Ahsay Backup

Ahsay Online Backup Manager v8

Microsoft Exchange Database Backup & Restore Guide

Ahsay Systems Corporation Limited

11 October 2021

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

Copyright Notice

Trademarks

Disclaimer

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

Revision History

Date	Descriptions	Type of modification
3 January 2020	Modified the diagram for the Overview of MS Exchange Database Backup Process and added a diagram for the Detailed Process of Periodic Data Integrity Check in Ch. 1.5	New / Modifications
20 January 2020	Included MS Exchange 2019;	Modifications
6 February 2020	Modified the structure of Ch.1 and 2;	Modifications
30 July 2020	Modified the Periodic Data Integrity Check (PDIC) diagram in Ch. 3; Added Temporary Directory and Periodic Backup Schedule in Ch. 2.2; Added Ch. 7.3 Configure Backup Schedule for Automated Backup	New / Modifications
23 September 2020	Modified the Periodic Data Integrity Check (PDIC) and Overview of MS Exchange Database Backup Process diagrams in Ch. 3	Modifications
25 January 2021	Updated screenshot in Ch. 2.1.4; Updated PDIC diagram in Ch. 3; Updated login steps in Ch. 4	Modifications
7 April 2021	Updated Ch. 3; Added sub-chapters for the detailed process diagrams in Ch. 3.1, 3.2, 3.2.1, 3.2.2 and 3.3	New / Modifications
11 October 2021	Updated login instructions in Ch. 4; Updated screenshot and removed reference to Microsoft Exchange Database 2010 in Ch. 7 and 8	Modifications

Table of Contents

1 Overview

1.1 Introduction

This user guide aims at providing detailed information for backing up and restoring Microsoft Exchange Database 2007/2010/2013/2016/2019 with AhsayOBM.

Microsoft Exchange Server is a mail server and calendar server, that helps small and medium scale organization to achieve better reliability and improved performance. It centralizes emails so that they can be backed up. It can also share calendars between different members of your organization.

AhsayOBM supports Standalone backup and Database Availability Group (DAG) backup option for Microsoft Exchange Server Database backup.

Microsoft Exchange Server Database 2013 backup and restore can be performed by installing AhsayOBM on Windows Server 2012 Standard and Windows Server 2012 R2.

Microsoft Exchange Server Database 2016 backup and restore can be performed by installing AhsayOBM either on Windows Server 2012 Standard, Windows Server 2012 R2, or Windows Server 2016 Standard.

Microsoft Exchange 2019 is supported on Windows 2019. Please refer to section, **Supported operating systems for Exchange 2019**
https://docs.microsoft.com/en-us/exchange/plan-and-deploy/system-requirements?view=exchserver-2019

1.2 What is this software?

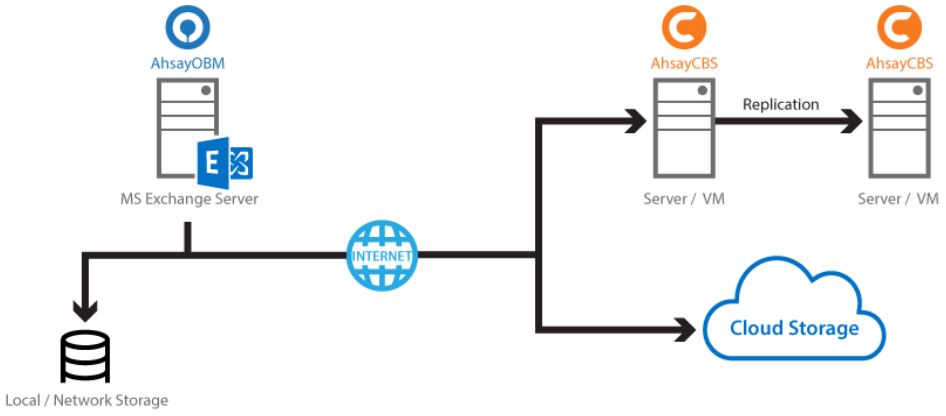
Ahsay brings you specialized client backup software, namely the AhsayOBM, to provide a set of tools to protect your databases on Microsoft Exchange Server 2007/2010/2013/2016/2019.

