

Ahsay Online Backup Manager v8 Cloud File Backup & Restore Guide for MacOS

Ahsay Systems Corporation Limited

11 October 2021

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

Copyright Notice

© 2021 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 (https://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 and Ahsay NAS Client Utility, Ahsay Mobile are trademarks of Ahsay Systems Corporation Limited.

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

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

Dropbox is a registered trademark of Dropbox Inc.

Google Cloud Storage, Google Drive, Google Authenticator, and Android are registered trademarks of Google Inc.

Wasabi Hot Cloud Storage is a registered trademark of Wasabi Technologies Inc.

Backblaze B2 Cloud Storage is a registered trademark of Backblaze Inc.

MariaDB is a registered trademark of MariaDB Corporation AB.

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

Microsoft Windows, Microsoft Exchange Server, Microsoft SQL Server, Microsoft Hyper-V, Microsoft Azure, OneDrive, OneDrive for Business, Microsoft Authenticator, and Microsoft Office 365 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 11g, Oracle 12c, Oracle 18c, Oracle 19c, 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 in the U.S. and other countries.

Ubuntu is a registered trademark of Canonical Ltd.

ShadowProtect is a registered trademark of StorageCraft Technology Corporation.

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

Table of Contents

1	Over	view	1
	1.1	What is this software?	1
	1.2	System Architecture	1
	1.3	Why should I use AhsayOBM (Agent-based) Solution to back up my cloud data	a?2
	1.4	About This Document	5
2	Prep	aring for Backup and Restore	7
	2.1	Hardware Requirement	7
	2.2	Software Requirement	7
	2.3	Internet / Network Connection	7
	2.4	AhsayOBM Installation	7
	2.5	Valid AhsayOBM User Account	7
	2.6	Ahsay License Requirements	7
	2.7	Add-on Module Requirements	7
	2.8	Backup Quota Requirement	8
	2.9	Cloud Sources	8
	2.10	Login Credentials to Cloud Storage	8
	2.11	Network Bandwidth	9
	2.12	Best Practices and Recommendations	9
	2.13	Limitations	10
3	Logg	jing in to AhsayOBM	13
	3.1	Login to AhsayOBM without 2FA	13
	3.2	Login to AhsayOBM with 2FA using authenticator app	14
	3.3	Login to AhsayOBM with 2FA using Twilio	17
4	Crea	ting a Cloud File Backup Set	19
5	Over	view of Run on Client Cloud File Backup Process	35
	5.1	Periodic Data Integrity Check (PDIC) Process	36
	5.2	Backup Set Index Handling Process	38
		5.2.1 Start Backup Job	38
		5.2.2 Completed Backup Job	39
	5.3	Data Validation Check Process	40
6	Runr	ning a Backup	41
7	Rest	oring with a Cloud File Backup Set	47
8		acting Ahsay	
	8.1	Technical Assistance	
	8.2	Documentation	

1 Overview

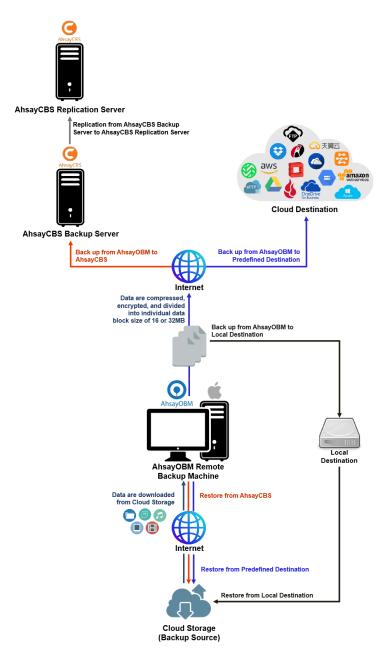
1.1 What is this software?

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

1.2 System Architecture

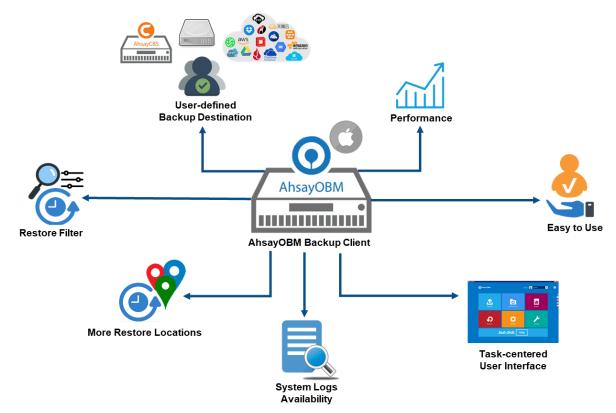
For agent-based backup and restore, the AhsayOBM initiates connection to the cloud storage (backup source) through the internet via the deployed backup agent on the customer's site.

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



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

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



User-defined Backup Destination

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

Performance

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

Easy to Use

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

Task-centered User Interface

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

System Logs Availability

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

More Restore Locations

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

Restore Filter

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

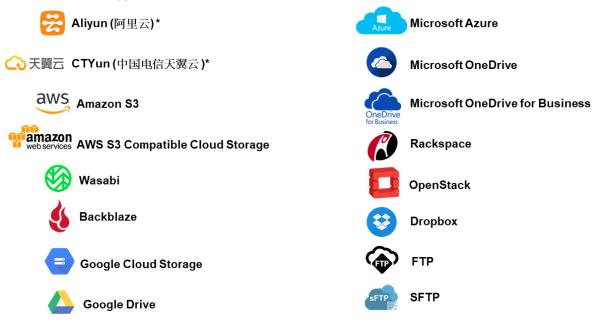
High Level of Security

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

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

Cloud Destinations Backup

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





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	✓	\checkmark
Backup Source	✓	\checkmark
Backup Schedule	✓	\checkmark
Continuous Backup	AhsayOBM / AhsayACB for Windows only	\checkmark
Destination	AhsayCBS, Predefined Destinations, Standard and Local	AhsayCBS or Predefined Destinations only
Multiple Destinations	\checkmark	×
In-File Delta	✓	\checkmark
Retention Policy	✓	\checkmark
Command Line Tool	AhsayOBM for Windows only	×
Reminder	AhsayOBM / AhsayACB for Windows only	×
Restore Filter	\checkmark	×
Bandwidth Control	✓	\checkmark
IP Allowed for Restore	✓	×
System Logs of Data Integrity Check and Space Freeing Up	✓	×
Others	✓	\checkmark
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	\checkmark	\checkmark
Space Freeing Up	\checkmark	\checkmark
Delete Backup Data	\checkmark	\checkmark
Decrypt Backup Data	\checkmark	×

NOTE

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

1.4 About This Document

What is the purpose of this document?

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

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

Part 1: Preparing for Cloud File Backup & Restore

Requirements Requirements on hardware & software installation

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

Part 2: Performing a Cloud File Backup

Logging in to AhsayOBM client Log in to AhsayOBM

Creating a Backup Set Create a backup set using AhsayOBM

Running a Backup Set Run a backup set using AhsayOBM

Part 3: Restoring a Cloud File Backup

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

What should I expect from this document?

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

Who should read this document?

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

2 Preparing for Backup and Restore

2.1 Hardware Requirement

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

2.2 Software Requirement

Refer to the following article for the list of compatible operating systems and application version.

FAQ: Ahsay Software Compatibility List (SCL) for version 8.1 or above

2.3 Internet / Network Connection

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

2.4 AhsayOBM Installation

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

2.5 Valid AhsayOBM User Account

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

2.6 Ahsay License Requirements

Licenses

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

For more details, please contact your backup service provider.

2.7 Add-on Module Requirements

In-File Delta

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

NOTE

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

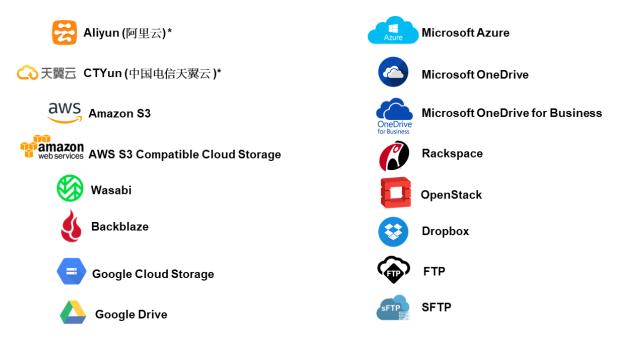
User Profile	General Backup Client Settings Contact User Group	Authentication
Backup Set	Settings of the client backup agent for this user.	
Settings		
Report	Backup Client	
Statistics	AhsayOBM User AhsayACB User	
Effective Policy		
	Add-on Modules	
	Microsoft Exchange Server	Microsoft SQL Server
	MySQL Database Server	Oracle Database Server
	Lotus. Lotus Domino	Lotus Notes
	Windows System Backup	Windows System State Backup
	WMware Guest VM V	Hyper-V Guest VM ~ 0
	Microsoft Exchange Mailbox	ShadowProtect System Backup
	NAS - QNAP	NAS - Synology
	Mobile (max. 10)	Continuous Data Protection
	Volume Shadow Copy	In-File Delta
	OpenDirect / Granular Restore 0	Office 365 Backup
	MariaDB Database Server	

2.8 Backup Quota Requirement

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

2.9 Cloud Sources

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



2.10 Login Credentials to Cloud Storage

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

2.11 Network Bandwidth

10 Mbps or above connection speed.

2.12 Best Practices and Recommendations

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

Backup Destination

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

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

Temporary Directory Folder Location

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

Performance Recommendations

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

Bucket Management for Enterprise Cloud Storage Providers

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

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

D Test Restore Operations

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

Periodic Backup Schedule

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

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

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

2.13 Limitations

For backup source selection:

 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.

	AhsayOBM			
	Backup Sour	rce		
Folders	Name	Size	Date modified	
Coogle Drive Ansay Backup Work Files	 Ahsay Backup Test Files Work Files VSAN-hosts.png vSAN-hosts.png www.workstation_01.png was_admin.png 	281KB 281KB 281KB	03/05/2021 11:34 03/05/2021 11:34 03/05/2021 11:34	
Show files	ltems per p	bage 50	✔ Page 1 / 1 ✔	
			Previous	ext Cancel

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.

• •	AhsayOBM		
Cloud File	Backup Source		
General	Folders Google Drive Ahsay Backup	Name Ahsay Backup Latest version	Size Date modified
Source	 Latest version New updates 	New updates	
Backup Schedule	 ▶ ♥ ■ Test Files ▶ ♥ ■ Work Files 	V Work Files V vSAN-hosts.png V vsAN-hosts.png	281KB 03/05/2021 11:34 281KB 03/05/2021 11:34
Destination		🗹 🗟 was_admin.png	281KB 03/05/2021 11:34
Show advanced settings			
	Show files	Items per page 50	♥ Page 1/1 ♥
Delete this backup set			Save Cancel

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.

