

# AhsayCBS v8.3.4.0 New Features Datasheet

Ahsay Systems Corporation Limited  
**30 July 2020**

## Table of Contents

<b>Improved Security for AhsayCBS “System” User Accounts .....</b>	<b>3</b>
<b>AhsayCBS Trial Users for Sub Admin (Reseller) .....</b>	<b>4</b>
<b>New Compression Type: Fast with optimization for local .....</b>	<b>6</b>
Best Practices for Compression Type Usage .....	7
<b>Enhancements on the Periodic Data Integrity Check (PDIC) and Data Integrity Check (DIC) Jobs ...</b>	<b>8</b>
How does the Periodic Data Integrity Check (PDIC) work? .....	10
How does the Data Integrity Check (DIC) work? .....	11
<b>VMware vCenter Server/ESXi version 7 supported on AhsayOBM .....</b>	<b>13</b>
<b>Improved Listing of Mailboxes or Public Folders for MS Exchange 2013/2016/2019 (EWS) Mail Level Backup .....</b>	<b>14</b>
<b>Data Synchronization Check (DSC) Process for Office 365 Backup .....</b>	<b>15</b>
Importance of Data Synchronization Check (DSC) .....	15
How does Data Synchronization Check (DSC) work? .....	16
How to configure the Data Synchronization Check (DSC)? .....	16
Best Practices for Data Synchronization Check (DSC) Usage .....	18
<b>Google Cloud Storage: Regional Location Supported .....</b>	<b>19</b>
<b>Improved Support for Network Drives (Windows).....</b>	<b>20</b>
<b>Periodic Backup Schedule .....</b>	<b>22</b>
Periodic Backup Schedule vs. Continuous Backup Schedule .....	23
<b>Newly Supported OS: Ubuntu 20 and MacOS 10.15.....</b>	<b>24</b>

## Improved Security for AhsayCBS “System” User Accounts

To enhance the AhsayCBS security, the AhsayCBS v8.3.4.0 (or above) has implemented additional password requirements for admin account types: **Admin**, **Read-only Admin**, **API**, and **Sub Admin**.

### Key Features

- ▶ On the initial AhsayCBS web console login, prompt to change the default password for “system” account.  
**Note:** Login will not be allowed until the “system” password has been changed
- ▶ Prompt to change the password if the “system” account password is restored to “system”.  
**Note:** This setting does not apply to other Admin, Read-only Admin, API, and Sub Admin account types
- ▶ Applicable to the new installation of AhsayCBS v8.3.4.0 (or above) and AhsayCBS v8.3.4.0 (or above) installations when upgraded from v6, v7, or pre-v8.3.4.0.



#### NOTE

These features cannot be disabled.

- ▶ Advanced password security settings for **Password Age**, **Password History**, and **Password Complexity** for admin account types: Admin, Read-only Admin, API, and Sub Admin.

### Password settings disabled by default

#### Password

Password Age
 

☐ Never expire
 

☒ 90
 days

☒ Enforce password history (30 passwords remembered)

Complexity Requirements
 

☐ Default
 

☒ Numbers (0-9)
 ☒ Uppercase
 ☒ Lowercase
 ☒ Minimum length 6

☒ Special characters (?!~\$%^&\*~+=;~'"~,)

☒ Custom (Regular expression)
 

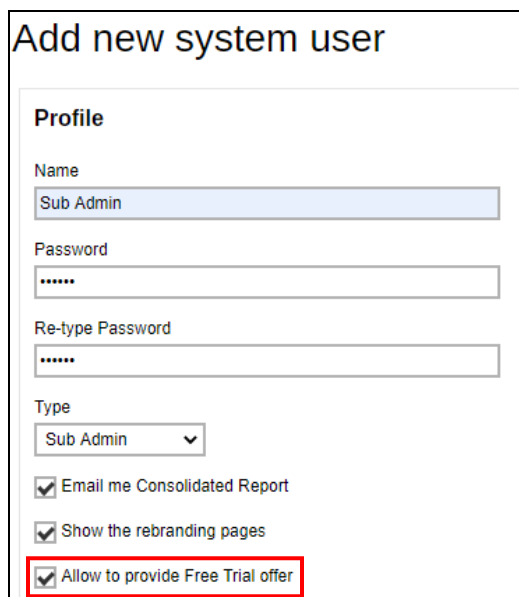
Custom Description

## AhsayCBS Trial Users for Sub Admin (Reseller)

The new AhsayCBS v8.3.4.0 (or above) has added a capability for the **Sub Admin (reseller)** account to offer a **free trial registration** to their potential customers or backup users which can be done through the AhsayOBM/AhsayACB client:

### **Allow to provide Free Trial offer** *(enabled by default)*

This option allows the Sub Admin to offer a free trial account for their backup users. Even if the Managed Service Provider (MSP) or other Sub Admin (reseller) does not offer this service, the Sub Admin can still offer Free Trial for their backup users once they enable this option after logging in.