1.3 System Architecture

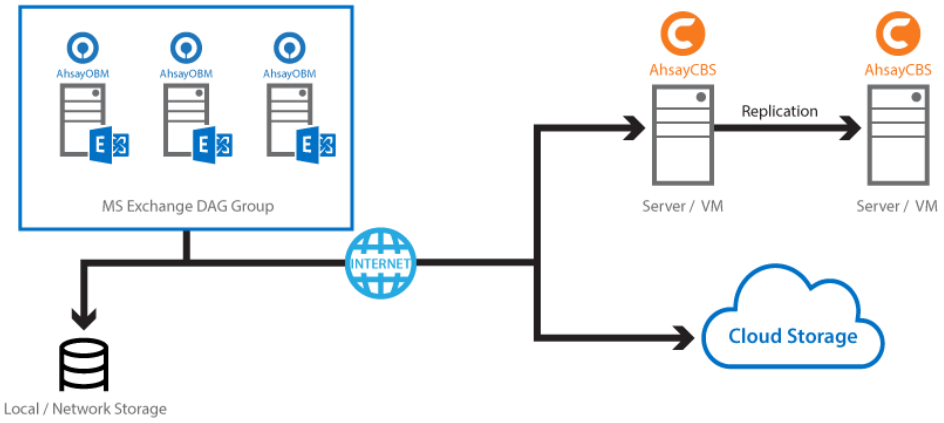
Below is the system architecture diagram illustrating the major elements involved in the backup and restore process among the Microsoft Exchange Server Database 2007/2010/2013/2016/2019, AhsayOBM and AhsayCBS.

1. **AhsayOBM v8.1.0.0 or later installed on Microsoft Exchange Server Database 2007/2010/2013/2016/2019**

    A. **Standalone:** The latest version of AhsayOBM is installed on Microsoft Exchange Server which is connected to AhsayCBS backup server through LAN or Internet.

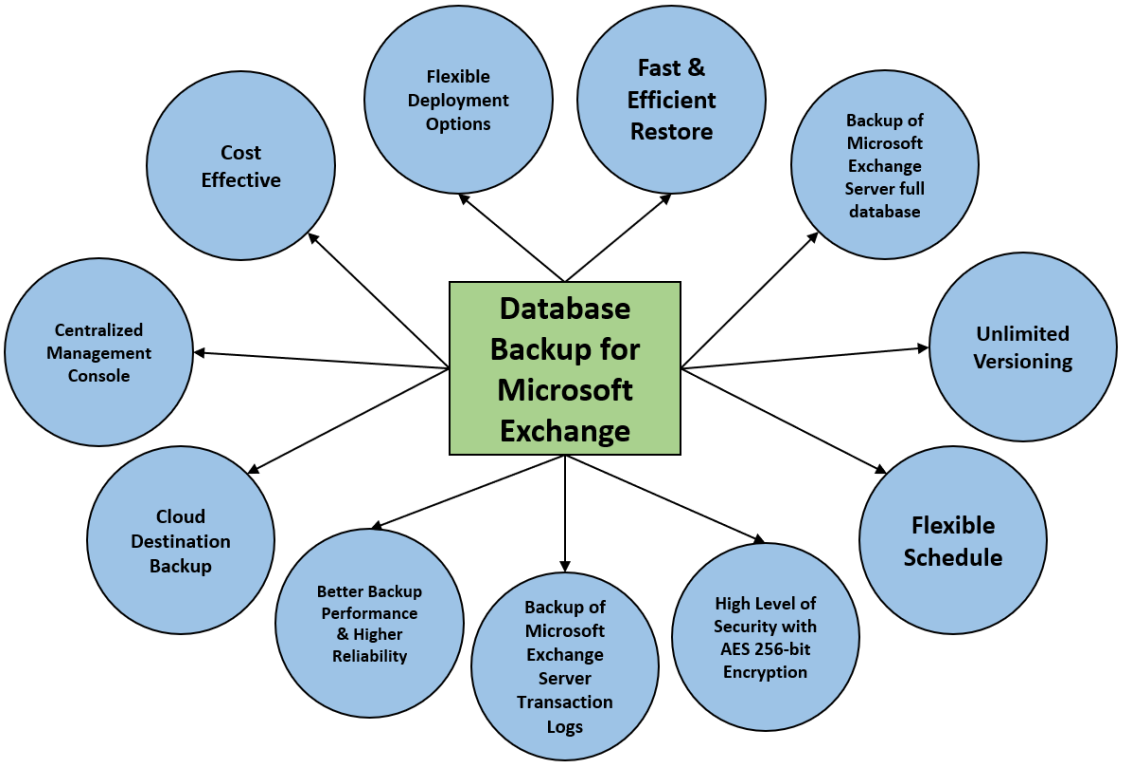


B. **Database Availability Group (DAG):** The latest version of AhsayOBM is installed on all the DAG members on Microsoft Exchange Server which is connected to AhsayCBS backup server through LAN or internet, and all the DAG members share the same backup set. Exchange DAG support for Microsoft Exchange Server Database 2013/2016/2019.