	AhsayOBM		
Cloud File Backup	Backup Source		
General	Folders Coogle Drive Ahsay Backup	Name Ahsay Backup Files	Size Date modified
Source	 Test Files Work Files 	✓ Work Files ✓ a vSAN-hosts.png	
Backup Schedule		vm_workstation_01.png	
Destination			
Show advanced settings			
	✓ Show files	Items per page 50	✔ Page 1/1 ✔
Delete this backup set			Save Cancel

Backup log

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

3 Logging in to AhsayOBM

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

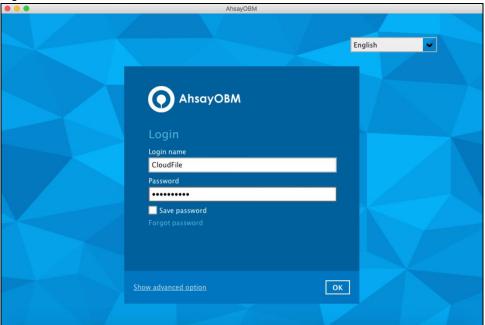
- Login without 2FA
- Login with 2FA using authenticator app
- Login with 2FA using Twilio

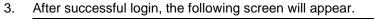
3.1 Login to AhsayOBM without 2FA

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



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





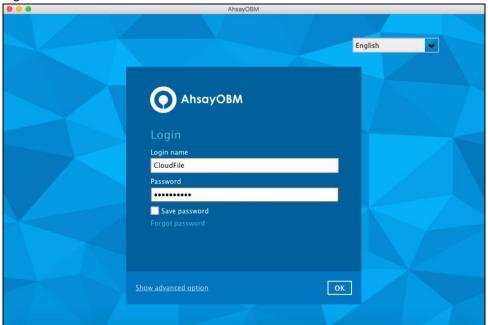


3.2 Login to AhsayOBM with 2FA using authenticator app

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



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



- 3. One of the two authentication methods will be displayed to continue with the login:
 - Push Notification and TOTP when using Ahsay Mobile app
 - TOTP only
 - If Ahsay Mobile app was configured to use Push Notification and TOTP then there are two 2FA modes that can be used:
 - Push Notification (default)

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



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

🚯 Ahsay Mobile	
O AhsayOBM CloudFile	٠
_	
Authorization Request	
Proceed authorization request for CloudFile	
REJECT ACCEPT	

TOTP

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

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

Two-Factor Authentication

Please approve notification request in one of registered Authenticator App.



9	7	1	2	9	3	(00:00:22)
---	---	---	---	---	---	------------

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

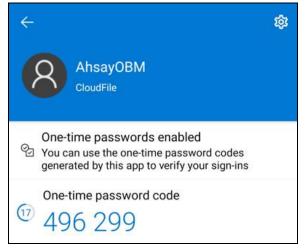


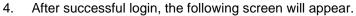
TOTP only

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

Two-F	actor	Authe	enticat	ion		
Enter one	-					
4	9	6	2	9	9	(00:00:13)

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





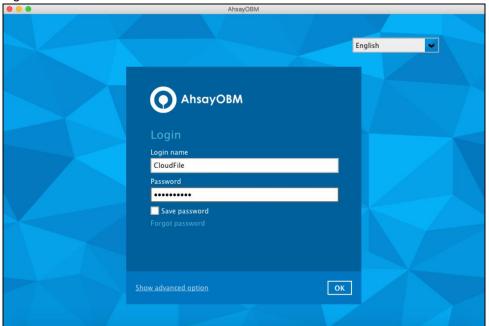


3.3 Login to AhsayOBM with 2FA using Twilio

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



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



3. Select your phone number to receive the passcode.

Philippines (-	+63) - ******6123		

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

Please enter the passcode to conti XIUA - 158074	(00:04:30)
Resend passcode	

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

AhsayOBM	Cloud	dFile 💄 English	• 0
Backup	Backup Sets	Report	
Restore	Settings	Utilities	k

4 Creating a Cloud File Backup Set

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



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

	AhsayOB	M		
	Backup	Sets	Sort by Creation Time	
Add ne	w backup set			
				Close

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

AhsayOBM
Create Backup Set
Name Client Run Cloud File Backup Backup set type File Backup Cloud File Backup MySQL Backup Office 365 Backup VMware Backup
Next Cancel

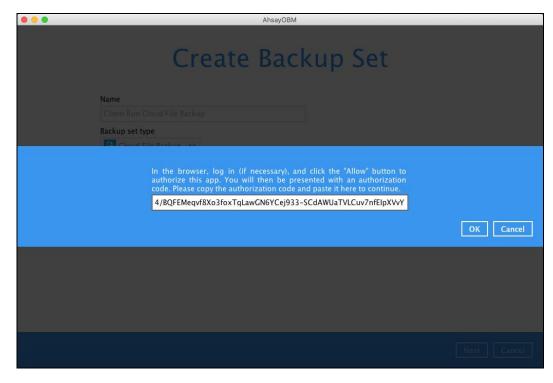
4. Select the **Cloud type** of the cloud storage that contain the data that you want to backup.

•••	AhsayOBM
	Create Backup Set
	Name
	Client Run Cloud File Backup
	Backup set type
	🕒 Cloud File Backup 🖌
	Cloud type
	Coogle Drive
	この理会
	△ 中国电信天翼云
	🚨 Amazon Cloud Drive
	🧊 Amazon S3
	🄐 AWS S3 Compatible Cloud Storage
	O Google Cloud Storage
	Coogle Drive
	Hicrosoft Azure
	Next Cancel

- 5. Depending on the cloud type you have selected, you will be prompted to enter the cloud service login details in either way below.
 - Click Test to get redirected to the login page of the cloud service provider on your default browser, then enter the login details there. Click Allow to permit AhsayOBM to access the cloud storage. Copy and paste the code generated by the cloud service provider to AhsayOBM where you will be prompted to

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

G	Sign in with Google
	Ahsay wants to access your Google Account testgdrive2019@gmail.com
	This will allow Ahsay to:
	See, edit, create, and delete all of your Google (i) Drive files
	Make sure you trust Ahsay
	You may be sharing sensitive info with this site or app. Learn about how Ahsay will handle your data by reviewing its privacy policies . You can always see or remove access in your Google Account .
	Learn about the risks
	Cancel
	Google
	Sign in
Ple	ase copy this code, switch to your application and paste it there
	BQFEMeqvf8Xo3foxTqLawGN6YCej933-



Create Backup Set
Name Client Run Cloud File Backup Backup set type Cloud File Backup v Cloud type Coogle Drive v Test completed successfully
Next Cancel
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.

AhsayOBM	
Backup Source	
Folders	
Show files	
Previous	Next Cancel

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

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

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.

	516 KB 516 KB 516 KB 516 KB 516 KB 516 KB 516 KB 516 KB 516 KB	05/03/2019 15:32 05/03/2019 15:32 05/03/2019 15:32 05/03/2019 15:32 05/03/2019 15:32 05/03/2019 15:32 05/03/2019 15:32 05/03/2019 15:32 05/03/2019 15:32 05/03/2019 15:32
☑ TestTIFF-2.ulff ☑ TestTIFF-3.ulff ☑ TestTIFF-4.ulff ☑ TestTIFF-5.ulff	516 KB 516 KB 516 KB 516 KB	05/03/2019 15:32 05/03/2019 15:32 05/03/2019 15:32 05/03/2019 15:32

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.

	AhsayOBM	
	Schedule	
	Run scheduled backup for this backup set On	
	Existing schedules Add new schedule	
•		
		Previous Next Cancel
	New Backup Schedule Name	
	Daily-2	
	Type Daily V	
	Start backup	
	at every ackup completed v	
	Run Retention Policy after backup	
		OK Cancel Help

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.

 $\ensuremath{\textbf{Daily}}$ – the time of the day or interval in minutes/hours when the backup job will run.

Backup Schedule
Name
Daily-1
Type Daily *
Start backup
Stop until full backup completed 🔻
Run Retention Policy after backup

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

Backup Schedule	
Name	
Weekly-1	
Type Weekly v	
Backup on these days of the week	at
Start backup at • 19 • : 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.
Backup Schedule
Name
Monthly-1
Type Monthly •
Backup on the following day every month
Last T Sunday T
Start backup at
Stop
until full backup completed 🔻
Run Retention Policy after backup

Custom – a specific date and the
Backup Schedule
Name
Custom-1
Type Custom *
Backup on the following day once
Start backup at
Stop
until full backup completed 🔻

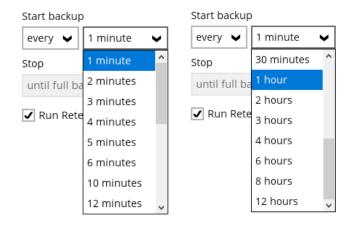
Custom – a specific date and the time when the backup job will run.

Start backup – the start time of the backup job.

🖌 Run Retention Policy after backup

at - this option will start a backup job at a specific time.

every - this option will start a backup job in intervals of minutes or hours.



Here is an example of backup set that has a daily and weekly backup schedule.

New Backup Schedule	New Backup Schedule
Name	Name
Weekly-1	Weekly-1
Type Weekly 🖌	Type Weekly 🗸
Backup on these days of the week □ Sun ✔ Mon ✔ Tue ✔ Wed ✔ Thu ✔ Fri □ Sat	Backup on these days of the week
Start backup	Start backup
every V 4 hours V	at 💙 21 💙 : 00 🗸
Stop	Stop
until full backup completed 🛛 🤟	until full backup completed 🖌
Run Retention Policy after backup	Run Retention Policy after backup

Figure 1.1

Figure 1.2

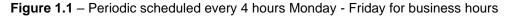


Figure 1.2 – Normal schedule run at 21:00 or 9:00 PM daily on Saturday & Sunday for weekend non-business hours

 Stop – the stop time of the backup job. This only applies to schedules with start backup "at" and is not supported for periodic backup schedule (start backup "every")

until full backup completed – this option will stop a backup job once it is complete. This is the configured stop time of the backup job by default.

after (defined no. of hrs.) – this option will stop a backup job after a certain number of hours regardless of whether the backup job has completed or not. This can range from 1 to 24 hrs.

The number of hours must be enough to complete a backup of all files in the backup set. For small files in a backup, if the number of hours is not enough to back up all files, then the outstanding files will be backed up in the next backup job. However, if the backup set contains large files, this may result in partially backed up files.

For example, if a backup has 100GB file size which will take approximately 15 hours to complete on your environment, but you set the "stop" after 10 hours, the file will be partially backed up and cannot be restored. The next backup will upload the files from scratch again.

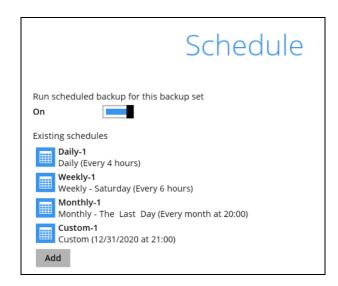
The partially backed up data will have to be removed by running the data integrity check.

As a general rule, it is recommended to review this setting regularly as the data size on the backup machine may grow over time.

 Run Retention Policy after backup – if enabled, the AhsayOBM will run a retention policy job to remove files from the backup destination(s) which have exceeded the retention policy after performing a backup job.

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

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



Click Next to proceed.

