Ahsay Backup

Ahsay Cloud Backup Suite v9

Run on Server (Agentless) Cloud File Backup & Restore Guide

Ahsay Systems Corporation Limited

6 May 2022

www.ahsay.com

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

Copyright Notice

Trademarks

Disclaimer

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

Revision History

Date	Descriptions	Version
25 January 2022	▪ Ch. 3 – added editing deduplication setting as optional step	9.1.0.0
18 March 2022	▪ Ch. 1.4 – removed space freeing up ▪ Ch. 2.8 – added space freeing up limitation	9.1.0.0
6 May 2022	▪ Ch. 2.8 – removed backup source selection limitation ▪ Ch. 3 – updated screenshot to show root folder selection is supported	9.1.4.0

Table of Contents

1 Overview

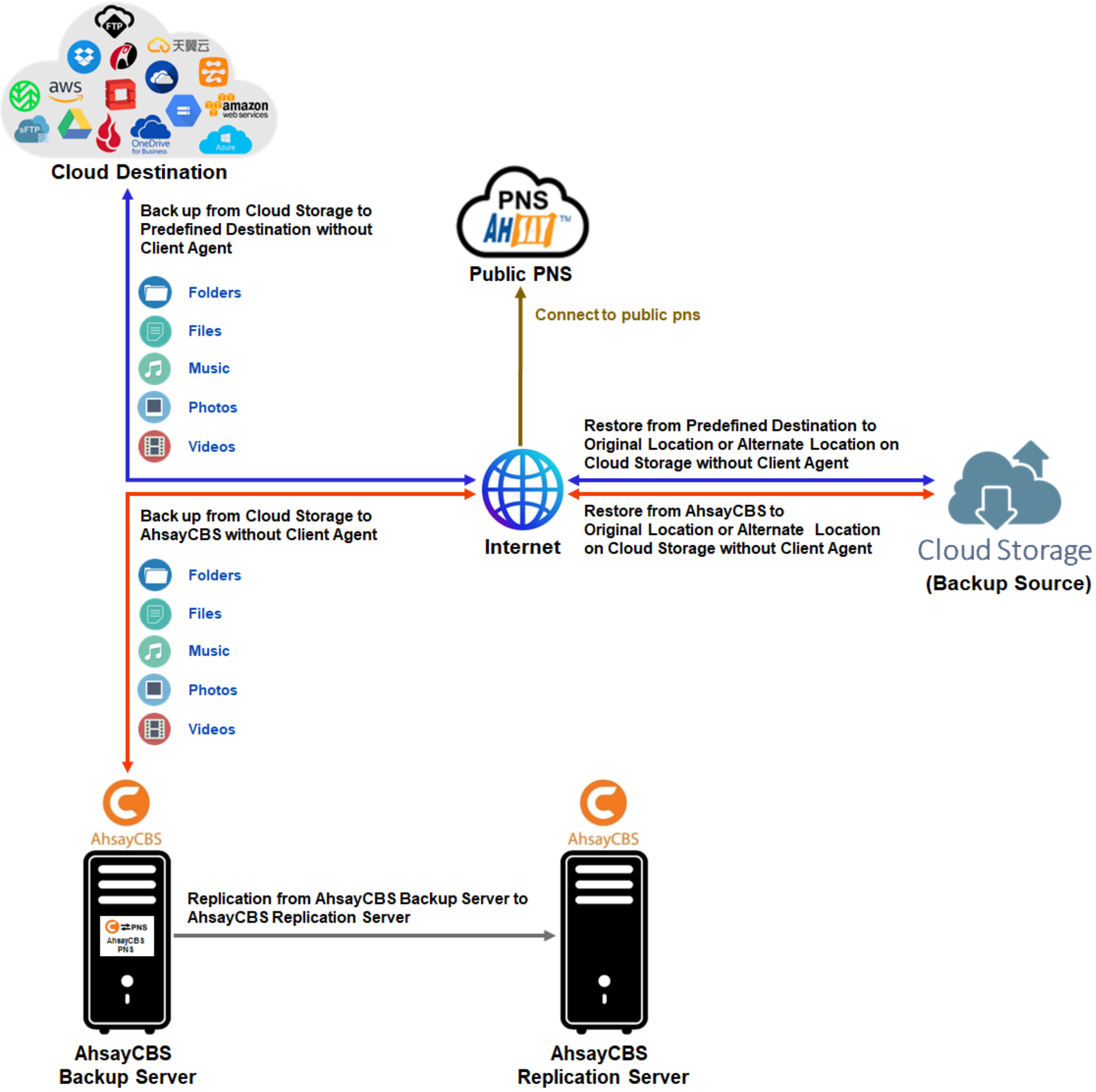
1.1 What is this software?

Ahsay Cloud Backup Suite v9 allows you to back up your data stored on the cloud storage to either the AhsayCBS backup server or another cloud. You can access the AhsayCBS server environment easily on a web-based management console. This is a user interface that allows you to log in remotely to a backup server to manage and monitor your backups.

1.2 System Architecture

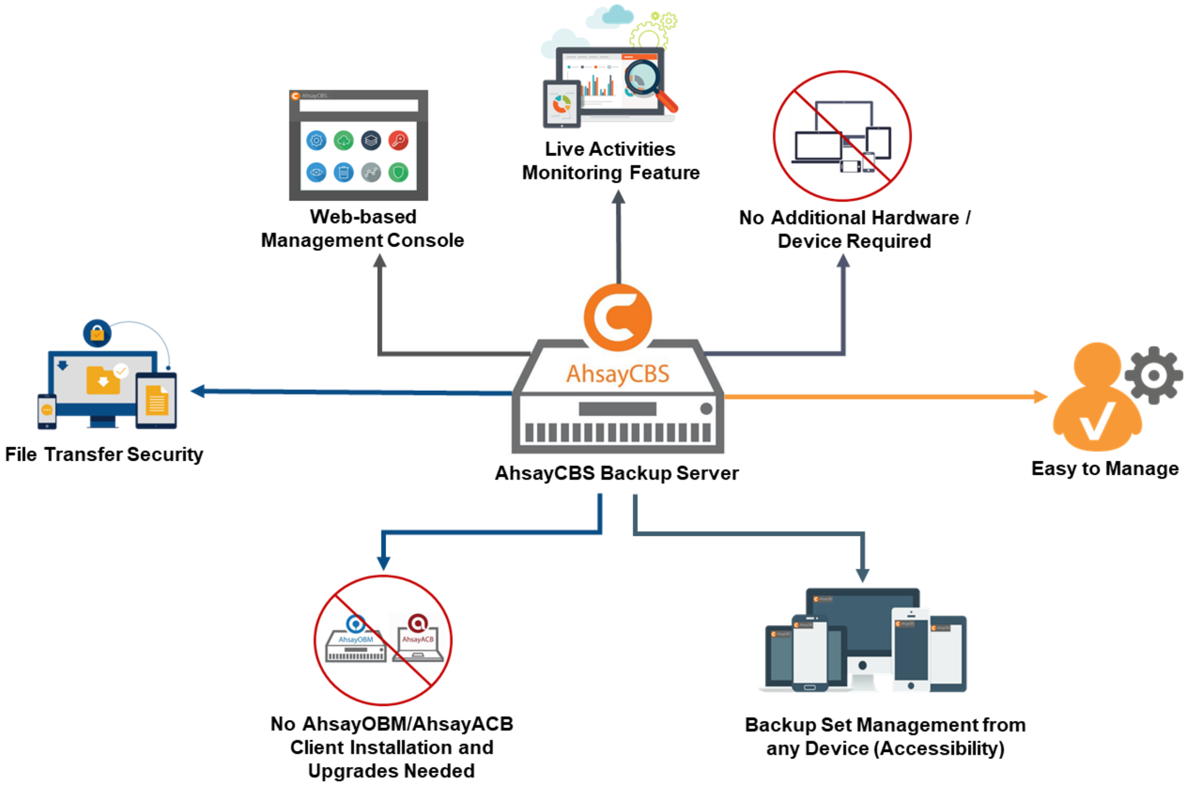
For agentless backup and restore, the AhsayCBS backup server connects to the cloud storage directly through the internet without the need to deploy additional backup agents on the customer's site.

Below is the system architecture diagram illustrating the major elements involved in the backup and restore process using AhsayCBS Run on Server (Agentless) backup configuration.


Cloud Destination
Back up from Cloud Storage to Predefined Destination without Client Agent
Folders
Files
Music
Photos
Videos
PNS
Public PNS
Connect to public pns
Restore from Predefined Destination to Original Location or Alternate Location on Cloud Storage without Client Agent
Internet
Restore from AhsayCBS to Original Location or Alternate Location on Cloud Storage without Client Agent
Cloud Storage
(Backup Source)
Back up from Cloud Storage to AhsayCBS without Client Agent
Folders
Files
Music
Photos
Videos
AhsayCBS
Replication from AhsayCBS Backup Server to AhsayCBS Replication Server
AhsayCBS
AhsayCBS Backup Server
AhsayCBS Replication Server

1.3 Why should I use AhsayCBS Run on Server (Agentless) Solution to back up my cloud data?

We are committed to bringing you a comprehensive Run on Server (Agentless) cloud backup and recovery solution with AhsayCBS. Below are some key areas that can help make your backup experience a better one.


Live Activities Monitoring Feature
Web-based Management Console
No Additional Hardware / Device Required
AhsayCBS
File Transfer Security
AhsayCBS Backup Server
Easy to Manage
AhsayOBM
AhsayACB
No AhsayOBM/AhsayACB Client Installation and Upgrades Needed
Backup Set Management from any Device (Accessibility)

Web-based Management Console

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

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

Live Activities Monitoring Feature

The AhsayCBS User Web Console has a live activities monitoring feature which is used to keep track of the backup and restore job(s). The following operations can be performed using this feature:

- View the status of the backup process that is currently running
- View the status of the restore process that is currently running

> **NOTE**
>
> There is an update interval of around 5 seconds for both backup and restore activities.

No Additional Hardware / Device Required

As the Run on Server (agentless) backup set utilizes the resources of the AhsayCBS backup server, there is no need to provision additional physical or virtual machine to run the backup/restore, which means the cost of each backup set is much lower than for an agent-based cloud file backup set.

Easy to Manage

The AhsayCBS User Web Console offers you an easy-to-manage user interface. This will help you save time, and it reduces the overall cost of support.

Backup Set Management from any Device (Accessibility)

Backup/restore operation(s), backup set settings configuration, and backup/restore process monitoring can be done from any device as long as a web browser and internet connection are present in the device.

No AhsayOBM/AhsayACB Client Installation and Upgrades Needed

Upgrading when a newer version becomes available is not necessary, as long as the AhsayCBS server version is upgraded by the backup service provider.

File Transfer Security

The AhsayCBS comes with a secure file transfer method using the https protocol that guarantees a highest level of security measure in safeguarding the movement of files from the backup source (cloud storage) to the backup destination (AhsayCBS server).

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.**

Compliance

Some organizations do not permit the installation of third-party applications on the production environments due to regulatory requirements. An agentless backup and recovery solution allow for compliance during backup or restore.

Less Resources Needed

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.

Cloud Destinations Backup

By default, the AhsayCBS is set as the storage destination in creating a cloud file backup set. However, you have the option of selecting another storage destination as provided by your backup service provider. Below is a list of supported cloud destinations:

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

NOTE

For more details, please contact your backup service provider.

Run on Server

A Run on Server Cloud File Backup Set provides you with an agentless backup solution. Manual or scheduled backup job is performed directly on the AhsayCBS backup server. You do not need to install a backup agent on your personal computer in order to back up your data on cloud storage(s).

Run on Server backup and restore can be managed on a computer or device running on Windows/MacOS/Linux /iOS/Android as long as the device is able to support a web browser and has an internet connection.

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

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

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

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

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

NOTE

For more details on the Run on Client backup option, please refer to the following guides:

AhsayOBM v9 User Guide – Cloud File Backup & Restore for Windows

AhsayOBM v9 User Guide – Cloud File Backup & Restore for Mac

AhsayACB v9 User Guide – Cloud File Backup & Restore for Windows

AhsayACB v9 User Guide – Cloud File Backup & Restore for Mac

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 Server Cloud File backup and restore, followed by step-by-step instructions on a creating a backup set, running a backup, restoring backup data, running a data integrity check and deleting backup data using the AhsayCBS User Web Console.

The document can be divided into six (6) main parts.

Part 1: Preparing for Cloud File Backup & Restore

Requirements
Requirements in setting up AhsayCBS User Web Console

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 AhsayCBS User Web Console
Log in to AhsayCBS User Web Console

Creating a Backup Set
Create a backup set using AhsayCBS User Web Console

Running a Backup Set
Run a backup set using AhsayCBS User Web Console

Part 3: Restoring a Cloud File Backup

Restoring a Backup Set using AhsayCBS User Web Console
Restore a backup set using AhsayCBS User Web Console

Part 4: Running a Data Integrity Check

Running a Data Integrity Check using AhsayCBS User Web Console
Run a data integrity check using AhsayCBS User Web Console

Part 5: Deleting Backup Data

Deleting a Backup Data using AhsayCBS User Web Console
Delete a backup data using AhsayCBS 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 User Web Console, as well as to carry out an end-to-end backup and restore process, and to be instructed about the other actions that can be performed through the User Web Console (i.e., Data Integrity Check and Delete Backup Data).

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.

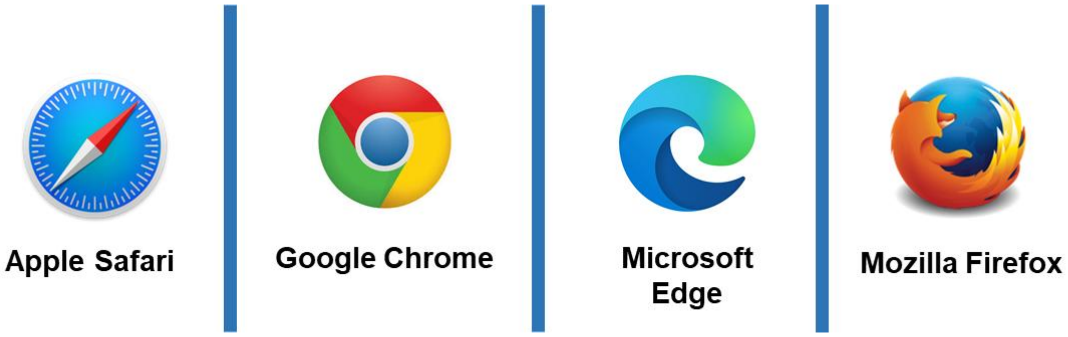
2 Preparing for Backup and Restore

2.1 Internet / Network Connection

In order to access the AhsayCBS backup server through the web-based management console, make sure you have an Internet connection or LAN access to the internal AhsayCBS server.

2.2 Supported Browsers

The AhsayCBS User Web Console runs in all major web browsers. Please make sure that you are using the latest version of the browser.



> **NOTE**
>
> Ensure to always allow pop-up windows in your web browser.

2.3 Valid AhsayOBM/AhsayACB User Account

A valid AhsayOBM/AhsayACB user account is required before you can access the AhsayCBS User Web Console. Please contact your system administrator for more details.

2.4 Ahsay License Requirements

◉ Licenses

Licenses are calculated on a per device basis for AhsayOBM and AhsayACB. For Agentless, to be able to back up using the AhsayCBS User Web Console, one AhsayOBM or AhsayACB license is required.

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

For more details, please contact your backup service provider.

2.5 Add-on Module Requirements

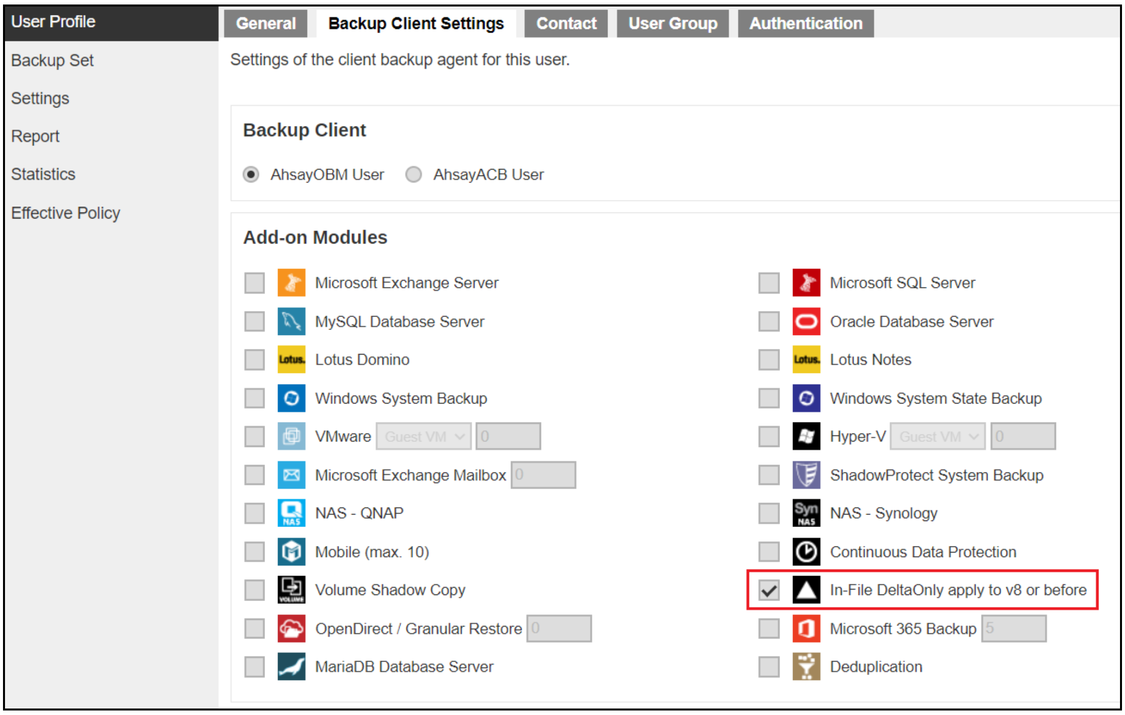
◉ In-File Delta

The In-File Delta add-on module must be added on the AhsayOBM/AhsayACB user account if you would like to use this feature. This only applies to backup sets created using AhsayOBM/AhsayACB v8 or before.