1.4 Why should I use AhsayOBM to backup Microsoft Exchange Server's full database?

We are committed to bringing you a comprehensive Microsoft Exchange Server Database 2007/2010/2013/2016/2019 backup solution with AhsayOBM. Below are some key areas that we can help to make your backup experience a better one.



1. **Fast and Efficient Restore**

   We understand that restore could be a time and resources consuming process, which is why AhsayOBM is designed with advanced technologies to make restore a fast and efficient process by restoring Microsoft Exchange Server full database.

   AhsayOBM supports recovery directly to a live production MS Exchange server, so there is no service interruption or downtime incurred, and the user mailboxes do not have to be disabled and can function normally during the recovery procedure.

2. **Unlimited Versioning**

   AhsayOBM provides backup and restore option for different version of exchange server to fulfill your requirement.

3. **Flexible Scheduling**

   You may wish to run backup at a specified time interval of your choice, that's why we also allow you to set your own backup schedules so that you can take full control of the time when to perform backup.

   - **Block Level Incremental Backup** – This technology breaks down the backup files into multiple blocks and only the changed blocks will be backed up each time.

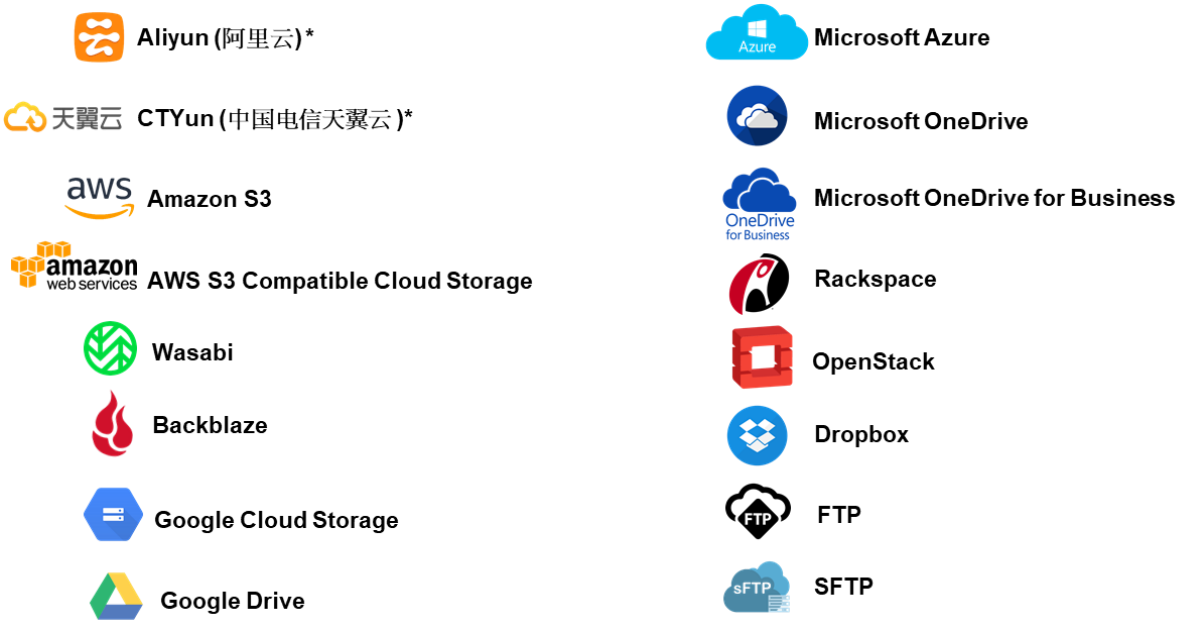
4. **High Level of Security with AES 256-bit Encryption**

We understand your Exchange mail objects may contain sensitive information that requires to be protected, that is why your backup data will be encrypted with the highest level of security measure.

5. **Cloud Destination Backup**

To offer you with the highest flexibility of backup destination, you can now back up mail objects to a wide range of cloud storage destinations. Utilizing cloud destination backup gives you an extra layer of protection in the event of a local drive corruption, where you will still be able to retrieve data from the cloud destination.

Below is a list of supported cloud destinations.



