



Ahsay Cloud Backup Suite v8

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

Ahsay Systems Corporation Limited

11 October 2021

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 |
| 25 January 2021 | Updated screenshot in Ch. 2.5; Updated login steps in Ch. 3; Updated PDIC diagram in Ch. 5 | Modification |
| 19 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 Limitations in Ch. 2.8 and added notes for Periodic Data Integrity Check (PDIC) Process in Ch. 5.1 | New |
| 11 October 2021 | Updated supported browsers in Ch. 2.2; Updated login instructions in Ch. 3; Added rebuild index in Ch. 8 | New / Modifications |

Table of Contents

| | | |
|-----------|--|-----------|
| 1 | Overview | 1 |
| 1.1 | What is this software?..... | 1 |
| 1.2 | System Architecture..... | 1 |
| 1.3 | Why should I use AhsayCBS Run on Server (Agentless) Solution to back up my cloud data? | 2 |
| 1.4 | About This Document | 6 |
| 2 | Preparing for Backup and Restore | 8 |
| 2.1 | Internet / Network Connection..... | 8 |
| 2.2 | Supported Browsers | 8 |
| 2.3 | Valid AhsayOBM/AhsayACB User Account | 8 |
| 2.4 | Ahsay License Requirements | 8 |
| 2.5 | Add-on Module Requirements | 8 |
| 2.6 | Cloud Sources | 10 |
| 2.7 | Login Credentials to Cloud Storage | 10 |
| 2.8 | Limitations | 10 |
| 2.9 | Best Practices and Recommendations..... | 13 |
| 3 | Logging in to AhsayCBS User Web Console | 15 |
| 3.1 | Login to AhsayCBS without 2FA | 15 |
| 3.2 | Login to AhsayCBS with 2FA using authenticator app | 17 |
| 3.3 | Login to AhsayCBS with 2FA using Twilio..... | 21 |
| 4 | Creating a Cloud File Backup Set | 23 |
| 5 | Overview of Run on Server Cloud File Backup Process | 33 |
| 5.1 | Periodic Data Integrity Check (PDIC) Process | 34 |
| 5.2 | Backup Set Index Handling Process | 36 |
| 5.2.1 | Start Backup Job..... | 36 |
| 5.2.2 | Completed Backup Job | 37 |
| 5.3 | Data Validation Check Process..... | 38 |
| 6 | Running a Backup Job | 39 |
| 7 | Restoring a Cloud File Backup Set | 44 |
| 8 | Running Data Integrity Check | 48 |
| 9 | Performing Space Freeing Up | 50 |
| 10 | Deleting Backup Data | 52 |
| 11 | Contact Ahsay | 55 |

11.1 Technical Assistance 55
11.2 Documentation..... 55

1 Overview

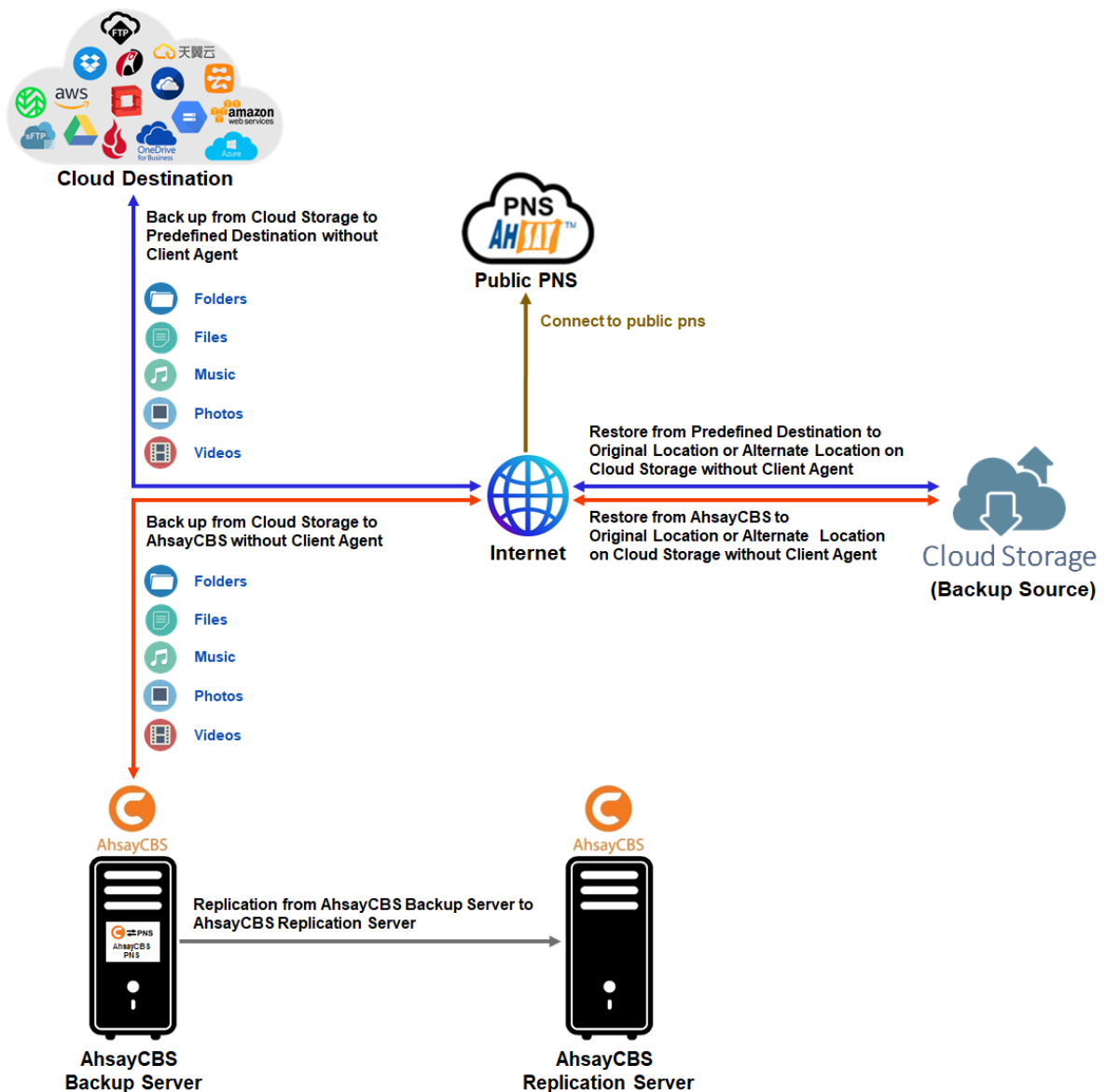
1.1 What is this software?

Ahsay Cloud Backup Suite v8 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, and to manage and monitor your backups.

1.2 System Architecture

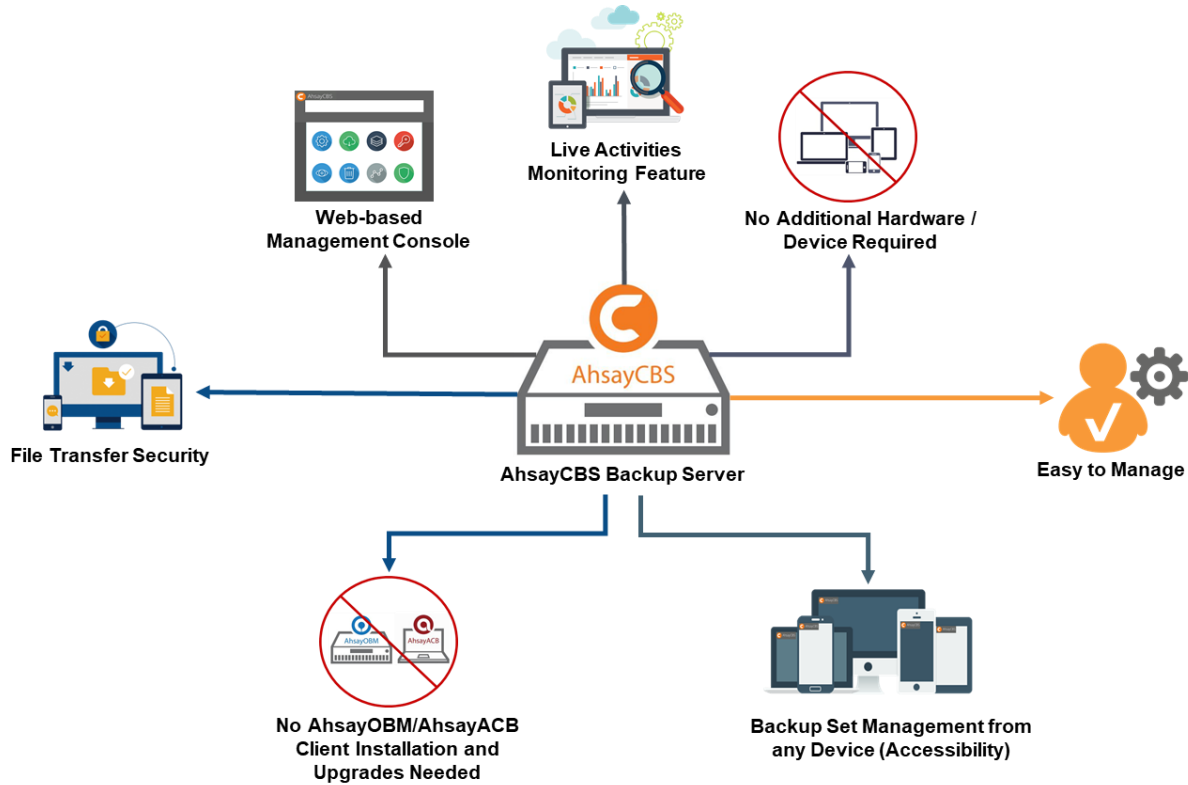
For agentless backup and restore, the AhsayCBS backup server connects to the cloud storage directly through the internet without the need to deploy additional backup agents on the customer's site.

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.



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.



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 or finished within 1 hour
- View the status of the restore process that is currently running or finished within 1 hour

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

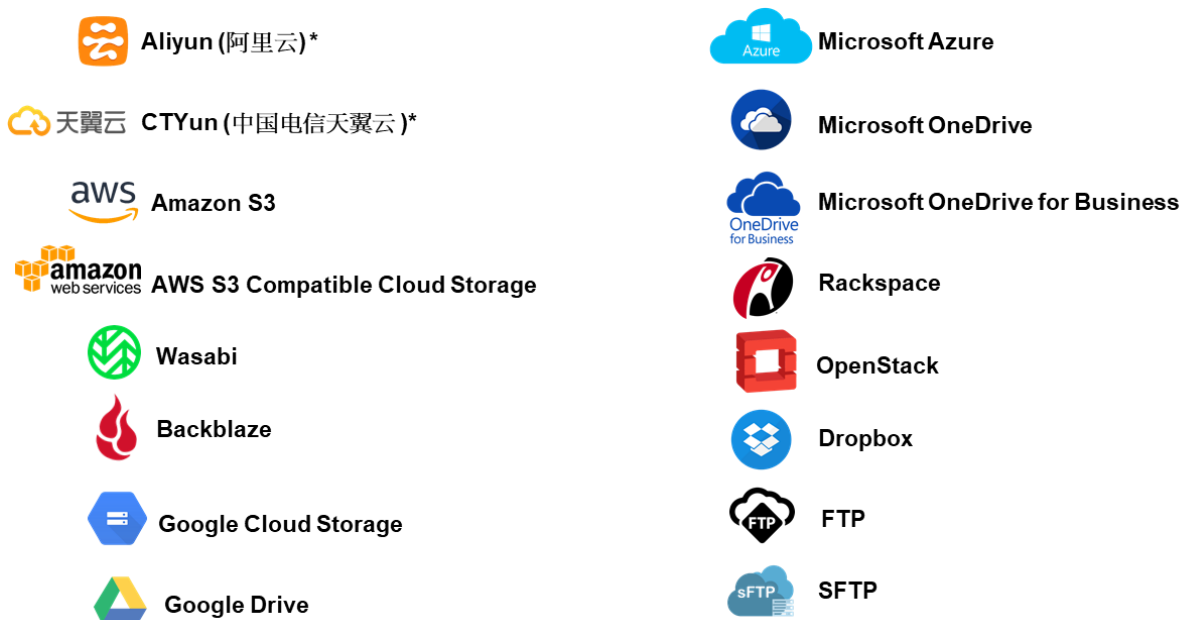
Some organizations do not permit the installation of third-party applications on the production environments due to regulatory requirements. An agentless backup and recovery solution allow for compliance during backup or restore.

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:



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 | ✗ | ✓ |
| In-File Delta | ✓ | ✓ |
| Retention Policy | ✓ | ✓ |
| Command Line Tool | ✗ | AhsayOBM / AhsayACB for Windows only |
| Reminder | ✗ | AhsayOBM / AhsayACB for Windows only |
| Restore Filter | ✗ | ✓ |
| Bandwidth Control | ✓ | ✓ |
| IP Allowed for Restore | ✗ | ✓ |
| System Logs of Data Integrity Check and Space Freeing Up | ✗ | ✓ |
| 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 v8 User Guide – Cloud File Backup & Restore for Windows](#)

[AhsayOBM v8 User Guide – Cloud File Backup & Restore for Mac](#)

[AhsayACB v8 User Guide – Cloud File Backup & Restore for Windows](#)

[AhsayACB v8 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, performing space freeing up 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: Performing a Space Freeing Up

Performing a Space Freeing Up using AhsayCBS User Web Console

Perform a space free up using AhsayCBS User Web Console

Part 6: 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, Space Freeing Up 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.

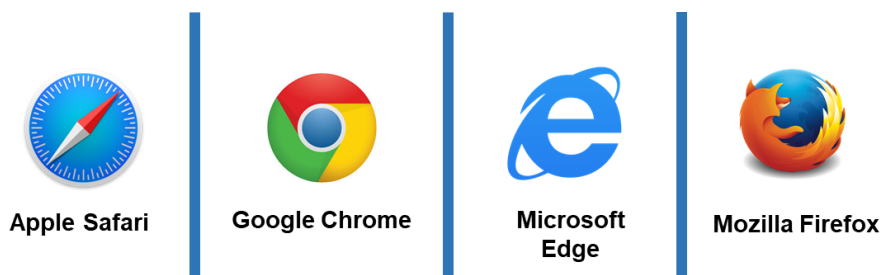
2 Preparing for Backup and Restore

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.

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

The screenshot shows the 'Backup Client Settings' tab for an AhsayOBM user account. The 'Backup Client' section has 'AhsayOBM User' selected. Under 'Add-on Modules', 'In-File Delta' is checked and highlighted with a red box. Other modules like Microsoft Exchange Server, MySQL Database Server, Lotus Domino, Windows System Backup, VMware, Microsoft Exchange Mailbox, NAS - QNAP, Mobile (max. 10), Volume Shadow Copy, OpenDirect / Granular Restore, and MariaDB Database Server are unchecked. On the right, Microsoft SQL Server, Oracle Database Server, Lotus Notes, Windows System State Backup, Hyper-V, ShadowProtect System Backup, NAS - Synology, Continuous Data Protection, and Office 365 Backup are also unchecked.