NOTE

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

For AhsayOBM user account


User Profile | Backup Set | Settings | Report | Statistics | Effective Policy

General | **Backup Client Settings** | Contact | User Group | Authentication

Settings of the client backup agent for this user.

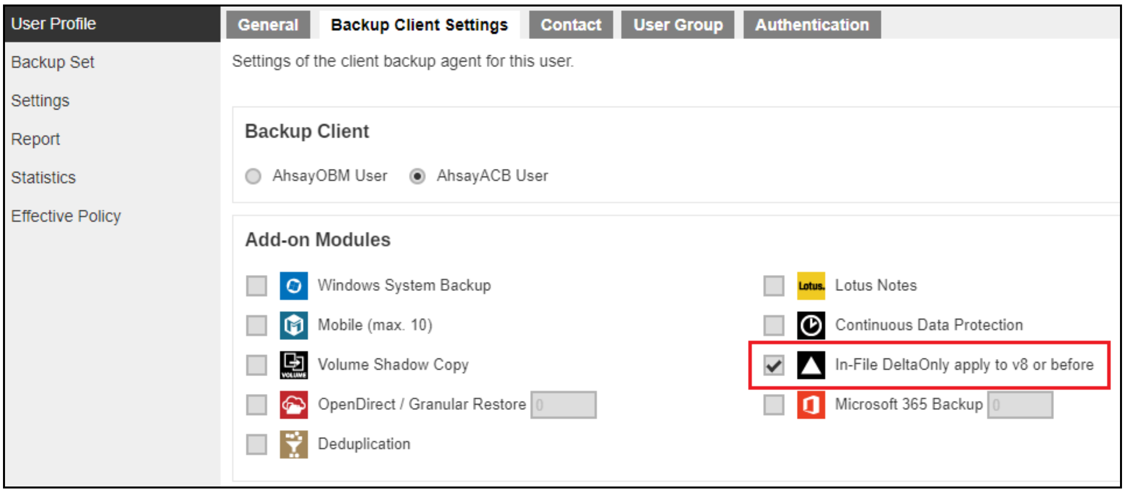
Backup Client

● AhsayOBM User ○ AhsayACB User

Add-on Modules

□ Microsoft Exchange Server	□ Microsoft SQL Server
□ MySQL Database Server	□ Oracle Database Server
□ Lotus Domino	□ Lotus Notes
□ Windows System Backup	□ Windows System State Backup
□ VMware Guest VM 0	□ Hyper-V Guest VM 0
□ Microsoft Exchange Mailbox 0	□ ShadowProtect System Backup
□ NAS - QNAP	□ NAS - Synology
□ Mobile (max. 10)	□ Continuous Data Protection
□ Volume Shadow Copy	☑ In-File DeltaOnly apply to v8 or before
□ OpenDirect / Granular Restore 0	□ Microsoft 365 Backup 5
□ MariaDB Database Server	□ Deduplication

For AhsayACB user account


User Profile | Backup Set | Settings | Report | Statistics | Effective Policy

General | **Backup Client Settings** | Contact | User Group | Authentication

Settings of the client backup agent for this user.

Backup Client

○ AhsayOBM User ● AhsayACB User

Add-on Modules

□ Windows System Backup	□ Lotus Notes
□ Mobile (max. 10)	□ Continuous Data Protection
□ Volume Shadow Copy	☑ In-File DeltaOnly apply to v8 or before
□ OpenDirect / Granular Restore 0	□ Microsoft 365 Backup 0
□ Deduplication	

Backup Quota Requirement

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

2.6 Cloud Sources

The AhsayCBS Run on Server (Agentless) Backup Solution supports the following cloud sources to back up as provided by your backup service provider:

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

2.7 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.

2.8 Limitations

Standard and Local Destination Settings

For the backup destination settings, only the AhsayCBS and predefined destination is supported in the AhsayCBS Run on Server (Agentless) backup. It is not possible to assign other standard destinations such as the customer’s personal Google Drive, OneDrive, Dropbox, Amazon S3, Microsoft Azure, etc. storage accounts as the backup destination for a Run on Server backup set.

Multiple Destinations Not Supported

AhsayCBS Run on Server (Agentless) backup is restricted to only one backup destination, either AhsayCBS or a Predefined destination.

Command Line Tool

An agent-based (AhsayOBM) backup has a command line tool feature that allows user to configure a pre and/or post-backup command which can be an operating system level command, script or batch file, or third-party utilities that will run before and/or after a backup job. In the AhsayCBS Run on Server (Agentless) backup, this feature is not supported.

- **Reminder**

  The reminder feature is not supported in the AhsayCBS User Web Console. Unlike with the agent-based backup, when this feature is enabled, a backup confirmation dialog box will prompt the user to run a backup job during machine log off, restart or shut down when the AhsayOBM/AhsayACB client is installed on a Windows platform.

- **Restore Filter**

  Restore filter feature is not supported in the AhsayCBS User Web Console which allows users to search directories, files, and/or folders to restore.

- **IP Allowed for Restore**

  This setting permits to predefine IP ranges that are allowed to perform restore as configured by the system administrator. This feature is only applicable in a Run on Client Cloud File restore operation and is not supported in a Run on Server Cloud File restore.

- **Space Freeing Up**

  Space freeing up feature is used to remove obsolete file(s) from your backup set and destination. This feature is only applicable in a Run on Client Cloud File Backup Set and is not supported in a Run on Server Cloud File Backup Set.

- **Decrypt Backup Data**

  Decrypt backup data feature is used to restore raw data by using the data encryption key that was set for the backup set. This feature is only applicable in a Run on Client Cloud File Backup Set and is not supported in a Run on Server Cloud File Backup.

- **System Logs**

  AhsayOBM/AhsayACB backup user account does not have access to the system logs related to the data integrity check operations through the AhsayCBS user console.

  Therefore, the backup user does not have the ability to verify the results of the data integrity check without the assistance of the backup service provider.

2.9 Best Practices and Recommendations

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

- **Bucket Management for Enterprise Cloud Storage Providers**

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

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

Test Restore Operations

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

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 that may be added etc.

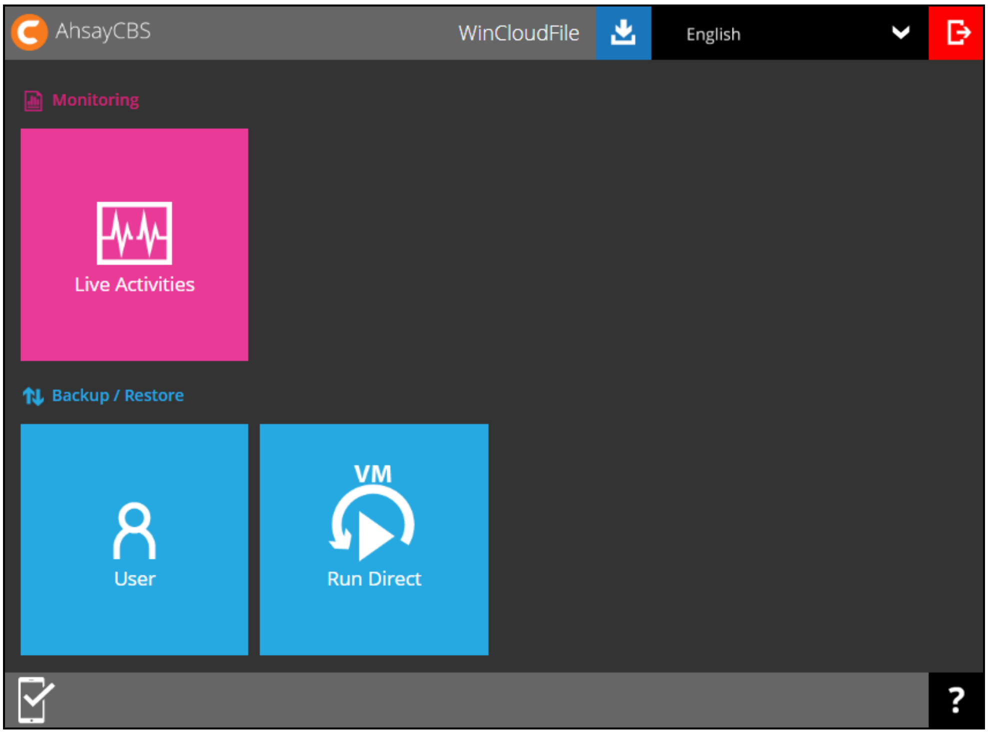
Consider the following key points to efficiently handle backup sets with periodic backup schedule.

- 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.

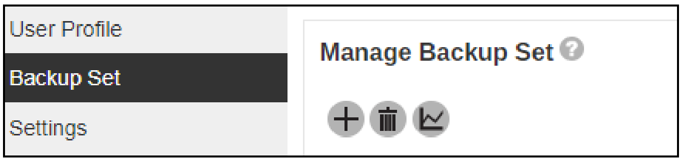
3 Creating a Cloud File Backup Set

1. Log in to the User Web Console. For instructions on how to do this please refer to Chapter 2 of the AhsayCBS v9 User Guide.

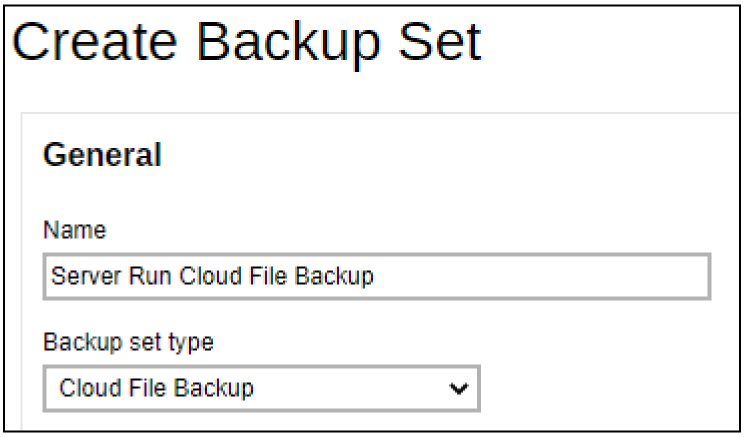
2. Click the **User** icon on the User Web Console landing page.



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



Create Backup Set

General

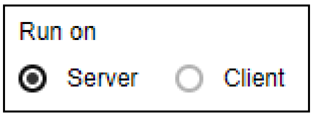
Name

Server Run Cloud File Backup

Backup set type

Cloud File Backup

5. On the same menu under **Run on**, select **Server** to create a run on server (agentless backup) cloud file backup set.



Run on

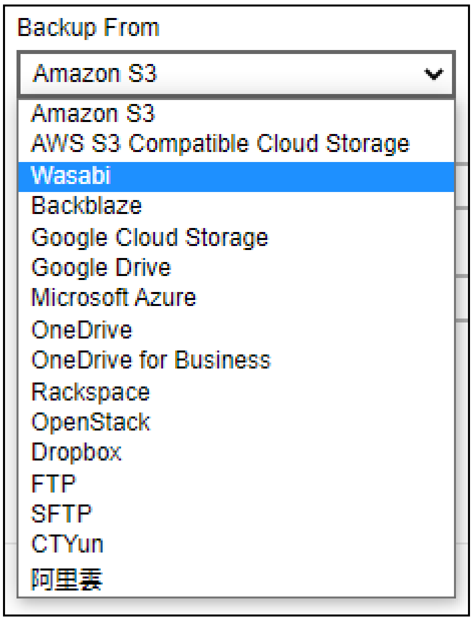
● Server ○ Client

6. If you choose to run the backup set on the AhsayCBS server, you won't be able to back up, restore or manage your backups on the AhsayOBM/AhsayACB client once the backup set is created.

NOTE

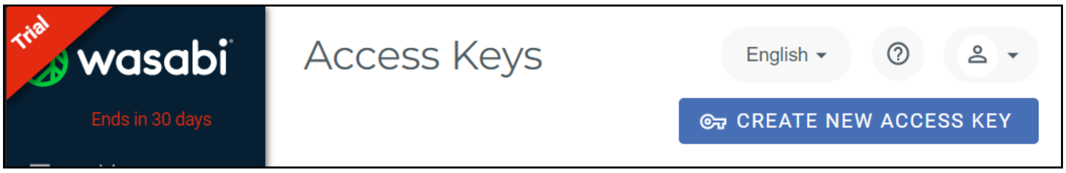
This setting **CANNOT** be altered once the backup set is created. If you wish to change the backup method later, you will have to create a new backup set and start over the configurations again.

7. Under the **Backup From**, select the cloud storage (e.g. Wasabi) that contains the data that you want to back up.

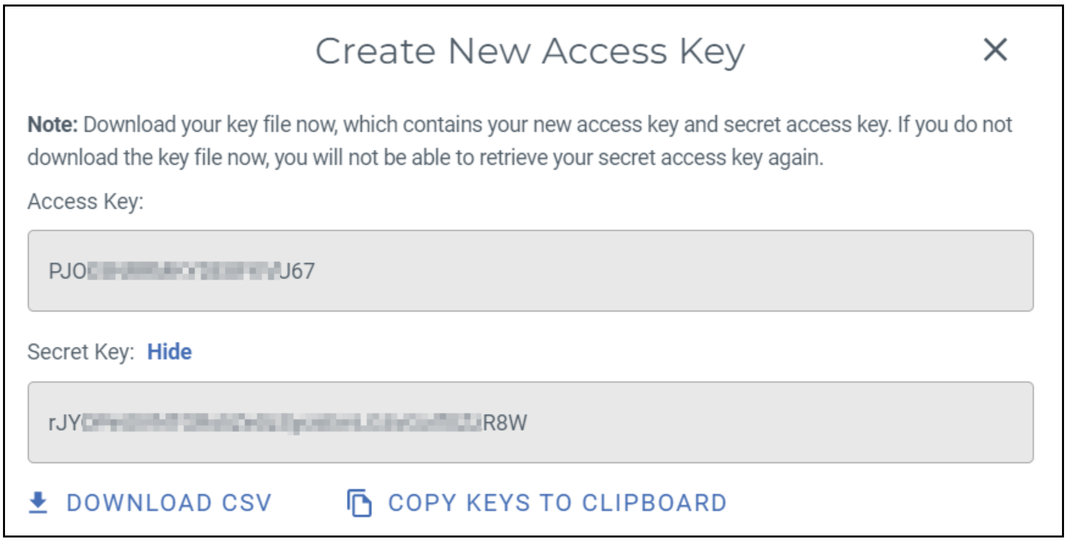


Backup From

8. On the Wasabi webpage, create a new access key (if you do not have an existing one).



9. Copy and paste the **Access Key** and **Secret Key** to the web console to authenticate AhsayCBS to access the cloud storage, then click **Test** to complete the authentication setup. If you do not have a Wasabi account, click **Sign up for Wasabi**.



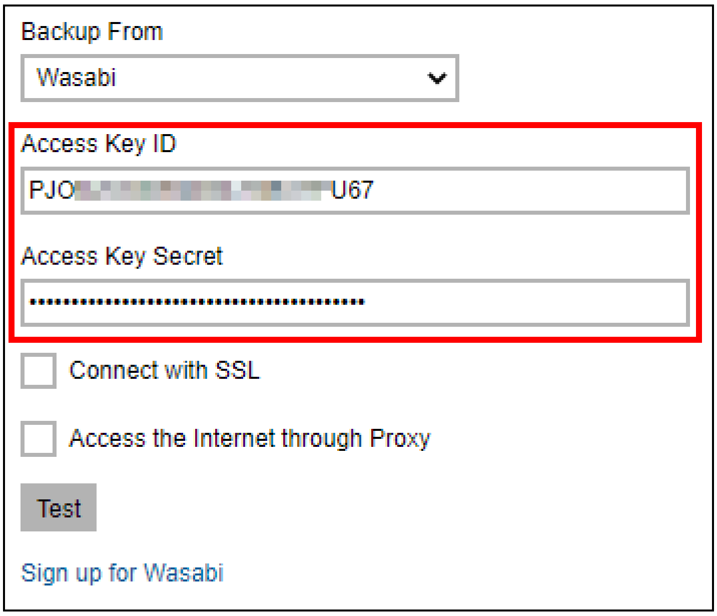
Create New Access Key

Note: Download your key file now, which contains your new access key and secret access key. If you do not download the key file now, you will not be able to retrieve your secret access key again.

Access Key: PJO[redacted]U67

Secret Key: Hide

rJY[redacted]R8W



Backup From: Wasabi

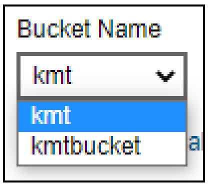
Access Key ID: PJO[redacted]U67

Access Key Secret: ••

□ Connect with SSL

□ Access the Internet through Proxy

10. Below the **Test** button, make sure to select the corresponding bucket name that contains the cloud data that you want to back up. Click **Next** to proceed.

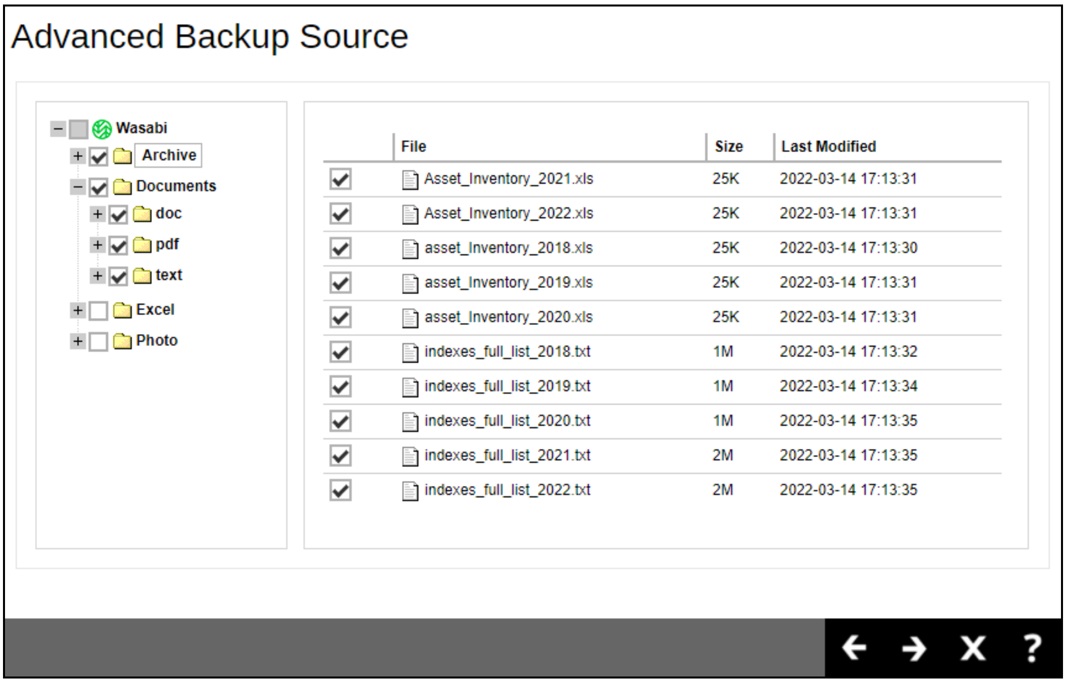


Bucket Name: kmt

NOTES

1. 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.
2. It is advised to have one (1) bucket name per cloud file backup set.