6. **Centralized Management Console**

Our enriched features on the centralized web console offers you a one-stop location for monitoring and managing your backup and restore. Below is an overview of what you can do with it. For more details regarding the setup and operations of the centralized management console, refer to the AhsayCBS User's Guide for details.

- Create / update / delete backup set
- Configure user settings
- Configure backup settings
- View and download backup and restore reports
- Monitor backup and restore live activities
- Monitor storage statistic

1.5 About this document

1.5.1 Document Main Part

The document can be divided into two (2) main parts.

Part 1: Preparation for Exchange Database 2007/2010/2013/2016/2019 Backup & Restore

Requirements
Requirements on AhsayOBM, Exchange Database 2007 / 2010 / 2013 / 2016 / 2019 and Windows Operating System

Supported Backup Source & Limitation
Supported backup source of Exchange Server 2007 / 2010 / 2013 / 2016 / 2019 and limitation

Best Practice and Recommendation
Items recommended to pay attention to before backup and restore

Part 2: Perform Database Backup and Restore for Microsoft Exchange 2007 / 2010 / 2013 / 2016 / 2019 on Exchange Server

Standalone Backup Option
Create Microsoft Exchange Server backup set, run database Level backup job and restore database backup

Database Availability Group (DAG) Backup Option
Create Microsoft Exchange Server backup set, run database backup job and restore database backup

1.5.2 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 make Database backup of Exchange Server 2007/ 2010/ 2013 / 2016 / 2019 on AhsayOBM, as well as to carry out an end-to-end backup and restore process.

1.5.3 Who should read this document?

This documentation is intended for backup administrators and IT professionals who are responsible for the Exchange Server 2007/ 2010/ 2013 / 2016 / 2019 Mail Level backup and restore.

2 Preparation for Backup and Restore

2.1 Requirement

You are strongly recommended to configure or check all the settings below to confirm all the requirements are met before you proceed with the Exchange Database backup and restoration.

2.1.1 Software Requirement

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

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

2.1.2 Antivirus Exclusion Requirement

To optimize performance of AhsayOBM on Windows, and to avoid conflict with your antivirus software, refer to the following article the list of processes and directory paths that should be added to all antivirus software white-list / exclusion list:

FAQ: Suggestion on antivirus exclusions to improve performance of Ahsay software on Windows

NOTE

The bJW.exe process is automatically added to Windows Defender exclusion list for Windows 2016 and 2019, during installation / upgrade via installer or upgrade via AUA.

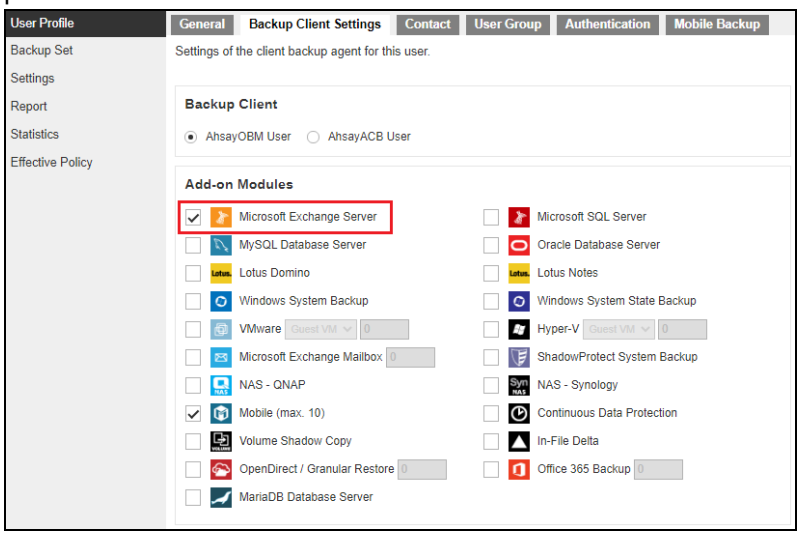
2.1.3 AhsayOBM Installation

AhsayOBM v8.1.0.0 or above must be installed directly on the MS Exchange Server 2007/2010/2013/2016/2019 hosting the database.

AhsayOBM v8.1.0.0 or above must be installed directly on the individual nodes for MS Exchange Server 2013/2016/2019 DAG.

2.1.4 Microsoft Exchange Server Add-On Module

Make sure the Microsoft Exchange Server feature has been enabled as an add-on module in your AhsayOBM user account. Please contact your backup service provider for more details.