For AhsayACB user account

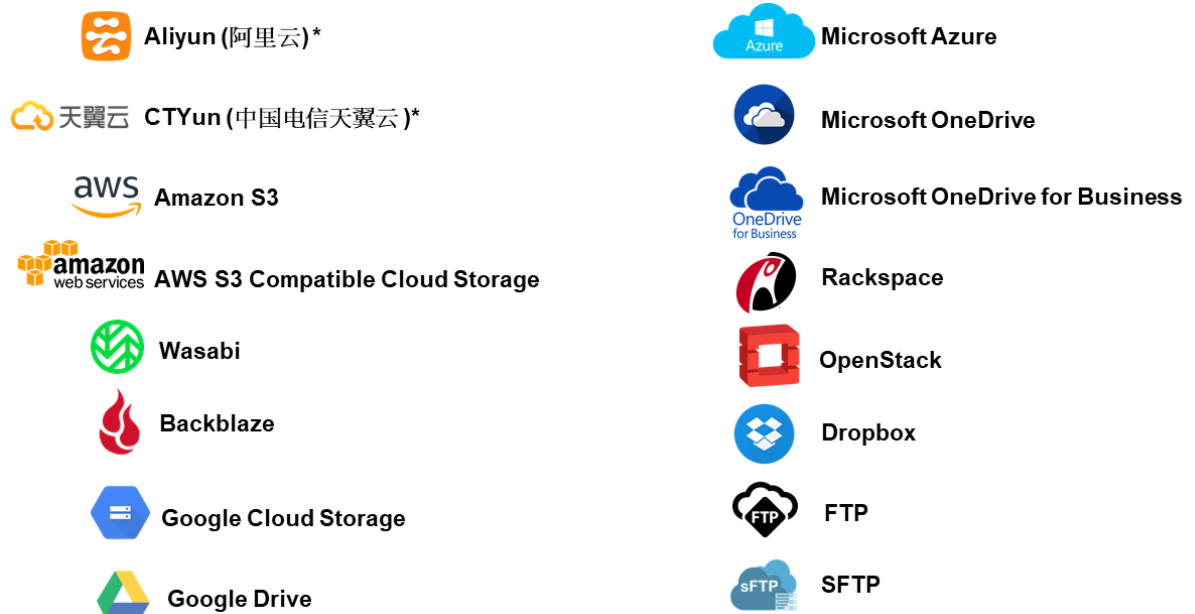
The screenshot shows the 'Backup Client Settings' tab for an AhsayACB user account. The 'Backup Client' section has 'AhsayACB User' selected. Under 'Add-on Modules', 'In-File Delta' is checked and highlighted with a red box. Other modules like Windows System Backup, Mobile (max. 10), Volume Shadow Copy, OpenDirect / Granular Restore, Lotus Notes, Continuous Data Protection, and Office 365 Backup are unchecked.

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:



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.

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 following operations through the AhsayCBS user console:

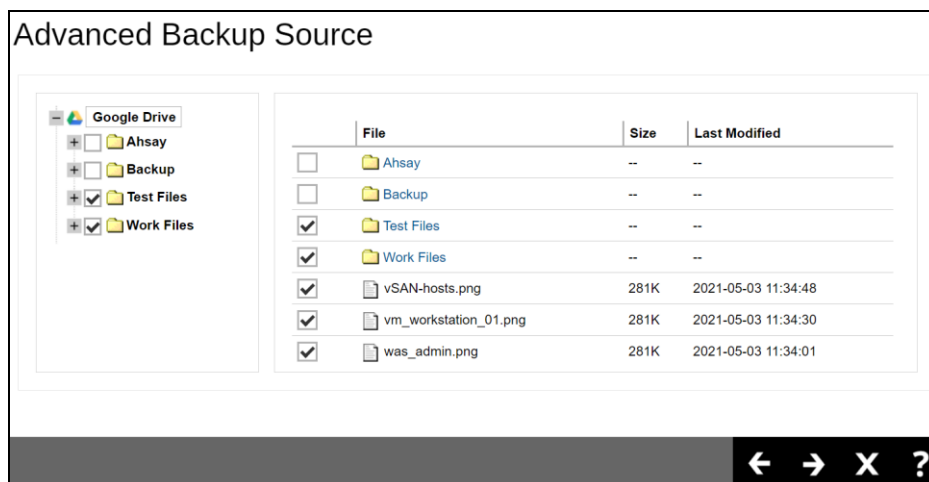
- Data Integrity Check
- Space Freeing Up

Therefore, the backup user does not have the ability to verify the results of these operations without the assistance of the backup service provider.

Backup Source Selection

For backup source selection:

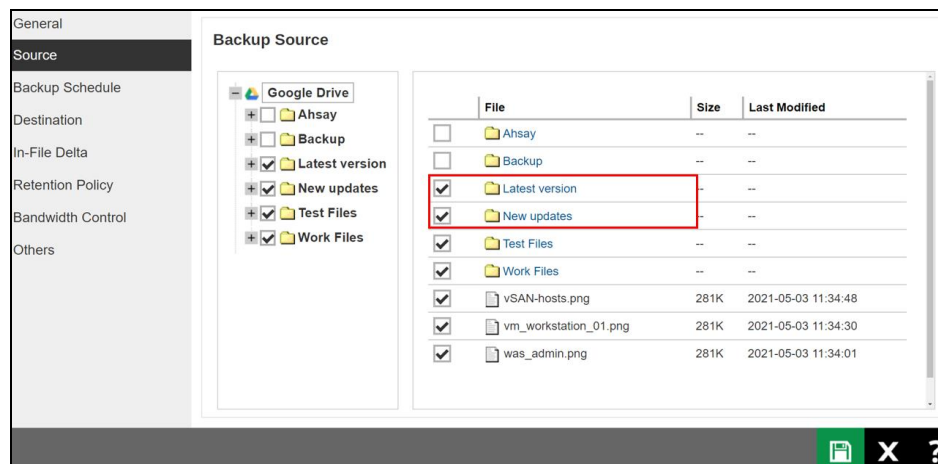
1. It is currently not possible to select the entire contents of the Cloud drive. Existing top level folders and/or files must be selected individually. If you need to back up the contents of the entire Cloud drive, then all top level folders and/or files must be selected.



- 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.

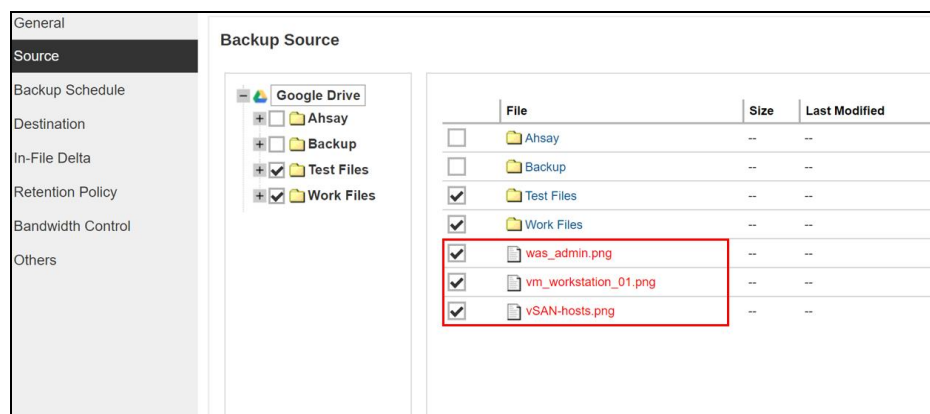


- If there are any top level folders and/or files which have been deleted from the Cloud drive since the last backup job, they will not be removed from the backup source automatically. The backup set will have to be manually updated to unselect the deleted top level folders and/or files. Otherwise, the backup job will be completed with warnings.

Example:

The following files were backed up but subsequently deleted from the top level backup source of the Cloud drive: **was_admin.png**, **vm_workstation_01.png**, **vSAN-hosts.png**. The next backup job will encounter the following warnings until these deleted files are unselected from the backup source.

The deleted files are highlighted in red on the backup source to indicate that they no longer exist on the Cloud storage account.



Backup log

```
[2021/05/04 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 !",0,0,0,,,
```

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 Logging in to AhsayCBS User Web Console

Starting with AhsayCBS 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 to AhsayCBS without 2FA](#)
- [Login to AhsayCBS with 2FA using authenticator app](#)
- [Login to AhsayCBS with 2FA using Twilio](#)

3.1 Login to AhsayCBS without 2FA

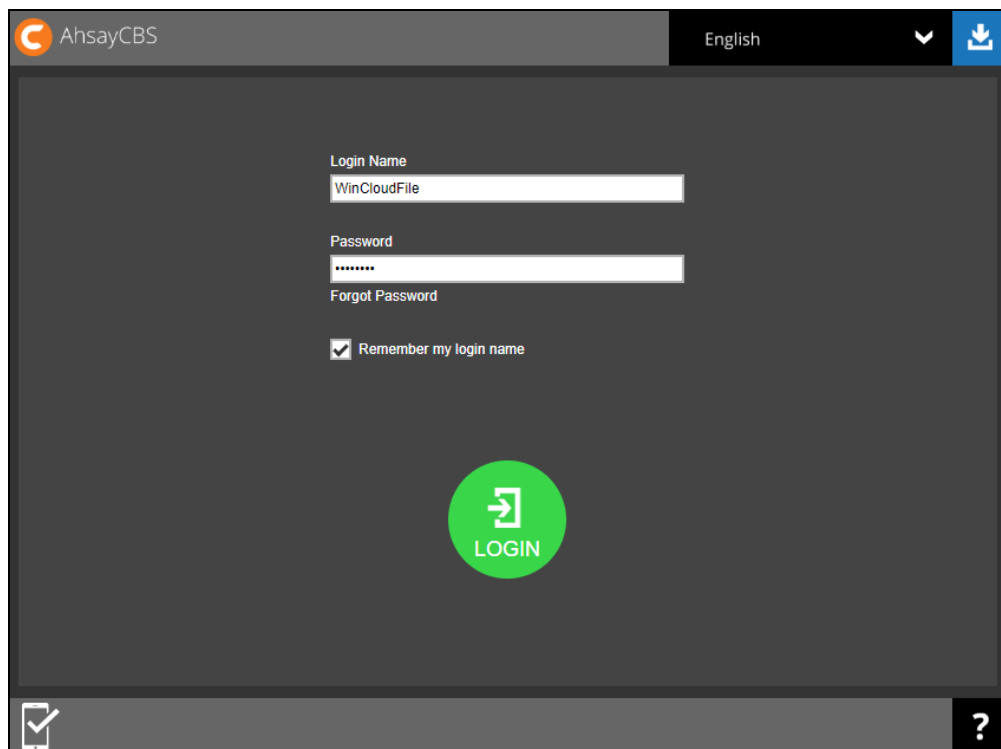
1. Log in to AhsayCBS web console at:

https://backup_server_hostname:port

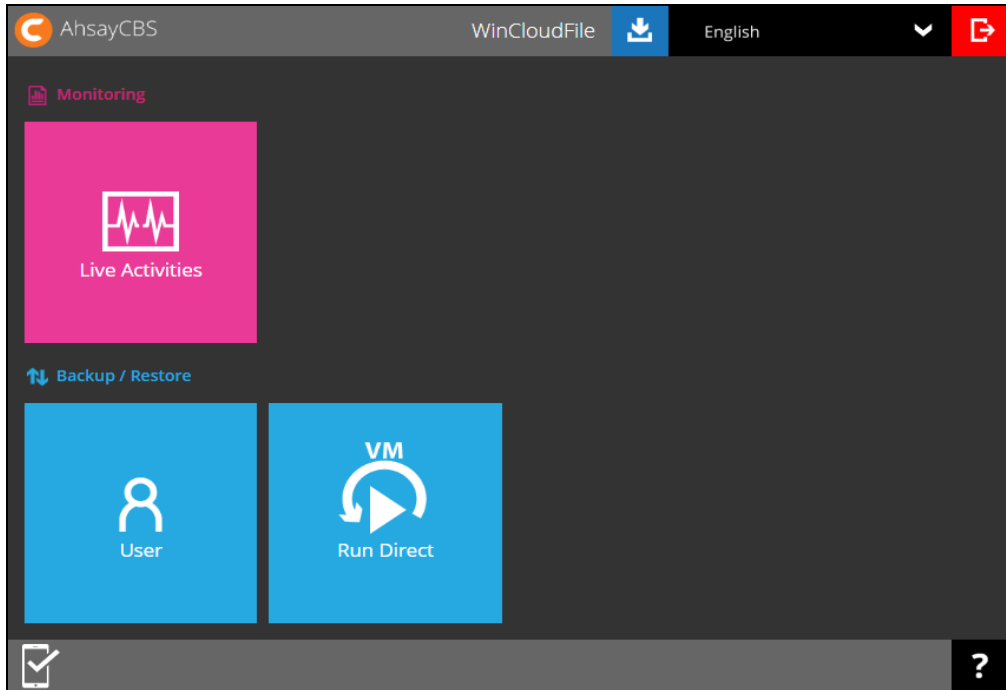
NOTE

Contact your backup service provider for the URL to connect to the web console if necessary.

2. Enter the **Login Name** and **Password** of your AhsayOBM/AhsayACB account then click **LOGIN**.



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



NOTE

The VM Run Direct tile may not be available. Please contact your backup service provider for more information.

3.2 Login to AhsayCBS with 2FA using authenticator app

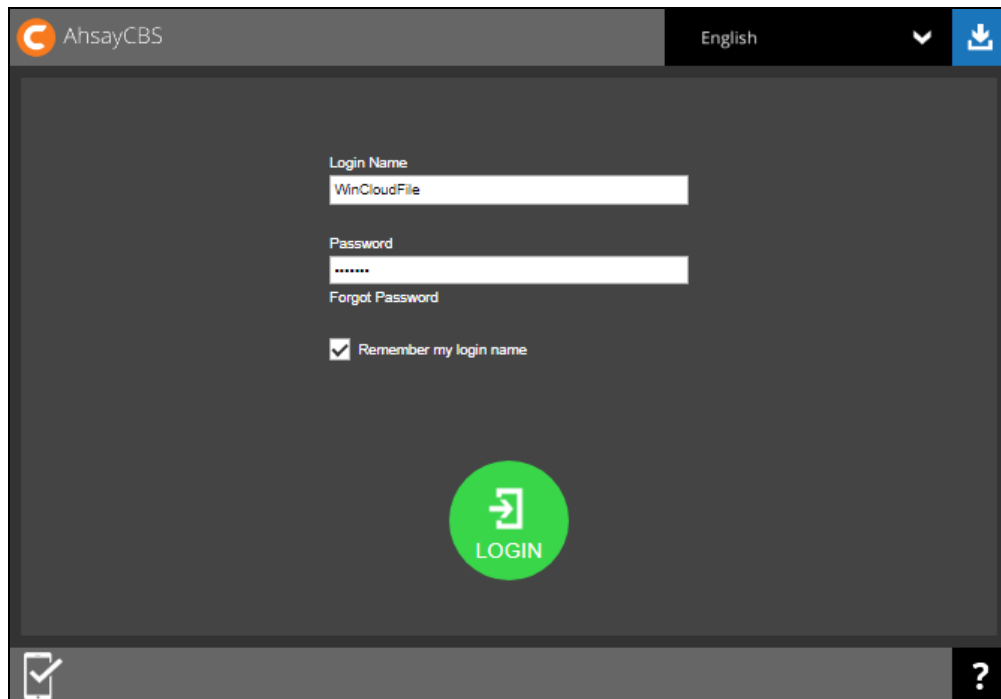
1. Log in to AhsayCBS web console at:

https://backup_server_hostname:port

NOTE

Contact your backup service provider for the URL to connect to the web console if necessary.