11. In the Advanced Backup Source, select the file(s) and/or folder(s) that you want to back up then click **Next** to proceed.



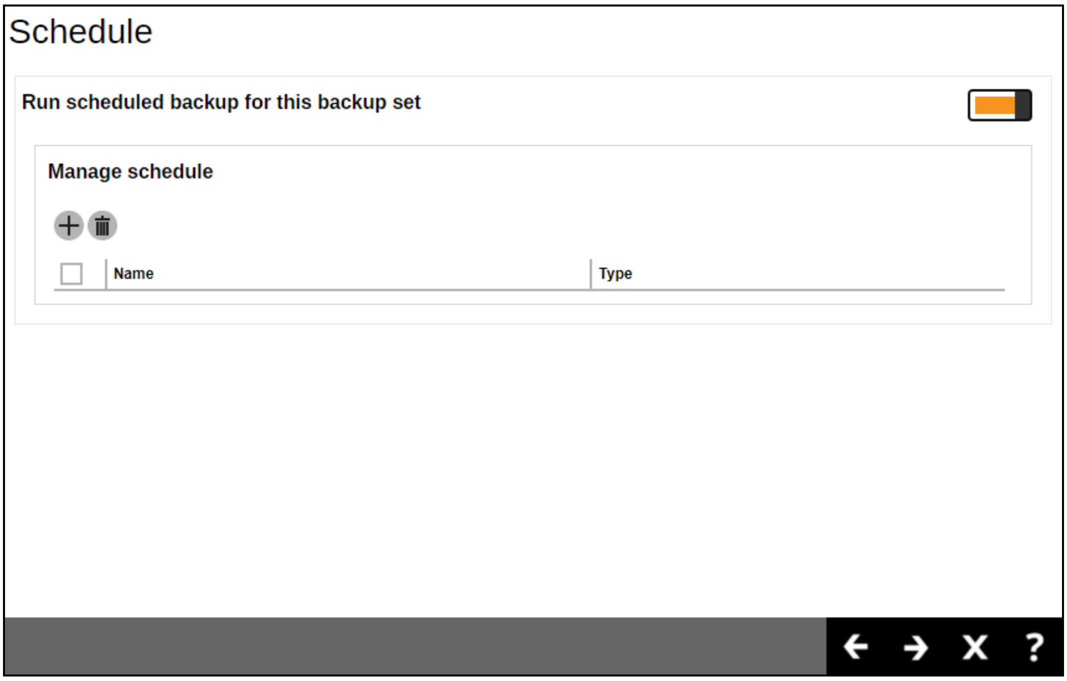
Advanced Backup Source

- ☐ Wasabi
  - ☑ Archive
  - ☑ Documents
    - ☑ doc
    - ☑ pdf
    - ☑ text
  - ☐ Excel
  - ☐ Photo

	File	Size	Last Modified
☑	Asset_Inventory_2021.xls	25K	2022-03-14 17:13:31
☑	Asset_Inventory_2022.xls	25K	2022-03-14 17:13:31
☑	asset_Inventory_2018.xls	25K	2022-03-14 17:13:30
☑	asset_Inventory_2019.xls	25K	2022-03-14 17:13:31
☑	asset_Inventory_2020.xls	25K	2022-03-14 17:13:31
☑	indexes_full_list_2018.txt	1M	2022-03-14 17:13:32
☑	indexes_full_list_2019.txt	1M	2022-03-14 17:13:34
☑	indexes_full_list_2020.txt	1M	2022-03-14 17:13:35
☑	indexes_full_list_2021.txt	2M	2022-03-14 17:13:35
☑	indexes_full_list_2022.txt	2M	2022-03-14 17:13:35

12. In the **Schedule** menu, configure a backup schedule for the backup job to run automatically at your specified time interval. If the **Run scheduled backup for this backup set** is off, switch it **On**.

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



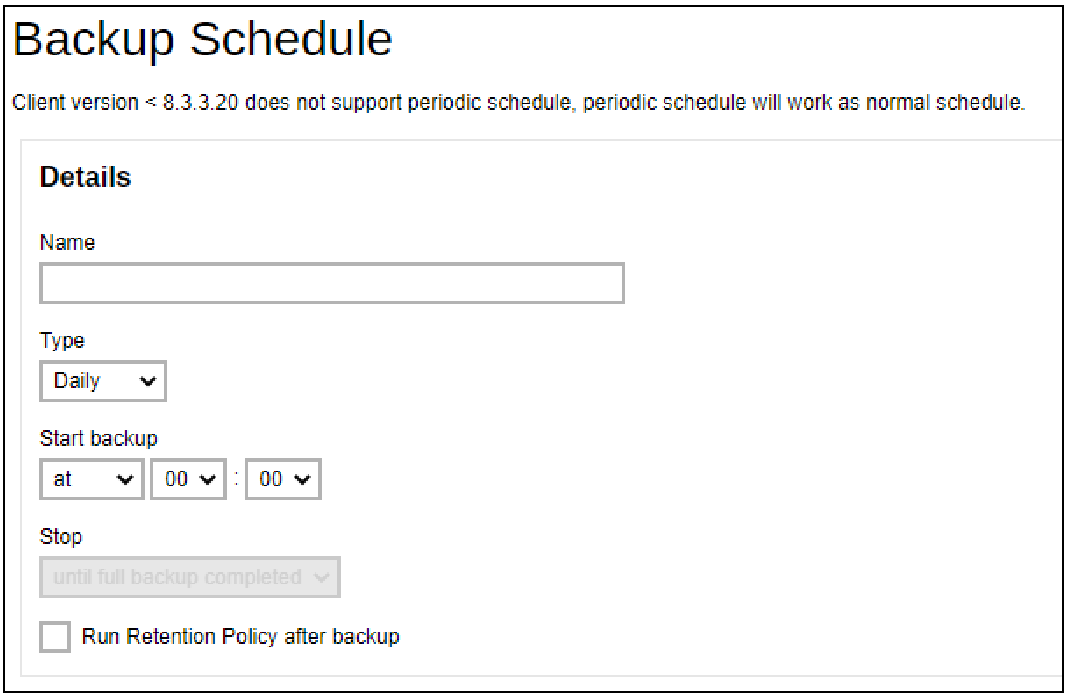
Schedule

Run scheduled backup for this backup set

Manage schedule

☐	Name	Type

The Backup Schedule window will appear.



Backup Schedule

Client version < 8.3.3.20 does not support periodic schedule, periodic schedule will work as normal schedule.

Details

Name

Type: Daily

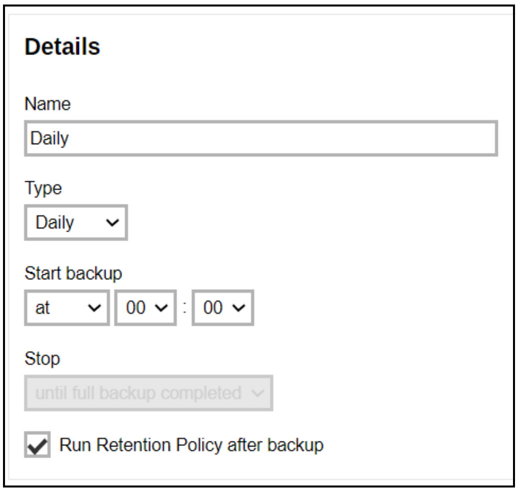
Start backup: at 00 : 00

Stop: until full backup completed

□ Run Retention Policy after backup

Configure the following backup schedule settings:

- **Name** – the name of the backup schedule.
- **Type** – the type of the backup schedule. There are four (4) different types of backup schedule: Daily, Weekly, Monthly and Custom.
  - **Daily** – the time of the day or interval in minutes/hours when the backup job will run.



Details

Name: Daily

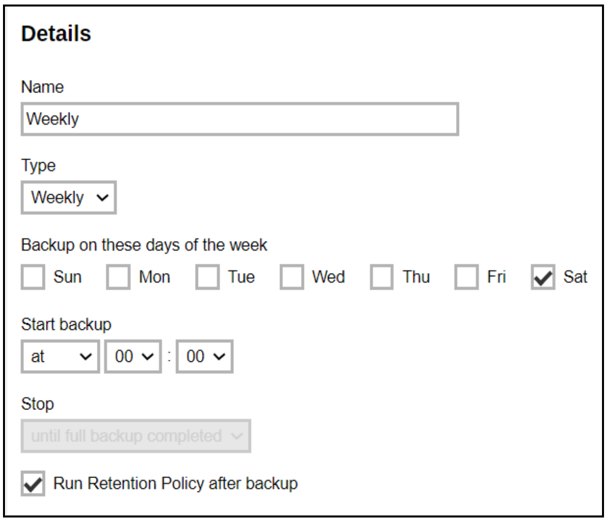
Type: Daily

Start backup: at 00 : 00

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.



Details

Name

Weekly

Type

Weekly

Backup on these days of the week

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

Start backup

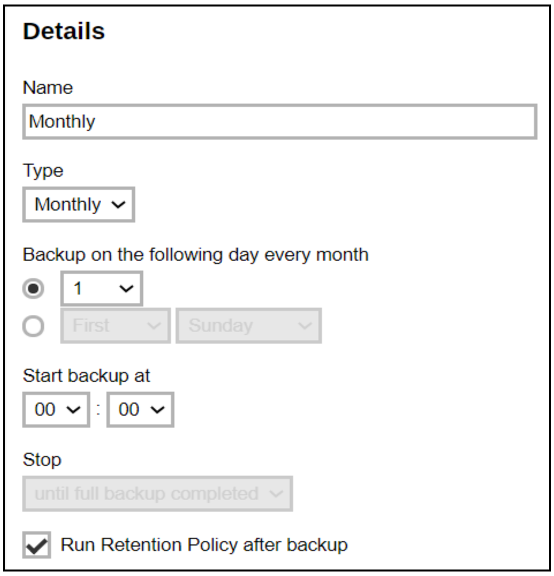
at 00 : 00

Stop

until full backup completed

☑ Run Retention Policy after backup

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



Details

Name

Monthly

Type

Monthly

Backup on the following day every month

● 1

○ First Sunday

Start backup at

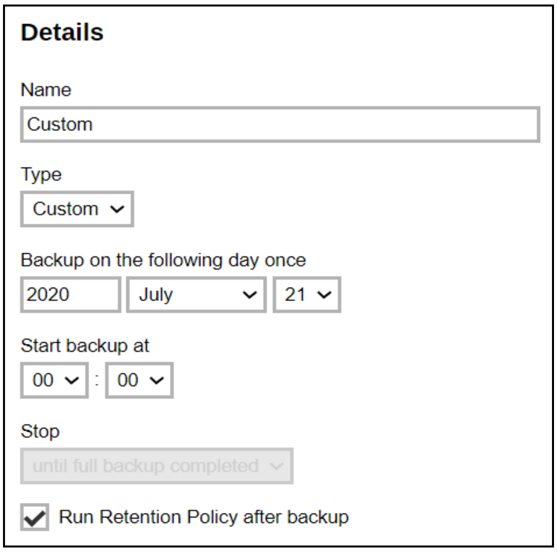
00 : 00

Stop

until full backup completed

☑ Run Retention Policy after backup

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



Details

Name

Custom

Type

Custom

Backup on the following day once

2020 July 21

Start backup at

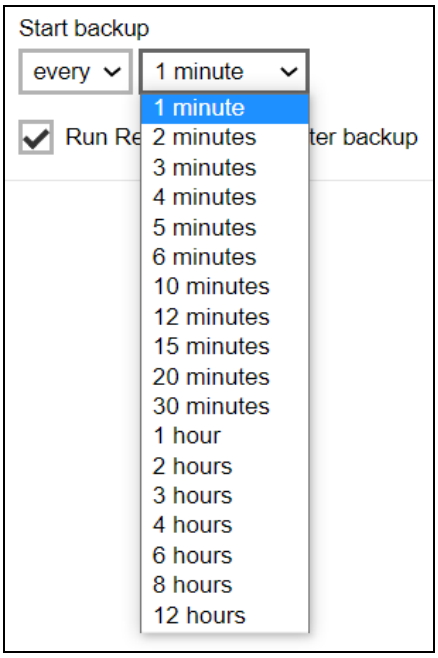
00 : 00

Stop

until full backup completed

☑ Run Retention Policy after backup

- **Start backup** – the start time of the backup job.
  - **at** – this option will start a backup job at a specific time.
  - **every** – this option will start a backup job in intervals of minutes or hours.

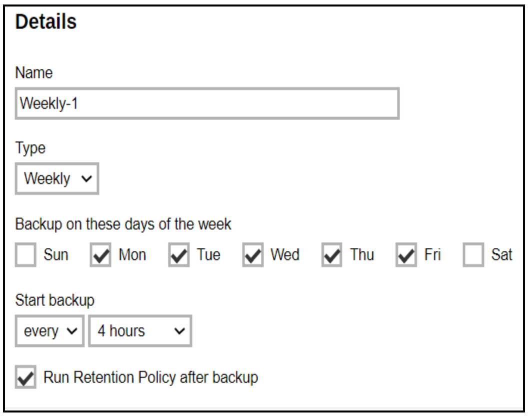


Start backup

every | 1 minute

☑ Run Re… …ter backup

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



Details

Name: Weekly-1

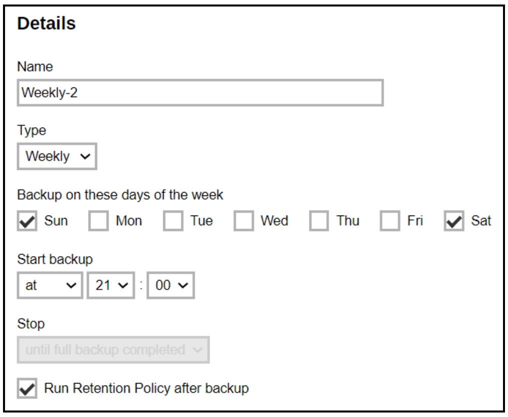
Type: Weekly

Backup on these days of the week: □ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri □ Sat

Start backup: every | 4 hours

☑ Run Retention Policy after backup

Figure 1.1



Details

Name: Weekly-2

Type: Weekly

Backup on these days of the week: ☑ Sun □ Mon □ Tue □ Wed □ Thu □ Fri ☑ Sat

Start backup: at | 21 : 00

Stop: until full backup completed

☑ Run Retention Policy after backup

Figure 1.2

Figure 1.1 – Periodic backup schedule runs every 4 hours from Monday – Friday during business hours

Figure 1.2 – Normal backup schedule runs at 21:00 or 9:00 PM on Saturday and Sunday on 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.

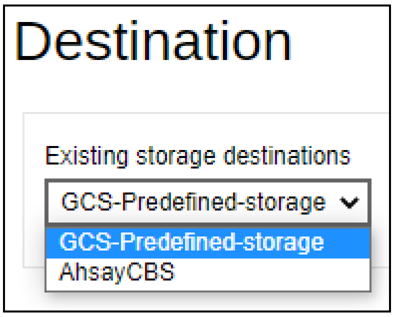
The partially backed up data will have to be removed by running the data integrity check.

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 AhsayCBS 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. To save hard disk quote in the long run, it is recommended to enable this option.

Click the + icon to save the configured backup schedule and then click **Next** to proceed.

13. To add a destination, select from the existing storage destinations listed on the drop-down list as provided by your backup service provider.


Destination

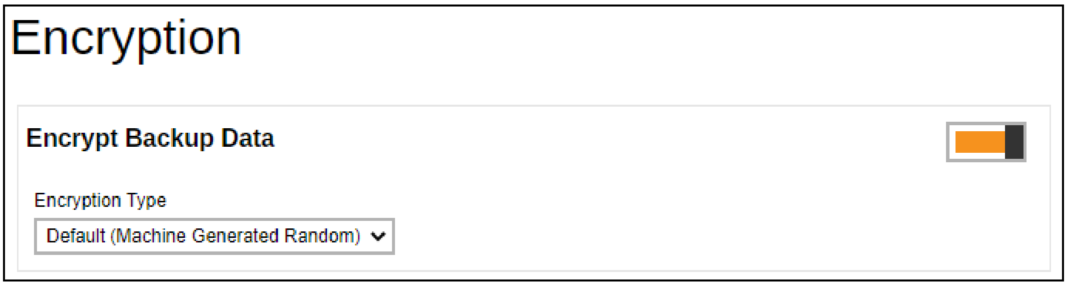
Existing storage destinations

GCS-Predefined-storage

GCS-Predefined-storage
AhsayCBS

In the sample screenshot above, the backup service provider has set up two (2) available destinations (i.e. GCS-Predefined-storage, and AhsayCBS).