2.1.5 Backup Quota Requirement

Make sure that your AhsayOBM user account has sufficient storage quota assigned to accommodate the storage of additional Microsoft Exchange Server backup set and retention policy.

Please contact your backup service provider for more details.

2.1.6 Continuous Backup Module

The Continuous backup add-on module is required if you would like to enable the continuous backup feature.

2.1.7 Java Heap Size

The default Java heap size setting on AhsayOBM is 2048MB. For Exchange Server 2007/2010/2013/2016/2019 Database backup, it is highly recommended to increase the Java heap size setting to be at least 4096MB to improve backup and restore performance. The actual heap size is dependent on amount of free memory available on your Exchange 2007/2010/2013/2016/2019 server.

2.1.8 Temporary Directory

Temporary Directory folder is used by AhsayOBM for storing backup set index files and any incremental or differential delta files generated during a backup job. To ensure optimal backup/restoration performance, it is highly recommended that the temporary directory folder is located on a local drive with sufficient free disk space. It should be on another location other than Drive C: (e.g. Drive E:).

The Exchange Server 2007/2010/2013/2016/2019 database files are no longer stored in the temporary directory during backup. However, the VSS-based Exchange backup will still require certain amount of disk space to operate. Microsoft suggested that certain shadow copy mechanism may require free space around 100% of the original database. Refer to the following URL for more information.

https://docs.microsoft.com/en-us/exchange/client-developer/exchange-server-development

2.1.9 System State

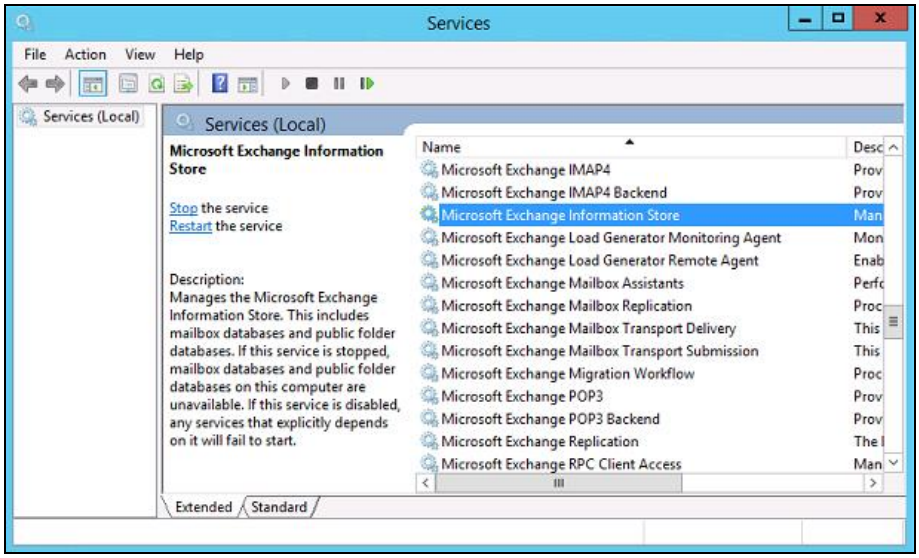
For Exchange server with Active Directory installed, as part of the restore, the system state of the server must also be restored.

Running regular system state backups of the Exchange is therefore crucial, as it ensures that the system state data is synchronized with the Exchange database data.

2.1.10 MS Exchange Information Store Service

Ensure that all MS Exchange related services have been started, particularly the **MS Exchange Information Store Service.**

To verify this setting, launch **Services** in Windows by clicking **Start** then typing “Services” in the search box. All Exchange related services should be started by default, in case if it is not, turn it on by right clicking the item then selecting **Start**.



Also make sure that circular logging is disabled for all Information Store(s) or Public Folder selected for backup.

I. Information Store – Exchange 2007

The Information Store of Exchange 2007 contains both mailbox store and public folder store data.

The server stores data in two files, namely the .edb and the .stm file, that form an Exchange store repository.

The default mailbox store on an Exchange 2007 server uses filename Priv1.edb and Priv1.stm; the default public folder store uses the filename Pub1.edb and Pub1.stm.

The .edb file contains tables that hold metadata for all e-mail messages and other items in the Exchange store, while .stm stores native Internet content.

II. Information Store – Exchange 2010/2013/2016/2019

The Information Store of Exchange 2010/2013 contains data, data definitions, indexes, checksums, flags, and other information that comprise mailboxes in Exchange.