2. Enter the **Login Name** and **Password** of your AhsayOBM/AhsayACB account then click **LOGIN**.



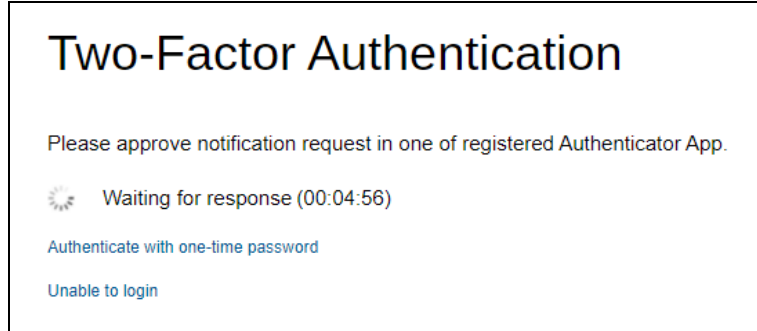
3. One of the two authentication methods will be displayed to continue with the login:

- ⦿ [Push Notification and TOTP when using Ahsay Mobile app](#)
- ⦿ [TOTP only](#)

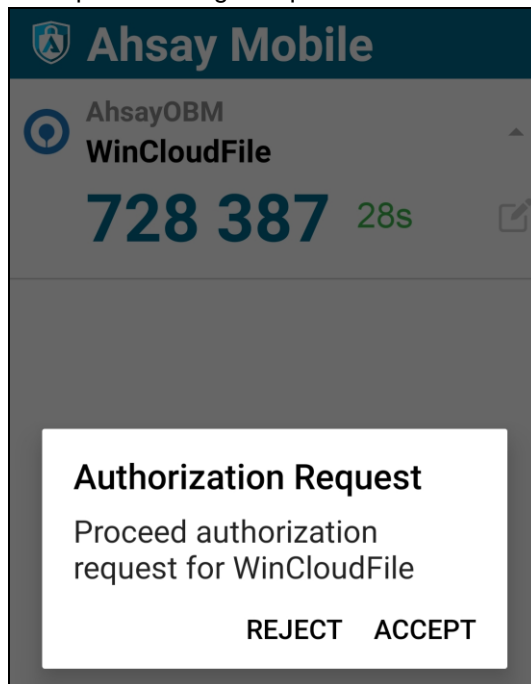
-
- ⦿ If **Ahsay Mobile app** was configured to use Push Notification and TOTP then there are two 2FA modes that can be used:

- Push Notification (default)

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

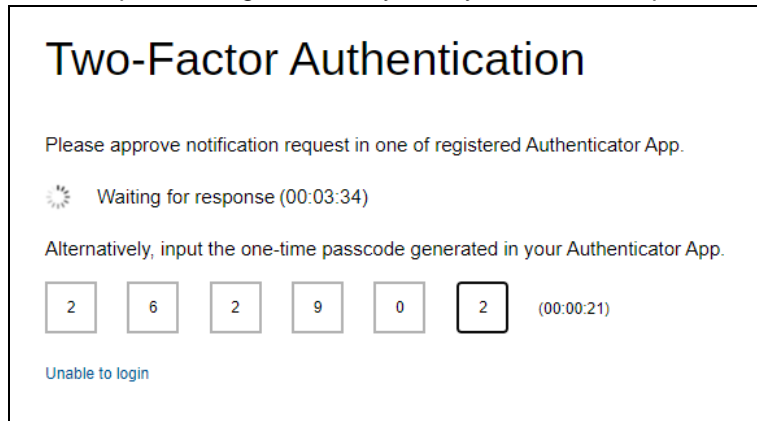


Example of the login request sent to the Ahsay Mobile app.



- 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.



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

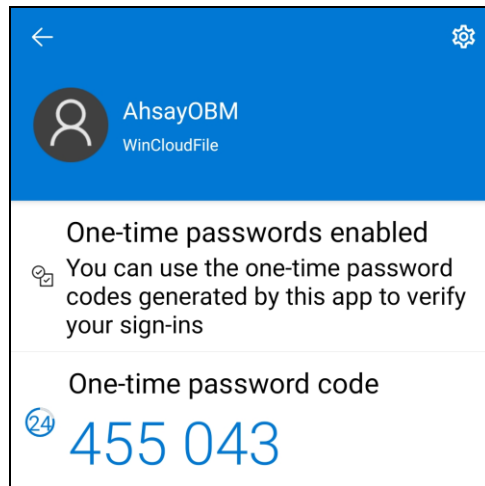


- TOTP only

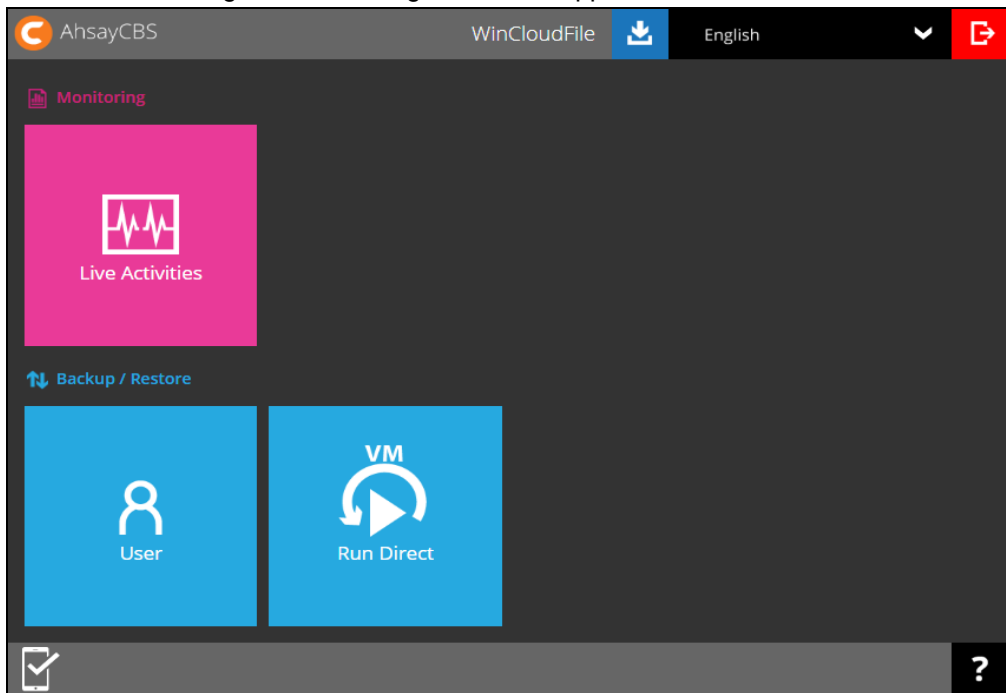
Enter the one-time passcode generated by the authenticator app to complete the login.



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



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



NOTE

The VM Run Direct tile may not be available. Please contact your backup service provider for more information.

3.3 Login to AhsayCBS with 2FA using Twilio

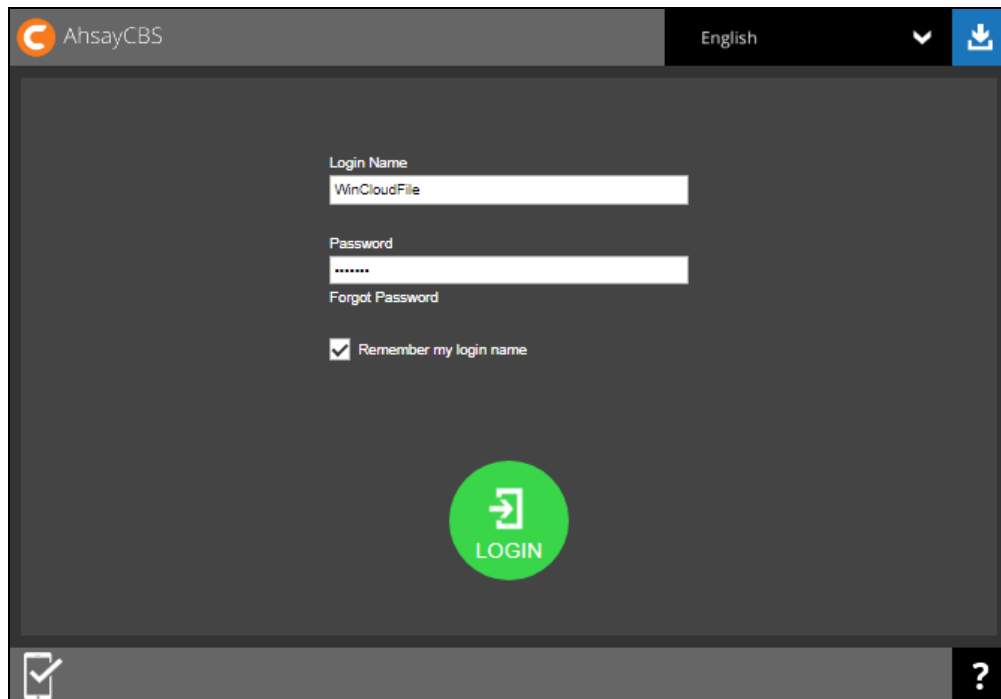
1. Log in to AhsayCBS web console at:

https://backup_server_hostname:port

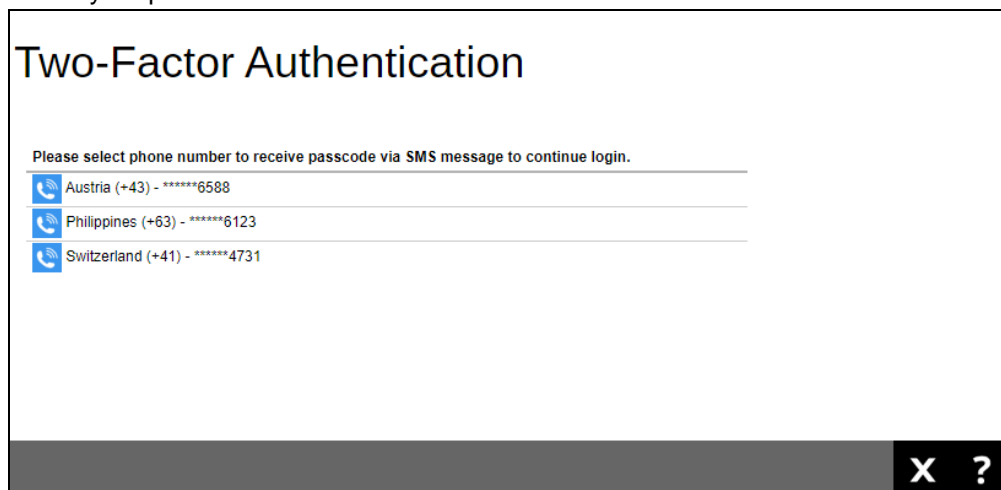
NOTE

Contact your backup service provider for the URL to connect to the web console if necessary.

2. Enter the **Login Name** and **Password** of your AhsayOBM/AhsayACB account then click LOGIN.



3. Select your phone number.



4. Enter the passcode and click Verify to login.

Two-Factor Authentication

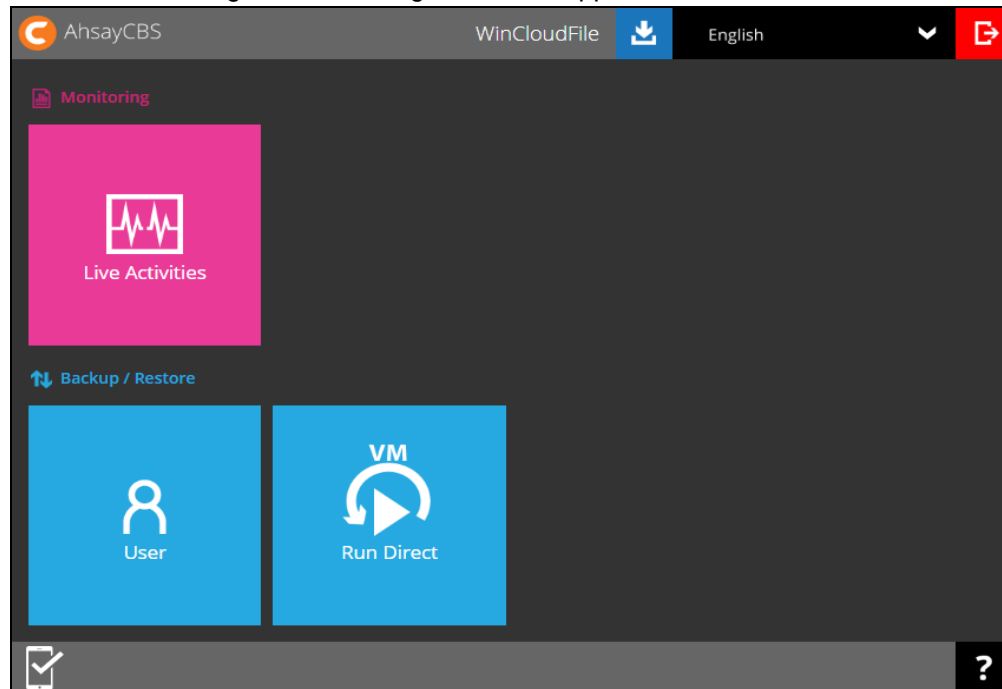
SMS message with a passcode was already sent to the phone number +63-*****6123 Please enter the passcode to continue login.

HQDW - (00:04:54)

Resend passcode

✓ ✕ ?

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

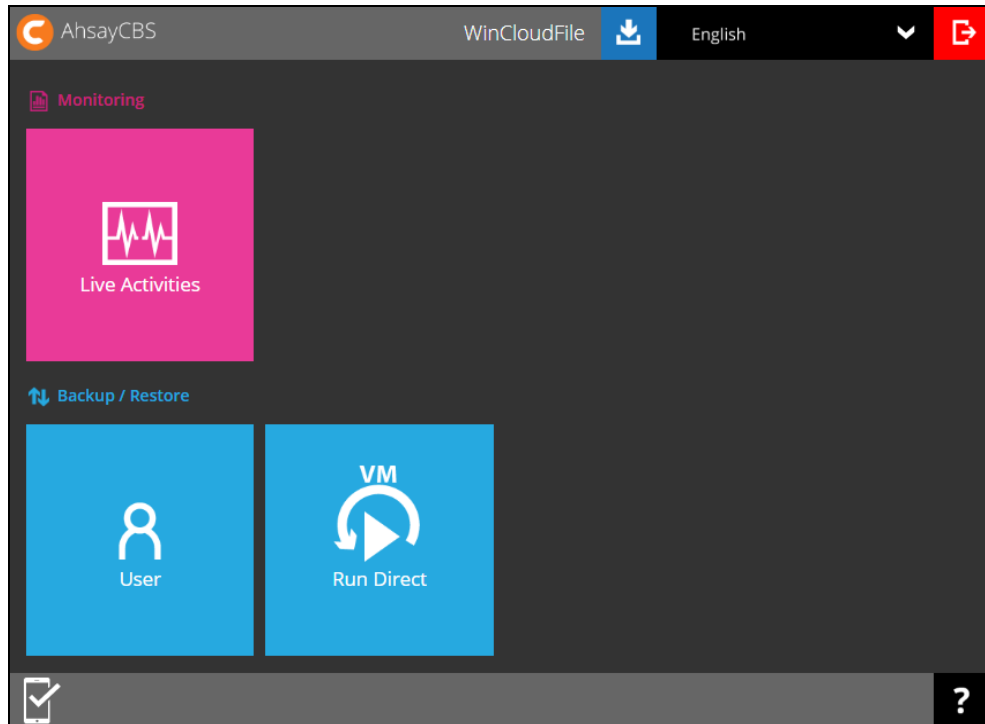


NOTE

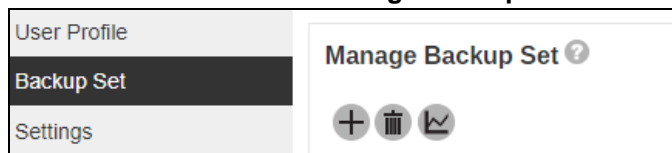
The VM Run Direct tile may not be available. Please contact your backup service provider for more information.