**Add new system user**

**Profile**

Name  
Sub Admin

Password  
\*\*\*\*\*

Re-type Password  
\*\*\*\*\*

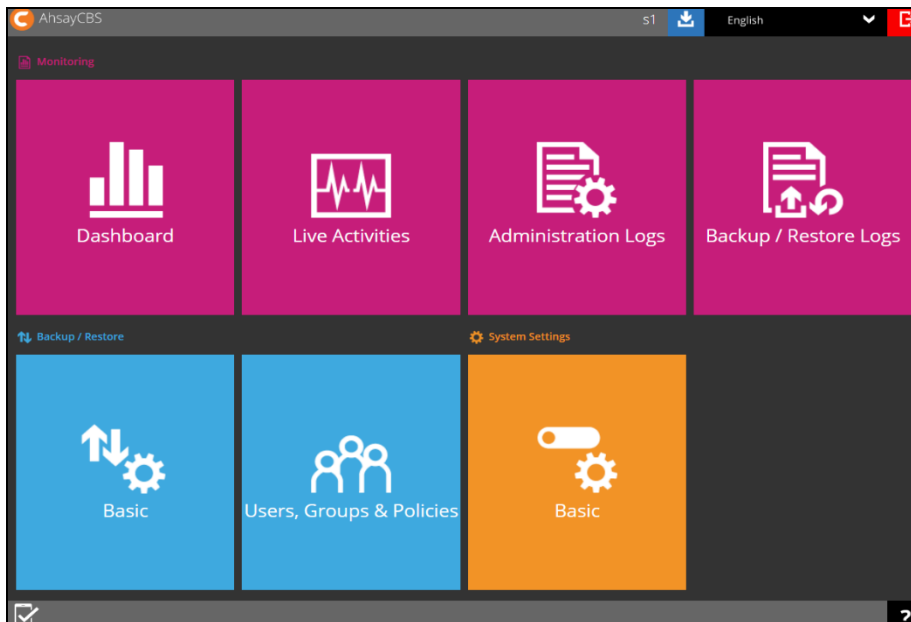
Type  
Sub Admin

☒ Email me Consolidated Report

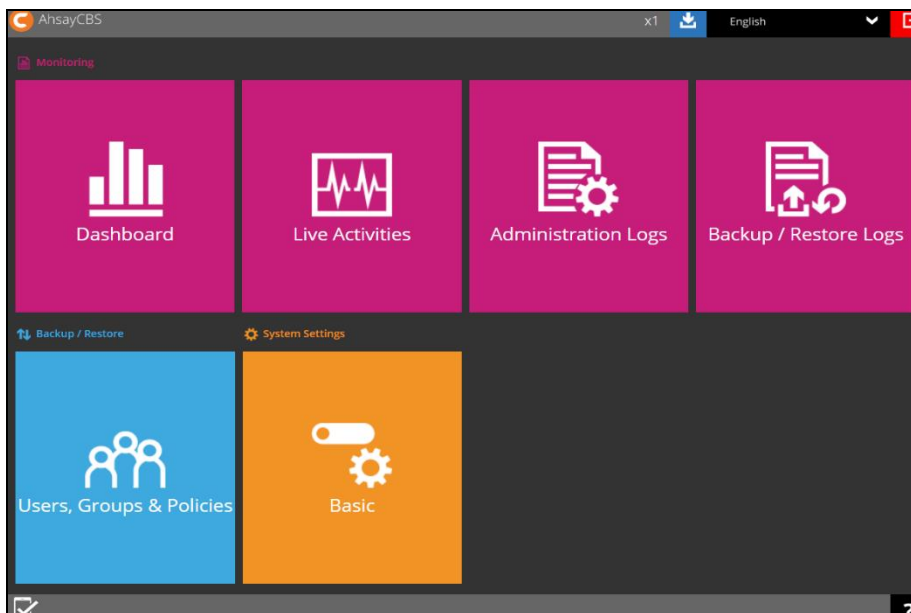
☒ Show the rebranding pages

☒ Allow to provide Free Trial offer

The following screen of AhsayCBS web console will be displayed for the Sub Admin (reseller) account with “**Allow to provide Free Trial offer**” option **enabled**:



The following screen of AhsayCBS web console will be displayed for the Sub Admin (reseller) account with “**Allow to provide Free Trial offer**” option **disabled**:



## New Compression Type: Fast with optimization for local

Although **compressing files into smallest possible file size** will reduce the overall file storage size and the backup set cost, as well as smaller files will take less time to back up to the cloud destination(s), it is one potential cause of high CPU resource usage which can affect the overall backup performance.

To provide users with additional option in reducing the CPU usage, the AhsayCBS v8.3.4.0 (or above) has added a new type of compression:

### ➡ **Fast with optimization for local**

This brings a total of four (4) compression types:

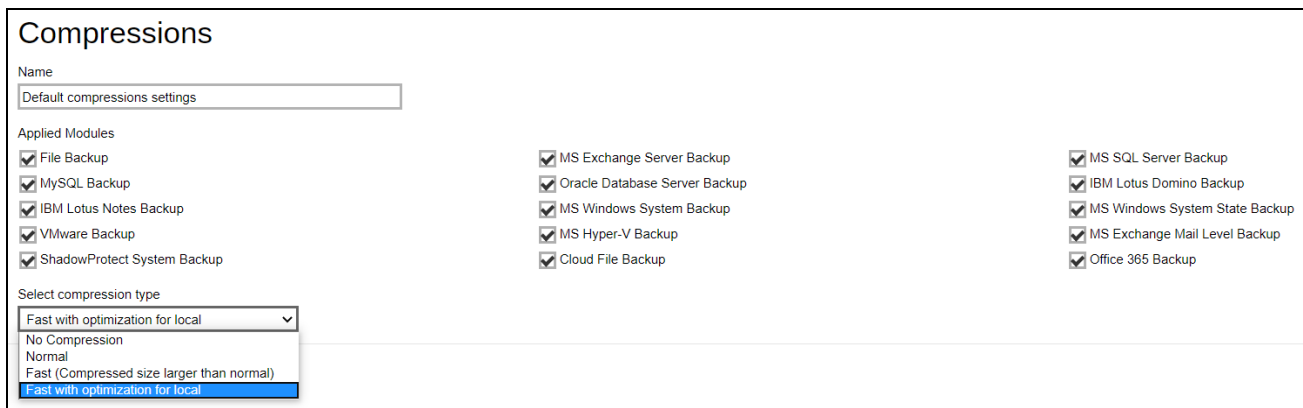
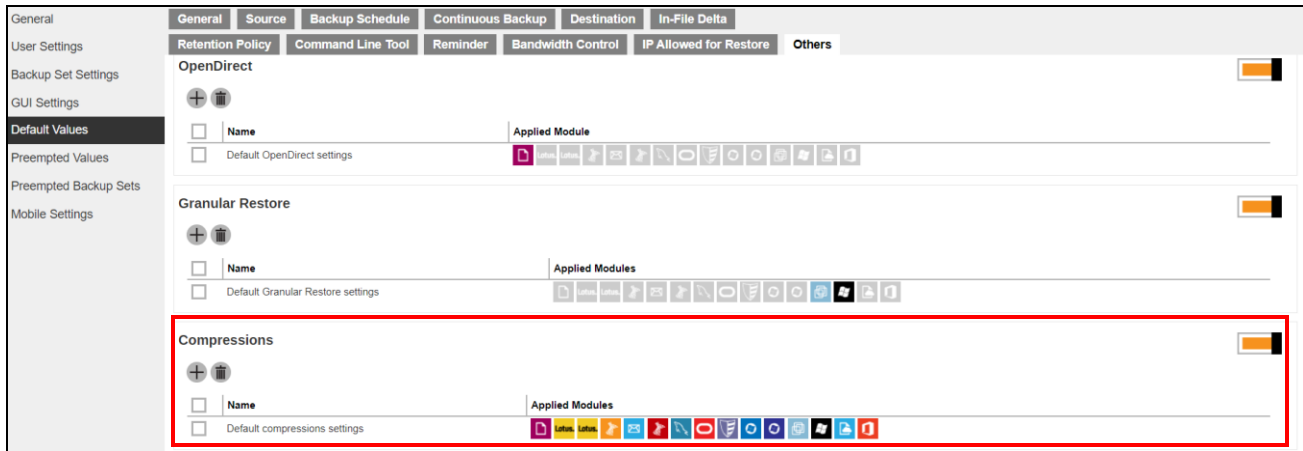
Compression Type	Description
<b>No Compression</b>	No compression of file will be made
<b>Normal</b>	Compressed file size is the smallest among all compression types but will result to high CPU usage
<b>Fast (Compressed size larger than normal)</b>	Compressed file size is larger than the <b>Normal</b> compression type and will result to lower CPU usage
<b>Fast with optimization for local</b>	Compressed file size is larger than the <b>Fast</b> compression type and will result to lowest CPU usage

- ▶ For newly created Run on Client and/or AhsayCBS Run on Server (Office 365 and Cloud File) backup sets on AhsayCBS v8.3.4.0 (or above), **Fast with optimization for local** is the default compression type.
- ▶ Existing AhsayOBS v6, AhsayCBS v7 and pre-AhsayCBS v8.3.4.0 backup sets with default **Fast (Compressed size larger than normal)** compression will not be affected when migrated to AhsayCBS v8.3.4.0 (or above). The **Fast** compression type for these backup sets will remain unchanged.