Mailbox databases hold data that is private to individual user and contain mailbox folders generated when a mailbox is created for that user. A mailbox database is stored as an Exchange database .edb file.

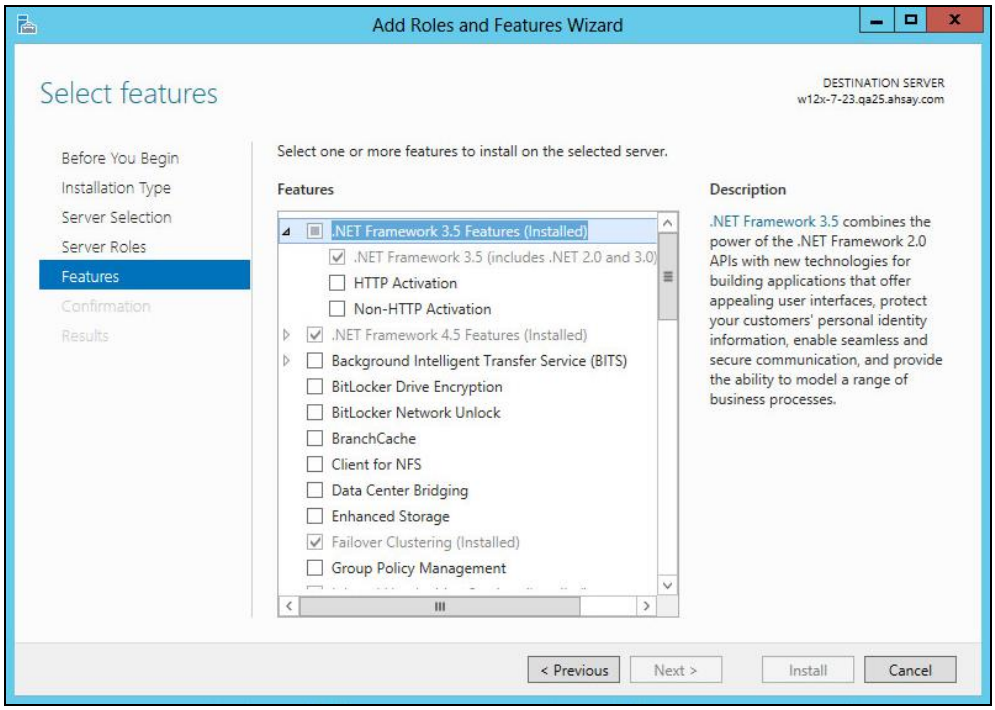
Public folder databases contain the data, data definitions, indexes, checksums, flags, and other information that comprise any public folders in your Exchange organization.

In Exchange Server 2010/2013, public folder is an optional feature.

2.1.11 .Net Framework

Net Framework 3.5 Features for Exchange Server 2013/2016/2019

Ensure that **.Net Framework 3.5 Features** is installed. This feature can be enabled by accessing Server Manager > Dashboard > Add Roles and Features Wizard > Feature Page.



2.1.12 Microsoft Exchange Writer

Ensure that the **Microsoft Exchange Writer** is installed and running on the Exchange Server, and the writer state is **Stable**. This can be verified by running the **vssadmin list writers** command.

