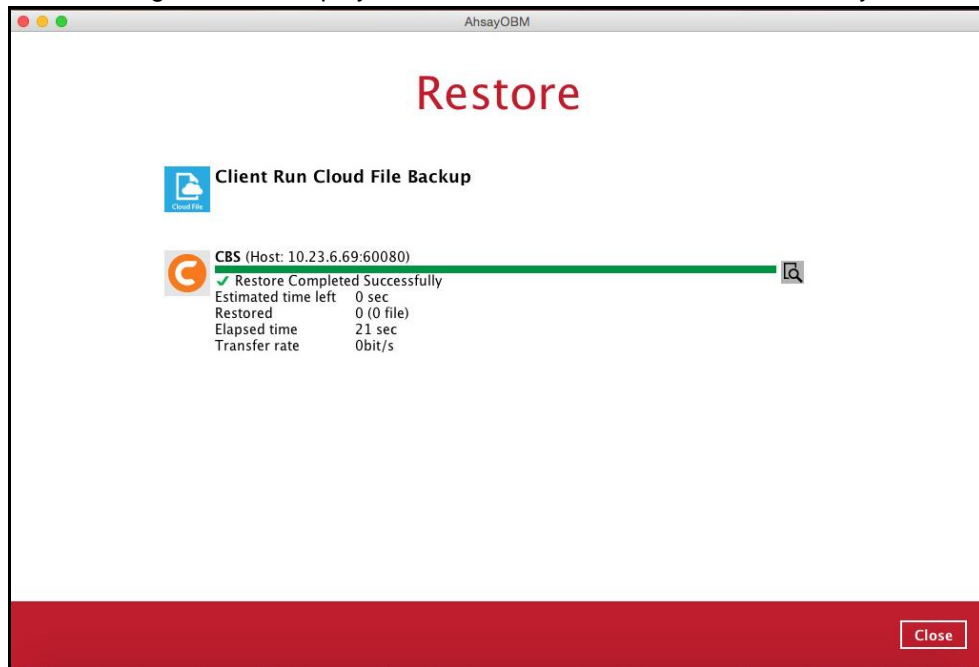
Important: Data can only be restored to a local computer, or to the original cloud storage that the data was backed up from (e.g. same cloud storage provider and same account). You cannot restore the data to a different cloud storage (e.g. a different cloud storage provider or different account)

7. Select the temporary directory for storing temporary files.

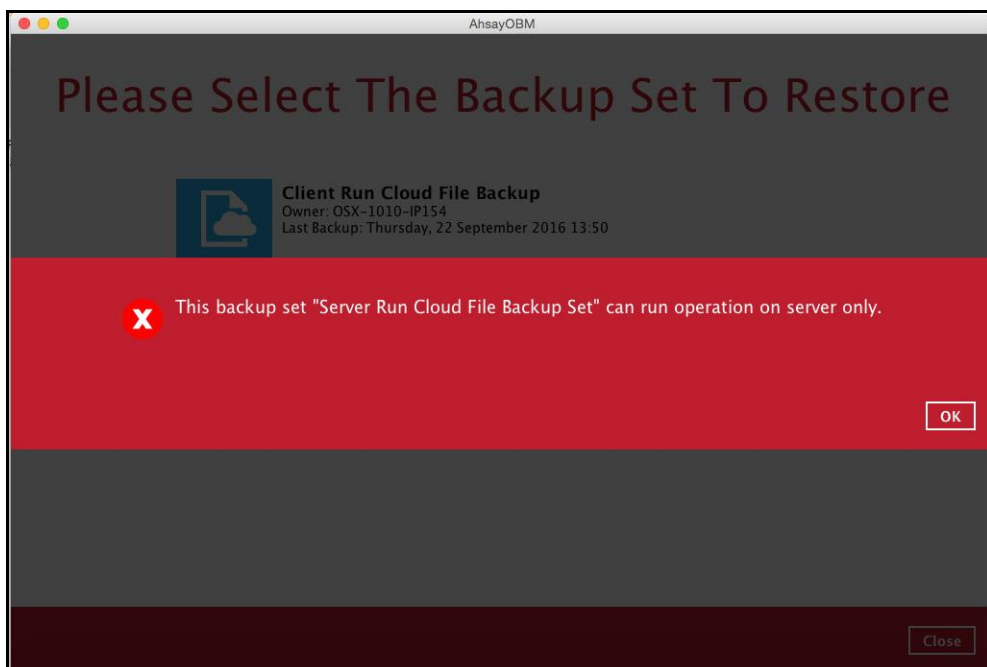


The screenshot shows a window titled "AhsayOBM" with the heading "Temporary Directory". Below the heading, there is a section "Temporary directory for storing restore files" with a text input field containing the path "/Users/admin/temp" and a "Browse" button. At the bottom of the window, there is a red bar containing three buttons: "Previous", "Restore", and "Cancel".