#### NOTE

The default value of compression type depends on the **AhsayCBS Policy Group > Default settings > Default Values > Others > Compressions** settings (*as shown on the images below*) which can be configured by the AhsayCBS administrators or Managed Service Providers (MSP).




## Best Practices for Compression Type Usage

It is recommended to use the **Fast with optimization for local** compression type for:

- ➡ AhsayCBS Run on Server (Office 365 and Cloud file) backup jobs since it requires the lowest CPU usage which can reduce the overall server load
- ➡ Backup sets which are running on machines with low hardware specifications, or where the CPU usage is already high

Although the **Fast with optimization for local** compression consumes the least CPU utilization which increases the backup performance, it has the smallest compression ratio among all compression types thus may increase the overall file storage size and the backup set cost.



**NOTE**

The compression type can be changed any time (e.g. after the backup set is created or even after a backup job), unless the compression type is fixed as in a pre-empted backup set. If the compression type is changed, the new compression method will take effect on the next run of backup job.

## Enhancements on the Periodic Data Integrity Check (PDIC) and Data Integrity Check (DIC) Jobs

Large number of Periodic Data Integrity Check (PDIC) jobs running at the same time on the AhsayCBS server has a huge impact on the overall server load. To reduce the potential load of a large number of PDIC jobs, the new AhsayCBS v8.3.4.0 (or above) has enhanced the approach of the *periodic data integrity check* job schedule.

For an efficient management of overall storage size of the backup destination(s), the *periodic data integrity check* and *data integrity check* jobs have also added a new feature where it will check for the backup destination(s) to remove old index files that are **more than ninety (90) days old** in the backup job folder(s).

### Key Features

- ▶ Modified approach in deciding the periodic data integrity check schedule.
- ▶ Periodic data integrity check to run in a weekday basis (i.e. Monday to Friday).
- ▶ Deletion of more than ninety (90) days old index files in the backup job folder(s).
- ▶ Applicable on AhsayOBM/AhsayACB client and AhsayCBS Web Console for Run on Server (Office 365 and Cloud File) backup.

The new schedule of the PDIC job for each backup set is automatically determined by the result of the following formula:

***Periodic Data Integrity Check (PDIC) schedule = %BackupSetID% modulo 5***

*or*

***%BackupSetID% mod 5***

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

0	Monday
1	Tuesday
2	Wednesday
3	Thursday
4	Friday

The *periodic data integrity* will start **automatically** with no user interaction needed. It will run once a week and will fall on a weekday (i.e. Monday to Friday).



#### NOTE

The PDIC schedule cannot be changed.



## Example

Backup set ID: 1594627447932

$1594627447932 \bmod 5 = 2$

In this example, the PDIC will run on the first backup job that falls on Wednesday.

2	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**.

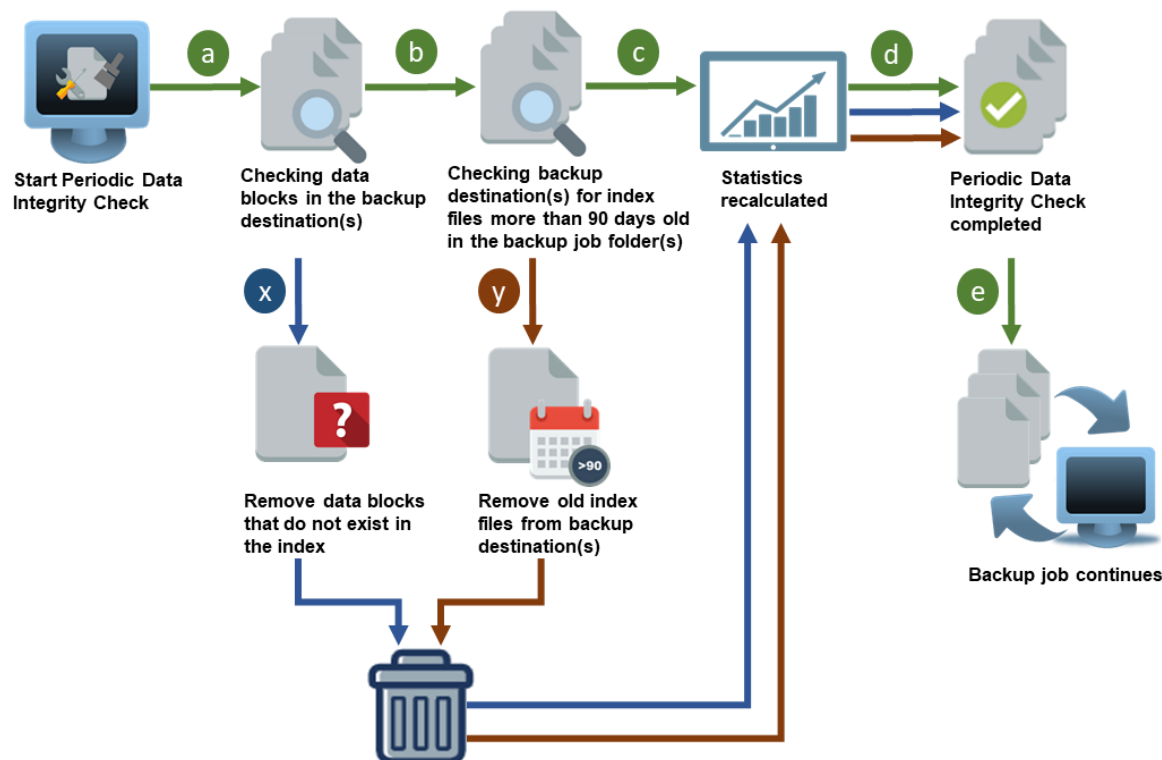


### WARNING

Corrupted data blocks (.bak files) can only be deleted by **manually running a full Data Integrity Check (DIC)** on the AhsayOBM/AhsayACB client or AhsayCBS Web Console for Run on Server (Office 365 and Cloud File) backup.

## How does the Periodic Data Integrity Check (PDIC) work?

The following diagram shows the detailed process of the Periodic Data Integrity Check (PDIC).



- a** Check the data blocks (.bak files) located in the backup destination(s) if they exist in the index.  
 → If **YES**, proceed to **b**  
 → If **NO**, proceed to **x**
- b** Check the index files in the backup job folder(s) if they were more than 90 days old.  
 → If **YES**, proceed to **y**  
 → If **NO**, proceed to **c**
- c** Statistics of the Data area and Retention area are recalculated.
- d** Periodic Data Integrity Check is completed.
- e** The backup job will continue.
- x** Data blocks (.bak files) that do not exist in the index will be removed from the backup destination(s).  
 Proceed to **c**
- y** Index files which are more than 90 days old will be removed from the backup destination(s).  
 Proceed to **c**

The Periodic Data Integrity Check (PDIC) will run once a week and will fall on a weekday (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 following formula:

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

The calculated **result** will map to the corresponding day of the week (from Monday to Friday):

0	Monday
1	Tuesday
2	Wednesday
3	Thursday
4	Friday

**Note:** The PDIC schedule cannot be changed.

For example:

Backup set ID: **1594627447932**

$1594627447932 \text{ mod } 5 = 2$

In this example, the PDIC will run on the first backup job that falls on Wednesday.