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

 AhsayOBM	
Destination	
Backup mode Sequential	
Existing storage destinations	
+ Add new storage destination / destination pool	
\sim	
Prev	ious Next Cancel

NOTE For more details on Backup Destination, refer to this article: <u>FAQ: Frequently Asked Questions on Backup Destination</u>

9. Select the Destination storage.

AhsayOBM
New Storage Destination / Destination Pool Name AhsayCB5 Destination storage C AhsayCB5 C AhsayCB5 C GoogleDrive-1 D Local / Mapped Drive / Removable Drive
ОК Салсе
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	n / Destination Pool
Name	Contract State of the second state of the seco
Local-1	
Destination storage	
Local / Mapped Drive / Removable D	Drive 🗸
Local path	
	Change
Test	
	OK Cancel
	Previous Next 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
Coogle Drive
Test
Sign up for Google Drive
ОК Cancel
Prestous Bést Concel

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

New Storage Destination For The Pool	
Name	
FTP-1	
Destination storage	
FTP 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 Car

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 ricon to alter the order. Click **Next** to proceed when you are done with the selection.

	AhsayOBM
	Destination
*	Backup mode Sequential Existing storage destinations
	Previous Next Cancel

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.

	Encryption
Encrypt Backup Data On Encryption Type	
Default 🗸 🗸	
Default	
User password	
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.

	Encrypti	on
Encrypt Backup Data		
On 📃		
Encryption Type		
Custom 🖌		
Algorithm		
AES 🗸		
Encryption key		
•••••		
Re-enter encryption key		
•••••		
Method		
🔾 ECB 💿 CBC		
Key length		
🔾 128-bit 💿 256-bit		

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

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

Encryption	
Encrypt Backup Data On Encryption Type Default	
You are advised to write this encryption key down on paper and keep i in a safe place. You will need it when you need to restore your files later Please confirm that you have done so.	
•••••• Unmask encryption key	
	Copy to clipboard Confirm

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

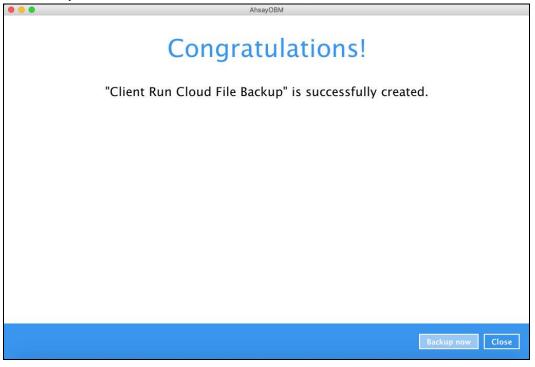
Unmask encryption key – The encryption key is masked by default. Click this option to show the encryption key.

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.		
ZPDWFyTrMWZ/o9MgcmOvWQAR9x8li367TAUfabDiR7I=		
Mask encryption key		
C	Copy to clipboard	Confirm

- Copy to clipboard Click to copy the encryption key, then you can paste it in another location of your choice.
- > Confirm Click to exit this pop-up window and proceed to the next step.

Click Next to create the backup set.

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



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

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

General	Temporary directory for storing backup files	
General	/Users/admin/temp 61.38GB free out of total 79.8GB space in /Users/adr	Change nin/temp
Source	Remove temporary files after backup	
Backup Schedule	Compressions	
Destination	Select compression type	
In-File Delta	Fast with optimization for local	
Retention Policy	Encryption	
Command Line Tool	Encryption key Copy to clipboard Unmask encryption key	
Bandwidth Control	Algorithm AES Method CBC	
Others	Key length 256 bits	
Hide advanced settings		

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

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

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

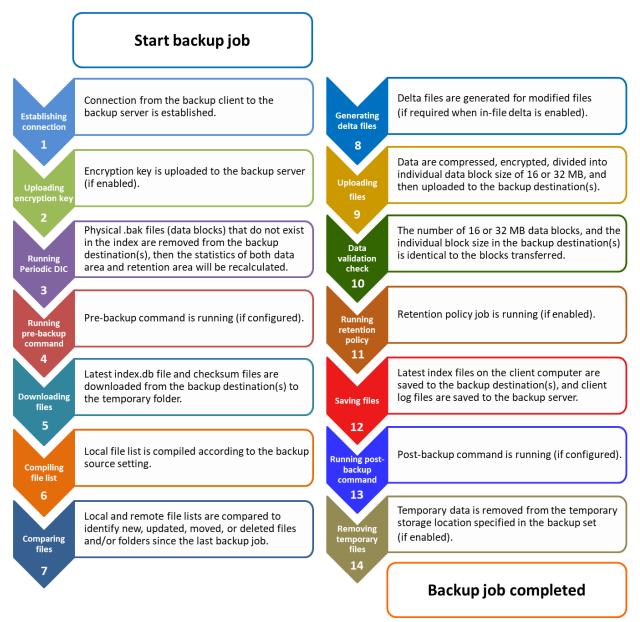
Backup Schedule	Compres	sions		
Destination	Select compress	sion type		
In-File Delta	Fast with optim	nization for local	~	
Retention Policy	Normal Fast (Compres	sed size larger than normal)		
Command Line Tool		nization for local		
Bandwidth Control	Algorithm Method	AES CBC		
Others	Key length	256 bits		
Hide advanced settings				
Delete this backup set				Save Cancel

5 Overview of Run on Client Cloud File Backup Process

The following steps are performed during a backup job. For an overview of the detailed process for Steps **3**, **5**, **10**, and **12**, please refer to the following chapters.

- Periodic Data Integrity Check (PDIC) Process (Step 3)
- Backup Set Index Handling Process
 - Start Backup Job (Step 5)
 - Completed Backup Job (Step 12)

Data Validation Check Process (Step 10)



5.1 Periodic Data Integrity Check (PDIC) Process

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

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

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

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

0	Monday
1	Tuesday
2	Wednesday
3	Thursday
4	Friday

NOTE: The PDIC schedule cannot be changed.

Example:

Backup set ID: 1594627447932

Calculation: 1594627447932 mod 5 = 2

2 Wednesday

In this example:

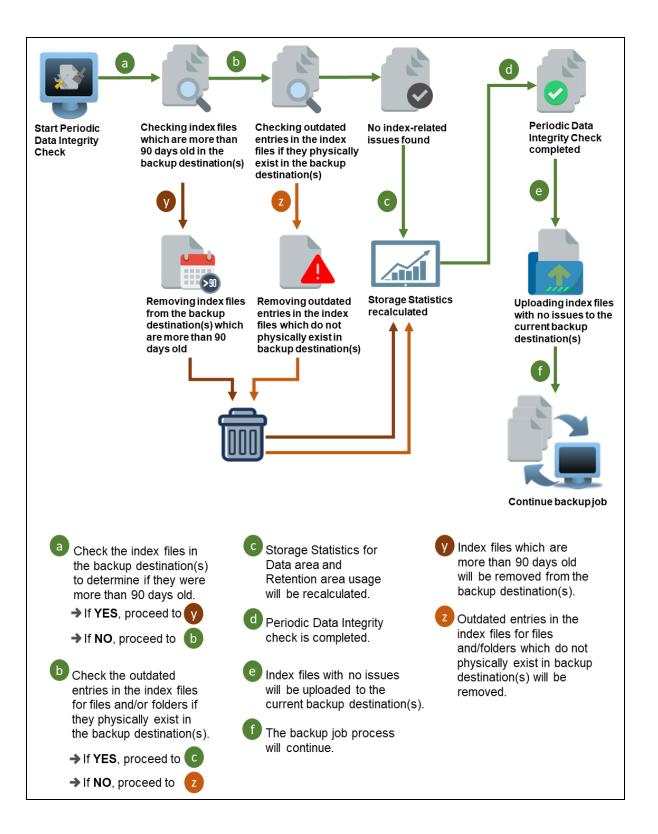
- the PDIC will run on the first backup job that falls on Wednesday; or
- if there is no active backup job(s) running from Monday to Friday, then the PDIC will run on the next available backup job.

NOTE

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

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

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



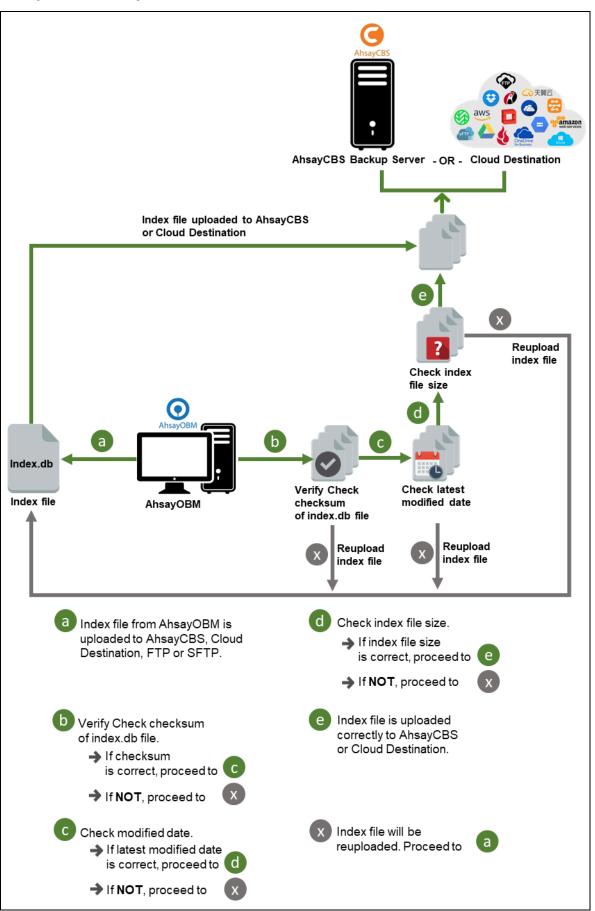
5.2 Backup Set Index Handling Process

To minimize the possibility of index related issues affecting backups, each time index files are downloaded from and uploaded to backup destination(s); the file size, last modified date, and checksum is verified to ensure index file integrity.