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.



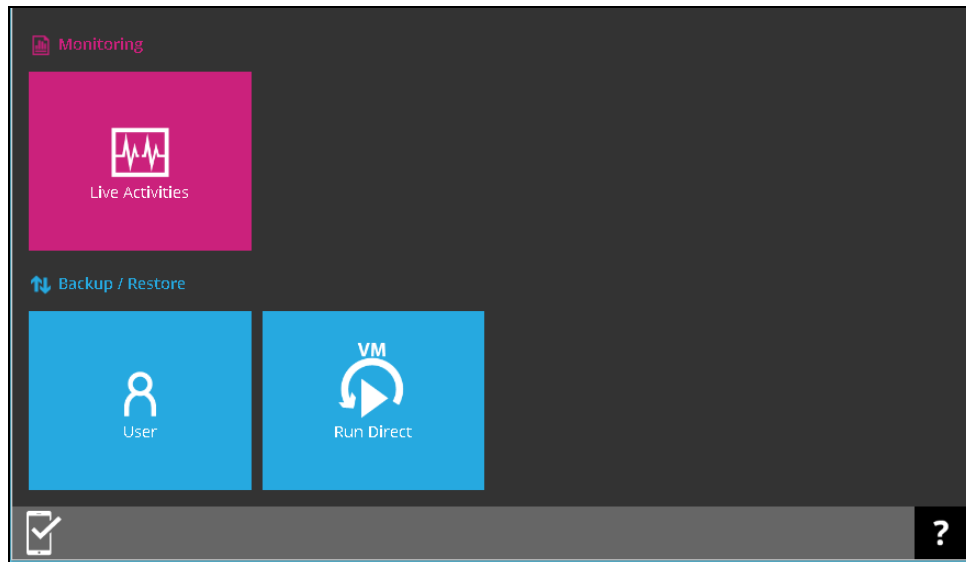
Refer to the chapter on [Restore with the AhsayCBS Web Console](#) for instruction on how to restore data for a **Run on Server** Cloud File backup set.

7.2 Restore with the AhsayCBS User Web Console

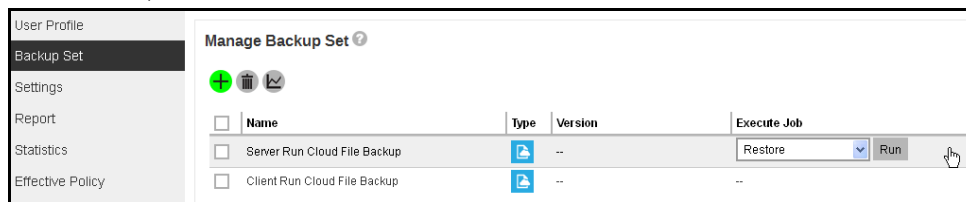
Login to the web console according to the instruction provided in the chapter on [Login to the AhsayCBS Web Console](#).

*Note: Data of a **Run on Server** Cloud File backup set can only be restored via the AhsayCBS web console.*

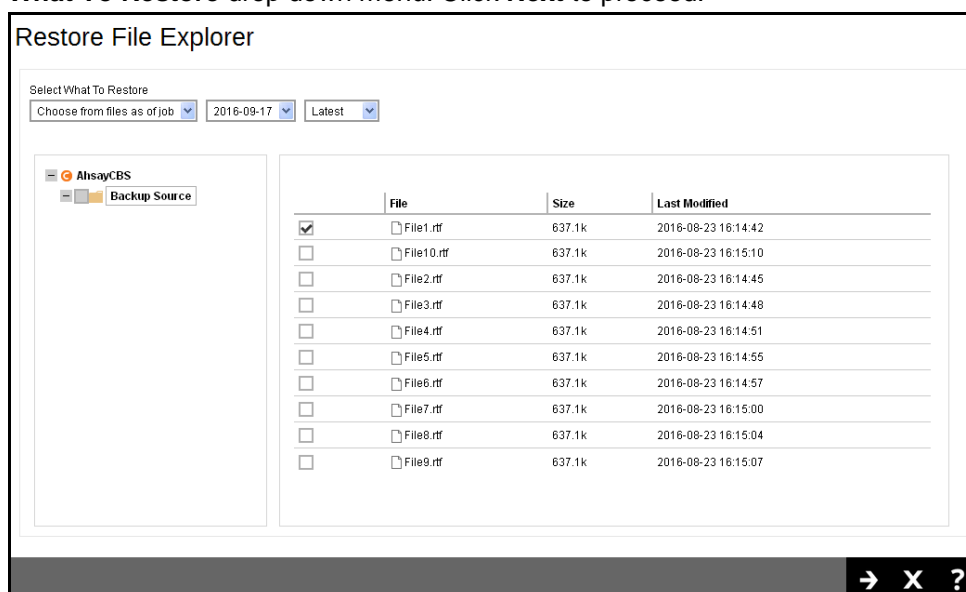
1. Click on the **User** icon.