2	Wednesday
---	-----------

or

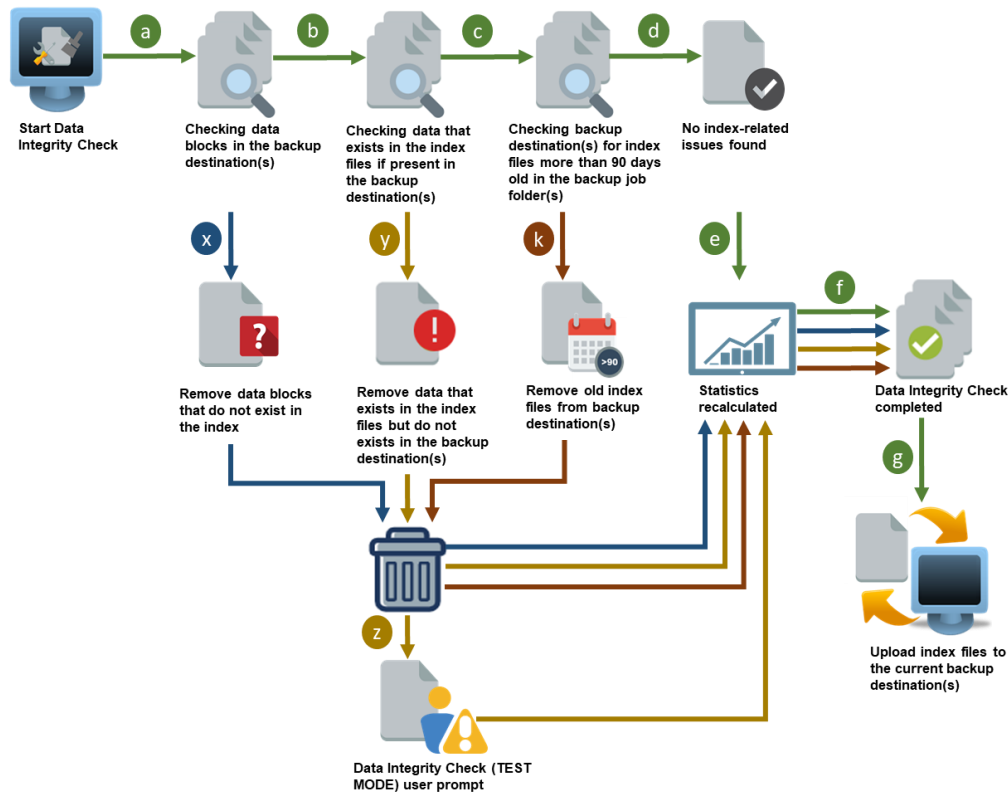
If there is no active backup job(s) running from Monday to Friday, then the PDIC will run on the **next available backup job**.

**Note:** Corrupted data blocks (.bak files) can only be deleted by **manually running a full Data Integrity Check (DIC)** on the AhsayOBM/AhsayACB client or AhsayCBS Web Console for Run on Server (Office 365 and Cloud File) backup.

## How does the Data Integrity Check (DIC) work?

The following diagram shows the detailed process of the Data Integrity Check (DIC).

### Disabled Run Cyclic Redundancy Check (CRC) – Default mode



**a** Check the data blocks (.bak files) located in the backup destination(s) if they exist in the index.

→ If **YES**, proceed to **b**  
→ If **NO**, proceed to **x**

**b** Check the data that exists in the index files if they appear in the backup destination(s).

→ If **YES**, proceed to **c**  
→ If **NO**, proceed to **y**

**c** Check the index files in the backup job folder(s) if they were more than 90 days old.

→ If **YES**, proceed to **k**  
→ If **NO**, proceed to **d**

**d** No index-related issues have been found.

**e** Statistics of the Data area and Retention area are recalculated.

**f** Data Integrity Check is completed.

**g** Index files will be uploaded to the current backup destination(s).

**x** Data blocks (.bak files) that do not exist in the index and partially uploaded orphan files will be automatically removed from the backup destination(s).

Proceed to **e**

**y** Data that exists in the index files but do not actually exist in the backup destination(s) will be removed.

→ If either of the **criteria's** matches, proceed to **z**

→ If **NOT**, proceed to **e**

**z** (TEST MODE) confirmation screen will prompt user to proceed with the corrective actions (**recommended**).

→ If the user selects **YES**, then the changes will be applied  
→ If the user selects **NO**, then the deletion of data will be discarded

Proceed to **e**

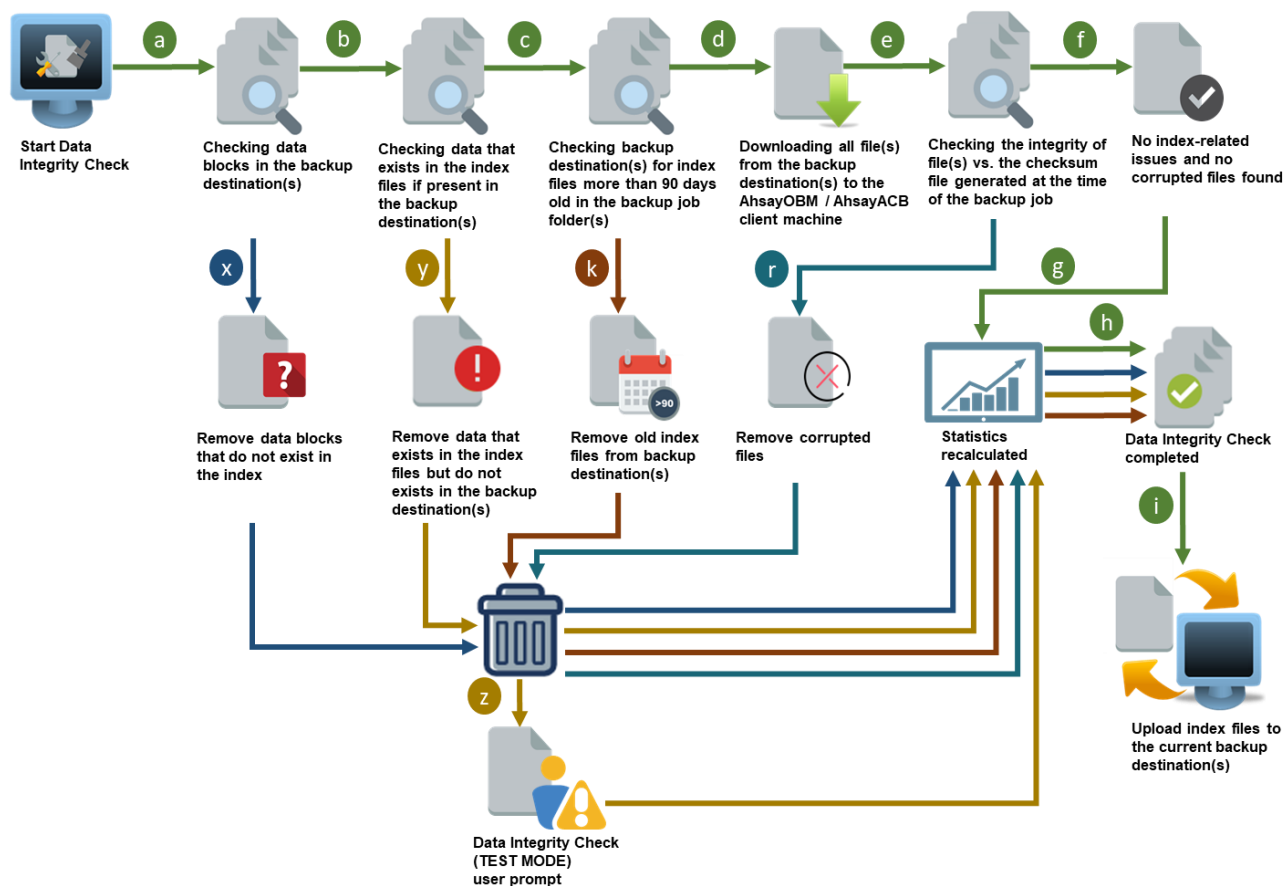
**k** Index files which are more than 90 days old will be removed from the backup destination(s).