O AhsayOBM Index file received by AhsayOBM Redownload index file Check index file size C AhsayCBS Backup Server - OR -Check latest Verify Check Download checksum modified date index.db file of index.db file Redownload Redownload Х Х index file index file Cloud Destination Index file is retrieved from а Check modified date. If index is valid, the current directory (i.e., If latest modified date use the index.db file AhsayCBS, Cloud is correct, proceed to to compile file list for е Destination, FTP or SFTP). backup. → If NOT, proceed to Index file will be downloaded. b e Check index file size. Verify Check checksum Index file will be redownloaded. of index.db file. ➔ If index file size Proceed to ➔ If checksum is correct, proceed to is correct, proceed to d > If NOT, proceed to → If NOT, proceed to X

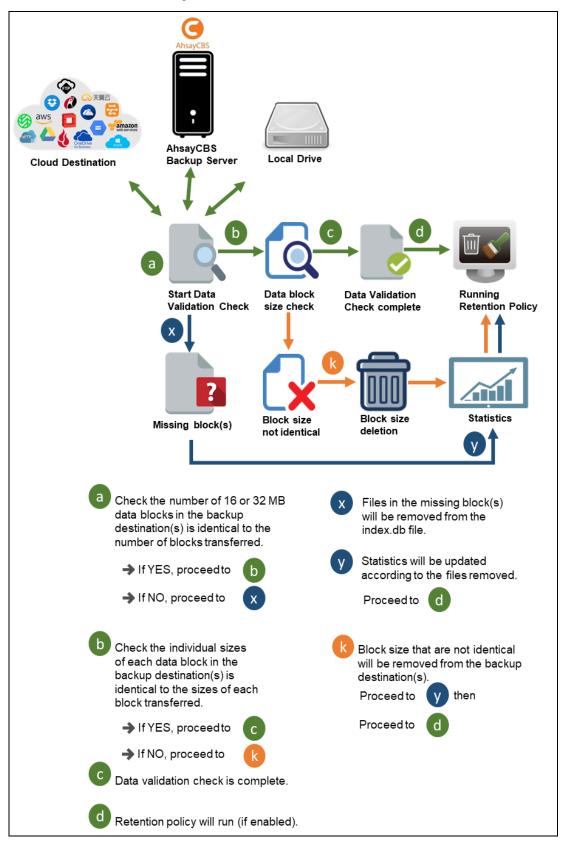
5.2.1 Start Backup Job

5.2.2 Completed Backup Job



5.3 Data Validation Check Process

As an additional measure to ensure that all files transferred to the backup destination(s) are received and saved correctly, both the number of 16 or 32 MB data block files and the size of each block file are checked again after the files are transferred.

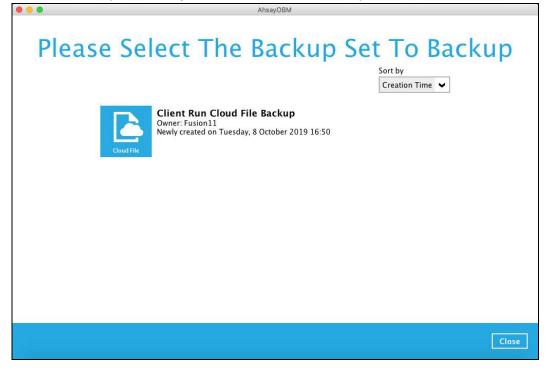


6 Running a Backup

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



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



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

🔴 💿 🕒 AhsayOBM	
Choose Your Backup Op	tions
Client Run Cloud File Backup	
Backup set type Cloud File	
In-File Delta type ● Full	
Differential	
Destinations Image: Construction of the state o	
Retention Policy	
Run Retention Policy after backup Hide advanced option	
	Previous Backup Cancel

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

		AhsayOBM		
		Backup		
Cloud File	Client Run Clou	ıd File Backup		
G	AhsayCBS (Host: 10 [New File] TestFiles; Estimated time left Backed up Elapsed time Transfer rate	Attendance_2016.doc (60%)	I	
				Cancel

5. The backup through AhsayOBM has been successful.

		AhsayOBM		
		Backup		
Cloud FA	Client Run Clou	id File Backup		
G	AhsayCBS (Host: 10 Backup Complete Estimated time left Backed up	ed Successfully	٦	
	Elapsed time Transfer rate	3 min 28 sec 5.88Mbit/s		
				Close

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

		Show All	~
Type	Log	Time	
0	Start [AhsayOBM v8.3.0.0]	08/10/2019 17:37:	14
0	Saving encrypted backup set encryption keys to server	08/10/2019 17:37:	15 ^
0	Start Backup [In-File Delta: Full]	08/10/2019 17:37:	17
0	Using Temporary Directory /Users/admin/.obm/temp/1570524625432/OBS@1570527203906	08/10/2019 17:37:	17
0	Start running pre-commands	08/10/2019 17:37:	18
0	Finished running pre-commands	08/10/2019 17:37:	18
0	Downloading server file list	08/10/2019 17:37:	18
0	Downloading server file list Completed	08/10/2019 17:37:	19
0	Reading backup source from hard disk	08/10/2019 17:37:	21
0	[New Directory] Photos	08/10/2019 17:37:	
0	[New Directory] TestFiles	08/10/2019 17:37:	
0	[New File] 10% of "Photos/TestJPG-2.jpg"	08/10/2019 17:37:	
0	[New File] 20% of "Photos/TestJPG-2.jpg"	08/10/2019 17:37:	
0	[New File] 30% of "Photos/TestJPG-2.jpg"	08/10/2019 17:37:	
0	[New File] 40% of "Photos/TestJPG-2.jpg"	08/10/2019 17:37:	
0	[New File] 50% of "Photos/TestJPG-2.jpg"	08/10/2019 17:37:	
0	[New File] 60% of "Photos/TestJPG-2.jpg"	08/10/2019 17:37:	
0	[New File] 70% of "Photos/TestJPG-2.jpg"	08/10/2019 17:37:	
0	[New File] 80% of "Photos/TestJPG-2.jpg"	08/10/2019 17:37:	
	[Now File] 00% of "Detec (TestIDC 2 ing"	00/10/2010 17-27-	
ogs	per page 50 🗸	Page 1 / 12	~

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



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

•	AhsayOBM
Report	Backup Report
	From To
Backup	01 V Oct V 2019 V 08 V Oct V 2019 V Go
Restore	Backup set 🗸 Destination 🗸 Completion Status 🗸
	No. of records per page 50 V Page 1/1 V
	Close