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


Encryption

Encrypt Backup Data

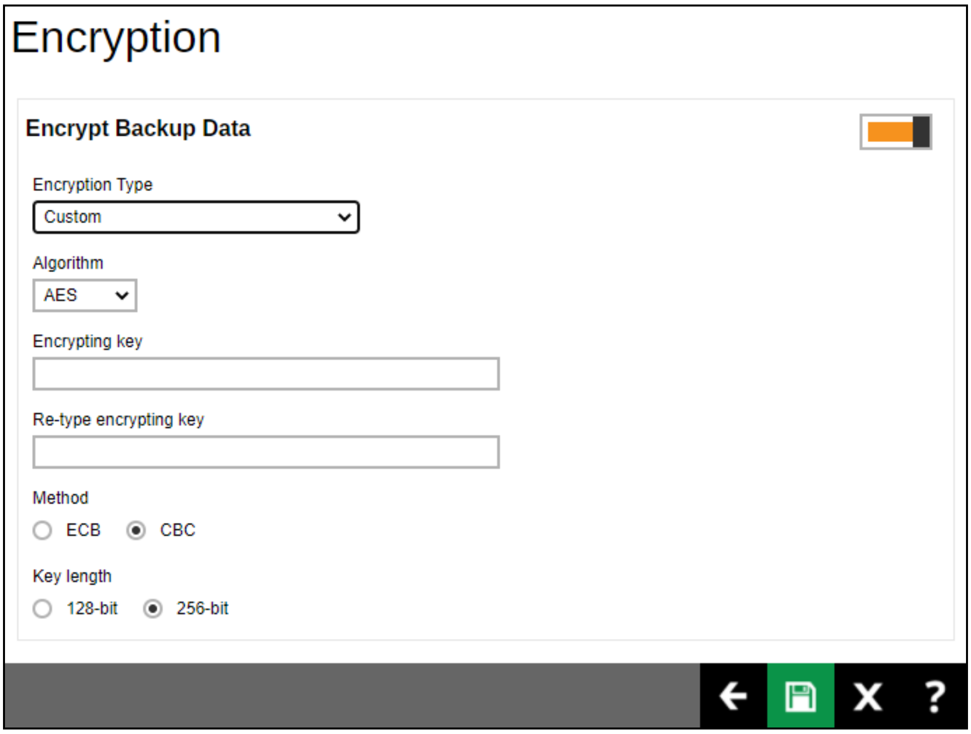
Encryption Type

Default (Machine Generated Random)

You can choose from one of the following three (3) Encryption Type options:

- **Default (Machine Generated Random)** – an encryption key with 44 alpha numeric characters will be randomly generated by the system.

- **User password** – the encryption key will be the same as the login password of your AhsayOBM/AhsayACB at the time when this backup set is created. Please be reminded that if you change the AhsayOBM/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.



Encryption

Encrypt Backup Data

Encryption Type: Custom

Algorithm: AES

Encrypting key

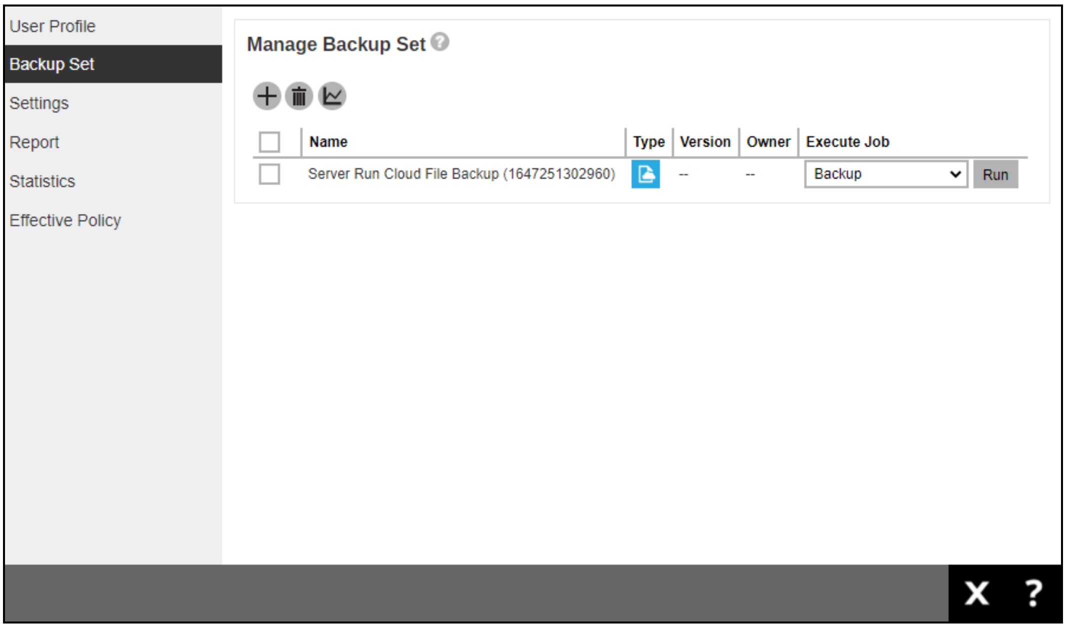
Re-type encrypting key

Method: ○ ECB ● CBC

Key length: ○ 128-bit ● 256-bit

Click the 💾 icon at the bottom right corner to confirm the creation of this backup set.

15. The cloud file backup set is succesfully created.



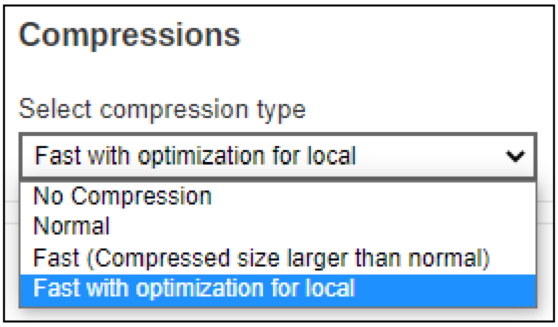
Manage Backup Set

□	Name	Type	Version	Owner	Execute Job
□	Server Run Cloud File Backup (1647251302960)		--	--	Backup Run

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

    Go to **Backup Set > Others > Compressions**, then select from the following:

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

    Compressions

    Select compression type

    Fast with optimization for local

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

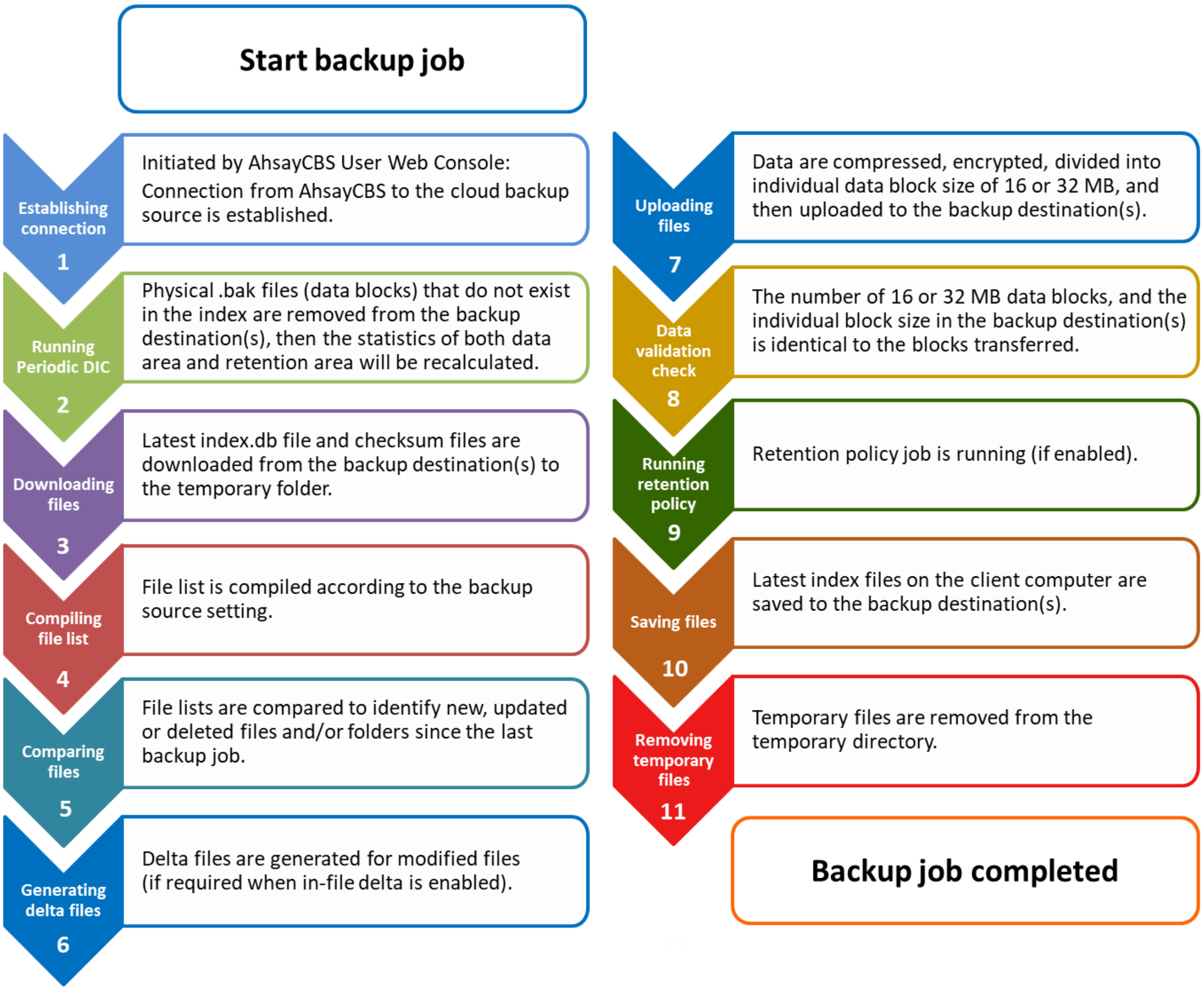
    Click the 💾 icon at the bottom right corner to save the selected compression type.

    NOTE
    For more information on the different configurable settings of a backup set, please refer to Chapter 6.2 of the AhsayCBS v9 User Guide.

4 Overview of Run on Server Cloud File Backup Process

The following steps are performed during a Run on Server Cloud File backup job. For an overview of the detailed process for Steps **2**, **3**, **8**, and **10**, please refer to the following chapters.

- Periodic Data Integrity Check (PDIC) Process **(Step 2)**
- Backup Set Index Handling Process
    - Start Backup Job **(Step 3)**
    - Completed Backup Job **(Step 10)**
- Data Validation Check Process **(Step 8)**



Start backup job

Establishing connection 1 — Initiated by AhsayCBS User Web Console: Connection from AhsayCBS to the cloud backup source is established.

Running Periodic DIC 2 — Physical .bak files (data blocks) that do not exist in the index are removed from the backup destination(s), then the statistics of both data area and retention area will be recalculated.

Downloading files 3 — Latest index.db file and checksum files are downloaded from the backup destination(s) to the temporary folder.

Compiling file list 4 — File list is compiled according to the backup source setting.

Comparing files 5 — File lists are compared to identify new, updated or deleted files and/or folders since the last backup job.

Generating delta files 6 — Delta files are generated for modified files (if required when in-file delta is enabled).

Uploading files 7 — Data are compressed, encrypted, divided into individual data block size of 16 or 32 MB, and then uploaded to the backup destination(s).

Data validation check 8 — The number of 16 or 32 MB data blocks, and the individual block size in the backup destination(s) is identical to the blocks transferred.

Running retention policy 9 — Retention policy job is running (if enabled).

Saving files 10 — Latest index files on the client computer are saved to the backup destination(s).

Removing temporary files 11 — Temporary files are removed from the temporary directory.

Backup job completed

4.1 Periodic Data Integrity Check (PDIC) Process

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:

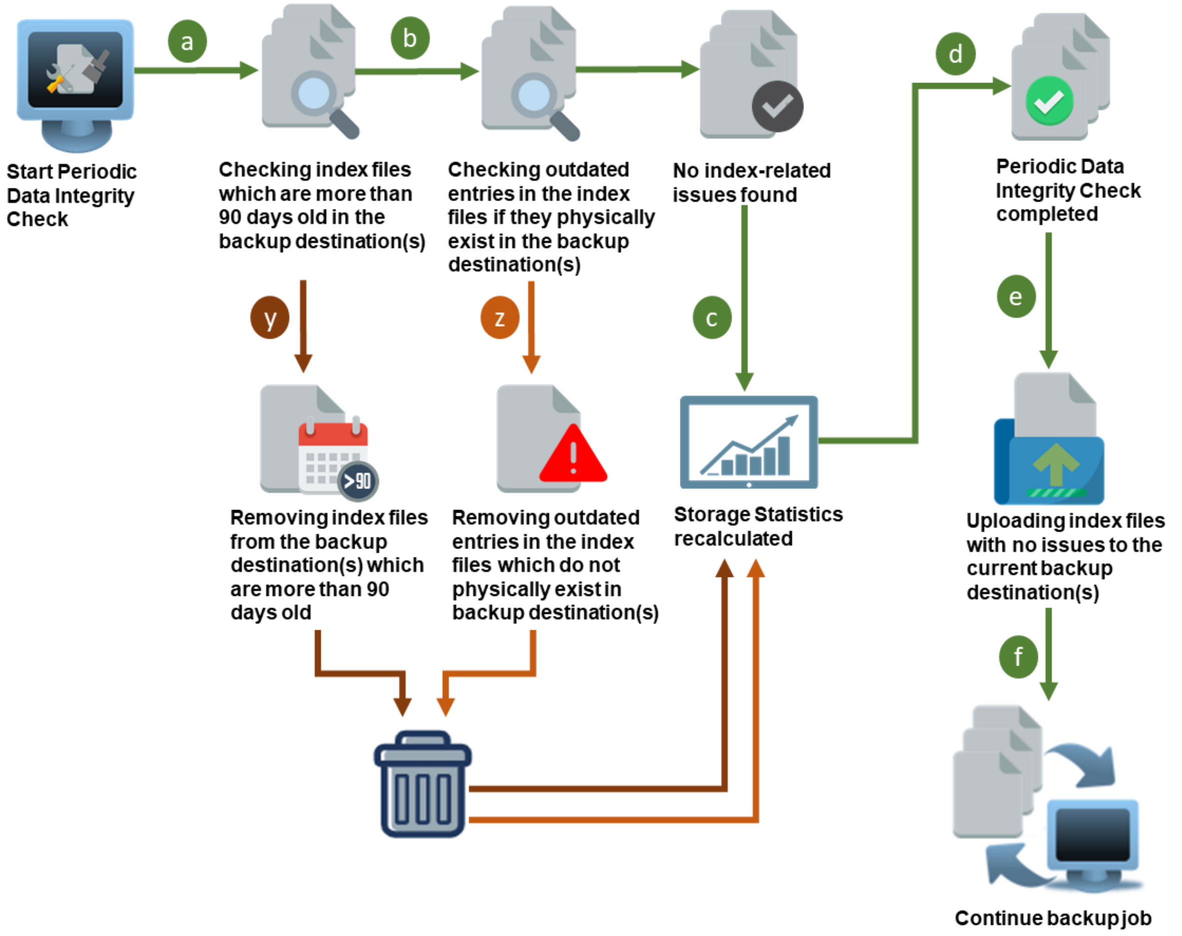
- the PDIC will run on the first backup job that falls on Wednesday; or
- if there is no active backup job(s) running from Monday to Friday, then the PDIC will run on the next available backup job.

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 AhsayCBS was upgraded to v9 (or above) from an older version 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.


Start Periodic Data Integrity Check
a
Checking index files which are more than 90 days old in the backup destination(s)
b
Checking outdated entries in the index files if they physically exist in the backup destination(s)
No index-related issues found
d
Periodic Data Integrity Check completed
y
z
c
e
>90
Removing index files from the backup destination(s) which are more than 90 days old
Removing outdated entries in the index files which do not physically exist in backup destination(s)
Storage Statistics recalculated
Uploading index files with no issues to the current backup destination(s)
f
Continue backup job

a Check the index files in the backup destination(s) to determine if they were more than 90 days old.

➔ If **YES**, proceed to y

➔ If **NO**, proceed to b

b Check the outdated entries in the index files for files and/or folders if they physically exist in the backup destination(s).

➔ If **YES**, proceed to c

➔ If **NO**, proceed to z

c Storage Statistics for Data area and Retention area usage will be recalculated.

d Periodic Data Integrity check is completed.

e Index files with no issues will be uploaded to the current backup destination(s).

f The backup job process will continue.

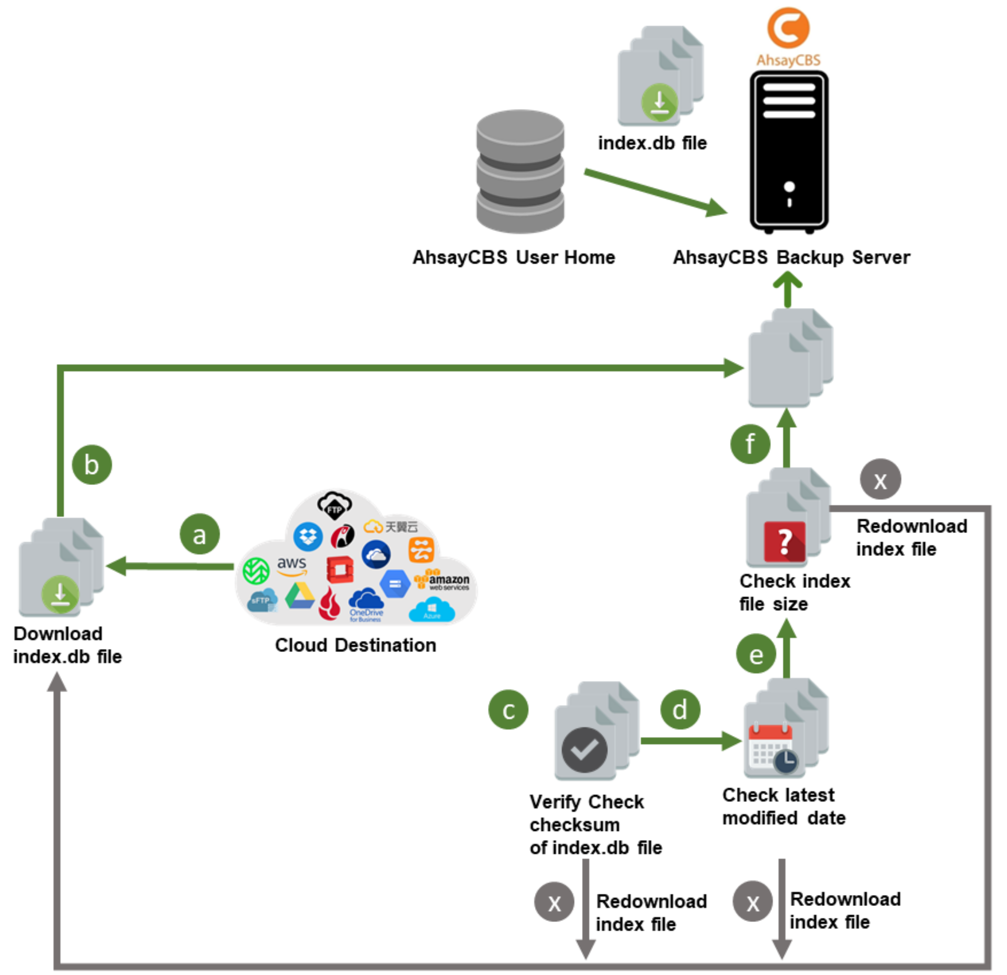
y Index files which are more than 90 days old will be removed from the backup destination(s).

z Outdated entries in the index files for files and/or folders which do not physically exist in backup destination(s) will be removed.