Proceed to **e**

By default, (TEST MODE) confirmation screen will only prompt if either of the **criteria's** below matches the backup data:

- deleted number of backup files is over 1000
- deleted number of backup file size is over 512 MB (in total)
- deleted number of backup files is over 10% of total backup files

### Enabled Run Cyclic Redundancy Check (CRC)



- a Check the data blocks (.bak files) located in the backup destination(s) if they exist in the index.  
→ If **YES**, proceed to **b**  
→ If **NO**, proceed to **x**
  - b Check the data that exists in the index files if they appear in the backup destination(s).  
→ If **YES**, proceed to **c**  
→ If **NO**, proceed to **y**
  - c Check the index files in the backup job folder(s) if they were more than 90 days old.  
→ If **YES**, proceed to **k**  
→ If **NO**, proceed to **d**
  - d For **Run on Client (agent-based)** backup sets, files in the backup set are downloaded from the backup destination(s) to the AhsayOBM / AhsayACB client. Proceed to **e**  
For **Run on Server (agentless)** backup sets, proceed to **e**
  - e Check the integrity of file(s) in the backup destination(s) against the checksum file generated at the time of the backup job.  
→ If any discrepancy is **FOUND**, proceed to **r**  
→ If **NO** discrepancy is found, proceed to **f**
  - f No index-related issues and no corrupted files have been found.
  - g Statistics of the Data area and Retention area are recalculated.
  - h Data Integrity Check is completed.
  - i Index files will be uploaded to the current backup destination(s).
  - x Data blocks (.bak files) that do not exist in the index and partially uploaded orphan files will be automatically removed from the backup destination(s). Proceed to **g**
  - y Data that exists in the index files but do not actually exist in the backup destination(s) will be removed.  
→ If either of the **criteria's** matches, proceed to **z**  
→ If **NOT**, proceed to **g**
  - z (TEST MODE) confirmation screen will prompt user to proceed with the corrective actions (**recommended**).  
→ If the user selects **YES**, then the changes will be applied  
→ If the user selects **NO**, then the deletion of data will be discarded. Proceed to **g**
  - k Index files which are more than 90 days old will be removed from the backup destination(s). Proceed to **g**
  - r Corrupted files will be automatically removed from the backup destination(s).

By default, (**TEST MODE**) confirmation screen will only prompt if either of the **criteria's** below matches the backup data:

  - deleted number of backup files is over 1000
  - deleted number of backup file size is over 512 MB (in total)
  - deleted number of backup files is over 10% of total backup files

## VMware vCenter Server/ESXi version 7 supported on AhsayOBM

To provide customer with more comprehensive VMware backup, the new AhsayCBS v8.3.4.0 (or above) offers support for:

### 🔍 VMware vCenter/ESXi 7

Supported for both VDDK and Non-VDDK backup modes.

## Requirements

### Windows OS Requirement

For VMware ESXi/vCenter 7 VDDK backups, AhsayOBM must be running on a 64-bit Windows machine and installed on the following Windows version:

Windows 2012	Windows 2016 ( <i>including versions 1709 and 1803</i> )
Windows 2012 R2	Windows 2019

## Limitation

For **Non-VDDK backup mode**, VMware vCenter/ESXi 7 can only be backed up if the VM is powered off during a backup job.



### WARNING

If a VMware vCenter/ESXi 5, 5.5, 6, 6.5 and 6.7 using Free License key is upgraded to v7, all non-VDDK backup jobs will stop running unless all guest VMs are powered off.

For backup of VMware vCenter/ESXi 7 hosts where AhsayOBM is installed on a non-Windows staging machine such as macOS or Linux/FreeBSD, the guest VMs must be powered off.

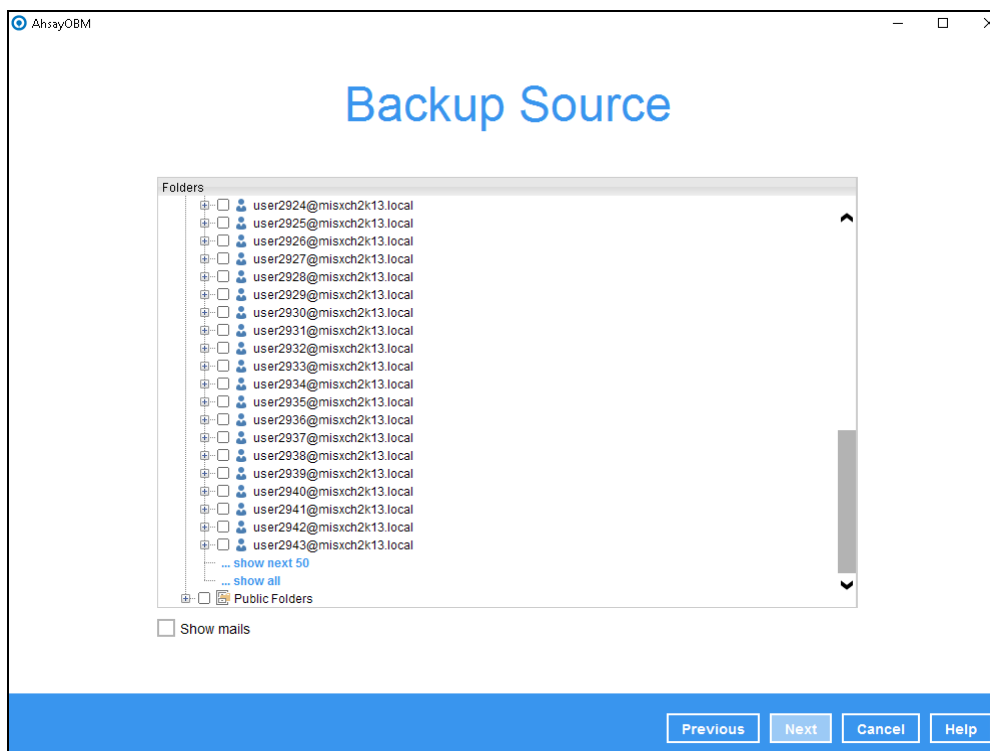
## Improved Listing of Mailboxes or Public Folders for MS Exchange 2013/2016/2019 (EWS) Mail Level Backup

For a more convenient selection of mailboxes and/or public folders, a new feature is added in the **Backup Source** menu of AhsayOBM v8.3.4.0 (or above) for MS Exchange (EWS) Mail Level backup.