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

<complex-block> Property Baba Baba Baba Image: Im</complex-block>			
PackupResordImage: Image: I		AhsayOBM	
PackupResordImage: Image: I	D		
PackupResordImage: Image: I	Keport	Rackup Report	
	перопе	васкар кероп	
		From To	
Restore Badya still Onderioni Status Image: Status Onderioni Status Image: Status	Desture		
accurate the standard st	васкир	$01 \checkmark \text{Oct} \checkmark 2019 \checkmark 08 \checkmark \text{Oct} \checkmark$	2019 V Go
accurate the standard st			
accurate the standard st	Restore	Backup set 👻 Destination 👻 Completi	ion Status 🗸
			and a second sec
		Backup set 🕒 Client Run Clou	d File Backup 🗙
		Destination G AhsavCBS	
Image: Marging Stranger (Stranger Stranger			
		Time Today 17:37 - 17:4	0 (HKT)
		Status Completed succe	ssfully
Image:		The second	ng pangangan di sa
			[(0/0)]
		Updated files * 0	
		Attributes Changed Files * 0	
• "the the of files [Total zipped size / Total unzipped size (compression ratio)] • We the offiles [Total zipped size / Total unzipped size (compression ratio)] • Or eccords per pag 0 • Pag 1< • Corce		122 123-12 22800 044 NO2	
Vew log 0 of records per pag		Deleted files * 0	
be of records per page 1 Page 1		* Unit = No of files [Total zipped size / Total unzipp	ed size (compression ratio)]
be of records per page 1 Page 1			
AbayOB		View log	
AbayOB			
AbayOB			
AbayOB			
AbayOB		No. of records per page 50 🗸	Page 1/1 🗸
AbayDM Becknet Backun Becknet Backun Becknet Backun Set Clerk Run Cloud File Backup Dg BakyDS Dg Backun Set Dg Backun Set Dg BakyDS Dg Dg Dg Dg Dg Dg Dg Dg Dg			
AbayDM Becknet Backun Becknet Backun Becknet Backun Set Clerk Run Cloud File Backup Dg BakyDS Dg Backun Set Dg Backun Set Dg BakyDS Dg Dg Dg Dg Dg Dg Dg Dg Dg			
AbayDM Becknet Backun Becknet Backun Becknet Backun Set Clerk Run Cloud File Backup Dg BakyDS Dg Backun Set Dg Backun Set Dg BakyDS Dg Dg Dg Dg Dg Dg Dg Dg Dg			Close
Backup set Client Run Cloud File Backup Destination AhsayCBS Log 08/10/2019 17:37 Show All Twe Sart [AhsayOBM v8.3.0.1] Show Ml Image: Sart [AhsayOBM v8.3.0.1] Show All Sart [AhsayOBM v8.3.0.1] Log 08/10/2019 17:37:14 08/10/2019 17:37:14 Image: Sart [AhsayOBM v8.3.0.1] Image: Sart [AhsayOBM v8.3.0.1] Show All Image: Sart [AhsayOBM v8.3.0.1] Image: Sart [AhsayOBM v8.3.0.1] </td <th></th> <td></td> <td>close</td>			close
Backup set Client Run Cloud File Backup Destination AhsayCBS Log 08/10/2019 17:37 Show All Twe Sart [AhsayOBM v8.3.0.1] Show Ml Image: Sart [AhsayOBM v8.3.0.1] Show All Sart [AhsayOBM v8.3.0.1] Log 08/10/2019 17:37:14 08/10/2019 17:37:14 Image: Sart [AhsayOBM v8.3.0.1] Image: Sart [AhsayOBM v8.3.0.1] Show All Image: Sart [AhsayOBM v8.3.0.1] Image: Sart [AhsayOBM v8.3.0.1] </th <th></th> <th></th> <th></th>			
Lg 08/10/2019 17:37 Show All Type Time 08/10/2019 17:37:14 Saving encrypted backup set encryption keys to server 08/10/2019 17:37:14 Saving encrypted backup set encryption keys to server 08/10/2019 17:37:14 Start Rackup [In-File Delta: Full] 08/10/2019 17:37:17 Start Rackup [In-File Delta: Full] 08/10/2019 17:37:17 Start Rackup [In-File Delta: Full] 08/10/2019 17:37:18 Start Rackup [In-File Delta: Full] 08/10/2019 17:37:18 Start Rackup server file Ist 08/10/2019 17:37:18 Downloading server file Ist 08/10/2019 17:37:18 Downloading server file Ist 08/10/2019 17:37:21 New Directory] Photos 08/10/2019 17:37:23 New Directory] Photos/TestyPG-2.jpg* 08/10/2019 17:37:23 New File] 10% of Photos/TestyPG-2.jpg* 08/10/2019 17:37:23 New File] 60% of Photos/TestyPG-2.jpg* 08/10/2019 1		Abaariophi	
Lg 08/10/2019 17:37 Show All Type Time 08/10/2019 17:37:14 Saving encrypted backup set encryption keys to server 08/10/2019 17:37:14 Saving encrypted backup set encryption keys to server 08/10/2019 17:37:14 Start Rackup [In-File Delta: Full] 08/10/2019 17:37:17 Start Rackup [In-File Delta: Full] 08/10/2019 17:37:17 Start Rackup [In-File Delta: Full] 08/10/2019 17:37:18 Start Rackup [In-File Delta: Full] 08/10/2019 17:37:18 Start Rackup server file Ist 08/10/2019 17:37:18 Downloading server file Ist 08/10/2019 17:37:18 Downloading server file Ist 08/10/2019 17:37:21 New Directory] Photos 08/10/2019 17:37:23 New Directory] Photos/TestyPG-2.jpg* 08/10/2019 17:37:23 New File] 10% of Photos/TestyPG-2.jpg* 08/10/2019 17:37:23 New File] 60% of Photos/TestyPG-2.jpg* 08/10/2019 1		AnsayOBM	
Lg 08/10/2019 17:37 Show All Type Time 08/10/2019 17:37:14 Saving encrypted backup set encryption keys to server 08/10/2019 17:37:14 Saving encrypted backup set encryption keys to server 08/10/2019 17:37:14 Start Rackup [In-File Delta: Full] 08/10/2019 17:37:17 Start Rackup [In-File Delta: Full] 08/10/2019 17:37:17 Start Rackup [In-File Delta: Full] 08/10/2019 17:37:18 Start Rackup [In-File Delta: Full] 08/10/2019 17:37:18 Start Rackup server file Ist 08/10/2019 17:37:18 Downloading server file Ist 08/10/2019 17:37:18 Downloading server file Ist 08/10/2019 17:37:21 New Directory] Photos 08/10/2019 17:37:23 New Directory] Photos/TestyPG-2.jpg* 08/10/2019 17:37:23 New File] 10% of Photos/TestyPG-2.jpg* 08/10/2019 17:37:23 New File] 60% of Photos/TestyPG-2.jpg* 08/10/2019 1		AnsayOBM	
Lg 08/10/2019 17:37 Show All Type Time 08/10/2019 17:37:14 Saving encrypted backup set encryption keys to server 08/10/2019 17:37:14 Saving encrypted backup set encryption keys to server 08/10/2019 17:37:14 Start Rackup [In-File Delta: Full] 08/10/2019 17:37:17 Start Rackup [In-File Delta: Full] 08/10/2019 17:37:17 Start Rackup [In-File Delta: Full] 08/10/2019 17:37:18 Start Rackup [In-File Delta: Full] 08/10/2019 17:37:18 Start Rackup server file Ist 08/10/2019 17:37:18 Downloading server file Ist 08/10/2019 17:37:18 Downloading server file Ist 08/10/2019 17:37:21 New Directory] Photos 08/10/2019 17:37:23 New Directory] Photos/TestyPG-2.jpg* 08/10/2019 17:37:23 New File] 10% of Photos/TestyPG-2.jpg* 08/10/2019 17:37:23 New File] 60% of Photos/TestyPG-2.jpg* 08/10/2019 1	Papart	Ansayobm	
Lg 08/10/2019 17:37 Show All Type Time 08/10/2019 17:37:14 Saving encrypted backup set encryption keys to server 08/10/2019 17:37:14 Saving encrypted backup set encryption keys to server 08/10/2019 17:37:14 Start Rackup [In-File Delta: Full] 08/10/2019 17:37:17 Start Rackup [In-File Delta: Full] 08/10/2019 17:37:17 Start Rackup [In-File Delta: Full] 08/10/2019 17:37:18 Start Rackup [In-File Delta: Full] 08/10/2019 17:37:18 Start Rackup server file Ist 08/10/2019 17:37:18 Downloading server file Ist 08/10/2019 17:37:18 Downloading server file Ist 08/10/2019 17:37:21 New Directory] Photos 08/10/2019 17:37:23 New Directory] Photos/TestyPG-2.jpg* 08/10/2019 17:37:23 New File] 10% of Photos/TestyPG-2.jpg* 08/10/2019 17:37:23 New File] 60% of Photos/TestyPG-2.jpg* 08/10/2019 1	Report	Rackup Roport	
Lg 08/10/2019 17:37 Show All Type Time 08/10/2019 17:37:14 Saving encrypted backup set encryption keys to server 08/10/2019 17:37:14 Saving encrypted backup set encryption keys to server 08/10/2019 17:37:14 Start Rackup [In-File Delta: Full] 08/10/2019 17:37:17 Start Rackup [In-File Delta: Full] 08/10/2019 17:37:17 Start Rackup [In-File Delta: Full] 08/10/2019 17:37:18 Start Rackup [In-File Delta: Full] 08/10/2019 17:37:18 Start Rackup server file Ist 08/10/2019 17:37:18 Downloading server file Ist 08/10/2019 17:37:18 Downloading server file Ist 08/10/2019 17:37:21 New Directory] Photos 08/10/2019 17:37:23 New Directory] Photos/TestyPG-2.jpg* 08/10/2019 17:37:23 New File] 10% of Photos/TestyPG-2.jpg* 08/10/2019 17:37:23 New File] 60% of Photos/TestyPG-2.jpg* 08/10/2019 1	Report	Rackup Report	
Type Log Time Satart [AhsayOBM v8.3.0.0] 08/10/2019 17:37:14 08/10/2019 17:37:14 Sating ackup [In-File Delta: Full] 08/10/2019 17:37:17 Using Temporary Directory /Users/admin/.obm/temp/1570524625432/OBS@1570527203906 08/10/2019 17:37:17 Start Backup [In-File Delta: Full] 08/10/2019 17:37:17 Start Tunning pre-commands 08/10/2019 17:37:18 Downloading server file list 08/10/2019 17:37:21 New Directory] Photos 08/10/2019 17:37:21 New Directory] Photos 08/10/2019 17:37:23 New File] 10% of "Photos/TestyPC-2.jpg" 08/10/2019 17:37:23 New File] 20% of "Photos/TestyPC-2.jpg" 08/10/2019 17:37:23 New File] 40% of "Photos/TestyPC-2.jpg" 08/10/2019 17:37:23 New File] 60% of "Photos/TestyPC-2.jpg" 08/10/2019 17:37:23 New File] 60% of "Photos/TestyPC-2.jpg" 08/10/2019 17:37:23 New File] 60% of "Photos/TestyPC-	Report	Rackup Report	
Type Log Time Satart [AhsayOBM v8.3.0.0] 08/10/2019 17:37:14 08/10/2019 17:37:14 Sating ackup [In-File Delta: Full] 08/10/2019 17:37:17 Using Temporary Directory /Users/admin/.obm/temp/1570524625432/OBS@1570527203906 08/10/2019 17:37:17 Start Backup [In-File Delta: Full] 08/10/2019 17:37:17 Start Tunning pre-commands 08/10/2019 17:37:18 Downloading server file list 08/10/2019 17:37:21 New Directory] Photos 08/10/2019 17:37:21 New Directory] Photos 08/10/2019 17:37:23 New File] 10% of "Photos/TestyPC-2.jpg" 08/10/2019 17:37:23 New File] 20% of "Photos/TestyPC-2.jpg" 08/10/2019 17:37:23 New File] 40% of "Photos/TestyPC-2.jpg" 08/10/2019 17:37:23 New File] 60% of "Photos/TestyPC-2.jpg" 08/10/2019 17:37:23 New File] 60% of "Photos/TestyPC-2.jpg" 08/10/2019 17:37:23 New File] 60% of "Photos/TestyPC-	Renort Backup set Client Run Cloud File Backup 🖌	Rackun Report	Destination AhsayCBS 🖌
① Start [AbsayOBM v8.3.0.0] 08/10/2019 17:37:14 ③ Start [AckayOBM v8.3.0.0] 08/10/2019 17:37:17 ④ Start Backup. [In-File Detai: Full] 08/10/2019 17:37:17 ④ Start Backup. [In-File Detaing pre-commands 08/10/2019 17:37:18 ● Downloading server file list 08/10/2019 17:37:18 ● Downloading server file list 08/10/2019 17:37:18 ● Downloading server file list 08/10/2019 17:37:11 ● Reading backup source from hard disk 08/10/2019 17:37:21 ● New Directory] Photos 08/10/2019 17:37:23 ● New File] 20% of Photos/TestyPC-2.jpg" 08/10/2019 17:37:23 ● New File] 30% of Photos/TestyPC-2.jpg" 08/10/2019 17:37:23 ● New File] 30% of Photos/TestyPC-2.jpg" 08/10/2019 17:37:23 ● New File] 60% of Photos/TestyPC-2.jpg" 08/10/2019 17:37:23 ● New File] 60% of Photos/TestyPC-2.jpg" 08/10/2019 17:37:23 ● New File] 60% of Photos/TestyPC-2.jpg" 08/10/2019 17:37:23 <		Rackun Ronort	
① Start [AbsayOBM v8.3.0.0] 08/10/2019 17:37:14 ③ Start [AckayOBM v8.3.0.0] 08/10/2019 17:37:17 ④ Start Backup. [In-File Detai: Full] 08/10/2019 17:37:17 ④ Start Backup. [In-File Detaing pre-commands 08/10/2019 17:37:18 ● Downloading server file list 08/10/2019 17:37:18 ● Downloading server file list 08/10/2019 17:37:18 ● Downloading server file list 08/10/2019 17:37:11 ● Reading backup source from hard disk 08/10/2019 17:37:21 ● New Directory] Photos 08/10/2019 17:37:23 ● New File] 20% of Photos/TestyPC-2.jpg" 08/10/2019 17:37:23 ● New File] 30% of Photos/TestyPC-2.jpg" 08/10/2019 17:37:23 ● New File] 30% of Photos/TestyPC-2.jpg" 08/10/2019 17:37:23 ● New File] 60% of Photos/TestyPC-2.jpg" 08/10/2019 17:37:23 ● New File] 60% of Photos/TestyPC-2.jpg" 08/10/2019 17:37:23 ● New File] 60% of Photos/TestyPC-2.jpg" 08/10/2019 17:37:23 <		Rackup Roport	