4.2 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.

4.2.1 Start Backup Job



a Index file is retrieved from AhsayCBS User Home and/ or downloaded from Cloud Destination.

b Index file will be downloaded.

c Verify Check checksum of index.db file.
- ➔ If checksum is correct, proceed to d
- ➔ If **NOT**, proceed to x

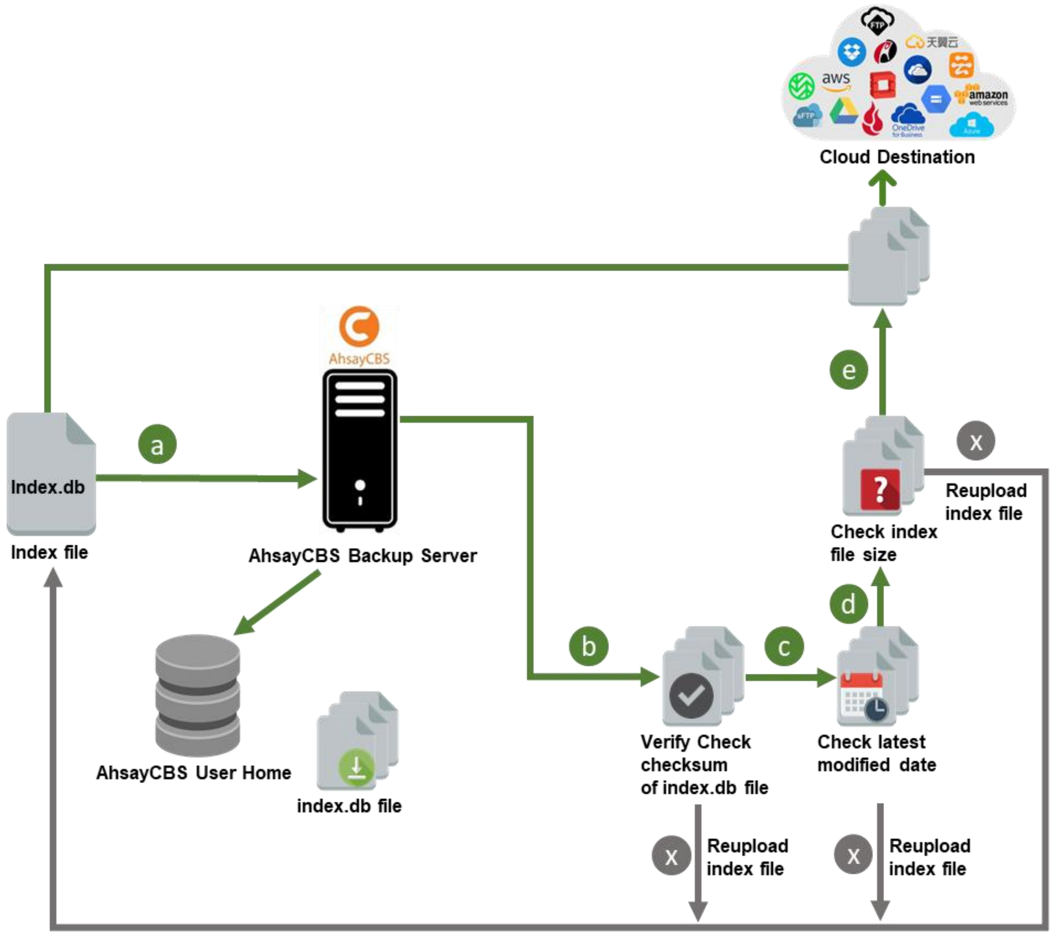
d Check modified date.
- ➔ If latest modified date is correct, proceed to e
- ➔ If **NOT**, proceed to x

e Check index file size.
- ➔ If index file size is correct, proceed to f
- ➔ If **NOT**, proceed to x

f If index is valid, use the index.db file to compile file list for backup.

x Index file will be redownloaded. Proceed to b

4.2.2 Completed Backup Job



a Index file is updated to AhsayCBS User Home and/or Cloud Destination and uploaded to AhsayCBS.

b Verify Check checksum of index.db file.

- ➔ If checksum is correct, proceed to c
- ➔ If **NOT**, proceed to x

c Check modified date.

- ➔ If latest modified date is correct, proceed to d
- ➔ If **NOT**, proceed to x

d Check index file size.

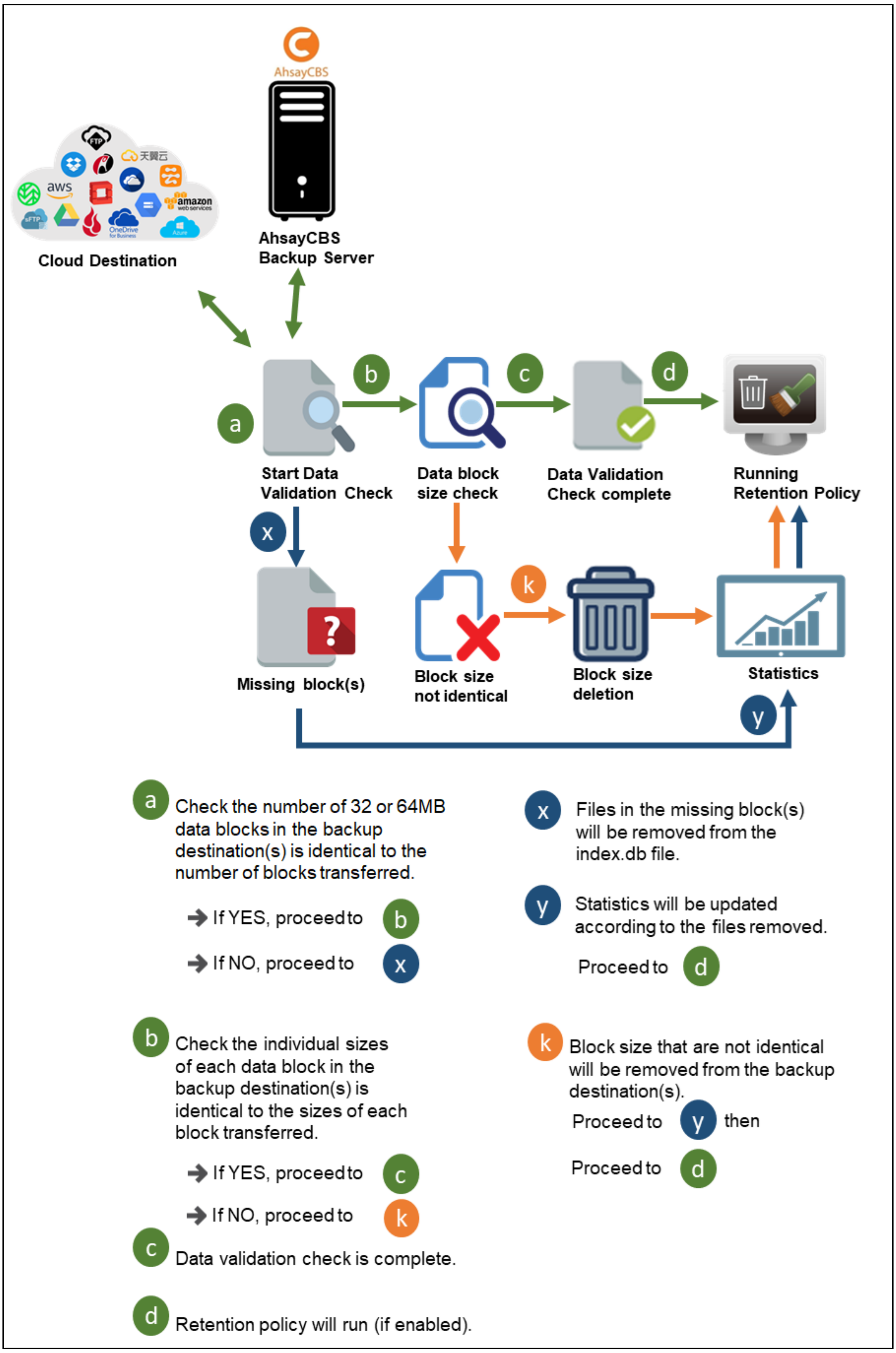
- ➔ If index file size is correct, proceed to e
- ➔ If **NOT**, proceed to x

e Index file is uploaded correctly to Cloud Destination.

x Index file will be reuploaded. Proceed to a

4.3 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 32 or 64 MB data block files and the size of each block file are checked again after the files are transferred.



a Check the number of 32 or 64MB data blocks in the backup destination(s) is identical to the number of blocks transferred.

➔ If YES, proceed to b

➔ If NO, proceed to x

b Check the individual sizes of each data block in the backup destination(s) is identical to the sizes of each block transferred.

➔ If YES, proceed to c

➔ If NO, proceed to k

c Data validation check is complete.

d Retention policy will run (if enabled).

x Files in the missing block(s) will be removed from the index.db file.

y Statistics will be updated according to the files removed.

Proceed to d

k Block size that are not identical will be removed from the backup destination(s).

Proceed to y then

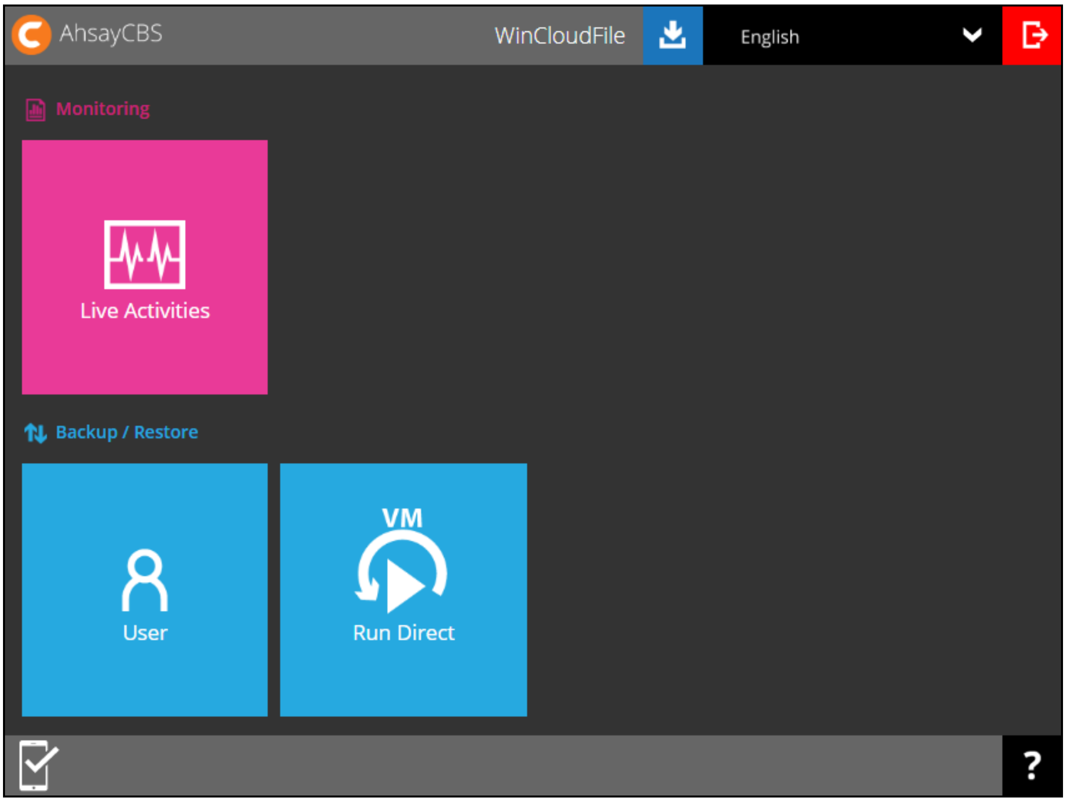
Proceed to d

5 Running a Backup Job

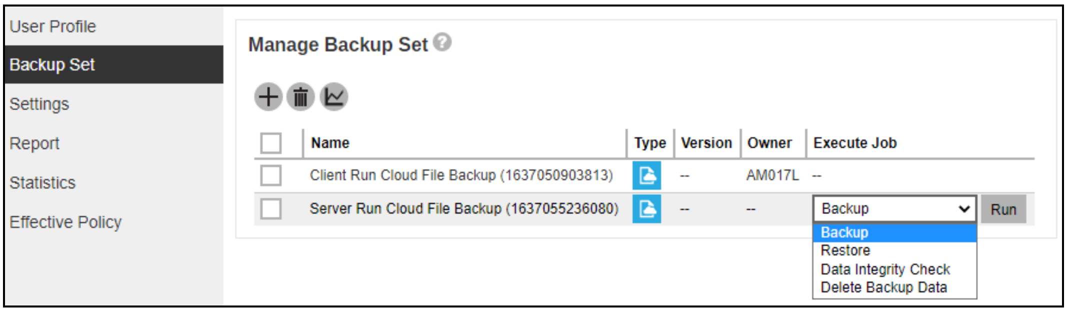
1. Log in to the User Web Console.

   For instructions on how to do this please refer to Chapter 2 of the AhsayCBS v9 User Guide.

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



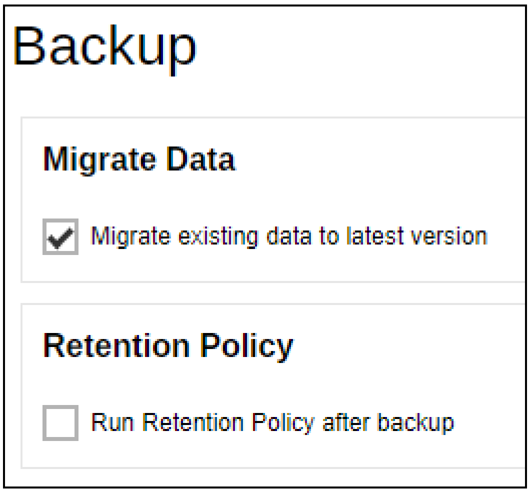
3. Select **Backup Set** from the left panel, then select **Backup** under **Execute Job** drop down menu and click **Run**.



Manage Backup Set

☐	Name	Type	Version	Owner	Execute Job
☐	Client Run Cloud File Backup (1637050903813)		--	AM017L	--
☐	Server Run Cloud File Backup (1637055236080)		--	--	Backup ▾ Run

4. Modify the **Migrate Data** and **Retention Policy** setting if necessary.



Backup

Migrate Data

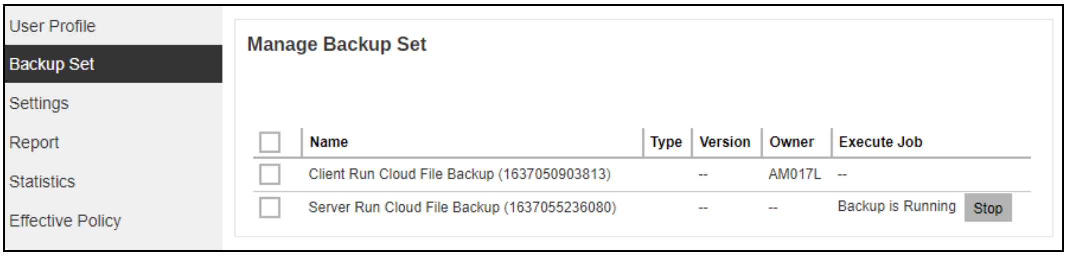
☑ Migrate existing data to latest version

Retention Policy

□ Run Retention Policy after backup

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

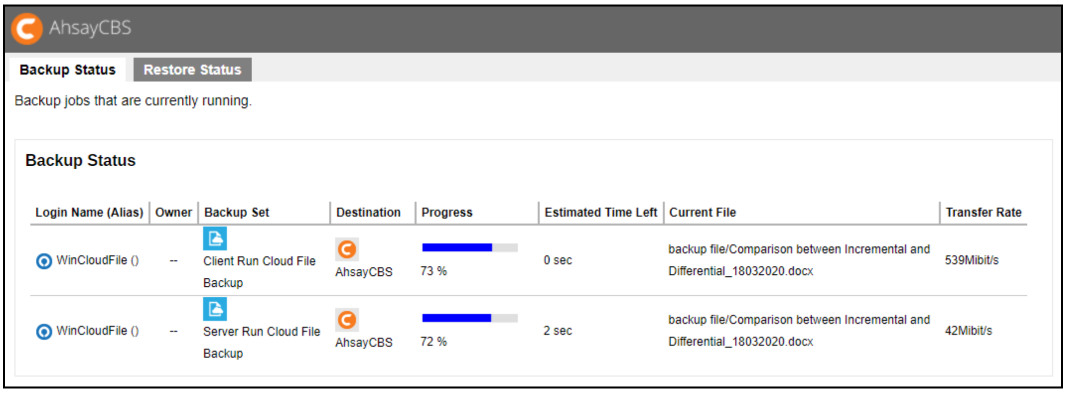
6. When a backup job is running, the status **Backup is Running** will be displayed. Click **Stop** to stop the backup job if necessary.