### Key Features

- ▶ In the backup source menu, fifty (50) users will be displayed by default.
- ▶ For MS Exchange Server account which consists of more than fifty (50) users or above, “**show next 50**” (users) button will be displayed.
- ▶ To display all users immediately, a “**show all**” button is provided.

In the creation of MS Exchange backup set, the first fifty (50) users is displayed by default in the backup source menu. If the MS Exchange Server account contains more than fifty (50) users or above, clicking the **show next 50** button will display the next users. Selecting the **show all** button will immediately display all users.



After selecting a mail folder to back up, clicking the **Next** button will save the selected backup source.

## Data Synchronization Check (DSC) Process for Office 365 Backup

**Change Key API** is introduced in the new AhsayCBS v8.3.4.0 (or above). With the implementation of *change key API*, backup sets with large number of Office 365 users/mailboxes can be completed within hours. Thus, this application has largely increased the backup performance for both **Full** and **Incremental** Office 365 backup jobs.

However, there is a trade-off with *change key API* that will **skip** the checking of **deselected files and/or folders** in the backup source, which may eventually result to having a discrepancy between the items in the backup source and backup destination(s).

While for **deselected Office 365 user accounts or site collections**, the *change key API* will **continue** checking for these items and will be automatically moved to the retention area once detected during an Office 365 backup job.



### NOTE

The Changed Key API cannot be disabled.

To resolve this, the AhsayCBS v8.3.4.0 (or above) has added a new feature in the AhsayOBM/AhsayACB Office 365 backup process:

#### **Data Synchronization Check (DSC)** (*enabled by default*)

The function of the *data synchronization check* is to establish a **synchronized data** in the backup source and backup destination(s). This feature is similar with *change key API* job but has an additional checking and handling process of deselected files and/or folders in the backup source.

### Key Features

- ▶ Data Synchronization Check (DSC) is enabled by default and is configured to run every sixty (60) days.
- ▶ Synchronization of deselected files and/folders in the backup source will be performed to ensure that there will be no data built up on the backup destination(s).
- ▶ The day interval of which the Data Synchronization Check (DSC) will run can be manually configured by the AhsayOBM/AhsayACB backup user.

### Importance of Data Synchronization Check (DSC)

It is necessary to run a *data synchronization check* **periodically** as it helps to avoid any data that is being built-up and/or left in the backup destination(s). Thus, the storage quota will be managed efficiently since the overall storage size and the backup set cost will be reduced.



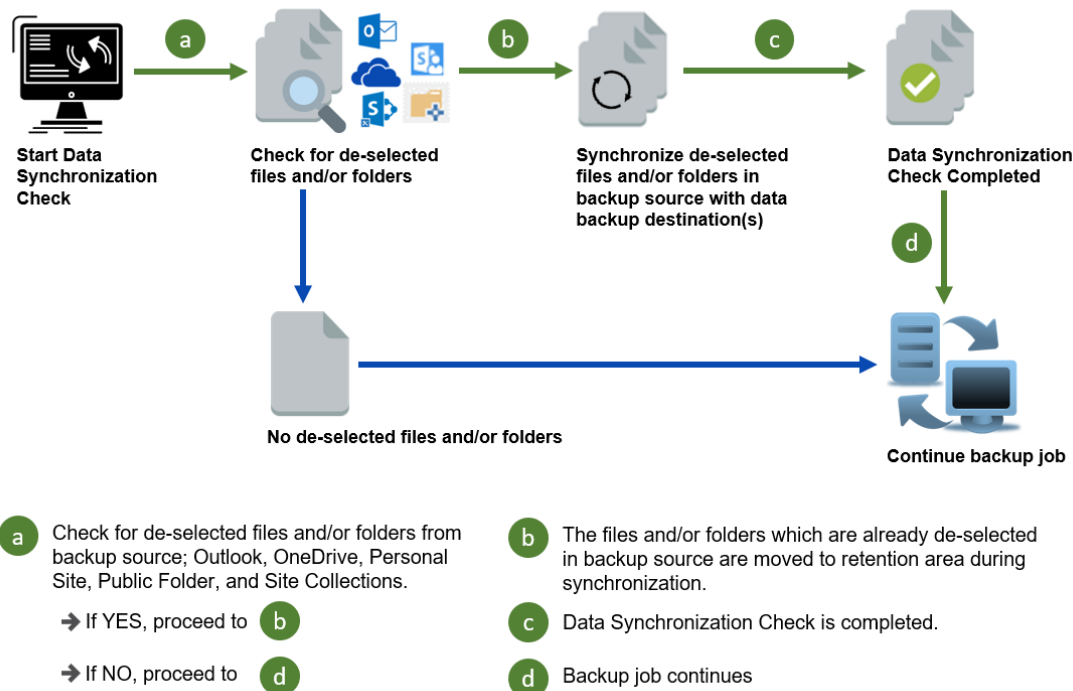
#### NOTE

If the *data synchronization check* is **disabled**, even though files and/or folders are already deselected from the backup source, these files will remain in the data area of the backup destination(s). Thus, more storage space will be used. The backup time for backup jobs with *data synchronization check* **disabled** will not be affected.

Backup time for backup jobs with *data synchronization check* **enabled** will take longer period than the usual backup job, as the checking of deselected files and/or folders in the backup source and backup destination(s) will be performed.

## How does Data Synchronization Check (DSC) work?

The following diagram shows the detailed process of the Data Synchronization Check (DSC).



## How to configure the Data Synchronization Check (DSC)?

The data synchronization check is configured by modifying the AhsayOBM/AhsayACB **cb.opt** file. If the **cb.opt** file has not been modified yet, the DSC is already enabled by default and will run with sixty (60) days interval.

There are three (3) data synchronization check settings that can be configured:

- ▶ Disabled data synchronization check
- ▶ Enabled data synchronization check (with day interval)
- ▶ Data synchronization check that runs at every backup job



To configure the *data synchronization check*, locate the following directory and look for the **cb.opt** file and open it with a text editor (e.g. Notepad or Notepad++).

**For AhsayOBM:**

*C:\Program Files\AhsayOBM\cb.opt*

**For AhsayACB:**

*C:\Program Files\AhsayACB\cb.opt*

In the **cb.opt** file, look for the **Office365.DSCInterval=xx** line. A **positive xx** value (or if the value is not -1) indicates the **enabled data synchronization check**, and the **xx** value represents the number of days until the next run of data synchronization check.