① Saving encrypted backup set encryption keys to server 08/10/2019 17:37:15 ③ Start Backup [In-File Delta: Full] 08/10/2019 17:37:15 ④ Using Temporary Directory (Users/admin/.obm/temp/1570524625432/085@1570527203906 08/10/2019 17:37:17 ④ Start running pre-commands 08/10/2019 17:37:18 ● Downloading server file list 08/10/2019 17:37:18 ● Downloading server file list 08/10/2019 17:37:18 ● Downloading server file list 08/10/2019 17:37:19 ● Reading backup source from hard disk 08/10/2019 17:37:21 ● Inew Directory] Photos 08/10/2019 17:37:21 ● Inew Directory] TestFiles 08/10/2019 17:37:22 ● Inew File] 20% of "Photos/TestJPC-2.jpg" 08/10/2019 17:37:23 ● Inew File] 30% of "Photos/TestJPC-2.jpg" 08/10/2019 17:37:23 ● Inew File] 40% of "Photos/TestJPC-2.jpg" 08/10/2019 17:37:23 ● Inew File] 60% of "Photos/TestJPC-2.jpg" 08/10/2019 17:37:23 ● Inew File] 60% of "Photos/TestJPC-2.jpg" 08/10/2019 17:37:23 ● Inew File] 60% of "Photos/TestJPC-2.jpg" 08/10/2019 17:37:23 <th>Log 08/10/2019 17:37 🖌</th> <td>Rackup Report</td> <td>Show All</td>	Log 08/10/2019 17:37 🖌	Rackup Report	Show All
● Start Backup [In-File Delta: Full] 08/10/2019 17:37:17 ● Using Temporary Directory / Users/admin/.obm/temp/1570524625432/085@1570527203906 08/10/2019 17:37:17 ● Start running pre-commands 08/10/2019 17:37:18 ● Downloading server file list 08/10/2019 17:37:18 ● Downloading server file list 08/10/2019 17:37:19 ● Reading backup source from hard disk 08/10/2019 17:37:21 ● New Directory Photos 08/10/2019 17:37:22 ● New Directory TestFiles 08/10/2019 17:37:23 ● New File 10% of "Photos/TestPC-2.jpg" 08/10/2019 17:37:23 ● New File 30% of "Photos/TestPC-2.jpg" 08/10/2019 17:37:23 ● New File 40% of "Photos/TestPC-2.jpg" 08/10/2019 17:37:23 ● New File 50% of "Photos/TestPC-2.jpg" 08/10/2019 17:37:23 ● New File 30% of "Photos/TestPC-2.jpg" 08/10/2019 17:37:23 ● New File 30% of "Photos/TestPC-2.jpg" 08/10/2019 17:37:23 ● New File 40% of "Photos/TestPC-2.jpg" 08/10/2019 17:37:23 ● New File 50% of "Photos/TestPC-2.jpg" 08/10/2019 17:37:23 ● New File 60% of "Photos/TestPC-2.jpg" 08/10/2019 17:37:23 ● New File 50% of "Photos/TestPC-2.jpg" 08/10/2019 17:37:23 ● New File	Log 08/10/2019 17:37 V	Rackup Report	Show All V Time
● Using Temporary Directory /Users/admin/.obm/temp/1570524625432/08S@1570527203906 08/10/2019 17:37:17 ● Start running pre-commands 08/10/2019 17:37:18 ● Downloading server file list 08/10/2019 17:37:21 ● Reading backup source from hard disk 08/10/2019 17:37:21 ● New Directory Photos 08/10/2019 17:37:22 ● New Directory Photos 08/10/2019 17:37:22 ● New File 20% of Photos/TestyPC-2.jpg" 08/10/2019 17:37:23 ● New File 30% of Photos/TestyPC-2.jpg" 08/10/2019 17:37:23 ● New File 30% of Photos/TestyPC-2.jpg" 08/10/2019 17:37:23 ● New File 60% of Photos/TestyPC-2.jpg" 08/10/2019 17:37:23 ● <	Log 08/10/2019 17:37 V Type Start [AhsayOBM v8.3.0.0]	Rackup Report	Show All Time 08/10/2019 17:37:14
Imished running pre-commands 08/10/2019 17:37:18 Downloading server file list 08/10/2019 17:37:18 Downloading server file list Completed 08/10/2019 17:37:19 Reading backup source from hard disk 08/10/2019 17:37:21 Image: the second se	Log 08/10/2019 17:37 V Type Start [AhsayOBM v8.3.0.0] Saving encrypted backup set encryption keys to	Rackup Report	Show All Time 08/10/2019 17:37:14 08/10/2019 17:37:15
● Downloading server file list 08/10/2019 17:37:18 ● Downloading server file list Completed 08/10/2019 17:37:19 ● Reading backup source from hard disk 08/10/2019 17:37:21 ● Reading backup source from hard disk 08/10/2019 17:37:21 ● INEW Directory] Photos 08/10/2019 17:37:21 ● INEW Directory] Photos 08/10/2019 17:37:22 ● INEW File] 20% of "Photos/TestyPC-2.jpg" 08/10/2019 17:37:23 ● INEW File] 30% of "Photos/TestyPC-2.jpg" 08/10/2019 17:37:23 ● INEW File] 30% of "Photos/TestyPC-2.jpg" 08/10/2019 17:37:23 ● INEW File] 50% of "Photos/TestyPC-2.jpg" 08/10/2019 17:37:23 ●	Log 08/10/2019 17:37 ✓ Type ③ Start [AhsayOBM v8.3.0.0] ④ Saving encrypted backup set encryption keys to ⑤ Start Backup [In-File Delta: Full] ④ Using Temporary Directory /Users/admin/.obm/	Rackup Roport Log server	Show All Time 08/10/2019 17:37:14 08/10/2019 17:37:15 08/10/2019 17:37:17
● Downloading server file list Completed 08/10/2019 17:37:19 ● Reading backup source from hard disk 08/10/2019 17:37:21 ● INew Directory) Tosts 08/10/2019 17:37:21 ● INew Directory) TostFiles 08/10/2019 17:37:21 ● INew Directory) TostFiles 08/10/2019 17:37:23 ● INew File) 10% of "Photos/TestyPC-2.jpg" 08/10/2019 17:37:23 ● INew File) 20% of "Photos/TestyPC-2.jpg" 08/10/2019 17:37:23 ● INew File) 30% of "Photos/TestyPC-2.jpg" 08/10/2019 17:37:23 ● INew File) 40% of "Photos/TestyPC-2.jpg" 08/10/2019 17:37:23 ● INew File) 60% of "Photos/TestyPC-2.jpg" 08/10/2019 17:37:23	Log 08/10/2019 17:37 V Type Start [AhsayOBM v8.3.0.0] Saving encrypted backup set encryption keys to Start Backup [In-File Delta: Full] Using Temporary Directory /Users/admin/.obm/ Start running pre-commands	Rackup Roport Log server	Show All Time 08/10/2019 17:37:14 08/10/2019 17:37:15 08/10/2019 17:37:17 08/10/2019 17:37:17
① Reading backup source from hard disk 08/10/2019 17:37:21 ① [New Directory] Photos 08/10/2019 17:37:22 ① [New File] 10% of "Photos/TestJPG-2.jpg" 08/10/2019 17:37:23 ② [New File] 20% of "Photos/TestJPG-2.jpg" 08/10/2019 17:37:23 ③ [New File] 20% of "Photos/TestJPG-2.jpg" 08/10/2019 17:37:23 ④ [New File] 40% of "Photos/TestJPG-2.jpg" 08/10/2019 17:37:23 ④ [New File] 40% of "Photos/TestJPG-2.jpg" 08/10/2019 17:37:23 ④ [New File] 60% of "Photos/TestJPG-2.jpg" 08/10/2019 17:37:23 ● [New File] 60% of "Photos/TestJPG-2.jpg" 08/10/2019 17:37:23 ● [New File] 60% of "Photos/TestJPG-2.jpg" 08/10/2019 17:37:23 ● [New File] 60% of "Photos/TestJPG-2.jpg" 08/10/201	Log 08/10/2019 17:37 Type Start [AhsayOBM v8.3.0.0] Saving encrypted backup set encryption keys to Start Backup [In-File Delta: Full] Using Temporary Directory /Users/admin/.obm/ Start running pre-commands Finished running pre-commands	Rackup Roport Log server	Show All Time 08/10/2019 17:37:14 08/10/2019 17:37:15 08/10/2019 17:37:17 08/10/2019 17:37:17 08/10/2019 17:37:18 08/10/2019 17:37:18
Image: New Directory] Photos 08/10/2019 17:37:21 Image: New File 08/10/2019 17:37:22 Image: New File 08/10/2019 17:37:23 Image: New File 08/10/2019 17	Log 08/10/2019 17:37 Type Start [AhsayOBM v8.3.0.0] Saving encrypted backup set encryption keys to Start Backup [In-File Delta: Full] Using Temporary Directory /Users/admin/.obm/ Start running pre-commands Finished running pre-commands Downloading server file list	Rackup Roport Log server	Show All Time 08/10/2019 17:37:14 08/10/2019 17:37:15 08/10/2019 17:37:17 08/10/2019 17:37:17 08/10/2019 17:37:18 08/10/2019 17:37:18
● New Directory] TestFiles 08/10/2019 17:37:22 ● [New File] 10% of "Photos/TestJPC-2.jpg" 08/10/2019 17:37:23 ● [New File] 20% of "Photos/TestJPC-2.jpg" 08/10/2019 17:37:23 ● [New File] 30% of "Photos/TestJPC-2.jpg" 08/10/2019 17:37:23 ● [New File] 40% of "Photos/TestJPC-2.jpg" 08/10/2019 17:37:23 ● [New File] 60% of "Photos/TestJPC-2.jpg" 08/1	Log 08/10/2019 17:37 Type Start [AhsayOBM v8.3.0.0] Saving encrypted backup set encryption keys to Start Backup [In-File Delta: Full] Using Temporary Directory /Users/admin/.obm/ Start running pre-commands Finished running pre-commands Downloading server file list Downloading server file list Completed	Rackup Roport Log server	Show All Time 08/10/2019 17:37:14 08/10/2019 17:37:17 08/10/2019 17:37:17 08/10/2019 17:37:17 08/10/2019 17:37:18 08/10/2019 17:37:18 08/10/2019 17:37:18 08/10/2019 17:37:19
Image: New File] 10% of "Photos/TestyPC-2.jpg" 08/10/2019 17:37:23 Image: New File] 20% of "Photos/TestyPC-2.jpg" 08/10/2019 17:37:23 Image: New File] 30% of "Photos/TestyPC-2.jpg" 08/10/2019 17:37:23 Image: New File] 30% of "Photos/TestyPC-2.jpg" 08/10/2019 17:37:23 Image: New File] 30% of "Photos/TestyPC-2.jpg" 08/10/2019 17:37:23 Image: New File] 50% of "Photos/TestyPC-2.jpg" 08/10/2019 17:37:23	Log 08/10/2019 17:37 ▼ Type Start [AhsayOBM v8.3.0.0] Saving encrypted backup set encryption keys to Start Backup [In-File Delta: Full] Using Temporary Directory /Users/admin/.obm/ Start running pre-commands Finished running pre-commands Downloading server file list Downloading server file list Reading backup source from hard disk	Rackup Roport Log server	Show All 08/10/2019 17:37:14 08/10/2019 17:37:15 08/10/2019 17:37:15 08/10/2019 17:37:17 08/10/2019 17:37:17 08/10/2019 17:37:18 08/10/2019 17:37:18 08/10/2019 17:37:18 08/10/2019 17:37:19 08/10/2019 17:37:19
● [New File] 20% of "Photos/TestyPC-2.jpg" 08/10/2019 17:37:23 ● [New File] 30% of "Photos/TestyPC-2.jpg" 08/10/2019 17:37:23 ● [New File] 40% of "Photos/TestyPC-2.jpg" 08/10/2019 17:37:23 ● [New File] 60% of "Photos/TestyPC-2.jpg" 08/10/2019 17:37:23 ■ Page 1 / 12 ●	Log 08/10/2019 17:37 ▼ Type Start [AhsayOBM v8.3.0.0] Saving encrypted backup set encryption keys to Start Backup [In-File Delta: Full] Using Temporary Directory /Users/admin/.obm/ Start running pre-commands Finished running pre-commands Downloading server file list Downloading server file list Completed Reading backup source from hard disk [New Directory] Photos	Rackup Roport Log server	Show All Time 08/10/2019 17:37:14 08/10/2019 17:37:15 08/10/2019 17:37:17 08/10/2019 17:37:17 08/10/2019 17:37:18 08/10/2019 17:37:18 08/10/2019 17:37:18 08/10/2019 17:37:21 08/10/2019 17:37:21
Image: New File] 30% of "Photos/TestyPC-2.jpg" 08/10/2019 17:37:23 Image: New File] 40% of "Photos/TestyPC-2.jpg" 08/10/2019 17:37:23 Image: New File] 50% of "Photos/TestyPC-2.jpg" 08/10/2019 17:37:23 Image: New File] 50% of "Photos/TestyPC-2.jpg" 08/10/2019 17:37:23 Image: New File] 50% of "Photos/TestyPC-2.jpg" 08/10/2019 17:37:23 Image: New File] 60% of "Photos/TestyPC-2.jpg" 08/10/2019 17:37:23	Log 08/10/2019 17:37 Type Start [AhsayOBM v8.3.0.0] Saving encrypted backup set encryption keys to Start Backup [In-File Delta: Full] Using Temporary Directory /Users/admin/.obm/ Start running pre-commands Finished running pre-commands Downloading server file list Downloading server file list Completed Reading backup source from hard disk [New Directory] PestFiles	Rackup Roport Log server	Show All Time 08/10/2019 17:37:14 08/10/2019 17:37:17 08/10/2019 17:37:17 08/10/2019 17:37:17 08/10/2019 17:37:18 08/10/2019 17:37:18 08/10/2019 17:37:18 08/10/2019 17:37:18 08/10/2019 17:37:18 08/10/2019 17:37:19 08/10/2019 17:37:21 08/10/2019 17:37:21 08/10/2019 17:37:21