Manage Backup Set

□	Name	Type	Version	Owner	Execute Job
□	Client Run Cloud File Backup (1637050903813)		--	AM017L	--
□	Server Run Cloud File Backup (1637055236080)		--	--	Backup is Running Stop

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

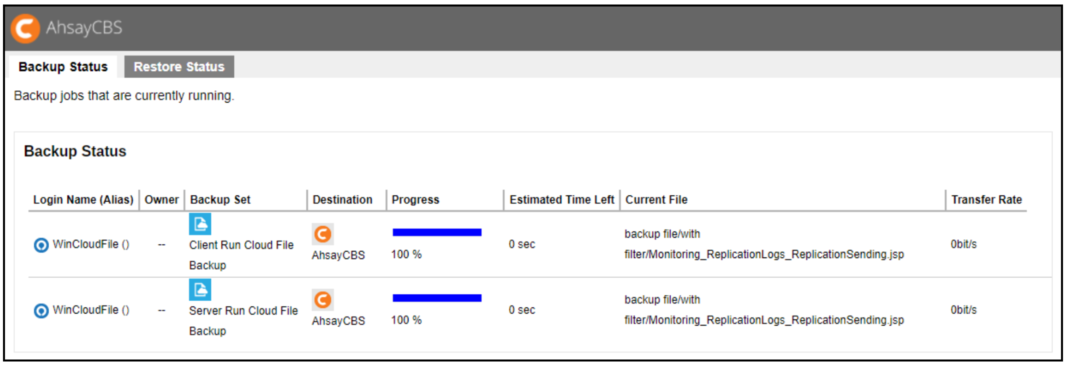


Backup jobs that are currently running.

Backup Status

Login Name (Alias)	Owner	Backup Set	Destination	Progress	Estimated Time Left	Current File	Transfer Rate
WinCloudFile ()	--	Client Run Cloud File Backup	AhsayCBS	73 %	0 sec	backup file/Comparison between Incremental and Differential_18032020.docx	539Mibit/s
WinCloudFile ()	--	Server Run Cloud File Backup	AhsayCBS	72 %	2 sec	backup file/Comparison between Incremental and Differential_18032020.docx	42Mibit/s

7. The backup through AhsayCBS User Web Console is successful.

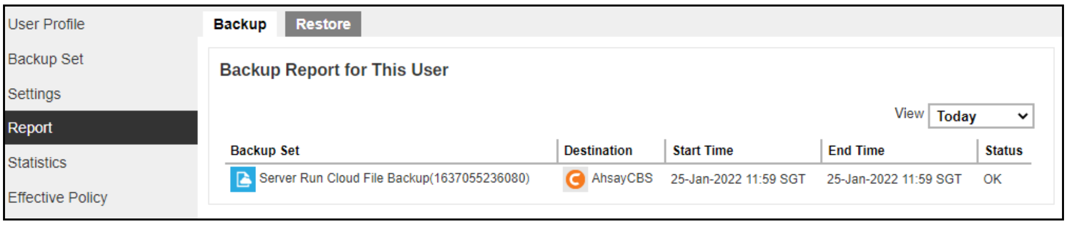


Backup jobs that are currently running.

Backup Status

Login Name (Alias)	Owner	Backup Set	Destination	Progress	Estimated Time Left	Current File	Transfer Rate
WinCloudFile ()	--	Client Run Cloud File Backup	AhsayCBS	100 %	0 sec	backup file/with filter/Monitoring_ReplicationLogs_ReplicationSending.jsp	0bit/s
WinCloudFile ()	--	Server Run Cloud File Backup	AhsayCBS	100 %	0 sec	backup file/with filter/Monitoring_ReplicationLogs_ReplicationSending.jsp	0bit/s

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

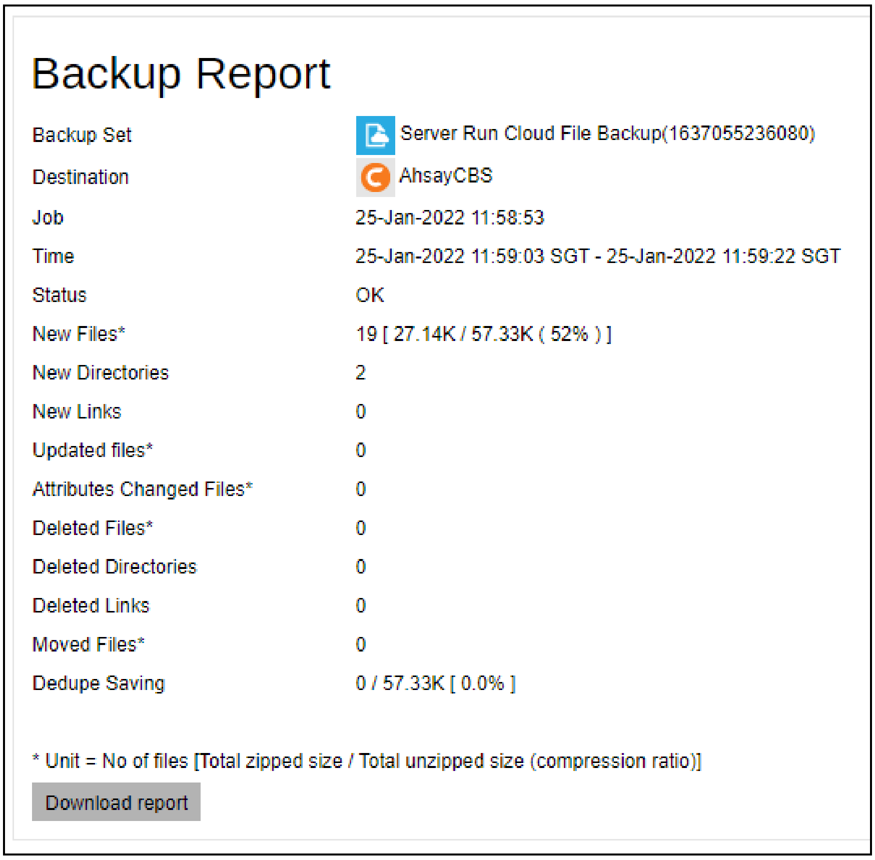


Backup Report for This User

View Today

Backup Set	Destination	Start Time	End Time	Status
Server Run Cloud File Backup(1637055236080)	AhsayCBS	25-Jan-2022 11:59 SGT	25-Jan-2022 11:59 SGT	OK

Click the backup set that you would like to view, and the following screen will be displayed. The summary of the backup job will be displayed. If you want to have a copy of the backup report, click the **Download report** button and a pdf file will be downloaded.

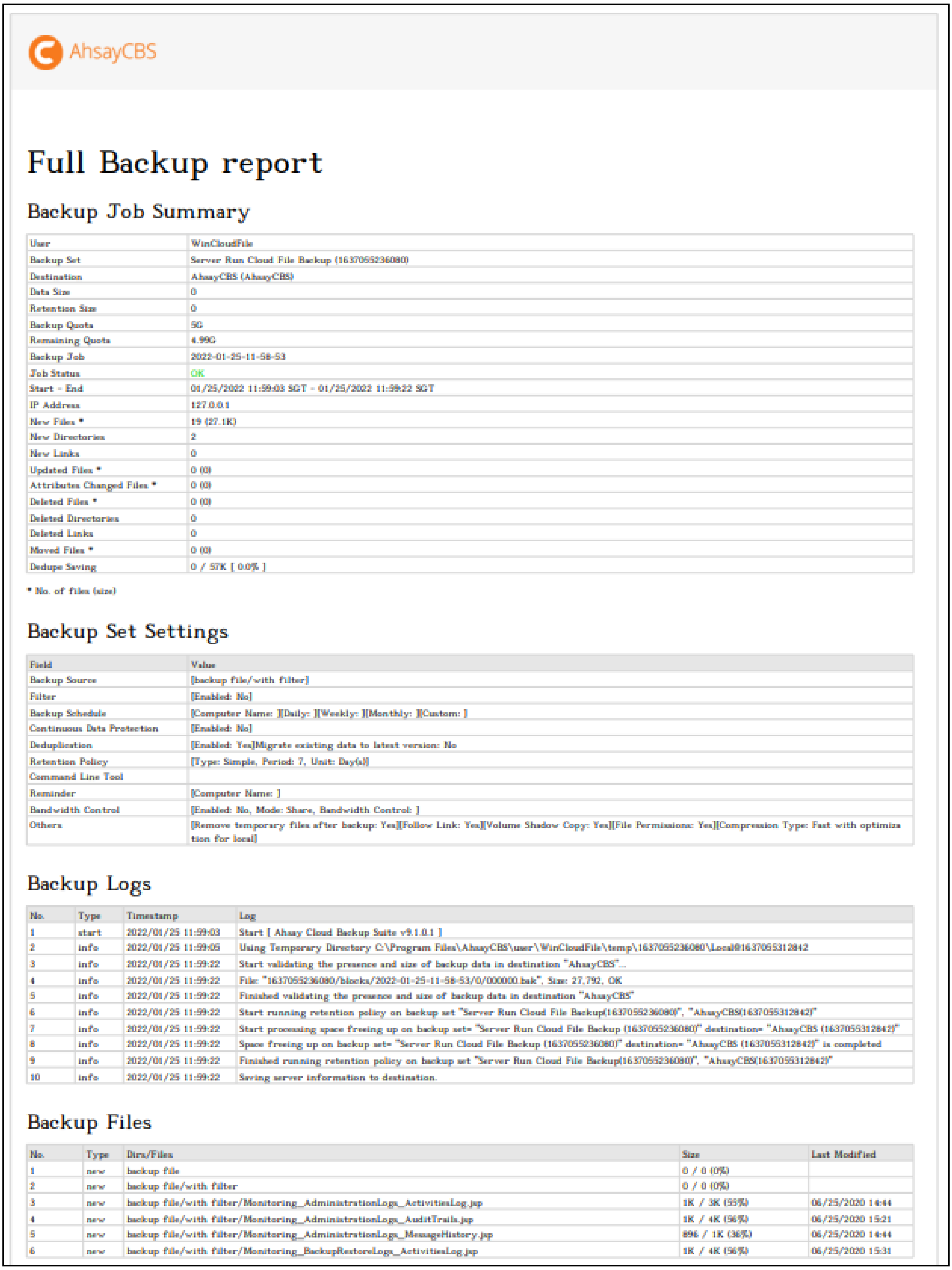


Backup Report

Backup Set	Server Run Cloud File Backup(1637055236080)
Destination	AhsayCBS
Job	25-Jan-2022 11:58:53
Time	25-Jan-2022 11:59:03 SGT - 25-Jan-2022 11:59:22 SGT
Status	OK
New Files*	19 [27.14K / 57.33K (52%)]
New Directories	2
New Links	0
Updated files*	0
Attributes Changed Files*	0
Deleted Files*	0
Deleted Directories	0
Deleted Links	0
Moved Files*	0
Dedupe Saving	0 / 57.33K [0.0%]

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

Below is an example of a backup job report:



AhsayCBS

Full Backup report

Backup Job Summary

User	WinCloudFile
Backup Set	Server Run Cloud File Backup (1637055236080)
Destination	AhsayCBS (AhsayCBS)
Data Size	0
Retention Size	0
Backup Quota	5G
Remaining Quota	4.99G
Backup Job	2022-01-25-11-58-53
Job Status	OK
Start - End	01/25/2022 11:59:03 SGT - 01/25/2022 11:59:22 SGT
IP Address	127.0.0.1
New Files *	19 (27.1K)
New Directories	2
New Links	0
Updated Files *	0 (0)
Attributes Changed Files *	0 (0)
Deleted Files *	0 (0)
Deleted Directories	0
Deleted Links	0
Moved Files *	0 (0)
Dedupe Saving	0 / 57K [0.0%]

* No. of files (size)

Backup Set Settings

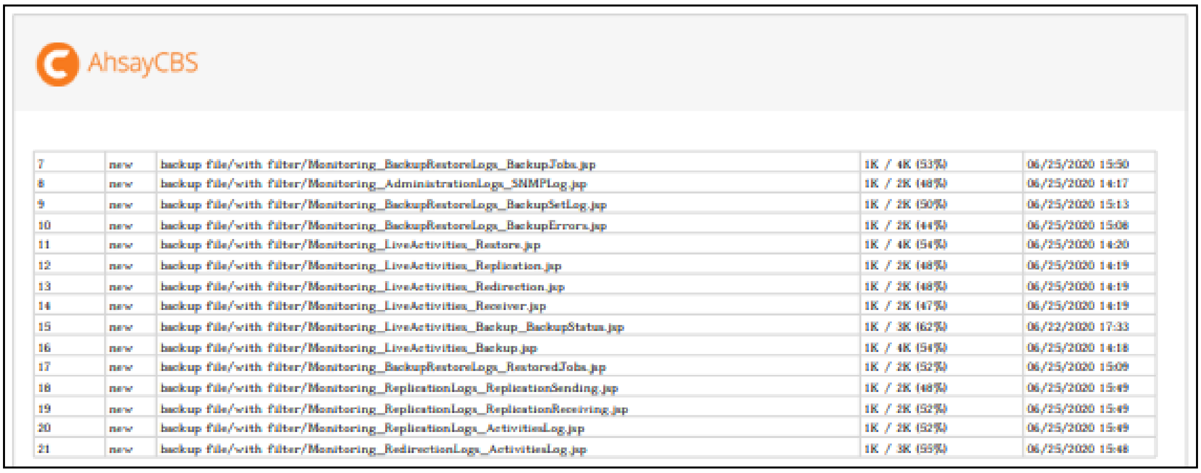
Field	Value
Backup Source	[backup file/with filter]
Filter	[Enabled: No]
Backup Schedule	[Computer Name:][Daily:][Weekly:][Monthly:][Custom:]
Continuous Data Protection	[Enabled: No]
Deduplication	[Enabled: Yes]Migrate existing data to latest version: No
Retention Policy	[Type: Simple, Period: 7, Unit: Day(s)]
Command Line Tool	
Reminder	[Computer Name:]
Bandwidth Control	[Enabled: No, Mode: Share, Bandwidth Control:]
Others	[Remove temporary files after backup: Yes][Follow Link: Yes][Volume Shadow Copy: Yes][File Permissions: Yes][Compression Type: Fast with optimization for local]

Backup Logs

No.	Type	Timestamp	Log
1	start	2022/01/25 11:59:03	Start [Ahsay Cloud Backup Suite v9.1.0.1]
2	info	2022/01/25 11:59:05	Using Temporary Directory C:\Program Files\AhsayCBS\user\WinCloudFile\temp\1637055236080\Local@1637055312842
3	info	2022/01/25 11:59:22	Start validating the presence and size of backup data in destination "AhsayCBS"...
4	info	2022/01/25 11:59:22	File: "1637055236080/blocks/2022-01-25-11-58-53/0/000000.bak", Size: 27,792, OK
5	info	2022/01/25 11:59:22	Finished validating the presence and size of backup data in destination "AhsayCBS"
6	info	2022/01/25 11:59:22	Start running retention policy on backup set "Server Run Cloud File Backup(1637055236080)", "AhsayCBS(1637055312842)"
7	info	2022/01/25 11:59:22	Start processing space freeing up on backup set= "Server Run Cloud File Backup (1637055236080)" destination= "AhsayCBS (1637055312842)"
8	info	2022/01/25 11:59:22	Space freeing up on backup set= "Server Run Cloud File Backup (1637055236080)" destination= "AhsayCBS (1637055312842)" is completed
9	info	2022/01/25 11:59:22	Finished running retention policy on backup set "Server Run Cloud File Backup(1637055236080)", "AhsayCBS(1637055312842)"
10	info	2022/01/25 11:59:22	Saving server information to destination.

Backup Files

No.	Type	Dirs/Files	Size	Last Modified
1	new	backup file	0 / 0 (0%)	
2	new	backup file/with filter	0 / 0 (0%)	
3	new	backup file/with filter/Monitoring_AdministrationLogs_ActivitiesLog.jsp	1K / 3K (55%)	06/25/2020 14:44
4	new	backup file/with filter/Monitoring_AdministrationLogs_AuditTrails.jsp	1K / 4K (56%)	06/25/2020 15:21
5	new	backup file/with filter/Monitoring_AdministrationLogs_MessageHistory.jsp	896 / 1K (36%)	06/25/2020 14:44
6	new	backup file/with filter/Monitoring_BackupRestoreLogs_ActivitiesLog.jsp	1K / 4K (56%)	06/25/2020 15:31



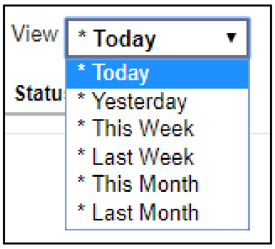
7	new	backup file/with filter/Monitoring_BackupRestoreLogs_BackupJobs.jsp	1K / 4K (53%)	06/25/2020 15:50
8	new	backup file/with filter/Monitoring_AdministrationLogs_SNMPLog.jsp	1K / 2K (48%)	06/25/2020 14:17
9	new	backup file/with filter/Monitoring_BackupRestoreLogs_BackupSetLog.jsp	1K / 2K (50%)	06/25/2020 15:13
10	new	backup file/with filter/Monitoring_BackupRestoreLogs_BackupErrors.jsp	1K / 2K (44%)	06/25/2020 15:08
11	new	backup file/with filter/Monitoring_LiveActivities_Restore.jsp	1K / 4K (54%)	06/25/2020 14:20
12	new	backup file/with filter/Monitoring_LiveActivities_Replication.jsp	1K / 2K (48%)	06/25/2020 14:19
13	new	backup file/with filter/Monitoring_LiveActivities_Redirection.jsp	1K / 2K (48%)	06/25/2020 14:19
14	new	backup file/with filter/Monitoring_LiveActivities_Receiver.jsp	1K / 2K (47%)	06/25/2020 14:19
15	new	backup file/with filter/Monitoring_LiveActivities_Backup_BackupStatus.jsp	1K / 3K (62%)	06/22/2020 17:33
16	new	backup file/with filter/Monitoring_LiveActivities_Backup.jsp	1K / 4K (54%)	06/25/2020 14:18
17	new	backup file/with filter/Monitoring_BackupRestoreLogs_RestoredJobs.jsp	1K / 2K (52%)	06/25/2020 15:09
18	new	backup file/with filter/Monitoring_ReplicationLogs_ReplicationSending.jsp	1K / 2K (48%)	06/25/2020 15:49
19	new	backup file/with filter/Monitoring_ReplicationLogs_ReplicationReceiving.jsp	1K / 2K (52%)	06/25/2020 15:49
20	new	backup file/with filter/Monitoring_ReplicationLogs_ActivitiesLog.jsp	1K / 2K (52%)	06/25/2020 15:49
21	new	backup file/with filter/Monitoring_RedirectionLogs_ActivitiesLog.jsp	1K / 3K (55%)	06/25/2020 15:48

To be able to download the backup report file, ensure that 15 to 20 minutes had passed after the backup job. Otherwise, the **Download report** button will not be displayed.