The following table shows the different types of Data Synchronization Check Setup in the **cb.opt** file.

DSC Configuration	Explanation	Result
<b>Office365.DSCInterval=-1</b>	The <b>=-1</b> value indicates that the data synchronization check is disabled.	Data synchronization check will not run.
<b>Office365.DSCInterval=60</b>	The <b>=60</b> value indicates the number of days or interval until the next run of data synchronization check. The value "60" can be adjusted according to end's user preference.	Data synchronization check will run every sixty (60) days.
<b>Office365.DSCInterval=0</b>	The <b>=0</b> value indicates that the data synchronization check will run at every backup job.	Data synchronization check will run at every backup job without any day interval.

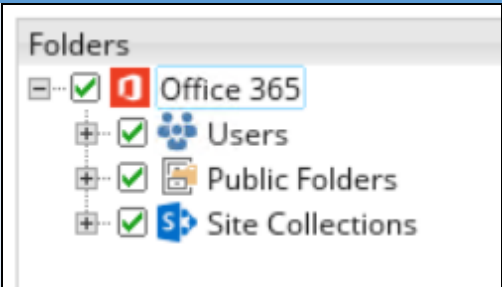
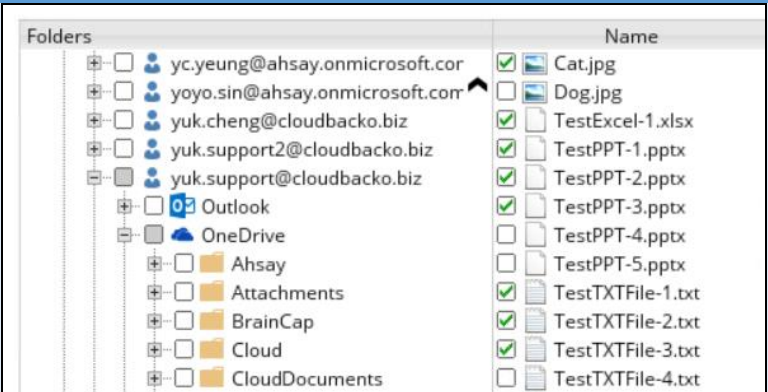


**WARNING**

Before starting an AhsayOBM/AhsayACB Office 365 backup with *data synchronization check enabled*, make sure there are no active backup/restore job running. Otherwise, it may result to a discrepancy between the data in the backup source that is currently being backed up and the data in the backup destination(s).

## Best Practices for Data Synchronization Check (DSC) Usage

There are two (2) methods in selecting files and/or folders in an Office 365 backup:

Root Selection	Example
Selecting the root folder which automatically selects all files and/or folders under all Office 365 user accounts (including Public Folders and Site Collections).	
Selective Files and/or Folders	Example
Selecting certain files and/or folders under chosen Office 365 user accounts.	

Since all selected files and/or folders will be backed up in the **root selection** method, enabling the data synchronization check **is not required**.

It is best to enable the data synchronization check for:

- ➡ **selective files and/or folder** as it will synchronize the deselected items in the backup source and backup destination(s). Since the *data synchronization check* will look for deselected items and will move them to the retention area, this guarantees that no backup data will be created on the backup destination(s). Thus, storage quota management will be more efficient as it will help to save more storage space.

## Google Cloud Storage: Regional Location Supported

Google Cloud Storage has only one (1) supported location type on the AhsayCBS v7 and pre-AhsayCBS v8.3.4.0, which is the **multi-regional**: i.e. United States, European Union, and Asia.

To align with the improved service offering from Google, the AhsayCBS v8.3.4.0 (or above) has improved its Google Cloud Storage location and classified into **four (4) types of Storage Class**:

 <b>Standard</b>	 <b>Nearline</b>	 <b>Coldline</b>	 <b>Archive</b>
---	---	---	--

Each storage class consists of **three (3) different location types**:

 <b>Multi-region</b>	 <b>Dual-region</b>	 <b>Region</b>
---	--	---

Each location type provides specific locations which are selected appropriately by the AhsayCBS administrator or Managed Service Providers (MSP) based on the end user's preference.

For a wide range of region(s) selection, newly supported regions were also added to **Amazon S3**, **Aliyun** and **Wasabi**.

<b>Amazon S3</b> 	<b>Aliyun</b> 	<b>Wasabi</b> 
 <b>Africa (Cape Town)</b>  <b>Europe (Milan)</b>	 <b>Heyuan</b>	 <b>US-East-2</b>

**Note:** For more information about the Google Cloud Storage regional locations, refer to: [Google Cloud Storage Locations](#)

**Changes on the selected multi-regional location on the previous versions after upgrading to AhsayCBS v8.3.4.0 (or above):**

<b>AhsayCBS v7 and pre-AhsayCBS v8.3.4.0</b>	<b>After upgrade (AhsayCBS v8.3.4.0 or above)</b>
<b>United States (US)</b>	<b>US (multiple regions in United States)</b>
<b>European Union (EU)</b>	<b>EU (multiple regions in European Union)</b>
<b>Asia</b>	<b>Asia (multiple regions in Asia)</b>



### WARNING

Each storage class has different data storage cost. It is very important to ensure that the specific location selected will meet the **availability, speed of access and durability requirements** of your backup data. To know more about Google Cloud Storage pricing, refer to the following link:

[Google Cloud Storage Pricing Overview](#)

## Improved Support for Network Drives (Windows)

AhsayCBS v8.3.4.0 (or above) has enhanced the **support for network drives** for Windows operating system. This feature allows the AhsayOBM/AhsayACB client to establish a connection to any available network drive (e.g. NAS or another computer).

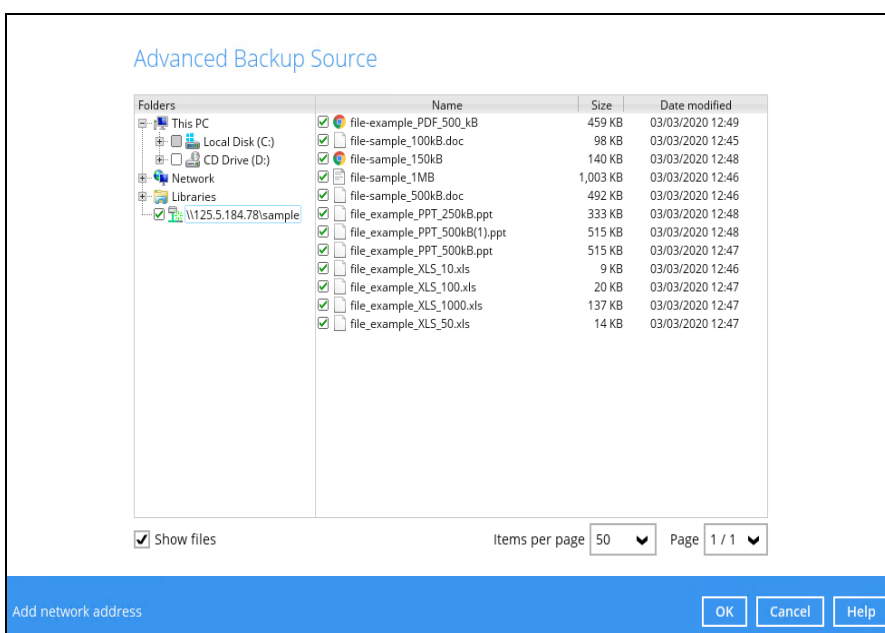
### Key Features

- ▶ Supports network drives with different login credentials instead of limiting to Windows User Authentication login or network drives without login credential.
- ▶ Supports network drives that are not set up or configured on a Windows computer.
- ▶ Supports network drives to be configured as:
  - ➊ Backup Source (including Filter)
  - ➋ Backup Destination
  - ➌ Restore Location (Original or Alternate Location)