Example**:**

```
C:\Users\Administrator>vssadmin list writers
vssadmin 1.1 - Volume Shadow Copy Service administrative
command-line tool
(C) Copyright 2001-2013 Microsoft Corp.

Writer name: 'System Writer'
   Writer Id: {e8132975-6f93-4464-a53e-1050253ae220}
   Writer Instance Id: {a2f2507d-b348-493a-9685-da3f20959e9d}
   State: [1] Stable
   Last error: No error

Writer name: 'COM+ REGDB Writer'
   Writer Id: {542da469-d3e1-473c-9f4f-7847f01fc64f}
   Writer Instance Id: {60b9b261-ab81-4c4d-be0f-5d432a4dea64}
   State: [1] Stable
   Last error: No error

Writer name: 'ASR Writer'
   Writer Id: {be000cbe-11fe-4426-9c58-531aa6355fc4}
   Writer Instance Id: {1aab9829-3b91-46bc-a7f1-ae9e1123c2fe}
   State: [1] Stable
```

```
   Last error: No error

Writer name: 'Microsoft Exchange Writer'
   Writer Id: {76fe1ac4-15f7-4bcd-987e-8e1acb462fb7}
   Writer Instance Id: {2e8409fa-1dd8-483c-ba95-5c9277be0509}
   State: [1] Stable
   Last error: No error

Writer name: 'IIS Metabase Writer'
   Writer Id: {59b1f0cf-90ef-465f-9609-6ca8b2938366}
   Writer Instance Id: {3303e28e-afae-4c99-8f1a-2ce23e6455a7}
   State: [1] Stable
   Last error: No error

Writer name: 'FRS Writer'
   Writer Id: {d76f5a28-3092-4589-ba48-2958fb88ce29}
   Writer Instance Id: {d35e3901-f9b9-4fa6-86af-36b8a4872933}
   State: [1] Stable
   Last error: No error

Writer name: 'Shadow Copy Optimization Writer'
   Writer Id: {4dc3bdd4-ab48-4d07-adb0-3bee2926fd7f}
   Writer Instance Id: {8e19e851-95ca-4c97-813d-4bc51898c7ac}
   State: [1] Stable
   Last error: No error

Writer name: 'WMI Writer'
   Writer Id: {a6ad56c2-b509-4e6c-bb19-49d8f43532f0}
   Writer Instance Id: {0619e684-14f3-495b-be59-e35fc0ec212b}
   State: [1] Stable
   Last error: No error

Writer name: 'BITS Writer'
   Writer Id: {4969d978-be47-48b0-b100-f328f07ac1e0}
   Writer Instance Id: {94991e66-e5c7-47a4-a0c9-3771e4761262}
   State: [1] Stable
   Last error: No error

Writer name: 'Registry Writer'
   Writer Id: {afbab4a2-367d-4d15-a586-71dbb18f8485}
   Writer Instance Id: {73c66436-c2e8-4d46-b88a-d866617eb95d}
   State: [1] Stable
   Last error: No error

Writer name: 'NTDS'
   Writer Id: {b2014c9e-8711-4c5c-a5a9-3cf384484757}
   Writer Instance Id: {14cedc8b-4c51-4a12-85c4-8cf8aa3545b6}
   State: [1] Stable
   Last error: No error

Writer name: 'IIS Config Writer'
   Writer Id: {2a40fd15-dfca-4aa8-a654-1f8c654603f6}
   Writer Instance Id: {5939e29f-bf43-4a39-a6b7-e3a838e75e3e}
   State: [1] Stable
   Last error: No error
```

2.2 Best Practices and Recommendations

1. For Exchange server with Active Directory installed, a Windows System State backup must be performed regularly with the MS Exchange Server backup.

2. System State backup must be performed regularly for the domain controller of the Exchange DAG setup.

3. Scheduled backup is required if you choose to back up with DAG option, as AhsayOBM on all DAG members will base on the scheduled backup time to start backups on individual DAG member at the same time.

   A DAG backup cycle is considered complete only when scheduled backup on all DAG members have been carried out. An email report will be generated when a complete DAG backup cycle has taken place.

   Please keep in mind that manual backup will only be considered as individual mail-level backup, and therefore will not be counted as part of the DAG backup cycle.

4. The MS Exchange Server Backup module will protect the Exchange server at the database level. If a full system backup (for bare-metal recovery) is required, please consider setting up a MS System Backup for each DAG member server.

5. To back up mailbox database within an Exchange DAG, AhsayOBM is required to be installed on each DAG member with mailbox role (e.g. servers that are hosting the mailbox databases). It is not necessary to install AhsayOBM on Exchange server with CAS (Client Access Server) role only.

6. To ensure optimal backup/restoration performance, it is recommended that the temporary directory folder is set to a local drive with sufficient free disk space and must be on another location other than Drive C: (e.g. Drive E:).

7. 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 production server, i.e. the number of new files created, the number of files which are updated/deleted, and new users may be added etc.

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

   - Hardware – to achieve optimal performance, compatible hardware requirements is a must. Ensure you have the backup machine's appropriate hardware specifications to accommodate frequency of backups,
     - so that the data is always backed up within the periodic backup interval
     - so that the backup frequency does not affect the performance of the production server
   - Network – make sure to have enough network bandwidth to accommodate the volume of data within the backup interval.
   - 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 Overview of MS Exchange Database Backup Process

The following steps are performed during an Exchange Database backup job. For an overview of the detailed process for Steps **3**, **5**, **13**, and **15**, please refer to the following chapters:

- Periodic Data Integrity Check (PDIC) Process **(Step 3)**
- Backup Set Index Handling Process
  - Start Backup Job **(Step 5)**
  - Completed Backup Job **(Step 15)**
- Data Validation Check **(Step 13)**

3.1 Periodic Data Integrity Check (PDIC) Process

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

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

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

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

0	**Monday**
1	**Tuesday**
2	**Wednesday**
3	**Thursday**
4	**Friday**

NOTE: The PDIC schedule cannot be changed.