You can also view the reports for the following choices:

- Today
- Yesterday
- This Week
- Last Week
- This Month
- Last Month

Pick from any of the choices and the available report(s) will be displayed.



6 Restoring a Cloud File Backup Set

AhsayCBS User Web Console has two (2) options for the restoration process: **Original** and **Alternate** location. After this quick walkthrough, you will see the step-by-step instructions with corresponding screenshots on how to restore your data using the following options below.

- **Original location**

  Restore your data to your original location (i.e. on the cloud storage) where you backed up them.

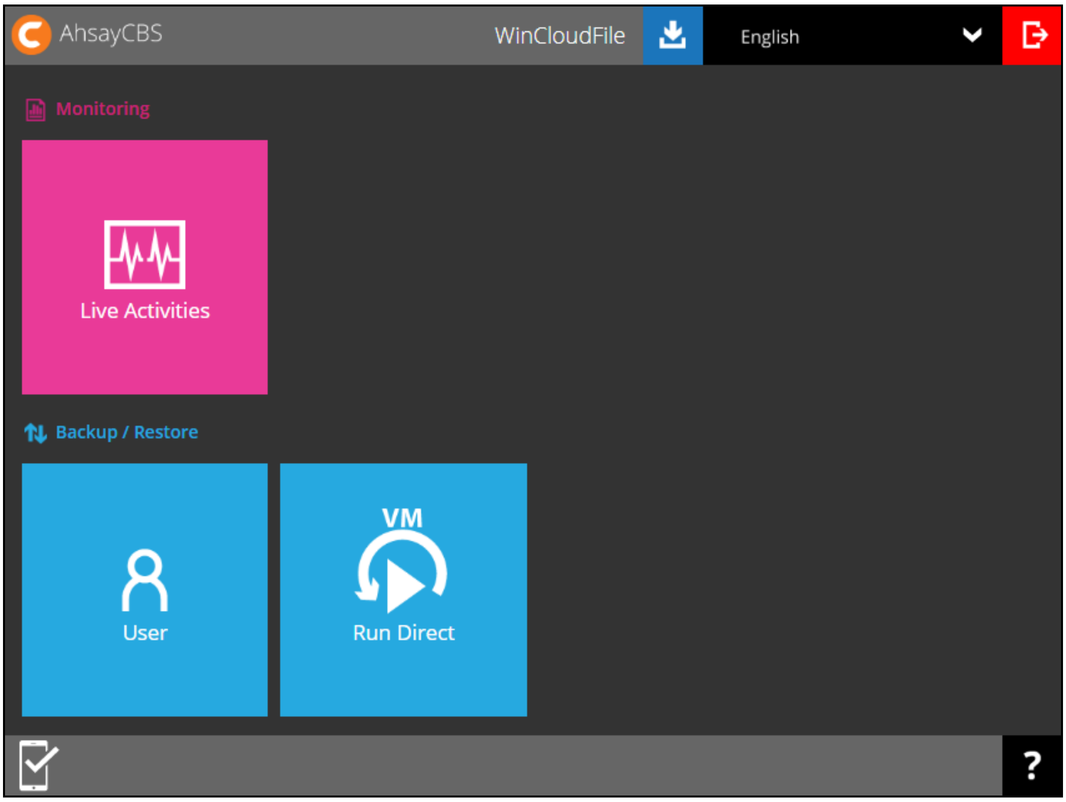
- **Alternate location**

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

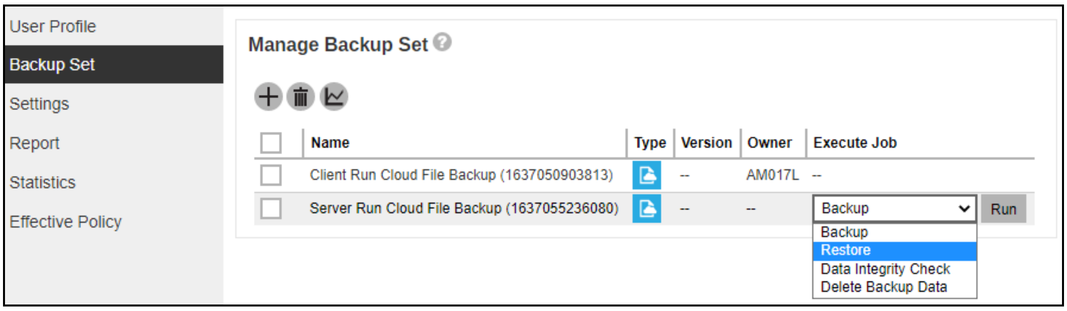
NOTE

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.



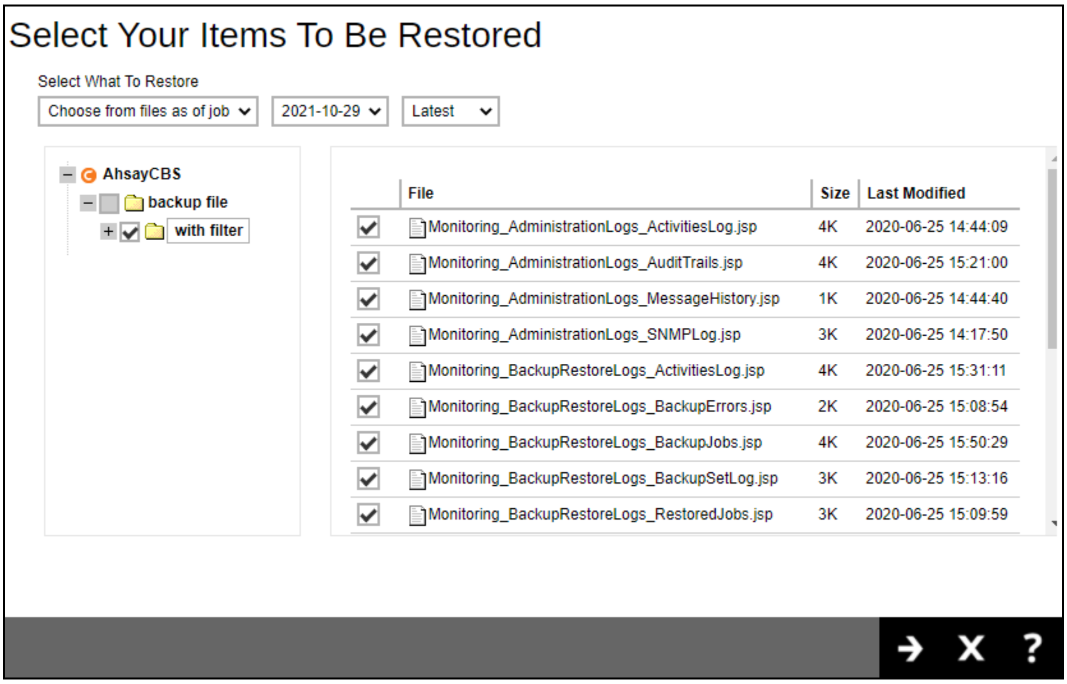
2. Select **Backup Set** from the left panel, then select **Restore** under **Execute Job** drop down menu and click **Run**.



Manage Backup Set

☐	Name	Type	Version	Owner	Execute Job
☐	Client Run Cloud File Backup (1637050903813)		--	AM017L	--
☐	Server Run Cloud File Backup (1637055236080)		--	--	Backup

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.



Select Your Items To Be Restored

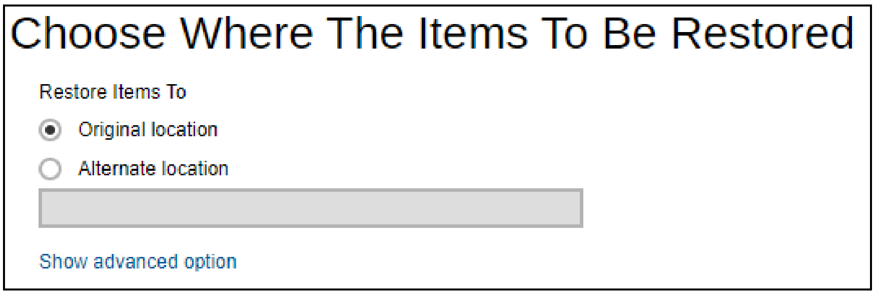
Select What To Restore

Choose from files as of job | 2021-10-29 | Latest

	File	Size	Last Modified
☑	Monitoring_AdministrationLogs_ActivitiesLog.jsp	4K	2020-06-25 14:44:09
☑	Monitoring_AdministrationLogs_AuditTrails.jsp	4K	2020-06-25 15:21:00
☑	Monitoring_AdministrationLogs_MessageHistory.jsp	1K	2020-06-25 14:44:40
☑	Monitoring_AdministrationLogs_SNMPLog.jsp	3K	2020-06-25 14:17:50
☑	Monitoring_BackupRestoreLogs_ActivitiesLog.jsp	4K	2020-06-25 15:31:11
☑	Monitoring_BackupRestoreLogs_BackupErrors.jsp	2K	2020-06-25 15:08:54
☑	Monitoring_BackupRestoreLogs_BackupJobs.jsp	4K	2020-06-25 15:50:29
☑	Monitoring_BackupRestoreLogs_BackupSetLog.jsp	3K	2020-06-25 15:13:16
☑	Monitoring_BackupRestoreLogs_RestoredJobs.jsp	3K	2020-06-25 15:09:59

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

- **Original Location**



Choose Where The Items To Be Restored

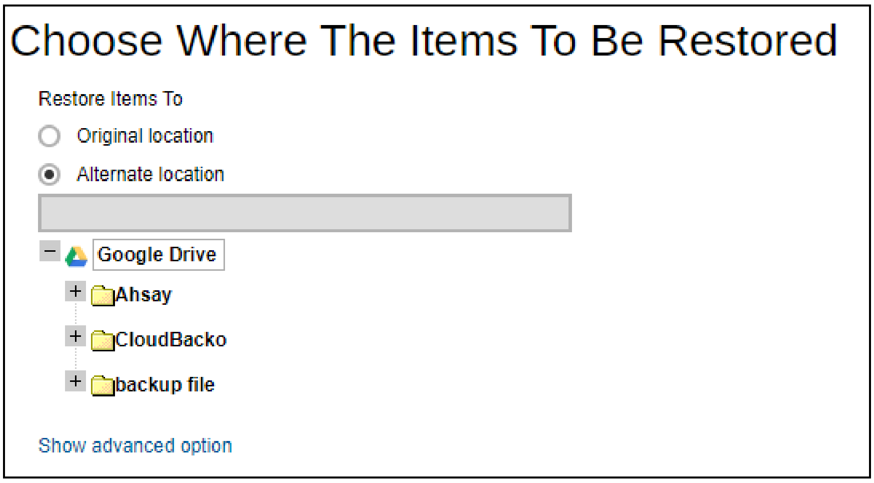
Restore Items To

● Original location

○ Alternate location

Show advanced option

- **Alternate Location**



Choose Where The Items To Be Restored

Restore Items To

○ Original location

● Alternate location

Google Drive
- Ahsay
- CloudBacko
- backup file

Show advanced option

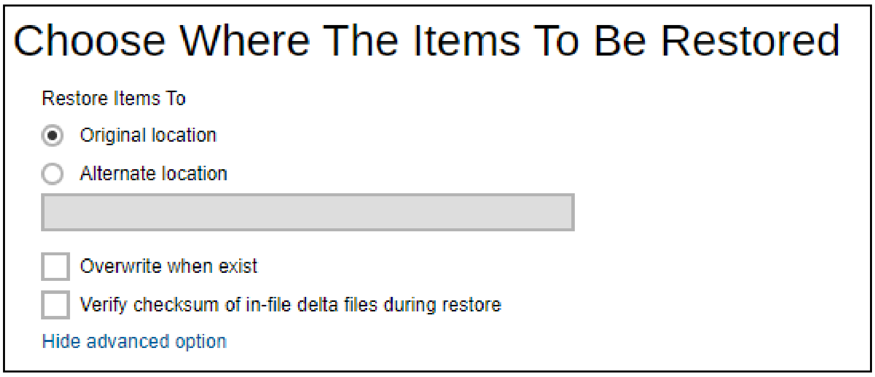
Expand the directory path to browse the alternate location(s) on the cloud storage.

IMPORTANT

Data can only be restored to the original cloud storage where the data was backed up from (i.e. same cloud storage provider and same account).

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

Original location



Choose Where The Items To Be Restored

Restore Items To

● Original location

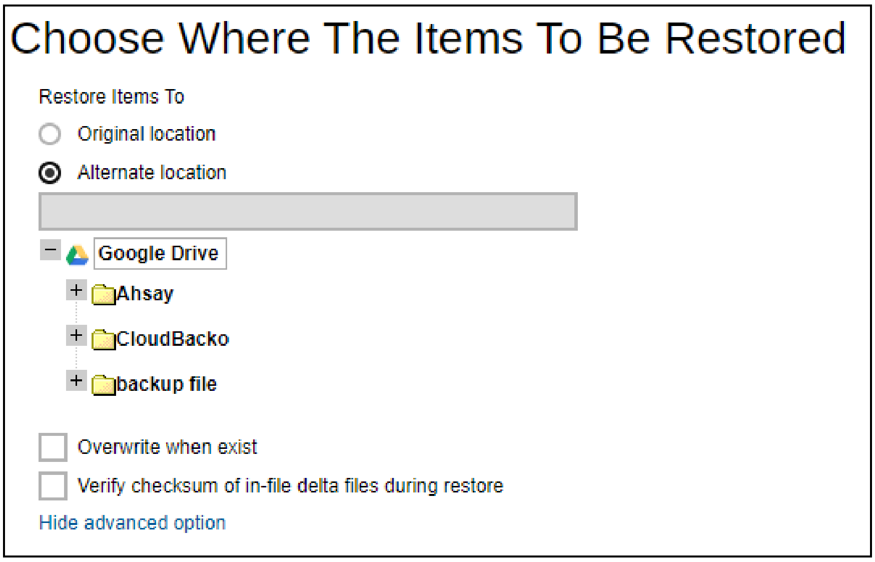
○ Alternate location

□ Overwrite when exist

□ Verify checksum of in-file delta files during restore

Hide advanced option

Alternate location



Choose Where The Items To Be Restored

Restore Items To

○ Original location

● Alternate location

− Google Drive
  + Ahsay
  + CloudBacko
  + backup file

□ Overwrite when exist

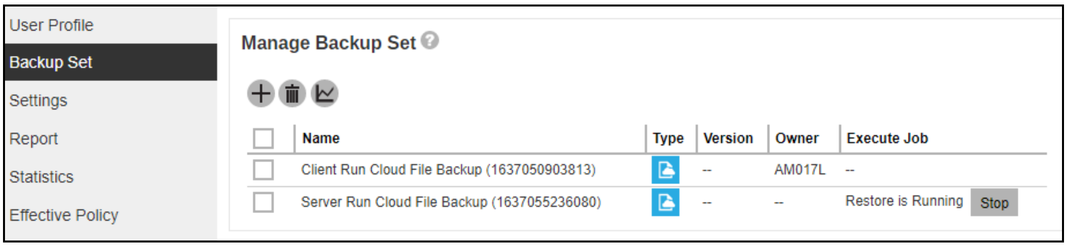
□ Verify checksum of in-file delta files during restore

Hide advanced option

- **Overwrite when exist**
  By enabling this option, this will overwrite your existing files. For example, if the files and/or folders you are going to restore are already available in your chosen alternate location, then your existing files will be overwritten during the restore process.
- **Verify checksum of in-file delta files during restore**
  By enabling this option, the checksum of in-file delta files will be verified during the restore process. This will check the data for errors during the restore process and create a data summary of the in-file delta files which will be included in the report.

5. Click the ⟲ icon to start the restoration.

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



User Profile
Backup Set
Settings
Report
Statistics
Effective Policy

Manage Backup Set

□	Name	Type	Version	Owner	Execute Job
□	Client Run Cloud File Backup (1637050903813)		--	AM017L	--
□	Server Run Cloud File Backup (1637055236080)		--	--	Restore is Running Stop

7 Running Data Integrity Check

Data Integrity Check can be done in two (2) ways:

- **AhsayOBM / AhsayACB User**

  This option allows the AhsayOBM and AhsayACB users to perform data integrity check, but the result of the data integrity check cannot be reviewed. It will only be available upon request from the backup service provider.