### Network drive as a Backup Source (Including Filter)

Backup source selection is improved on the AhsayCBS v8.3.4.0 (or above). Files and/or folders that are located in a network drive from a remote device (e.g. NAS or another computer) can be configured as a backup source, as long as the network drive is set to **read and write permission** to ensure that the AhsayOBM/AhsayACB can access these files for backup.

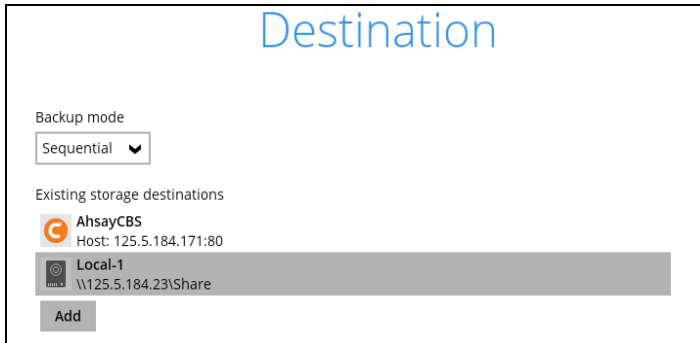
Below is an example of configured network drive as a backup source.



## Network Drive as a Backup Destination

Network drive can be configured as a **backup destination**. The files to be backed up will be stored to a network drive from a remote device (e.g. NAS or another computer).



Below is an example of a network drive configured as a backup destination.



Destination

Backup mode  
Sequential ▼

Existing storage destinations

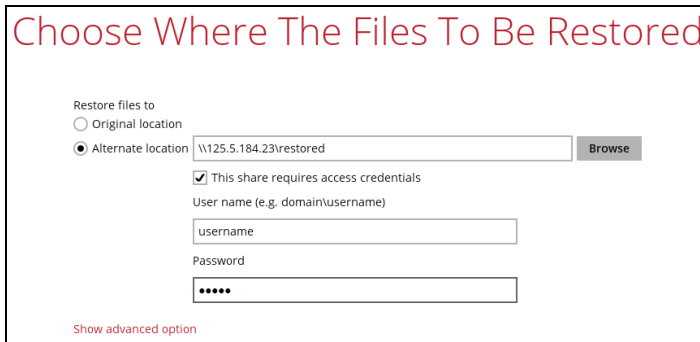
	AhsayCBS Host: 125.5.184.171:80
	Local-1 \\125.5.184.23\\Share

Add

## Network Drive as a Restore Location (Original or Alternate Location)

After the upgrade to v8.3.4.0 (or above), network drive can be set up as a restore location (original or alternate location).

Below is an example of setting up a network drive as a restore location.



Choose Where The Files To Be Restored

Restore files to  
☐ Original location  
☒ Alternate location

\\125.5.184.23\\restore Browse

☒ This share requires access credentials

User name (e.g. domain/username)

Password

[Show advanced option](#)

## Limitations

- ➡ Temporary folder location is not supported with individual login credentials but can still be set up separately using the existing Windows User Authentication login credentials.
- ➡ Does not support Pre-Backup and Post-Backup Commands.
- ➡ Does not support “Restore Raw file” and “Restore to local computer” options.
- ➡ Does not support temporary location for storing images generated by WBADMIN for Windows System State and Windows System backups.

## Periodic Backup Schedule

A periodic backup schedule enables a backup set to be configured to run a backup job every x no. of minutes or x no. of hours. This feature was previously supported on the AhsayOBS v6 but was subsequently de-supported on AhsayCBS v7. As a result, AhsayOBS v6 backup sets with periodic backup schedules on Windows platforms were **automatically migrated** to the new Continuous Backup Schedule after upgrading to AhsayCBS v7/v8.

However, due to the increasing customers' interest for periodic backup schedule especially on non-Windows operating systems, Ahsay have decided to reintroduce an improved version in the AhsayCBS v8.3.4.0 (or above) to provide customer with more flexible backup schedule options.

The v8.3.4.0 periodic backup schedule can be configured using the following scheduled intervals, which are identical to the v6 settings:

- ➡ Minute intervals: 1, 2, 3, 4, 5, 6, 10, 12, 15, 20, or 30 minutes
- ➡ Hour intervals: 1, 2, 3, 4, 6, 8, or 12 hours

## Key Features

- ▶ Supported on AhsayOBM/AhsayACB client.
- ▶ Supported on AhsayCBS for Run on Server (Office 365 and Cloud File) backup sets.
- ▶ Supports all operating systems: **Windows, MacOS, Linux, FreeBSD, QNAP, and Synology**
- ▶ Supports all backup set types.
- ▶ 100% backward compatible with the AhsayOBS v6 periodic backup schedule. Therefore, will support upgrade to all related backup sets from AhsayOBS v6 to AhsayCBS v8.3.4.0 (or above).
- ▶ Only the File backup sets on Windows operating system will support Continuous Backup Schedule on the AhsayCBS v8.3.4.0 (or above).
- ▶ All AhsayCBS v7 and pre-AhsayCBS v8.3.4.0 Windows non-File backup sets with Continuous Backup Schedules will be automatically converted to periodic backup schedules after upgrading to v8.3.4.0 (or above).

## Periodic Backup Schedule vs. Continuous Backup Schedule

The following table shows the comparison between a periodic and continuous backup schedule.

Features	Periodic Backup Schedule	Continuous Backup Schedule
Will run whether or not a change on the backup source is made	✓	✗
Run Retention Policy after backup	✓	✗
Exclude system files from the backup	✗	✓
Only apply to files smaller than (MB) size	✗	✓
Exclude Filter	✗	✓
Supported on all operating systems (i.e. Windows, MacOS, Linux, FreeBSD, QNAP, and Synology)	✓	Only supported on Windows operating system
Supports all backup set types	✓	Only supports File Backup Sets



### NOTE

Although it is possible to set up both Periodic Backup and Continuous Backup schedules on a Windows platform for File backup sets, it is highly recommended to **only use one backup schedule** as only one backup schedule can run at a time.

## Newly Supported OS: Ubuntu 20 and MacOS 10.15

For more comprehensive backup in different platforms, the AhsayCBS v8.3.4.0 (or above) has offer support for these operating systems:

- ➡ **Ubuntu 20**
- ➡ **MacOS 10.15**