4 Creating a Cloud File Backup Set

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



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



4. 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

- 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

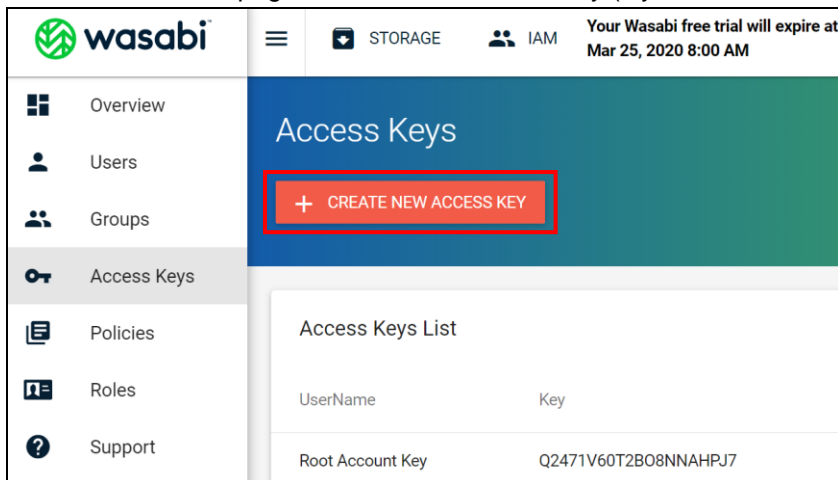
This setting **CANNOT** be altered once the backup set is created. If you wish to change the backup method later, you will have to create a new backup set and start over the configurations again.

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

Backup From


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


- 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**.

[DOWNLOAD CSV](#) [COPY KEYS TO CLIPBOARD](#)

Access Key:
11L1RS7KSCS14APIKQIV 

Secret Key: [Hide](#)
dfXPW71bmB3JvrPjemXdatU3j89J2eZeMhp4TKLT 

[CLOSE](#)

Backup From

Access Key ID

Access Key Secret

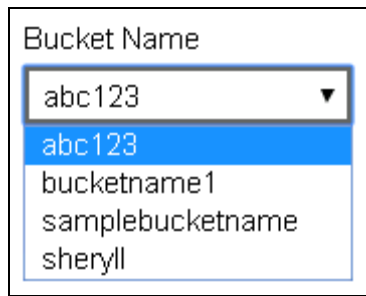
Connect with SSL

Access the Internet through Proxy

[Test](#)

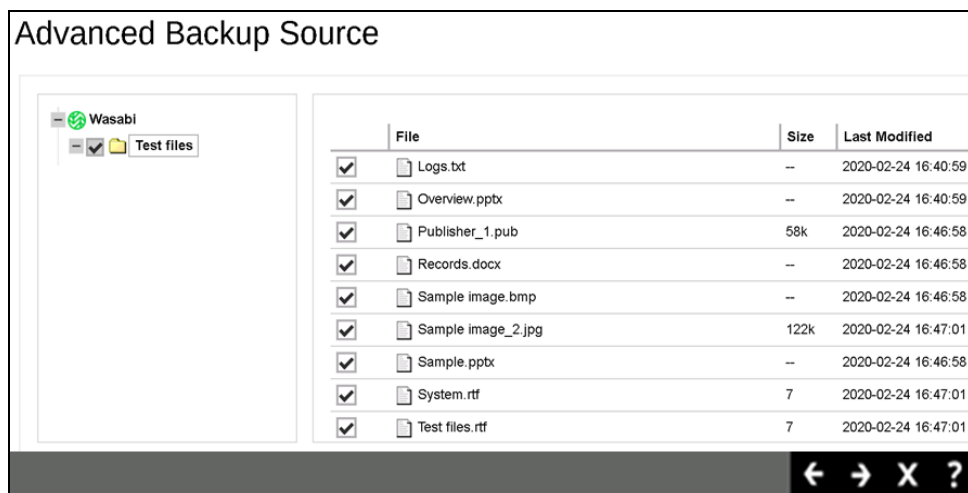
[Sign up for Wasabi](#)

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.



NOTES

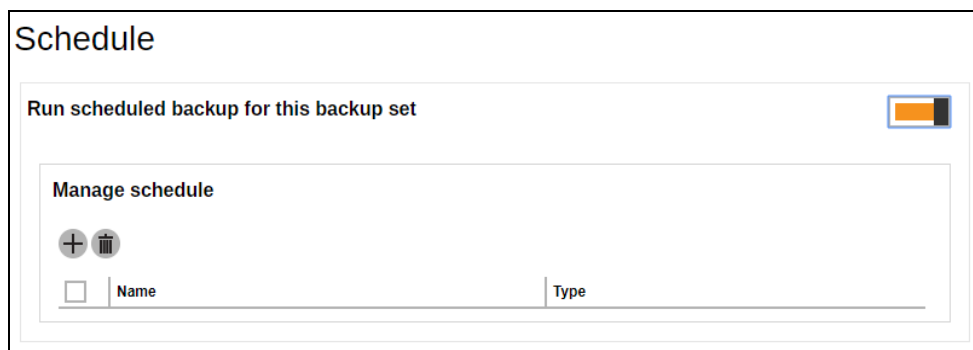
1. The authentication request will be opened in a new tab or window. Ensure that the pop-up window is not blocked, and pop-up blocker is disabled in your browser.
 2. It is advised to have one (1) bucket name per cloud file backup set.
11. In the Advanced Backup Source, select the file(s) and/or folder(s) that you want to back up then click **Next** to proceed.



NOTE: There are limitations in selecting files and/or folders in the backup source menu. For further details, please refer to the [Backup Source Selection](#) on **Chapter 2.8 Limitations**.

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.



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 which 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 which 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 the time of that which 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 the time of that date which the backup job will run.

Details

Name
Custom

Type
Custom

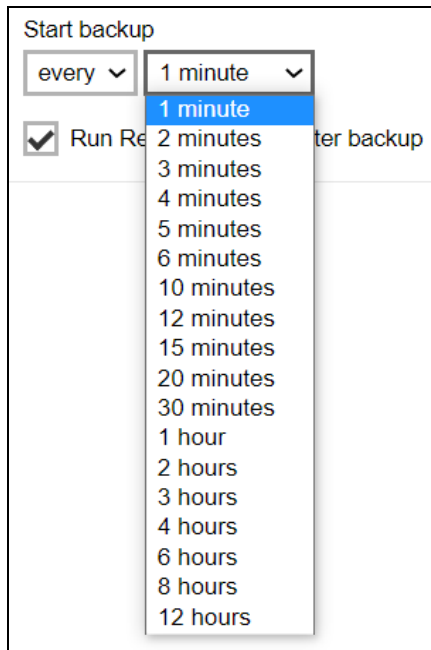
Backup on the following day once
2020 July 21

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.



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

 A screenshot of a backup configuration form titled 'Details'. The 'Name' field contains 'Weekly-1'. The 'Type' is set to 'Weekly'. Under 'Backup on these days of the week', checkboxes for Sun, Mon, Tue, Wed, Thu, and Fri are checked, while Sun and Sat are unchecked. The 'Start backup' is set to 'every' with a '4 hours' interval. The 'Run Retention Policy after backup' checkbox is checked.

Figure 1.1

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

 A screenshot of a backup configuration form titled 'Details'. The 'Name' field contains 'Weekly-2'. The 'Type' is set to 'Weekly'. Under 'Backup on these days of the week', checkboxes for Sun and Sat are checked, while Mon, Tue, Wed, Thu, and Fri are unchecked. The 'Start backup' is set to 'at' with a time of '21 : 00'. The 'Stop' dropdown is set to 'until full backup completed'. The 'Run Retention Policy after backup' checkbox is checked.

Figure 1.2

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.



In the sample screenshot above, the backup service provider has set up four (4) available destinations (i.e. ColdStor, AWSComStor, 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 alphanumeric 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

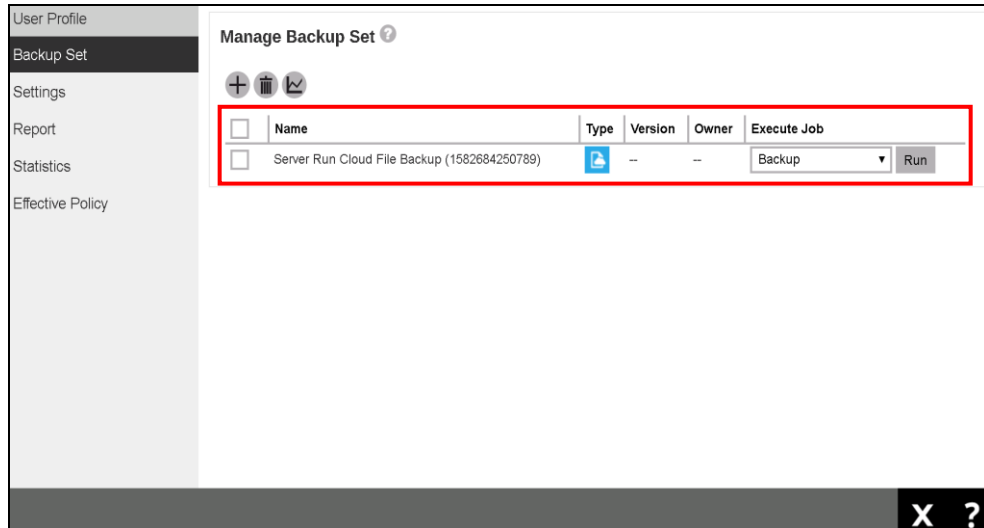
Re-type encrypting key

Method
 ECB CBC

Key length
 128-bit 256-bit

← X ?

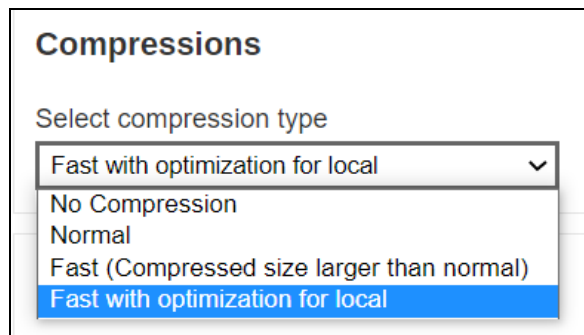
15. Click the  icon at the bottom right corner to confirm the creation of this backup set.
16. The cloud file backup set is created successfully.




17. The cloud file backup set is successfully created.
18. 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

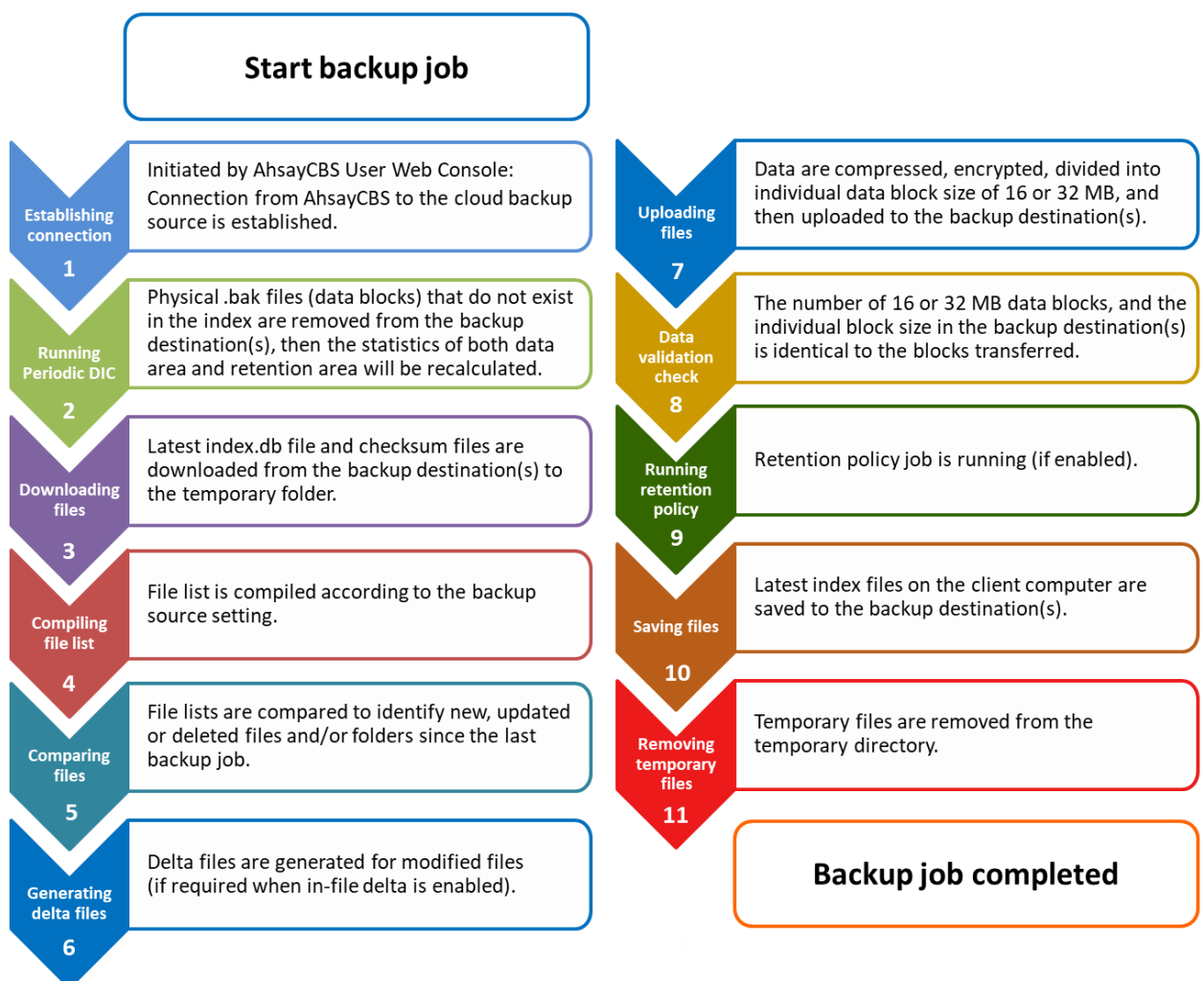


Click the  icon at the bottom right corner to confirm the selected compression type.