Image: State Stat	Log 08/10/2019 17:37 ▼ Type Start [AhsayOBM v8.3.0.0] Saving encrypted backup set encryption keys to Start Backup [In-File Delta: Full] Using Temporary Directory /Users/admin/.obm/ Start running pre-commands Finished running pre-commands Downloading server file list Downloading server file list Downloading server file list Downloading server file list [New Directory] Photos [New Directory] TestFiles [New File] 10% of "Photos/TestJPG-2.jpg"	Rackup Roport Log server	Show All Time 08/10/2019 17:37:14 08/10/2019 17:37:15 08/10/2019 17:37:15 08/10/2019 17:37:17 08/10/2019 17:37:17 08/10/2019 17:37:18 08/10/2019 17:37:18 08/10/2019 17:37:18 08/10/2019 17:37:18 08/10/2019 17:37:19 08/10/2019 17:37:21 08/10/2019 17:37:22 08/10/2019 17:37:22
● [New File] 50% of "Photos/TestyPC-2.jpg" 08/10/2019 17:37:23 ● [New File] 60% of "Photos/TestyPC-2.jpg" 08/10/2019 17:37:23 ● [New File] 60% of "Photos/TestyPC-2.jpg" 08/10/2019 17:37:23 Logs per page 50 ✓ Page 1 / 12 ✓	Log 08/10/2019 17:37 ▼ Type Start [AhsayOBM v8.3.0.0] Saving encrypted backup set encryption keys to Start Backup [In-File Delta: Full] Using Temporary Directory /Users/admin/.obm/ Start running pre-commands Finished running pre-commands Downloading server file list Downloading server file list Downloading server file list Mew Directory] Photos [New Directory] Photos/TestJPG-2.jpg" [New File] 20% of "Photos/TestJPG-2.jpg"	Rackup Roport Log server	Show All Time 08/10/2019 17:37:14 08/10/2019 17:37:15 08/10/2019 17:37:15 08/10/2019 17:37:17 08/10/2019 17:37:18 08/10/2019 17:37:18 08/10/2019 17:37:18 08/10/2019 17:37:21 08/10/2019 17:37:21 08/10/2019 17:37:22 08/10/2019 17:37:23 08/10/2019 17:37:23
Interverties 08/10/2019 17:37:23 Logs per page 50	Log 08/10/2019 17:37 ▼ Type Start [AhsayOBM v8.3.0.0] Saving encrypted backup set encryption keys to Start Backup [In-File Detta: Full] Using Temporary Directory (/Users/admin/.obm/ Start running pre-commands Downloading server file list Downloading server file list New Directory] Ptots [New File] 10% of "Photos/TestyPC-2.jpg" [New File] 30% of "Photos/TestyPC-2.jpg"	Rackup Roport Log server	Show All Time 08/10/2019 17:37:14 08/10/2019 17:37:17 08/10/2019 17:37:17 08/10/2019 17:37:17 08/10/2019 17:37:18 08/10/2019 17:37:18 08/10/2019 17:37:18 08/10/2019 17:37:18 08/10/2019 17:37:18 08/10/2019 17:37:19 08/10/2019 17:37:21 08/10/2019 17:37:21 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:23
Logs per page 50 V Close	Log 08/10/2019 17:37 ▼ Type Start [AhsayOBM v8.3.0.0] Saving encrypted backup set encryption keys to Start Backup [In-File Delta: Full] Using Temporary Directory /Users/admin/.obm/ Start running pre-commands Finished running pre-commands Downloading server file list Downloading server file list Downloading server file list (New Directory) Photos [New File] 10% of "Photos/TestyPG-2.jpg" [New File] 20% of "Photos/TestyPG-2.jpg" [New File] 40% of "Photos/TestyPG-2.jpg"	Rackup Roport Log server	Show All Time 08/10/2019 17:37:14 08/10/2019 17:37:15 08/10/2019 17:37:15 08/10/2019 17:37:17 08/10/2019 17:37:17 08/10/2019 17:37:18 08/10/2019 17:37:18 08/10/2019 17:37:18 08/10/2019 17:37:19 08/10/2019 17:37:21 08/10/2019 17:37:22 08/10/2019 17:37:22 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:23
Close	Log 08/10/2019 17:37 ▼ Type Start [AhsayOBM v8.3.0.0] Saving encrypted backup set encryption keys to Start Backup [In-File Delta: Full] Using Temporary Directory /Users/admin/.obm/ Start running pre-commands Finished running pre-commands Downloading server file list Downloading server file list Downloading server file list Downloading server file list Mew Directory] Potos [New File] 10% of 'Photos/TestyPG-2.jpg'' [New File] 30% of 'Photos/TestyPG-2.jpg'' [New File] 30% of 'Photos/TestyPG-2.jpg'' [New File] 30% of 'Photos/TestyPG-2.jpg'' [New File] 30% of 'Photos/TestyPG-2.jpg'' [New File] 50% of 'Photos/TestyPG-2.jpg'' [New File] 60% of 'Photos/TestyPG-2.jpg'' [New File] 60% of 'Photos/TestyPG-2.jpg''	Rackup Roport Log server	Show All Time 08/10/2019 17:37:14 08/10/2019 17:37:15 08/10/2019 17:37:15 08/10/2019 17:37:17 08/10/2019 17:37:18 08/10/2019 17:37:18 08/10/2019 17:37:18 08/10/2019 17:37:21 08/10/2019 17:37:21 08/10/2019 17:37:23 08/10/2019 17
Close	Log 08/10/2019 17:37 ▼ Type Start [AhsayOBM v8.3.0.0] Saving encrypted backup set encryption keys to Start Backup [In-File Delta: Full] Using Temporary Directory /Users/admin/.obm/ Start running pre-commands Finished running pre-commands Downloading server file list Downloading server file list Downloading server file list Downloading server file list Mew Directory] Potos [New File] 10% of 'Photos/TestyPG-2.jpg'' [New File] 30% of 'Photos/TestyPG-2.jpg'' [New File] 30% of 'Photos/TestyPG-2.jpg'' [New File] 30% of 'Photos/TestyPG-2.jpg'' [New File] 30% of 'Photos/TestyPG-2.jpg'' [New File] 50% of 'Photos/TestyPG-2.jpg'' [New File] 60% of 'Photos/TestyPG-2.jpg'' [New File] 60% of 'Photos/TestyPG-2.jpg''	Rackup Roport Log server	Show All Time 08/10/2019 17:37:14 08/10/2019 17:37:14 08/10/2019 17:37:15 08/10/2019 17:37:15 08/10/2019 17:37:17 08/10/2019 17:37:18 08/10/2019 17:37:18 08/10/2019 17:37:18 08/10/2019 17:37:18 08/10/2019 17:37:19 08/10/2019 17:37:21 08/10/2019 17:37:21 08/10/2019 17:37:22 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:23
	Log 08/10/2019 17:37 ▼ Type Start [Ahsay0BM v8.3.0.0] Saving encrypted backup set encryption keys to Start Backup[In-File Delta: Full] Using Temporary Directory /Users/admin/.obm/ Start start running pre-commands Finished running pre-commands Downloading server file list Downloading server file list Downloading server file list Downloading server file list New Directory] Post5 [New File] 10% of 'Photos/TestyPC-2.jpg" [New File] 20% of 'Photos/TestyPC-2.jpg" [New File] 20% of 'Photos/TestyPC-2.jpg" [New File] 20% of 'Photos/TestyPC-2.jpg" [New File] 50% of 'Photos/TestyPC-2.jpg" [New File] 50% of 'Photos/TestyPC-2.jpg" [New File] 50% of 'Photos/TestyPC-2.jpg"	Rackup Roport Log server	Show All Time 08/10/2019 17:37:14 08/10/2019 17:37:15 08/10/2019 17:37:17 08/10/2019 17:37:17 08/10/2019 17:37:18 08/10/2019 17:37:18 08/10/2019 17:37:19 08/10/2019 17:37:21 08/10/2019 17:37:22 08/10/2019 17:37:23 08/10/2019 17
	Log 08/10/2019 17:37 ▼ Type Start [Ahsay0BM v8.3.0.0] Saving encrypted backup set encryption keys to Start Backup[In-File Delta: Full] Using Temporary Directory /Users/admin/.obm/ Start start running pre-commands Finished running pre-commands Downloading server file list Downloading server file list Downloading server file list Downloading server file list New Directory] Post5 [New File] 10% of 'Photos/TestyPC-2.jpg" [New File] 20% of 'Photos/TestyPC-2.jpg" [New File] 20% of 'Photos/TestyPC-2.jpg" [New File] 20% of 'Photos/TestyPC-2.jpg" [New File] 50% of 'Photos/TestyPC-2.jpg" [New File] 50% of 'Photos/TestyPC-2.jpg" [New File] 50% of 'Photos/TestyPC-2.jpg"	Rackup Roport Log server	Show All Time 08/10/2019 17:37:14 08/10/2019 17:37:15 08/10/2019 17:37:17 08/10/2019 17:37:17 08/10/2019 17:37:18 08/10/2019 17:37:18 08/10/2019 17:37:19 08/10/2019 17:37:21 08/10/2019 17:37:22 08/10/2019 17:37:23 08/10/2019 17
	Log 08/10/2019 17:37 ▼ Type Start [Ahsay0BM v8.3.0.0] Saving encrypted backup set encryption keys to Start Backup[In-File Delta: Full] Using Temporary Directory /Users/admin/.obm/ Start nunning pre-commands Finished running pre-commands Downloading server file list Downloading server file list Downloading server file list Downloading server file list New Directory] Potos [New File] 10% of 'Photos/TestyPC-2.jpg" [New File] 20% of 'Photos/TestyPC-2.jpg" [New File] 20% of 'Photos/TestyPC-2.jpg" [New File] 20% of 'Photos/TestyPC-2.jpg" [New File] 50% of 'Photos/TestyPC-2.jpg" [New File] 50% of 'Photos/TestyPC-2.jpg" [New File] 50% of 'Photos/TestyPC-2.jpg"	Rackup Roport Log server	Show All Time 08/10/2019 17:37:14 08/10/2019 17:37:15 08/10/2019 17:37:17 08/10/2019 17:37:17 08/10/2019 17:37:18 08/10/2019 17:37:18 08/10/2019 17:37:19 08/10/2019 17:37:21 08/10/2019 17:37:22 08/10/2019 17:37:23 08/10/2019 17
	Log 08/10/2019 17:37 ▼ Type Start [Ahsay0BM v8.3.0.0] Saving encrypted backup set encryption keys to Start Backup[In-File Delta: Full] Using Temporary Directory /Users/admin/.obm/ Start nunning pre-commands Finished running pre-commands Downloading server file list Downloading server file list Downloading server file list Downloading server file list New Directory] Potos [New File] 10% of 'Photos/TestyPC-2.jpg" [New File] 20% of 'Photos/TestyPC-2.jpg" [New File] 20% of 'Photos/TestyPC-2.jpg" [New File] 20% of 'Photos/TestyPC-2.jpg" [New File] 50% of 'Photos/TestyPC-2.jpg" [New File] 50% of 'Photos/TestyPC-2.jpg" [New File] 50% of 'Photos/TestyPC-2.jpg"	Rackup Roport Log server	Show All Time 08/10/2019 17:37:14 08/10/2019 17:37:17 08/10/2019 17:37:18 08/10/2019 17:37:18 08/10/2019 17:37:18 08/10/2019 17:37:18 08/10/2019 17:37:18 08/10/2019 17:37:18 08/10/2019 17:37:18 08/10/2019 17:37:19 08/10/2019 17:37:21 08/10/2019 17:37:21 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:24 08/10/2019 17:37:25
	Log 08/10/2019 17:37 ▼ Type Start [Ahsay0BM v8.3.0.0] Saving encrypted backup set encryption keys to Start Backup[In-File Delta: Full] Using Temporary Directory /Users/admin/.obm/ Start nunning pre-commands Finished running pre-commands Downloading server file list Downloading server file list Downloading server file list Downloading server file list New Directory] Potos [New File] 10% of 'Photos/TestyPC-2.jpg" [New File] 20% of 'Photos/TestyPC-2.jpg" [New File] 20% of 'Photos/TestyPC-2.jpg" [New File] 20% of 'Photos/TestyPC-2.jpg" [New File] 50% of 'Photos/TestyPC-2.jpg" [New File] 50% of 'Photos/TestyPC-2.jpg" [New File] 50% of 'Photos/TestyPC-2.jpg"	Rackup Roport Log server	Show All Time 08/10/2019 17:37:14 08/10/2019 17:37:17 08/10/2019 17:37:18 08/10/2019 17:37:18 08/10/2019 17:37:18 08/10/2019 17:37:18 08/10/2019 17:37:18 08/10/2019 17:37:18 08/10/2019 17:37:18 08/10/2019 17:37:19 08/10/2019 17:37:21 08/10/2019 17:37:21 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:24 08/10/2019 17:37:25
	Log 08/10/2019 17:37 ▼ Type Start [Ahsay0BM v8.3.0.0] Saving encrypted backup set encryption keys to Start Backup[In-File Delta: Full] Using Temporary Directory /Users/admin/.obm/ Start nunning pre-commands Finished running pre-commands Downloading server file list Downloading server file list Downloading server file list Downloading server file list New Directory] Potos [New File] 10% of 'Photos/TestyPC-2.jpg" [New File] 20% of 'Photos/TestyPC-2.jpg" [New File] 20% of 'Photos/TestyPC-2.jpg" [New File] 20% of 'Photos/TestyPC-2.jpg" [New File] 50% of 'Photos/TestyPC-2.jpg" [New File] 50% of 'Photos/TestyPC-2.jpg" [New File] 50% of 'Photos/TestyPC-2.jpg"	Rackup Roport Log server	Show All Time 08/10/2019 17:37:14 08/10/2019 17:37:17 08/10/2019 17:37:18 08/10/2019 17:37:18 08/10/2019 17:37:18 08/10/2019 17:37:18 08/10/2019 17:37:18 08/10/2019 17:37:18 08/10/2019 17:37:18 08/10/2019 17:37:19 08/10/2019 17:37:21 08/10/2019 17:37:21 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:23 08/10/2019 17:37:24 08/10/2019 17:37:25