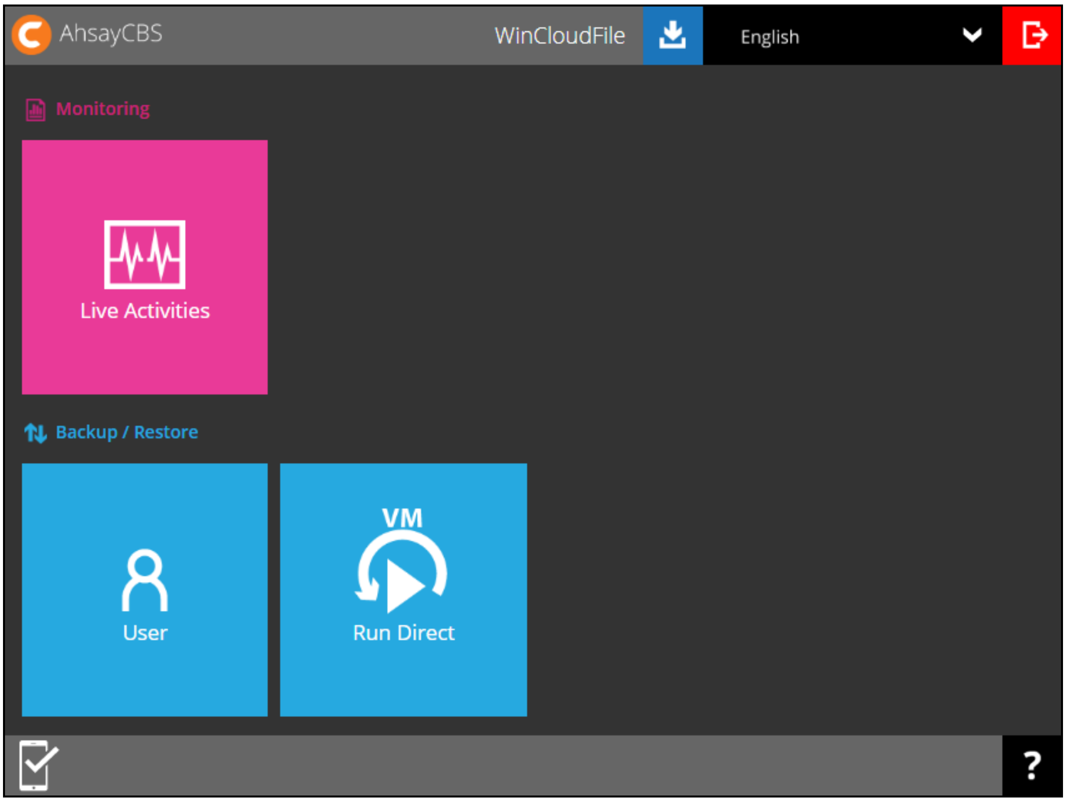
- **Backup Service Provider**

  This option allows the AhsayOBM and AhsayACB users to request their backup service provider to perform data integrity check and provide them with the report of the result and/or solution.

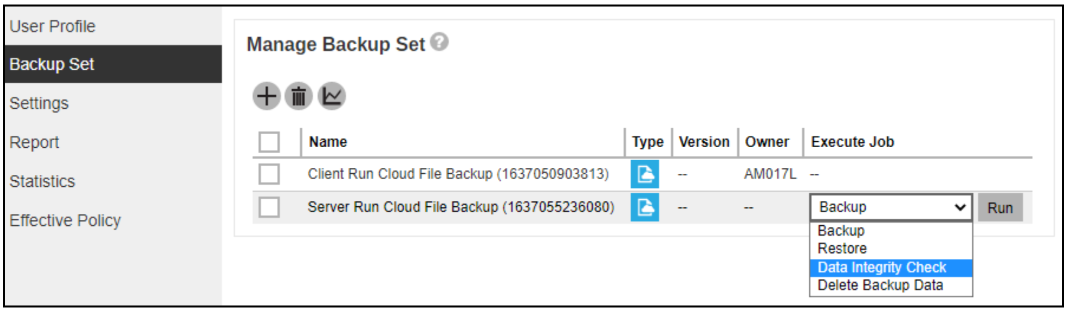
1. Log in to the User Web Console.

   For instructions on how to do this please refer to Chapter 2 of the AhsayCBS v9 User Guide.

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



3. Select **Backup Set** from the left panel, then select **Data Integrity Check** under the **Execute Job** drop-down menu. Click **Run** to proceed.



User Profile
Backup Set
Settings
Report
Statistics
Effective Policy

Manage Backup Set

□	Name	Type	Version	Owner	Execute Job
□	Client Run Cloud File Backup (1637050903813)		--	AM017L	--
□	Server Run Cloud File Backup (1637055236080)		--	--	Backup ▾ Run

Run Cyclic Redundancy Check (CRC)

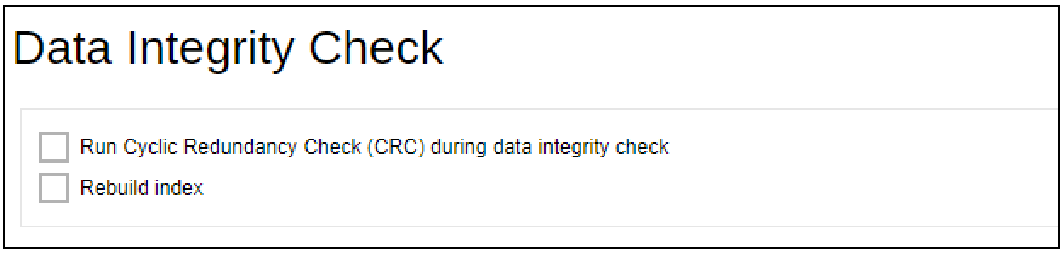
This option is disabled by default. When this option is enabled, the data integrity check will perform check on the integrity of the files on the backup destination(s) against the checksum file generated at the time of the backup job.

If there is a discrepancy, this indicates that the files on the backup destination(s) are corrupted. These corrupted files will be removed from the backup destination(s). If these files still exist on the backup server on the next backup job, the AhsayCBS will upload the latest copy.

However, if the corrupted files are in the retention area, they will not be backed up again as the source file has already been deleted from the backup server.

Rebuild index

This option is disabled by default. When this option is enabled, the data integrity check will start rebuilding corrupted index and/or broken data blocks if there are any.



Data Integrity Check

□ Run Cyclic Redundancy Check (CRC) during data integrity check
□ Rebuild index

4. Click the icon to begin the data integrity check process.

During a backup job, a Periodic Data Integrity Check (PDIC) will be performed as part of the backup process. This feature provides an additional regular data integrity check of the backup data. The PDIC will start **automatically** (with no user interaction needed) and will be performed once either of the following conditions is met:

- Will run once a week and will fall on a weekday (i.e. Monday to Friday)

OR

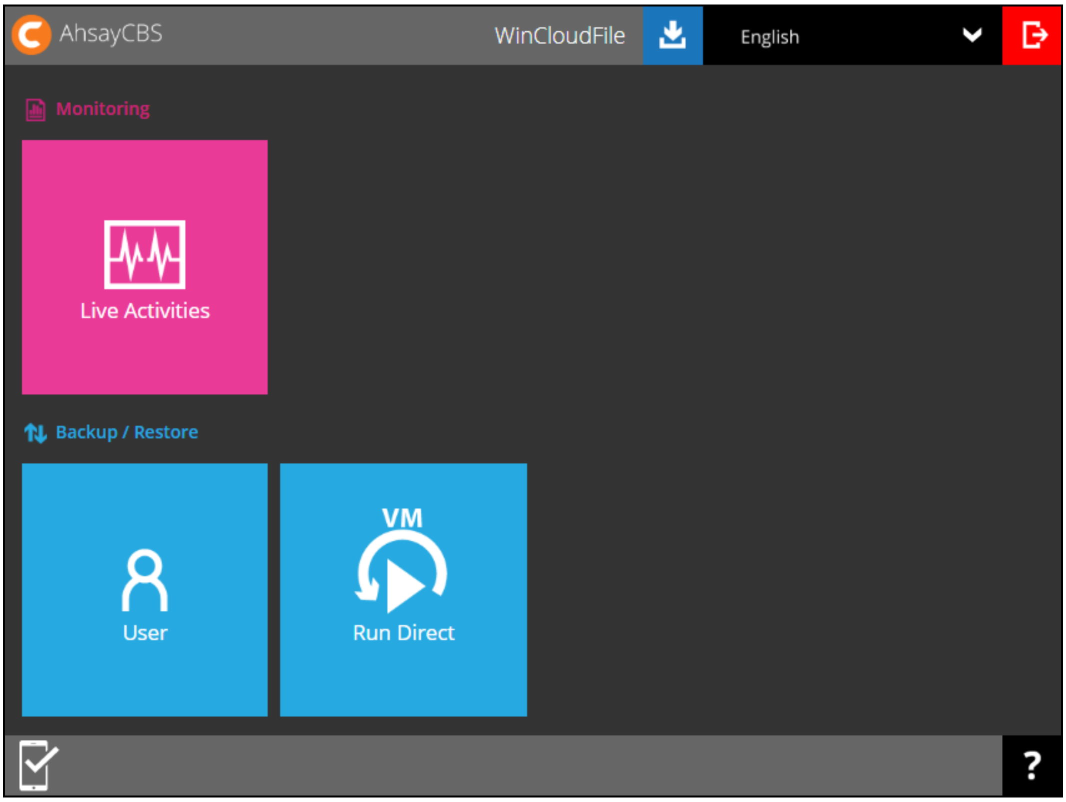
- If there is no active backup job(s) running from Monday to Friday, then the PDIC will be triggered on the next available backup job

8 Deleting Backup Data

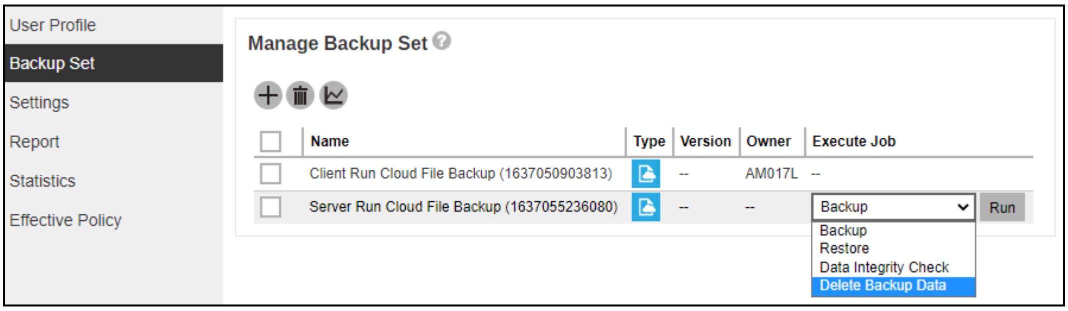
1. Log in to the User Web Console.

   For instructions on how to do this please refer to Chapter 2 of the AhsayCBS v9 User Guide.

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



3. Select **Backup Set** from the left panel, then select **Delete Backup Data** under the **Execute Job** drop-down menu. Click **Run** to proceed.

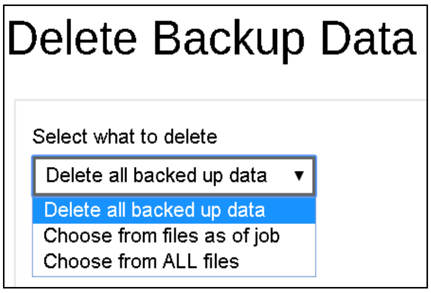


□	Name	Type	Version	Owner	Execute Job
□	Client Run Cloud File Backup (1637050903813)		--	AM017L	--
□	Server Run Cloud File Backup (1637055236080)		--	--	Backup

4. There are three options in performing delete backup data:

- Delete all backed up data

  When this option is selected, all the backup data on the selected backup set will be deleted.



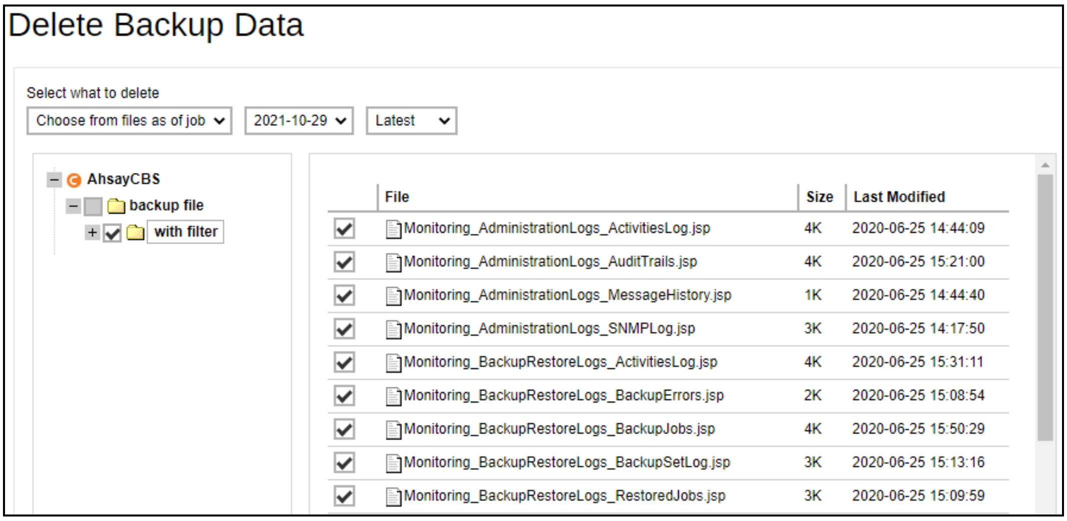
Delete Backup Data

Select what to delete

Delete all backed up data ▼

- Choose from files as of job

  When this option is selected, you can choose to delete file(s) and/or folder(s) from a backup snapshot.



Delete Backup Data

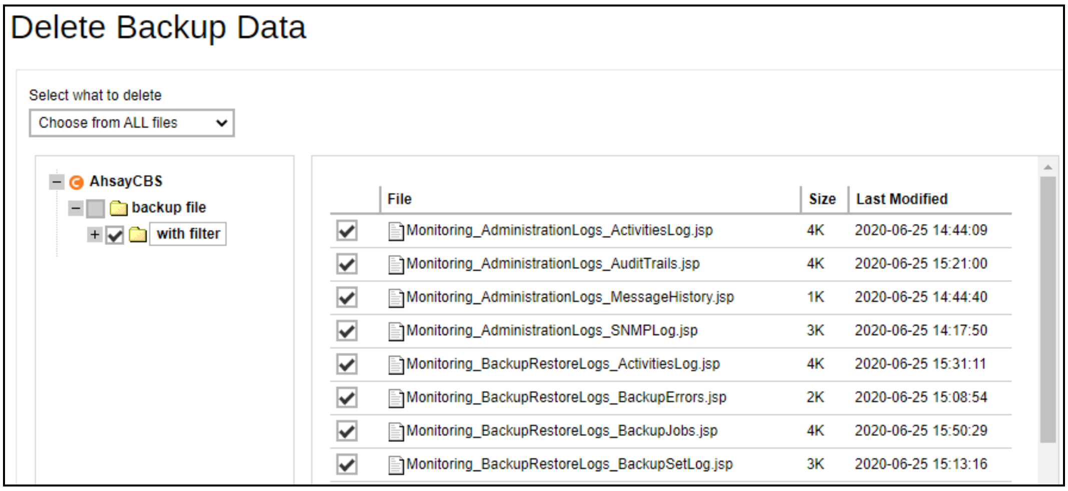
Select what to delete

Choose from files as of job | 2021-10-29 | Latest

	File	Size	Last Modified
☑	Monitoring_AdministrationLogs_ActivitiesLog.jsp	4K	2020-06-25 14:44:09
☑	Monitoring_AdministrationLogs_AuditTrails.jsp	4K	2020-06-25 15:21:00
☑	Monitoring_AdministrationLogs_MessageHistory.jsp	1K	2020-06-25 14:44:40
☑	Monitoring_AdministrationLogs_SNMPLog.jsp	3K	2020-06-25 14:17:50
☑	Monitoring_BackupRestoreLogs_ActivitiesLog.jsp	4K	2020-06-25 15:31:11
☑	Monitoring_BackupRestoreLogs_BackupErrors.jsp	2K	2020-06-25 15:08:54
☑	Monitoring_BackupRestoreLogs_BackupJobs.jsp	4K	2020-06-25 15:50:29
☑	Monitoring_BackupRestoreLogs_BackupSetLog.jsp	3K	2020-06-25 15:13:16
☑	Monitoring_BackupRestoreLogs_RestoredJobs.jsp	3K	2020-06-25 15:09:59

- Choose from ALL files

  When this option is selected, you can choose to delete any file(s) and/or folder(s) in the selected backup set.



Delete Backup Data

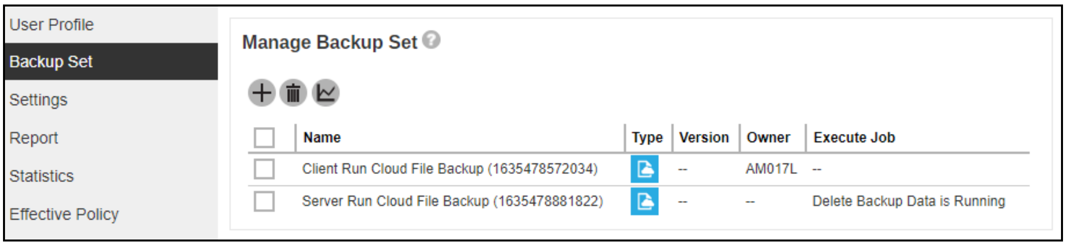
Select what to delete

Choose from ALL files

	File	Size	Last Modified
☑	Monitoring_AdministrationLogs_ActivitiesLog.jsp	4K	2020-06-25 14:44:09
☑	Monitoring_AdministrationLogs_AuditTrails.jsp	4K	2020-06-25 15:21:00
☑	Monitoring_AdministrationLogs_MessageHistory.jsp	1K	2020-06-25 14:44:40
☑	Monitoring_AdministrationLogs_SNMPLog.jsp	3K	2020-06-25 14:17:50
☑	Monitoring_BackupRestoreLogs_ActivitiesLog.jsp	4K	2020-06-25 15:31:11
☑	Monitoring_BackupRestoreLogs_BackupErrors.jsp	2K	2020-06-25 15:08:54
☑	Monitoring_BackupRestoreLogs_BackupJobs.jsp	4K	2020-06-25 15:50:29
☑	Monitoring_BackupRestoreLogs_BackupSetLog.jsp	3K	2020-06-25 15:13:16

5. After selecting the backup data to be deleted, click the 🗑 icon to proceed.

6. Running delete backup data job will be indicated.



Manage Backup Set

□	Name	Type	Version	Owner	Execute Job
□	Client Run Cloud File Backup (1635478572034)		--	AM017L	--
□	Server Run Cloud File Backup (1635478881822)		--	--	Delete Backup Data is Running

NOTE

Delete backup data action is not reversible. It will physically delete the selected backup data regardless of the defined retention policy settings. Therefore, make sure to select the correct backup data to be deleted before you proceed.

9 Contact Ahsay

9.1 Technical Assistance

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

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

9.2 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.