5 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 \(Step 8\)](#)



5.1 Periodic Data Integrity Check (PDIC) Process

For AhsayCBS 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:

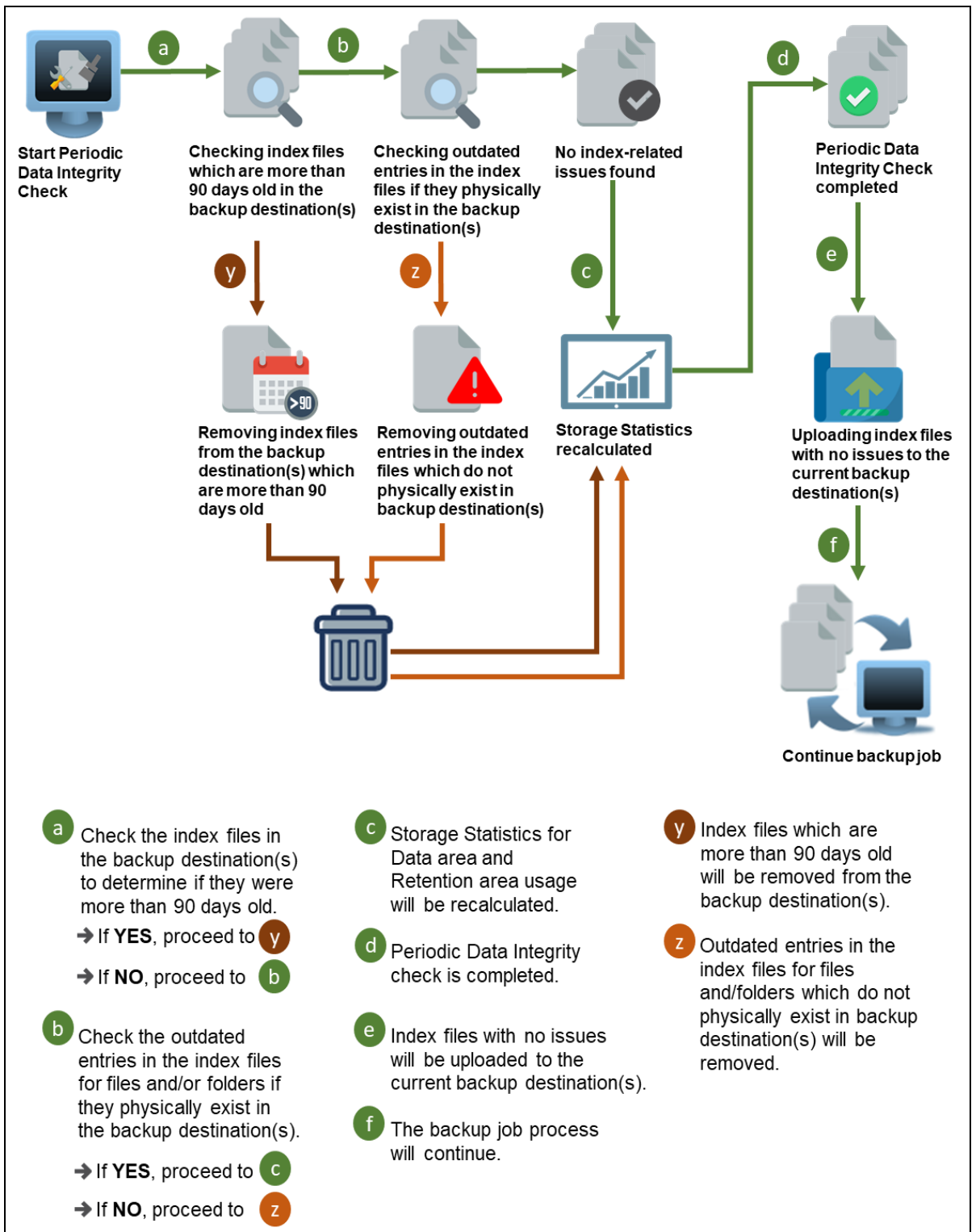
- the PDIC will run on the first backup job that falls on Wednesday; or
- if there is no active backup job(s) running from Monday to Friday, then the PDIC will run on the next available backup job.

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:

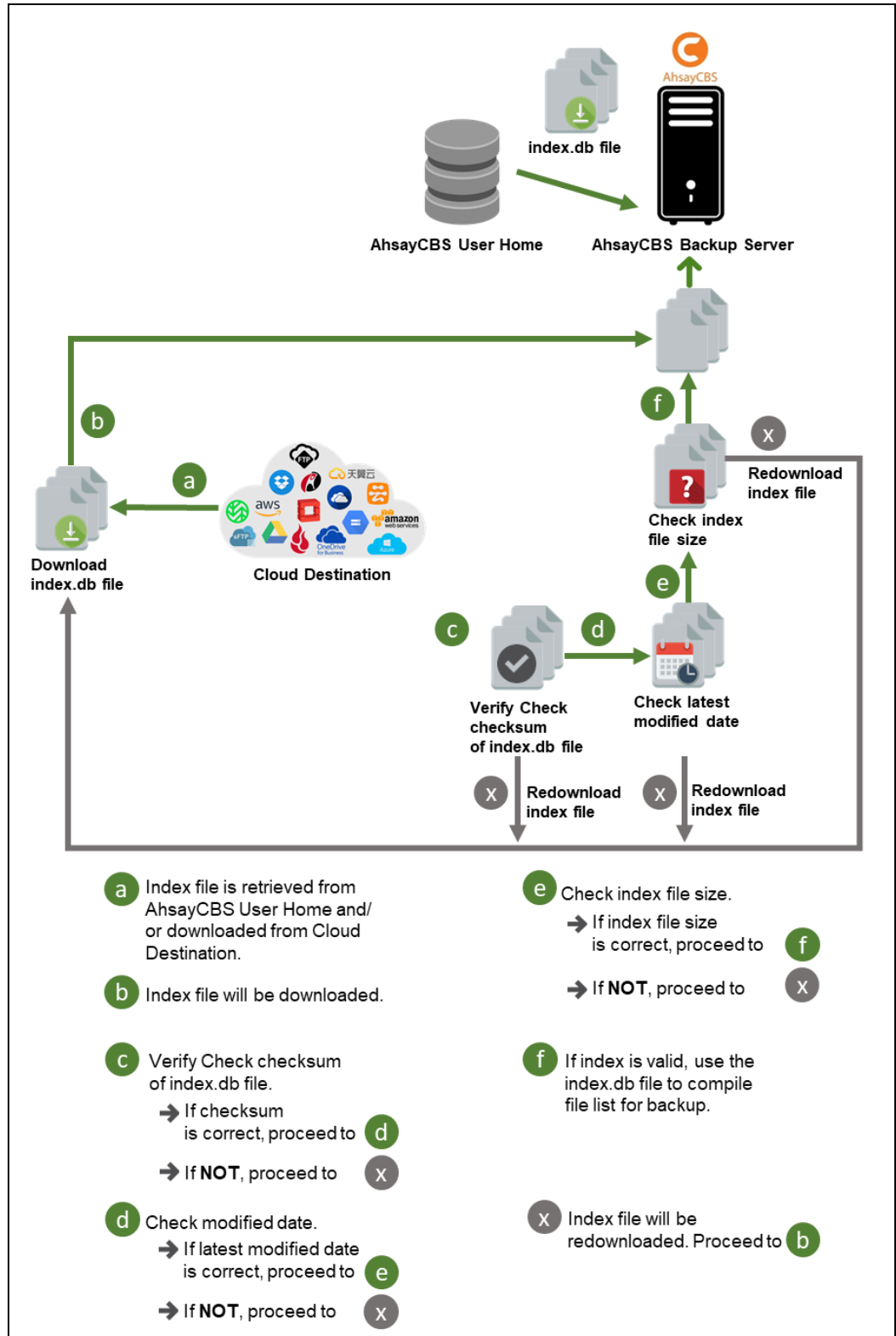
1. If AhsayCBS was upgraded to v8.5 (or above) from an older version v7, or pre-8.3.6.0 version. In this case, the PDIC job will run on the first backup job after upgrade.
2. If backup jobs for a backup set are not run on a regular daily backup schedule (for example: on a weekly or monthly schedule), 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.



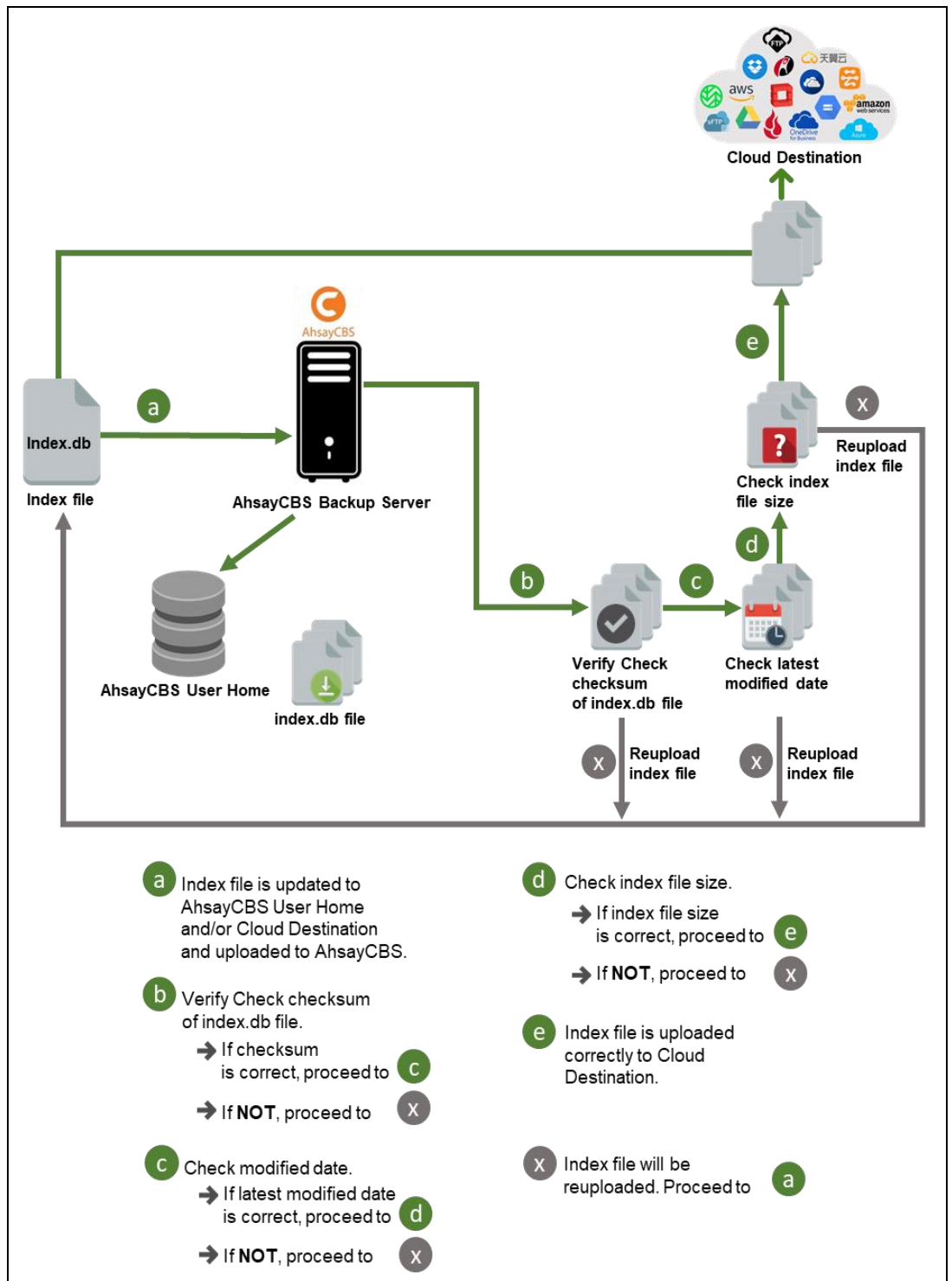
5.2 Backup Set Index Handling Process

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.