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



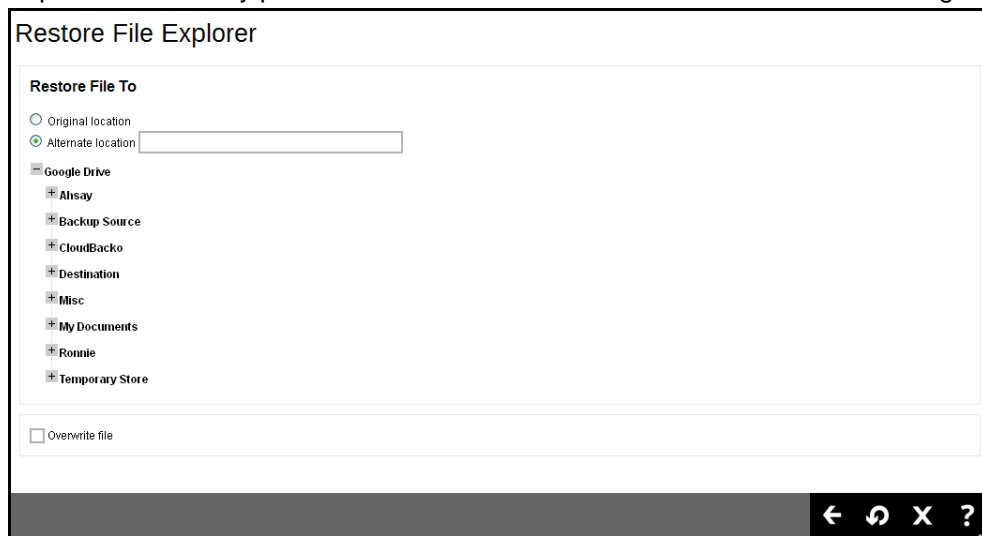
3. Select to restore from a specific backup job, or the latest job available from the **Select What To Restore** drop down menu. Click **Next** to proceed.




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



Expand the directory path to browse to the alternate location on the cloud storage.



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).

5. Click the  icon to start the restoration.
6. You will see the status showing **Restore is Running** when the restore is in progress.

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:

<https://forum.ahsay.com>

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 Created on User Web Console

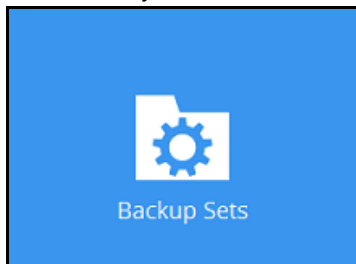
You need to read the instructions below only if you:

- 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

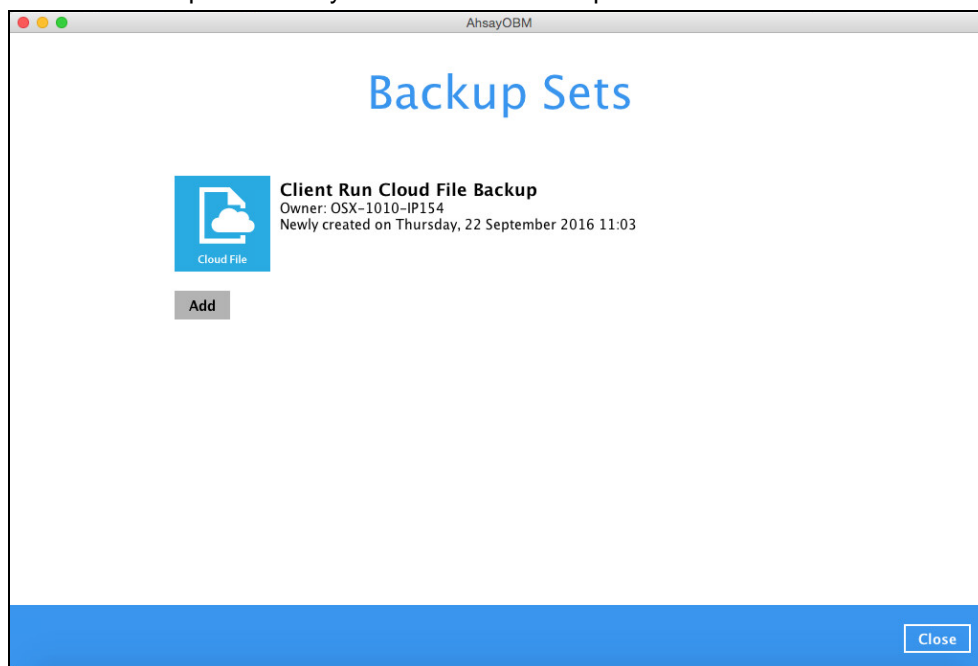
-OR-

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

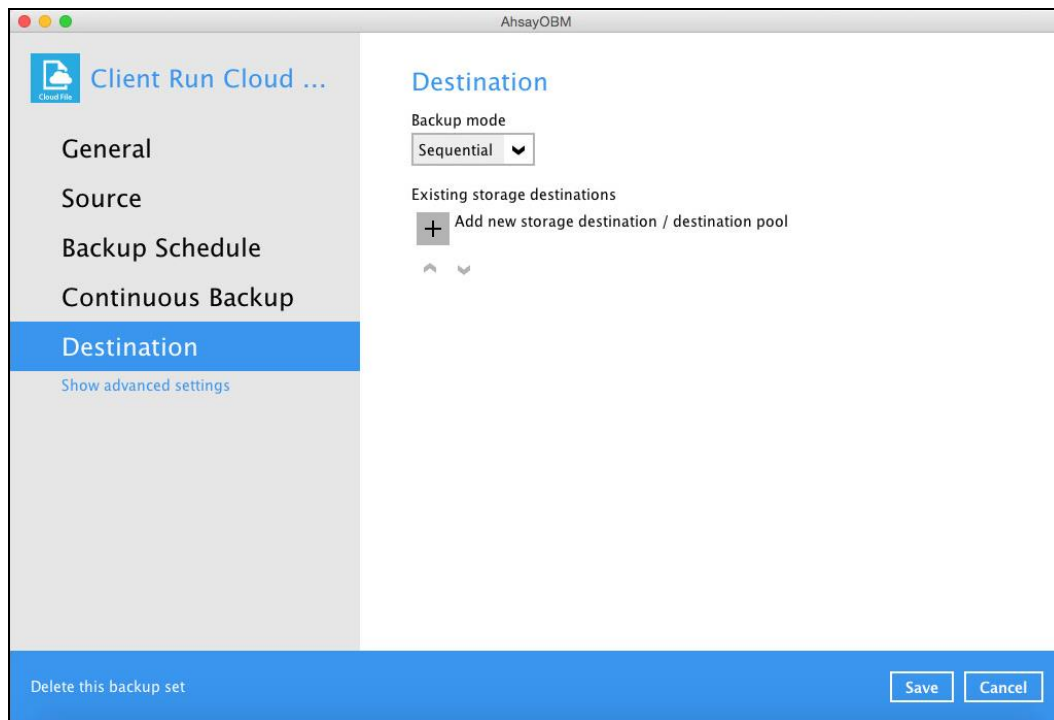
1. Log in to AhsayOBM according to the instructions in [Login to AhsayOBM](#).
2. In the AhsayOBM main interface, click **Backup Sets**.