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

From	n		13		7	То	li li	201		-	5.5	
01	~	Oct	~	2019	~	31	~	Oct	~	2019	~	Go

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

From 01 V Feb V 2019 V	To 01 ✔ Mar ✔ 2019 ✔ Go
Report Backup Restore	AhsayOBM Backup Report From To To 01 V Oct V 2019 V O5 V Oct V 2019 V Go Backup set V Destination V Completion Status V
	No records found
	No. of records per page 50 🗸 Page – 🗸
	Close

7 Restoring with a Cloud File Backup Set

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

Local machine

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

Original location

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

Alternate location

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

NOTE Login to the AhsayOBM application according to the instruction provided in the chapter on <u>Log in to</u> <u>AhsayOBM</u>.

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.

	Ahsa	OBM		
Select	The Destination	n From	Which	To Re
	Client Run Cloud File Backup			
	G AhsayCBS Host: 10.90.10.14:443			
				Previous Cancel

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

Select what to restore Choose from files as of job 08/10/2019 Latest Folders Name Size Date modified
▼ ● AhsayCBS ♥ ■ TestPG-1.jpg 516 KB 05/03/2019 15:32 ♥ ● Photos ♥ ■ TestPG-2.jpg 516 KB 05/03/2019 15:32 ▶ ■ TestFiles ♥ ■ TestPG-3.jpg 516 KB 05/03/2019 15:32 ♥ ■ TestFiles ♥ ■ TestPG-3.jpg 516 KB 05/03/2019 15:32 ♥ ■ TestPG-5.jpg 516 KB 05/03/2019 15:32 ♥ ■ TestPG-5.jpg 516 KB 05/03/2019 15:32 ♥ ■ TestPG-2.png 516 KB 05/03/2019 15:32 ♥ ■ TestPG-3.png 516 KB 05/03/2019 15:32
▼ ● AhsayCBS ♥ ■ TestPG-1.jpg 516 KB 05/03/2019 15:32 ♥ ● Photos ♥ ■ TestPG-2.jpg 516 KB 05/03/2019 15:32 ▶ ■ TestFiles ♥ ■ TestPG-3.jpg 516 KB 05/03/2019 15:32 ♥ ■ TestFiles ♥ ■ TestPG-3.jpg 516 KB 05/03/2019 15:32 ♥ ■ TestPG-5.jpg 516 KB 05/03/2019 15:32 ♥ ■ TestPG-5.jpg 516 KB 05/03/2019 15:32 ♥ ■ TestPG-2.png 516 KB 05/03/2019 15:32 ♥ ■ TestPG-3.png 516 KB 05/03/2019 15:32
☑ TestPNG-5.png 516 KB 05/03/2019 15:32 ☑ TestTIFF-1.tiff 516 KB 05/03/2019 15:32 ☑ TestTIFF-3.tiff 516 KB 05/03/2019 15:32 ☑ TestTIFF-3.tiff 516 KB 05/03/2019 15:32 ☑ TestTIFF-4.tiff 516 KB 05/03/2019 15:32 ☑ TestTIFF-5.tiff 516 KB 05/03/2019 15:32

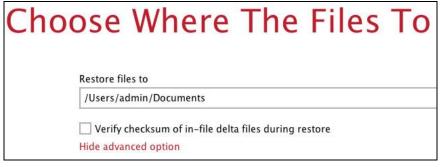
5. Select **Restore to local computer** if you want to restore the backed-up data to the location computer. Click **Next** to continue.

		Be Restored
Select what to restore		
Choose from files as of job	o ♥ 08/10/2019 ♥ Latest ♥	
Folders	Name	Size Date modified
G AhsayCBS	🖉 🗟 TestJPG-1.jpg	516 KB 05/03/2019 15:32
Photos	🗹 🗟 TestJPG-2.jpg	516 KB 05/03/2019 15:32
TestFiles	🗹 🚡 TestJPG-3.jpg	516 KB 05/03/2019 15:32
	🗹 👼 TestJPG-4.jpg	516 KB 05/03/2019 15:32
	🗹 🚡 TestJPG-5.jpg	516 KB 05/03/2019 15:32
	🗹 👼 TestPNG-1.png	516 KB 05/03/2019 15:32
	🗹 💼 TestPNG-2.png	516 KB 05/03/2019 15:32
	🗹 👼 TestPNG-3.png	516 KB 05/03/2019 15:32
	🗹 📓 TestPNG-4.png	516 KB 05/03/2019 15:32
	🗹 👼 TestPNG-5.png	516 KB 05/03/2019 15:32
	🗹 🗟 TestTIFF-1.tiff	516 KB 05/03/2019 15:32
	🗹 🗟 TestTIFF-2.tiff	516 KB 05/03/2019 15:32
	🗹 📓 TestTIFF-3.tiff	516 KB 05/03/2019 15:32
	🗹 🚡 TestTIFF-4.tiff	516 KB 05/03/2019 15:32
	🗹 🗟 TestTIFF-5.tiff	516 KB 05/03/2019 15:32
Restore to local computies	ter Items p	er page 50 V Page 1/1 V
· · · · · · · · · · · · · · · · · · ·	NOTE CONTRACTOR OF	

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



Click Show advanced option to configure other restore settings.



• Verify checksum of in-file delta files during restore

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

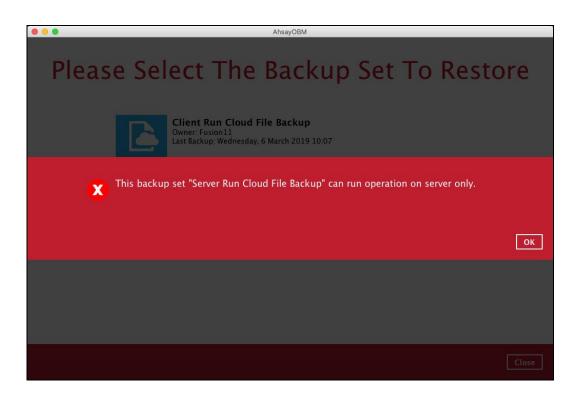
7. Select the temporary directory for storing temporary files.

• • •	AhsayOBM
	Temporary Directory
	Temporary directory for storing restore files
	/Users/admin/.obm/temp Browse
	Previous Restore Cancel

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

• • •	AhsayOBM				
Restore					
Client R	un Cloud File Backup				
C Restore	i (Host: 10.90.10.14:443) e Completed Successfully time left 0 sec	لم			
Restored Elapsed ti Transfer r					
		Close			

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.



8 Contacting Ahsay

8.1 Technical Assistance

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

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

8.2 Documentation

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

You can send us suggestions for improvements or report on issues in the documentation by contacting us at:

https://www.ahsay.com/partners/

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