5.2.1 Start Backup Job

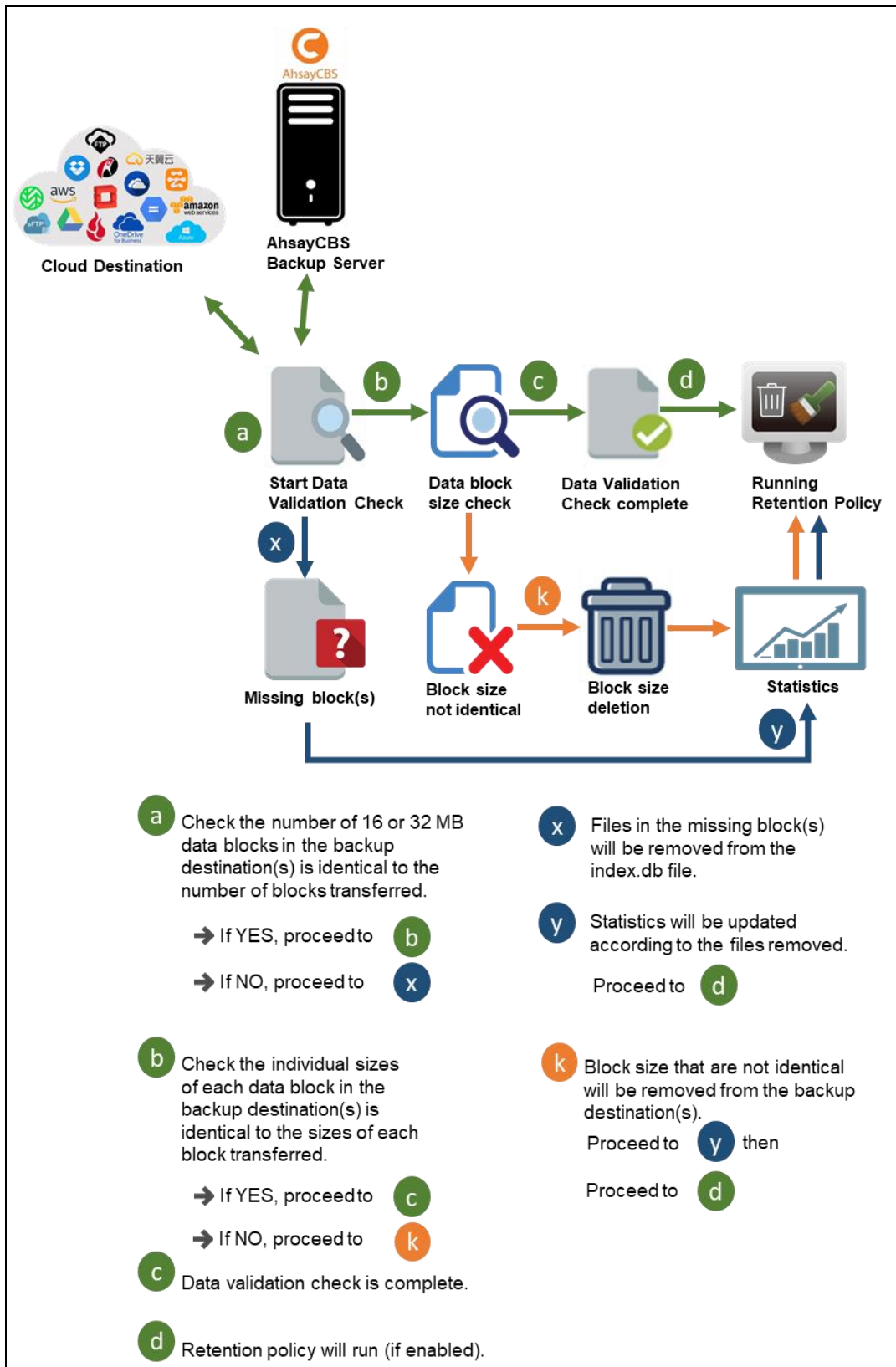


5.2.2 Completed Backup Job



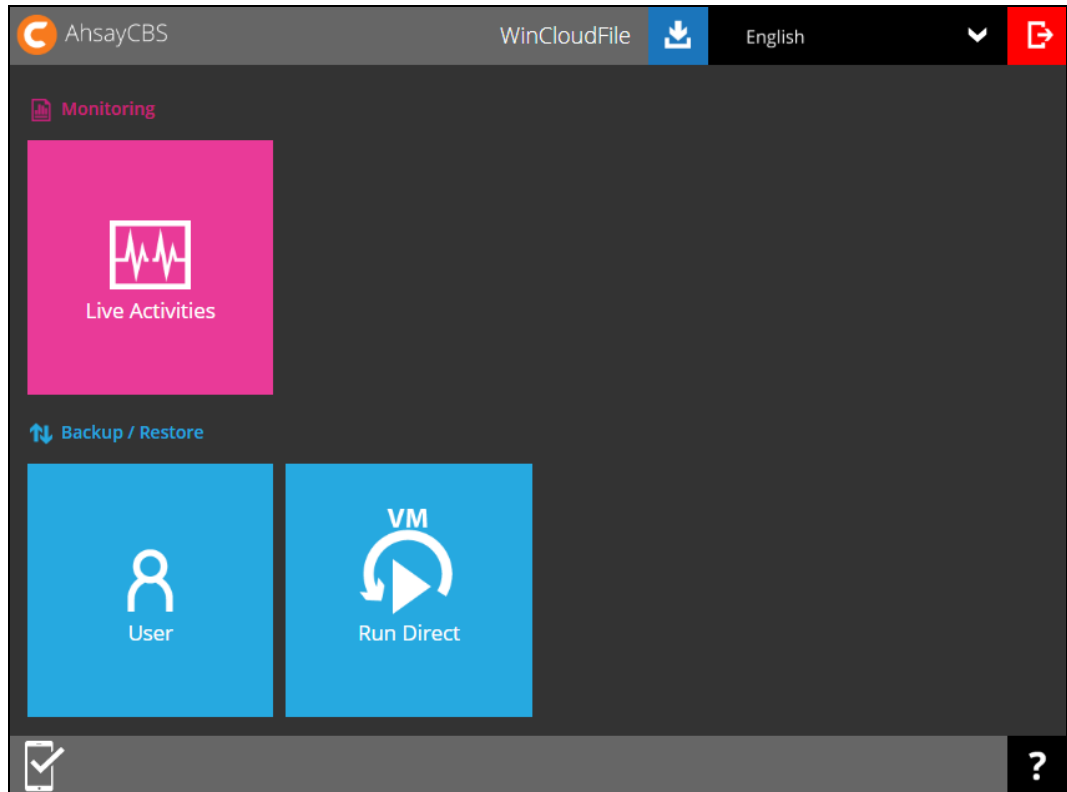
5.3 Data Validation Check Process

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.

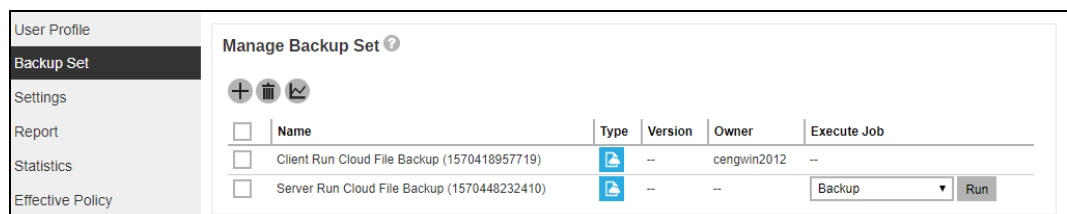
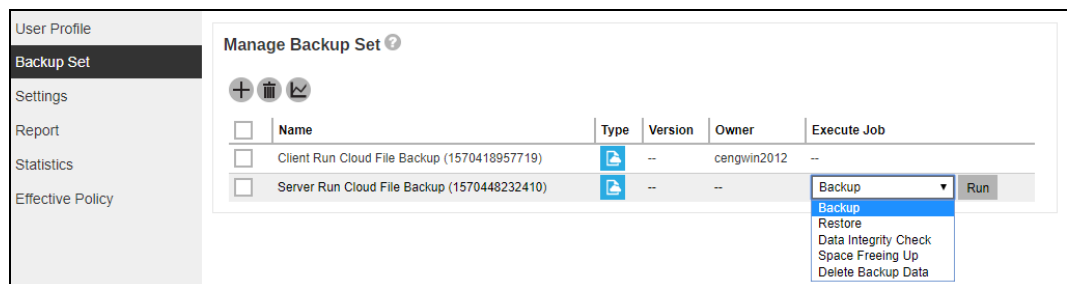


6 Running a Backup Job

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



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



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


Backup

In-File Delta type


Full
 Differential
 Incremental

Retention Policy

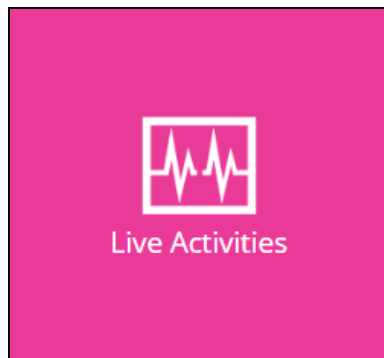
Run Retention Policy after backup

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.

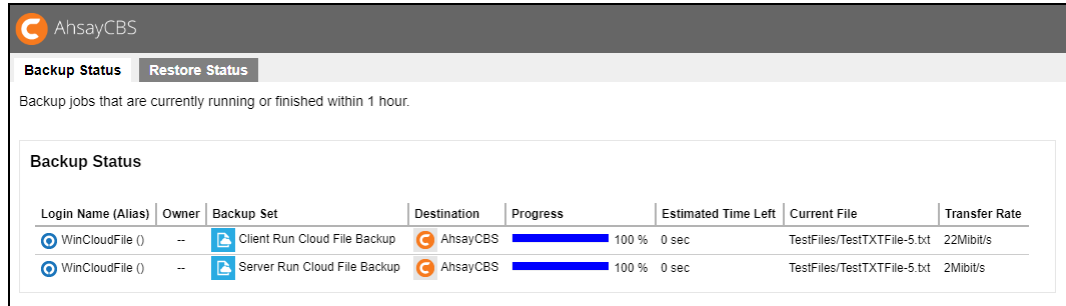
| User Profile Backup Set Settings Report Statistics Effective Policy | <h3 style="margin: 0;">Manage Backup Set ?</h3> <div style="text-align: center; margin-bottom: 10px;">  </div> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 5%;"></th> <th style="width: 60%;">Name</th> <th style="width: 10%;">Type</th> <th style="width: 10%;">Version</th> <th style="width: 10%;">Owner</th> <th style="width: 5%;">Execute Job</th> </tr> </thead> <tbody> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td>Client Run Cloud File Backup (1570418957719)</td> <td></td> <td>--</td> <td>cengwin2012</td> <td style="text-align: center;">--</td> </tr> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td>Server Run Cloud File Backup (1570448232410)</td> <td></td> <td>--</td> <td>--</td> <td style="text-align: center;">Backup is Running Stop</td> </tr> </tbody> </table> | | Name | Type | Version | Owner | Execute Job | <input type="checkbox"/> | Client Run Cloud File Backup (1570418957719) | | -- | cengwin2012 | -- | <input type="checkbox"/> | Server Run Cloud File Backup (1570448232410) | | -- | -- | Backup is Running Stop |
|---|---|------|---------|-------------|---|-------|-------------|--------------------------|--|--|----|-------------|----|--------------------------|--|--|----|----|---|
| | Name | Type | Version | Owner | Execute Job | | | | | | | | | | | | | | |
| <input type="checkbox"/> | Client Run Cloud File Backup (1570418957719) | | -- | cengwin2012 | -- | | | | | | | | | | | | | | |
| <input type="checkbox"/> | Server Run Cloud File Backup (1570448232410) | | -- | -- | Backup is Running Stop | | | | | | | | | | | | | | |

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

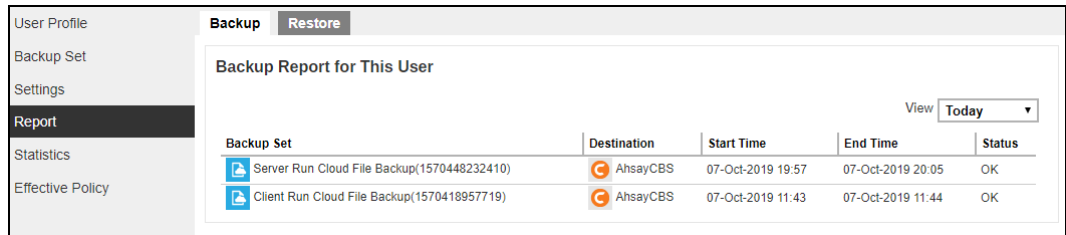


| <div style="display: flex; align-items: center;"> AhsayCBS </div> | | | | | | | |
|--|-------|------------------------------|-------------|--|---------------------|-------------------------------|---------------|
| Backup Status | | Restore Status | | | | | |
| Backup jobs that are currently running or finished within 1 hour. | | | | | | | |
| Backup Status | | | | | | | |
| Login Name (Alias) | Owner | Backup Set | Destination | Progress | Estimated Time Left | Current File | Transfer Rate |
| WinCloudFile () | -- | Client Run Cloud File Backup | AhsayCBS | <div style="width: 100%; height: 10px; background-color: #007bff; border: 1px solid #007bff;"></div> 100 % | 0 sec | TestFiles/TestTXTFile-5.txt | 22Mbit/s |
| WinCloudFile () | -- | Server Run Cloud File Backup | AhsayCBS | <div style="width: 17%; height: 10px; background-color: #007bff; border: 1px solid #007bff;"></div> 17 % | 4 min 45 sec | TestFiles/Attendance_2014.doc | 3Mbit/s |

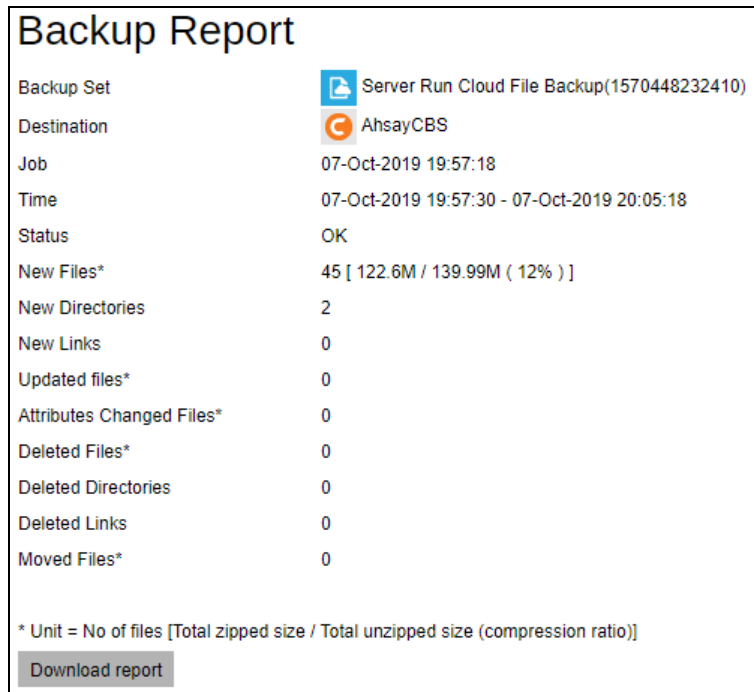
7. The backup through AhsayCBS User Web Console is successful.




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.



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.



Below is an example of a backup job report:


Full Backup report

Backup Job Summary

| | |
|----------------------------|--|
| User | WinCloudFile |
| Backup Set | Server Run Cloud File Backup (1570448232410) |
| Destination | AhsayCBS (AhsayCBS) |
| Data Size | 122.6M |
| Retention Size | 0 |
| Backup Quota | 50G |
| Remaining Quota | 49.76G |
| Backup Job | 2019-10-07-19-57-18 |
| Job Status | OK |
| Start - End | 10/07/2019 19:57:29 - 10/07/2019 20:05:18 |
| IP Address | 125.5.184.164 |
| New Files * | 45 (122.6M) |
| 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) |

* No. of files (size)

Backup Set Settings

| | |
|----------------------------|--|
| Field | Value |
| Backup Source | [Photos][TestFiles] |
| Filter | [Enabled: No] |
| Backup Schedule | [Computer Name: *][Daily:][Name: Daily Backup Schedule 01, Time: 20: 0, Type: , Duration: -1, Retention Policy: No][Weekly:][Monthly:][Custom:] |
| Continuous Data Protection | [Enabled: No] |
| In-File Delta | [Enabled: Yes, Default Type: I, Block Size: -1, Minimum Size = 2621440, Maximum No. of Delta = 100, Delta Ratio = 50, Weekly: [], Monthly: [], Day: 0, Criteria: Friday, Day of selected months in yearly variations: First] |
| Retention Policy | [Type: Simple, Period: 7, Unit: Day(s)] |
| Command Line Tool | |
| Reminder | [Computer Name: cengwin2012] |
| Bandwidth Control | [Enabled: No, Mode: Independent, Bandwidth Control:] |
| Others | [Remove temporary files after backup: Yes][Follow Link: Yes][Volume Shadow Copy: Yes][File Permissions: Yes][Compression Type: Fast (Compressed size larger than normal)] |

Backup Logs

| No. | Type | Timestamp | Log |
|-----|-------|---------------------|--|
| 1 | start | 2019/10/07 19:57:29 | Start [Ahsay Cloud Backup Suite v8.3.0.0] |
| 2 | info | 2019/10/07 19:57:33 | Using Temporary Directory C:\Program Files\AhsayCBS\temp\1570448232410\Local@1570448463820 |
| 3 | info | 2019/10/07 20:05:02 | Start validating the presence and size of backup data in destination "AhsayCBS"... |
| 4 | info | 2019/10/07 20:05:02 | File: "1570448232410/blocks/2019-10-07-19-57-18/0/000000.bak", Size: 23,620,368, OK |
| 5 | info | 2019/10/07 20:05:02 | File: "1570448232410/blocks/2019-10-07-19-57-18/0/000001.bak", Size: 26,348,096, OK |
| 6 | info | 2019/10/07 20:05:02 | File: "1570448232410/blocks/2019-10-07-19-57-18/0/000002.bak", Size: 26,348,096, OK |
| 7 | info | 2019/10/07 20:05:02 | File: "1570448232410/blocks/2019-10-07-19-57-18/0/000003.bak", Size: 20,833,312, OK |
| 8 | info | 2019/10/07 20:05:02 | File: "1570448232410/blocks/2019-10-07-19-57-18/0/000004.bak", Size: 20,833,312, OK |
| 9 | info | 2019/10/07 20:05:02 | File: "1570448232410/blocks/2019-10-07-19-57-18/0/000005.bak", Size: 10,567,536, OK |
| 10 | info | 2019/10/07 20:05:02 | Finished validating the presence and size of backup data in destination "AhsayCBS" |

Backup Files

| No. | Type | Dirs/Files | Size | Last Modified |
|-----|------|----------------------|------------------|------------------|
| 1 | new | Photos | 0 / 0 (0%) | |
| 2 | new | TestFiles | 0 / 0 (0%) | |
| 3 | new | Photos/TestJPG-1.jpg | 516k / 516k (0%) | 03/05/2019 15:32 |
| 4 | new | Photos/TestJPG-2.jpg | 516k / 516k (0%) | 03/05/2019 15:32 |
| 5 | new | Photos/TestJPG-3.jpg | 516k / 516k (0%) | 03/05/2019 15:32 |