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

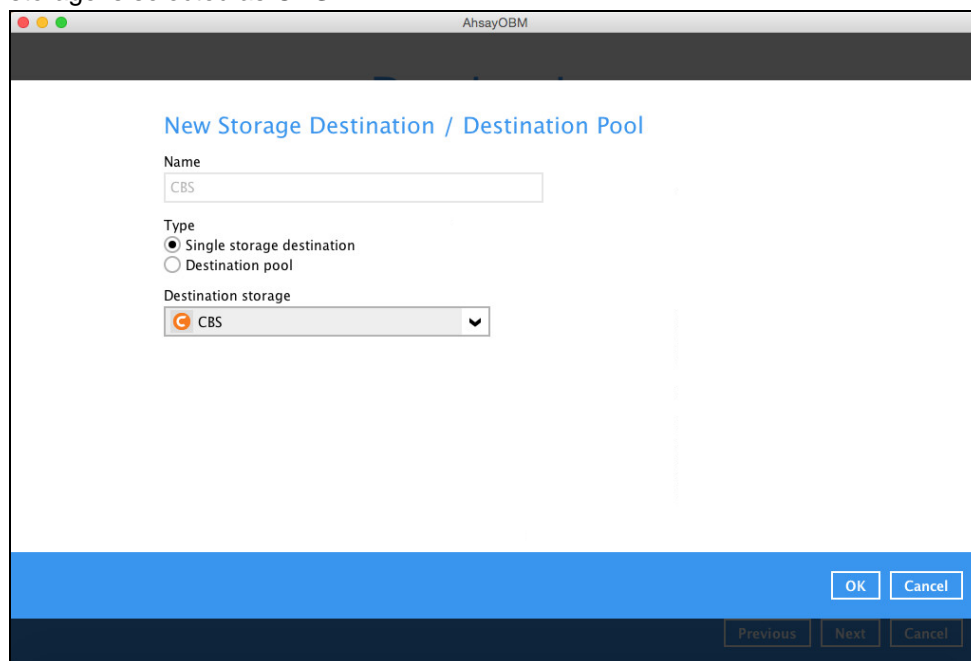


- Click the **Destination** menu on the left side, then click the **Add** button on the right to add backup destination.



- Select the storage type.

- **Single storage destination** – the entire backup will be uploaded to one single destination you selected under the **Destination storage** drop-down list. By default, the destination storage is selected as **CBS**.



- **Destination pool** – the backup will be spread over on the destinations you have selected. Enter a **Name** for the destination pool and then click **Add new storage destination to the pool** to select the desired storage destinations.

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

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

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

AhsayOBM

New Storage Destination For The Pool

Name
GoogleDrive-1

Destination storage
Google Drive

Test

[Sign up for Google Drive](#)

OK Cancel

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

AhsayOBM

New Storage Destination For The Pool

Name
FTP-1

Destination storage
FTP

Host Port

Username



Password

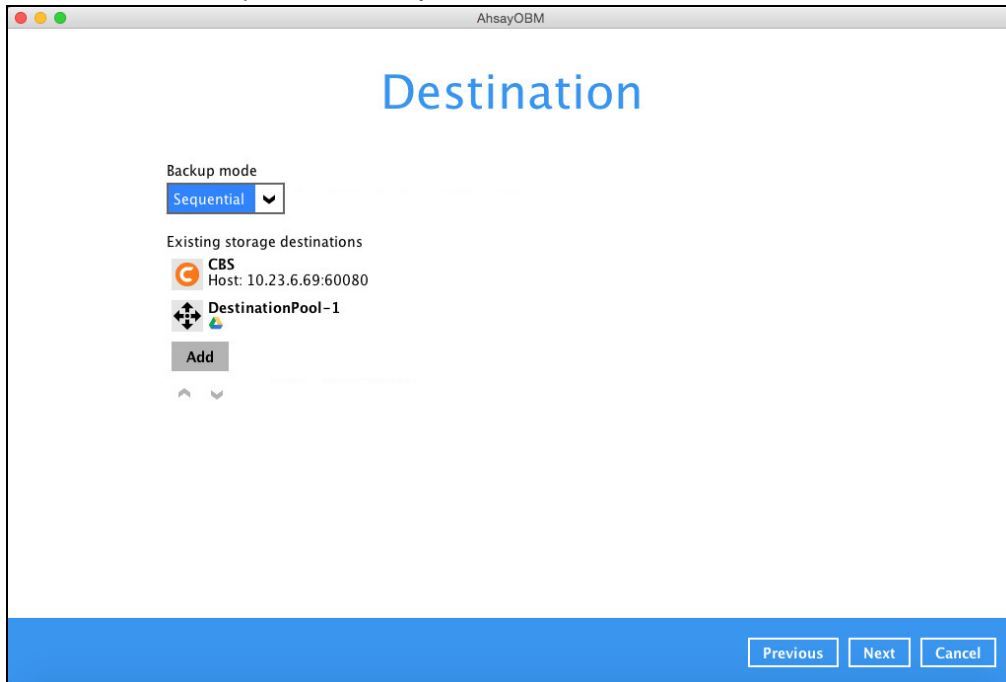
(optional) FTP directory to store backup data (default to ~/AhsayCSV)

☐ Connect with SSL/TLS (explicit only)

☐ Access the Internet through proxy

OK Cancel

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 **Next** to proceed when you are done with the selection.





AhsayOBM

Destination

Backup mode
Sequential

Existing storage destinations

-  CBS
Host: 10.23.6.69:60080
-  DestinationPool-1

Add

Previous Next Cancel