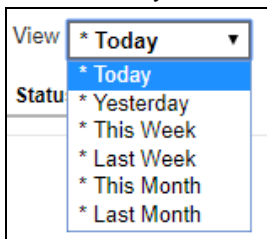
| | | | | |
|----|-----|--------------------------------|-----------------------|------------------|
| 6 | new | Photos/TestJPG-4.jpg | 516k / 516k (0%) | 03/05/2019 15:32 |
| 7 | new | Photos/TestJPG-5.jpg | 516k / 516k (0%) | 03/05/2019 15:32 |
| 8 | new | Photos/TestPNG-1.png | 516k / 516k (0%) | 03/05/2019 15:32 |
| 9 | new | Photos/TestPNG-2.png | 516k / 516k (0%) | 03/05/2019 15:32 |
| 10 | new | Photos/TestPNG-3.png | 516k / 516k (0%) | 03/05/2019 15:32 |
| 11 | new | Photos/TestPNG-4.png | 516k / 516k (0%) | 03/05/2019 15:32 |
| 12 | new | Photos/TestPNG-5.png | 516k / 516k (0%) | 03/05/2019 15:32 |
| 13 | new | Photos/TestTIFF-1.tiff | 516k / 516k (0%) | 03/05/2019 15:32 |
| 14 | new | Photos/TestTIFF-2.tiff | 516k / 516k (0%) | 03/05/2019 15:32 |
| 15 | new | Photos/TestTIFF-3.tiff | 516k / 516k (0%) | 03/05/2019 15:32 |
| 16 | new | Photos/TestTIFF-4.tiff | 516k / 516k (0%) | 03/05/2019 15:32 |
| 17 | new | Photos/TestTIFF-5.tiff | 516k / 516k (0%) | 03/05/2019 15:32 |
| 18 | new | TestFiles/AlertMessage0001.jpg | 490k / 490k (0%) | 08/27/2019 11:24 |
| 19 | new | TestFiles/AlertMessage0002.jpg | 490k / 490k (0%) | 08/27/2019 11:24 |
| 20 | new | TestFiles/AlertMessage0003.jpg | 490k / 490k (0%) | 08/27/2019 11:24 |
| 21 | new | TestFiles/AlertMessage0004.jpg | 490k / 490k (0%) | 08/27/2019 11:24 |
| 22 | new | TestFiles/AlertMessage0005.jpg | 490k / 490k (0%) | 08/27/2019 11:24 |
| 23 | new | TestFiles/Attendance_2014.doc | 12.56M / 14.18M (11%) | 08/27/2019 11:24 |
| 24 | new | TestFiles/Attendance_2015.doc | 12.56M / 14.18M (11%) | 08/27/2019 11:24 |
| 25 | new | TestFiles/Attendance_2016.doc | 12.56M / 14.18M (11%) | 08/27/2019 11:24 |
| 26 | new | TestFiles/Attendance_2017.doc | 12.56M / 14.18M (11%) | 08/27/2019 11:24 |
| 27 | new | TestFiles/Attendance_2018.doc | 12.56M / 14.18M (11%) | 08/27/2019 11:24 |
| 28 | new | TestFiles/ManualABC.pdf | 9.93M / 11.73M (15%) | 08/27/2019 11:24 |
| 29 | new | TestFiles/ManualDEF.pdf | 9.93M / 11.73M (15%) | 08/27/2019 11:24 |
| 30 | new | TestFiles/ManualGHI.pdf | 9.93M / 11.73M (15%) | 08/27/2019 11:25 |
| 31 | new | TestFiles/ManualJKL.pdf | 9.93M / 11.73M (15%) | 08/27/2019 11:25 |
| 32 | new | TestFiles/ManualMNL.pdf | 9.93M / 11.73M (15%) | 08/27/2019 11:25 |
| 33 | new | TestFiles/Presentation_A.pptx | 23k / 31k (25%) | 08/27/2019 11:24 |
| 34 | new | TestFiles/Presentation_B.pptx | 23k / 31k (25%) | 08/27/2019 11:24 |
| 35 | new | TestFiles/Presentation_C.pptx | 23k / 31k (25%) | 08/27/2019 11:24 |
| 36 | new | TestFiles/Presentation_D.pptx | 23k / 31k (25%) | 08/27/2019 11:24 |
| 37 | new | TestFiles/Presentation_E.pptx | 23k / 31k (25%) | 08/27/2019 11:24 |
| 38 | new | TestFiles/SpreadSheet_01.xlsx | 5k / 8k (28%) | 08/27/2019 11:24 |
| 39 | new | TestFiles/SpreadSheet_02.xlsx | 5k / 8k (28%) | 08/27/2019 11:24 |
| 40 | new | TestFiles/SpreadSheet_03.xlsx | 5k / 8k (28%) | 08/27/2019 11:24 |
| 41 | new | TestFiles/SpreadSheet_04.xlsx | 5k / 8k (28%) | 08/27/2019 11:24 |
| 42 | new | TestFiles/SpreadSheet_05.xlsx | 5k / 8k (28%) | 08/27/2019 11:24 |
| 43 | new | TestFiles/TestTXTFile-1.txt | 368 / 56k (99%) | 08/27/2019 11:24 |
| 44 | new | TestFiles/TestTXTFile-2.txt | 368 / 56k (99%) | 08/27/2019 11:24 |
| 45 | new | TestFiles/TestTXTFile-3.txt | 368 / 56k (99%) | 08/27/2019 11:24 |
| 46 | new | TestFiles/TestTXTFile-4.txt | 368 / 56k (99%) | 08/27/2019 11:24 |
| 47 | new | TestFiles/TestTXTFile-5.txt | 368 / 56k (99%) | 08/27/2019 11:24 |

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.



7 Restoring a Cloud File Backup Set

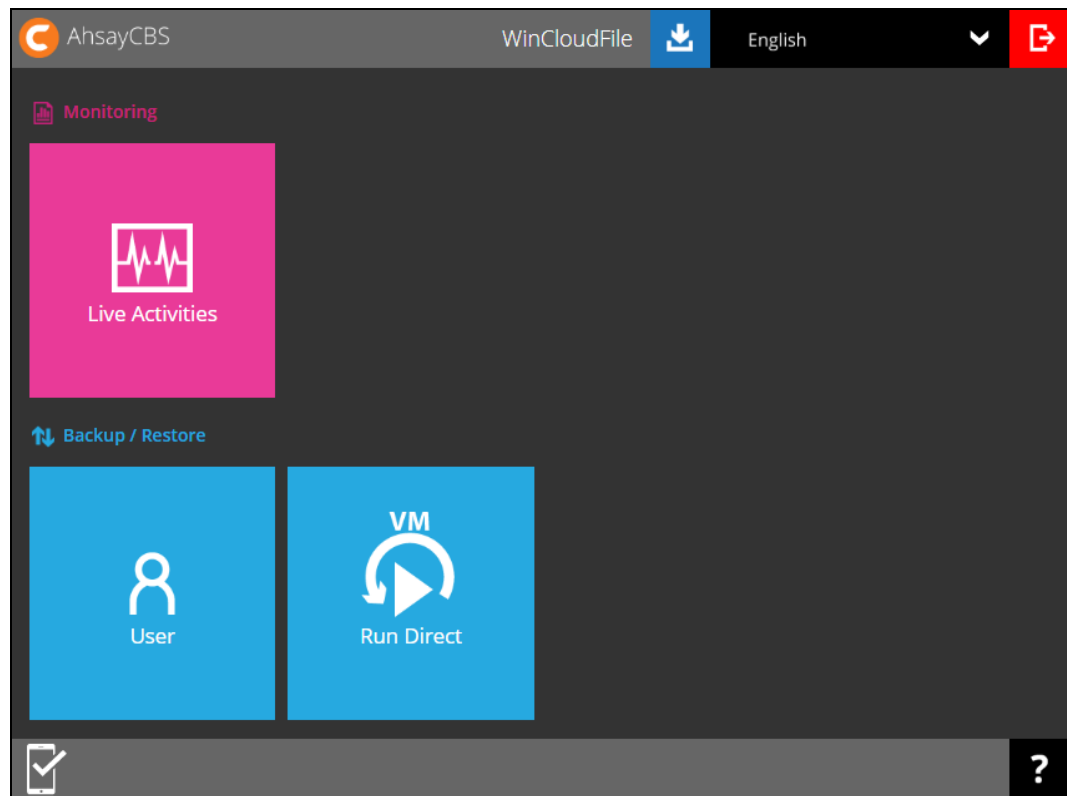
AhsayCBS User Web Console has two (2) options for the restoration process: **Original** and **Alternate** location. After this quick walkthrough, you will see the step-by-step instructions with corresponding screenshots on how to restore your data using the following options below.

- **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.

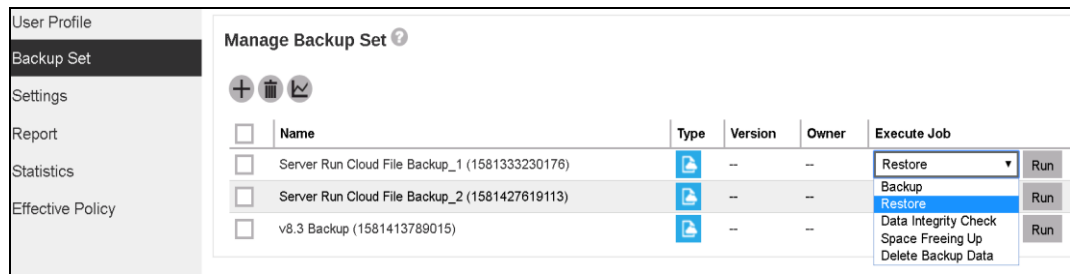
NOTE

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

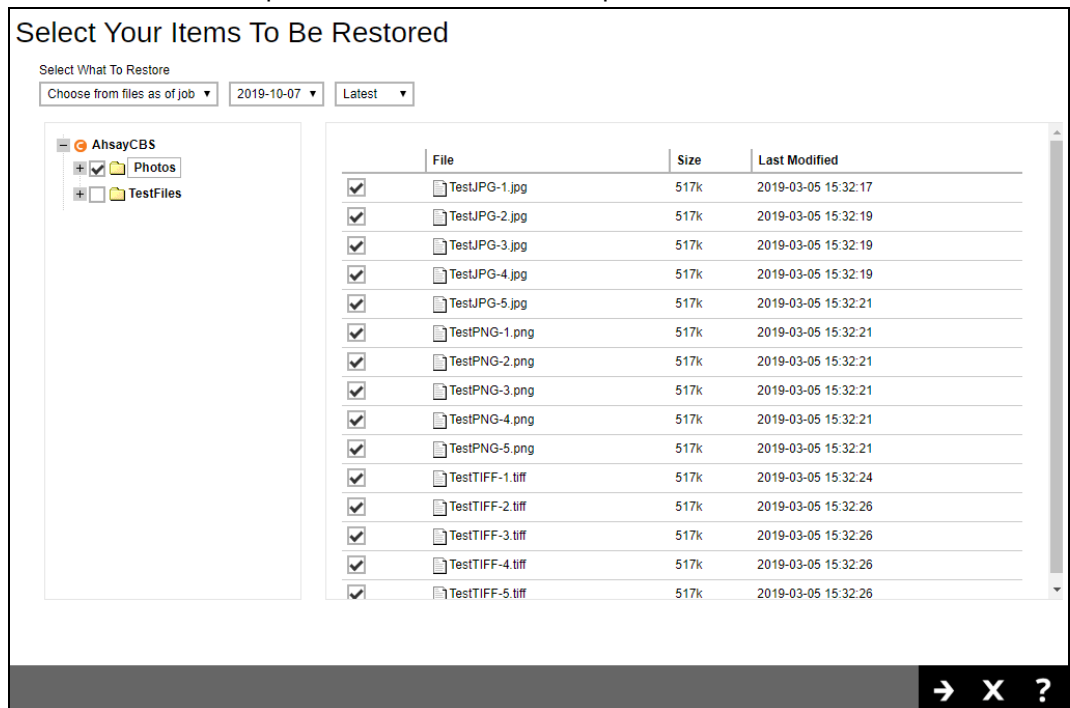
1. Click on the **User** icon.



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



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



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

Original Location

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

- Backup
- Documents
- Test files
- v8.3

[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

Restore Items To

Original location

Alternate location

Overwrite file

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

- Backup
- Documents
- Test files
- v8.3

Overwrite file

Verify checksum of in-file delta files during restore


[Hide advanced option](#)







Overwrite file

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 | Manage Backup Set  | | | | |
| Backup Set |    | | | | |
| Settings | <input type="checkbox"/> | Name | Type | Version | Owner |
| Report | <input type="checkbox"/> | Client Run Cloud File Backup (1570418957719) |  | -- | cengwin2012 |
| Statistics | <input type="checkbox"/> | Server Run Cloud File Backup (1570448232410) |  | -- | -- |
| Effective Policy | | | | | Restore is Running <input type="button" value="Stop"/> |

8 Running Data Integrity Check

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

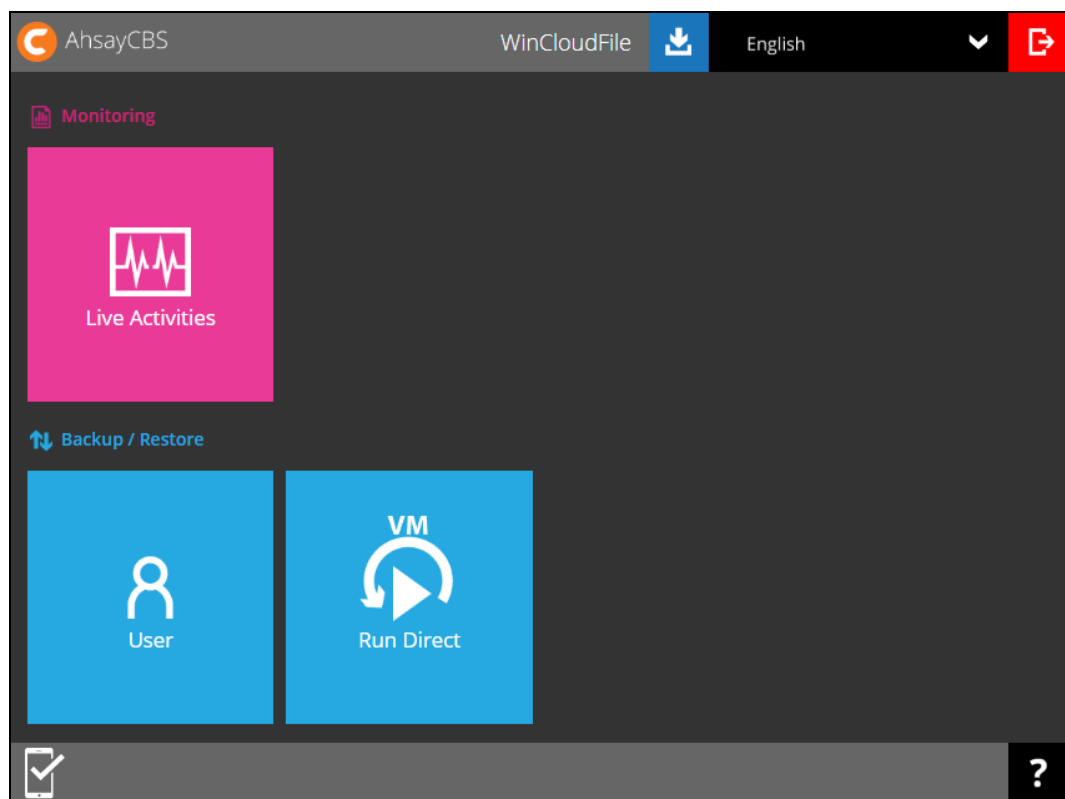
- AhsayOBM / AhsayACB User

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.

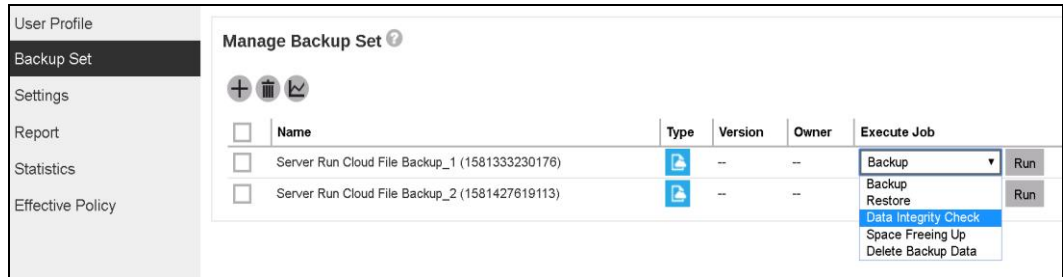
- Backup Service Provider

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 according to the instructions in [Log in to AhsayCBS User Web Console](#).
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.



Run Cyclic Redundancy Check (CRC)

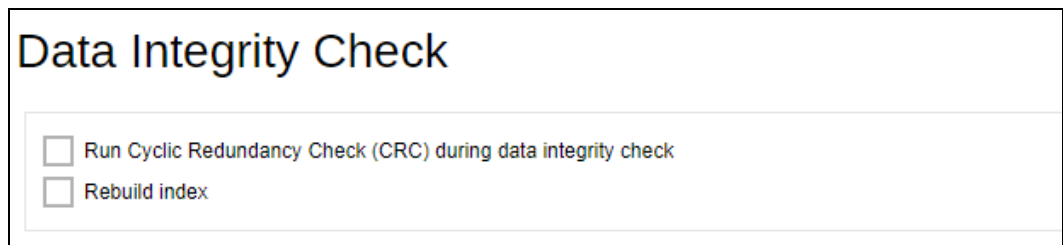
This option is disabled by default. When this option is enabled, the data integrity check will perform check on the integrity of the files on the backup destination(s) against the checksum file generated at the time of the backup job.


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.



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

9 Performing Space Freeing Up

Space Free Up can be done in two (2) ways:

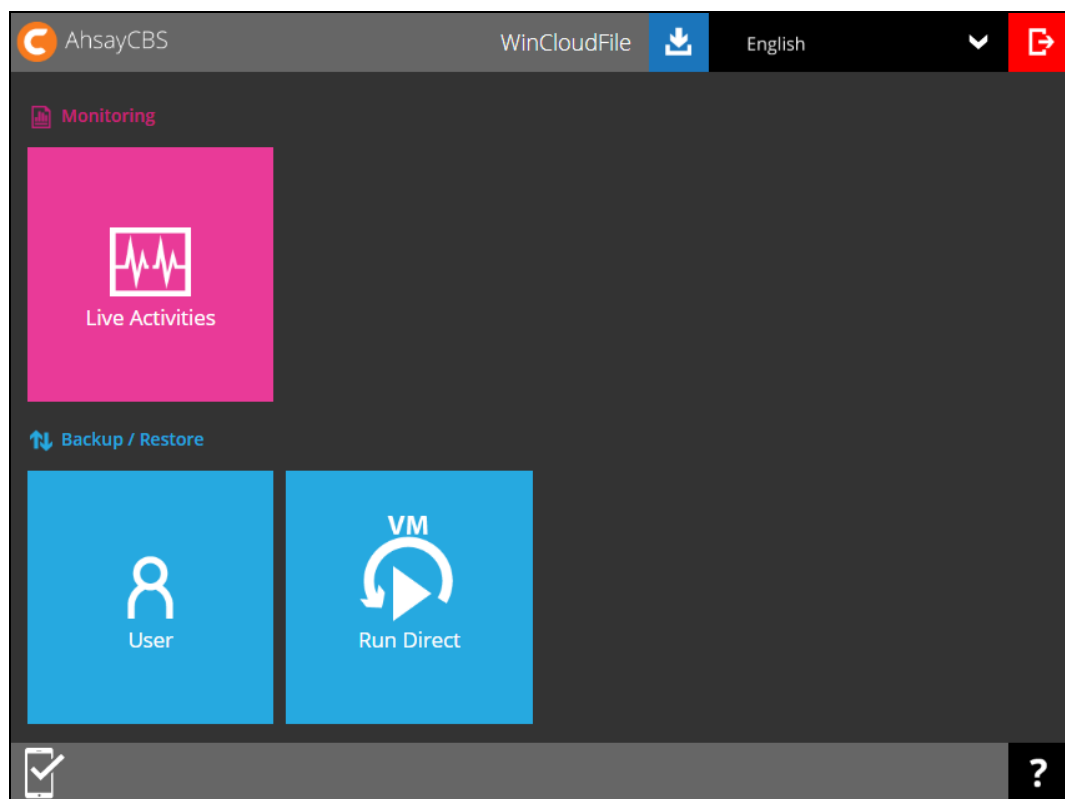
- AhsayOBM / AhsayACB User

This option allows the AhsayOBM and AhsayACB users to perform space freeing up, but the result of the space freeing up 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 space freeing up and provide them with the report of the result and/or solution.

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



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

User Profile

Backup Set

Settings

Report


Statistics

Effective Policy

Manage Backup Set ?

+ - ↺

| <input type="checkbox"/> | Name | Type | Version | Owner | Execute Job | |
|--------------------------|--|------|---------|-------|--|-----|
| <input type="checkbox"/> | Server Run Cloud File Backup_1 (1581333230176) | | -- | -- | Backup | Run |
| <input type="checkbox"/> | Server Run Cloud File Backup_2 (1581427619113) | | -- | -- | Backup Restore | Run |
| <input type="checkbox"/> | v8.3 Backup (1581413789015) | | -- | -- | Data Integrity Check Space Freeing Up Delete Backup Data | Run |

4. Running space freeing up job will be indicated. Click the  button to stop the space freeing up job if necessary.

User Profile

Backup Set

Settings

Report

Statistics

Effective Policy

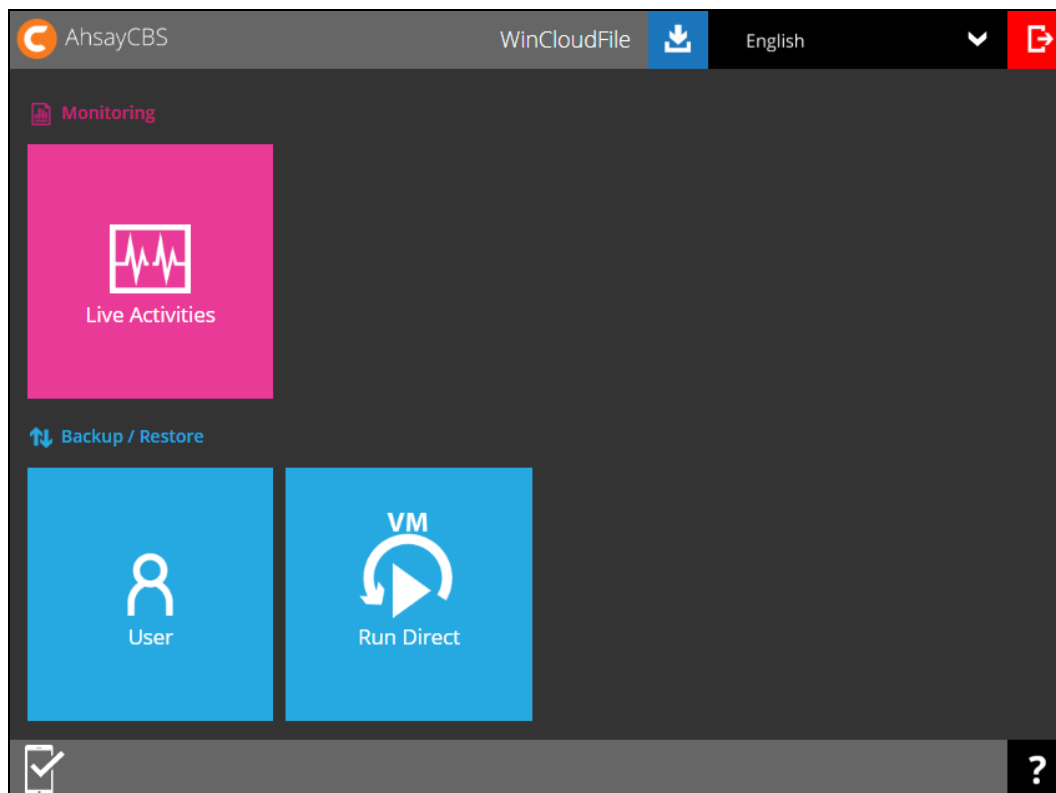
Manage Backup Set ?

+ - ↺

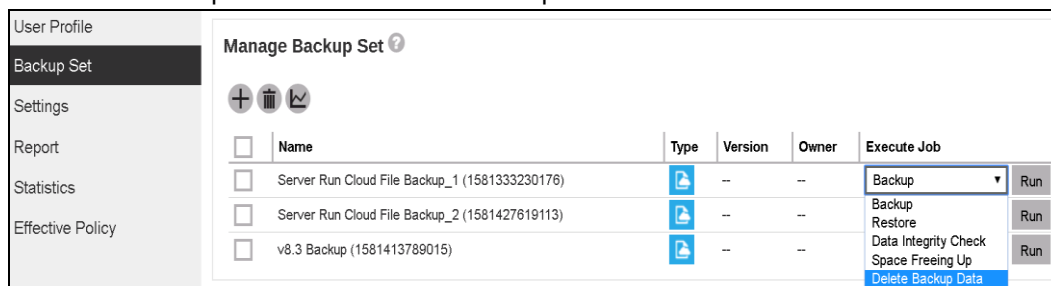
| <input type="checkbox"/> | Name | Type | Version | Owner | Execute Job | |
|--------------------------|--|------|---------|-------|-----------------------------|------|
| <input type="checkbox"/> | Server Run Cloud File Backup_1 (1581333230176) | | -- | -- | Space Freeing Up is Running | Stop |
| <input type="checkbox"/> | Server Run Cloud File Backup_2 (1581427619113) | | -- | -- | Backup | Run |
| <input type="checkbox"/> | v8.3 Backup (1581413789015) | | -- | -- | Backup | Run |

10 Deleting Backup Data

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

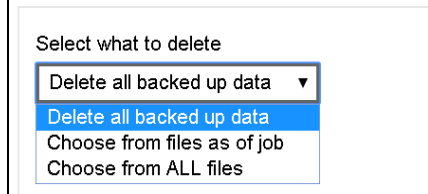


3. Select **Backup Set** from the left panel, then select **Delete Backup Data** under the **Execute Job** drop-down menu. Click **Run** to proceed.



4. There are three options in performing delete backup data:
 - Delete all backed up data
 - Choose from files as of job
 - Choose from ALL files

Delete Backup Data

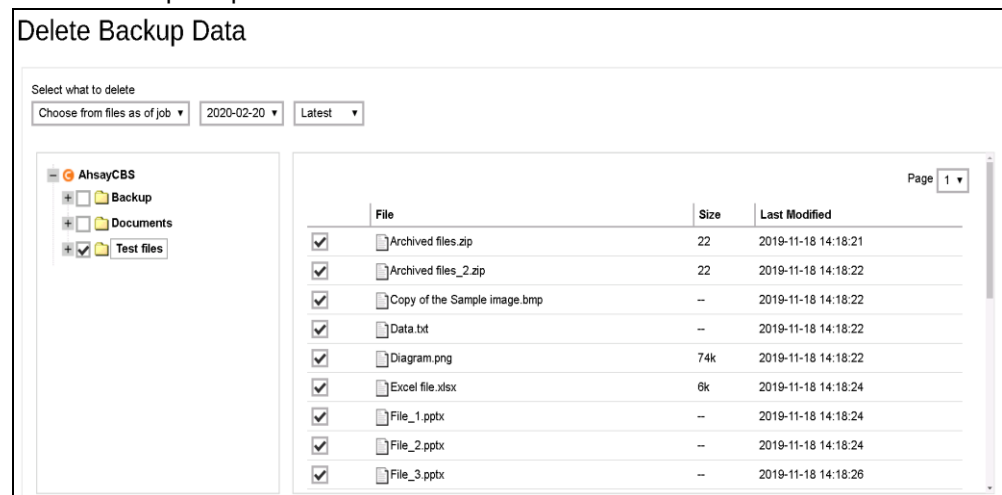


- Delete all backed up data

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

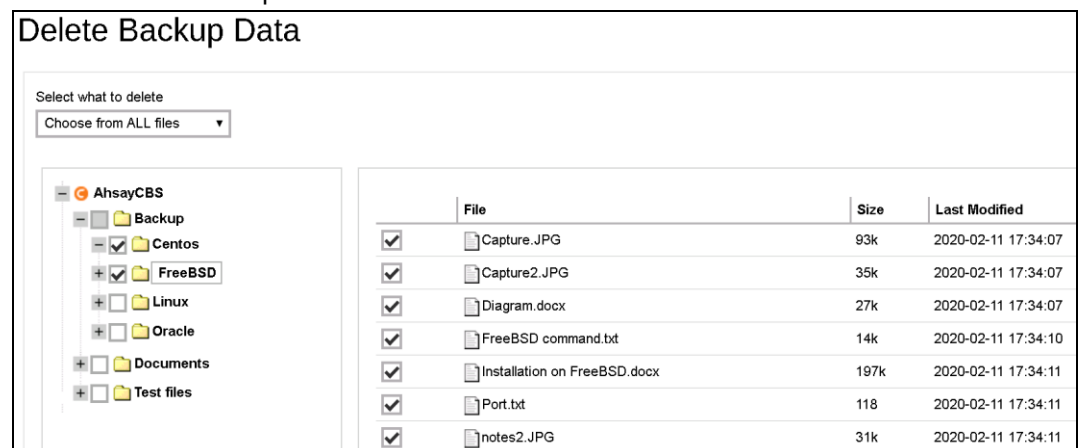
- Choose from files as of job


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



- 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.



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

6. Running delete backup data job will be indicated.

The screenshot shows a web interface for managing backup sets. On the left is a navigation menu with options: User Profile, Backup Set (selected), Settings, Report, Statistics, and Effective Policy. The main area is titled 'Manage Backup Set' and contains a table of backup sets. Above the table are three icons: a plus sign, a trash can, and a refresh symbol. The table has columns for Name, Type, Version, Owner, and Execute Job. The 'Execute Job' column contains a dropdown menu and a 'Run' button. The third row shows the status 'Delete Backup Data is Running'.

| <input type="checkbox"/> | Name | Type | Version | Owner | Execute Job |
|--------------------------|--|------|---------|-------|---|
| <input type="checkbox"/> | Server Run Cloud File Backup_1 (1581333230176) | | -- | -- | Backup <input type="button" value="Run"/> |
| <input type="checkbox"/> | Server Run Cloud File Backup_2 (1581427619113) | | -- | -- | Backup <input type="button" value="Run"/> |
| <input type="checkbox"/> | v8.3 Backup (1581413789015) | | -- | -- | 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.

11 Contact Ahsay

11.1 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/>

11.2 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.