Example:

Backup set ID: 1594627447932

Calculation*:* 1594627447932 *mod 5* = ***2***

2	**Wednesday**

In this example:

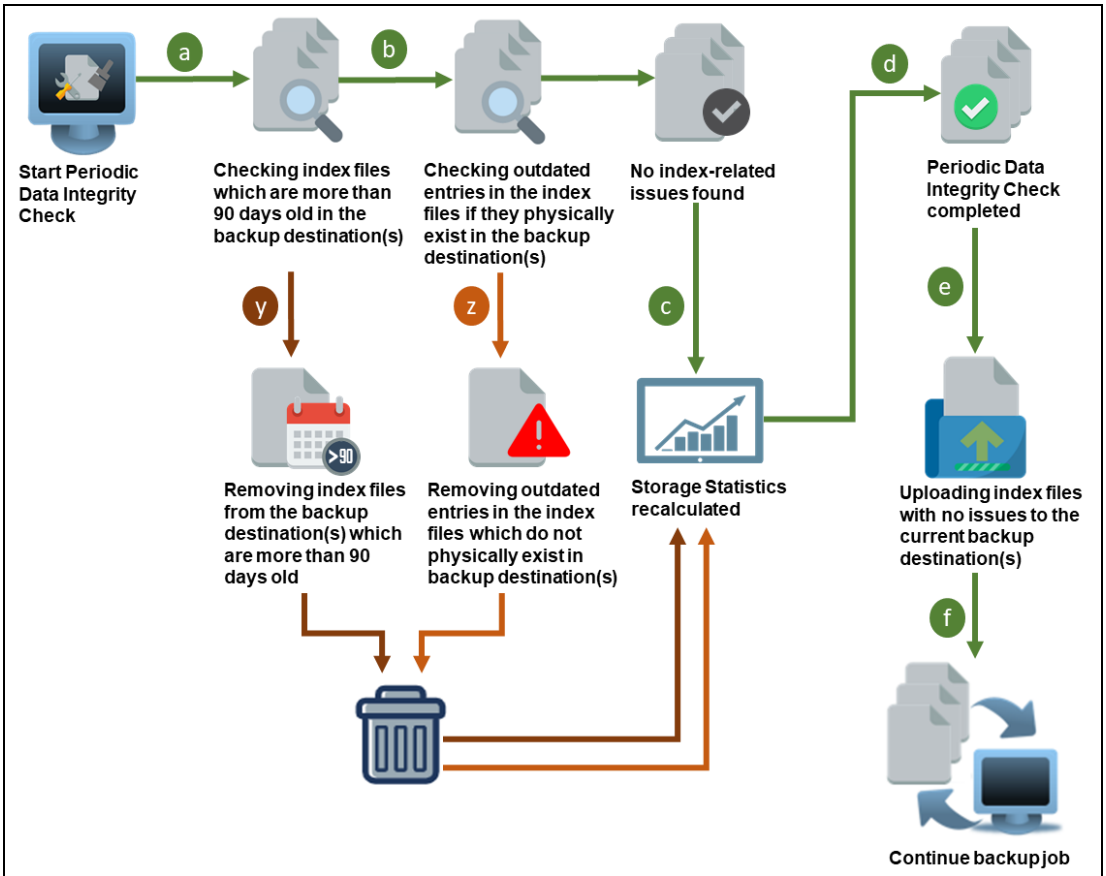
- the PDIC will run on the first backup job that falls on Wednesday; or
- if there is no active backup job(s) running from Monday to Friday, then the PDIC will run on the next available backup job.

NOTE

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

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

1. If AhsayOBM was upgraded to v8.5 (or above) from an older version v6, v7, or pre-8.3.6.0 version. In this case, the PDIC job will run on the first backup job after upgrade.
2. If backup jobs for a backup set are not run on a regular daily backup schedule (for example: on a weekly or monthly schedule), then the PDIC job will run if it detects that the previous PDIC job was run more than 7 days ago.



a Check the index files in the backup destination(s) to determine if they were more than 90 days old.
- If **YES**, proceed to y
- If **NO**, proceed to b

b Check the outdated entries in the index files for files and/or folders if they physically exist in the backup destination(s).
- If **YES**, proceed to c
- If **NO**, proceed to z

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

d Periodic Data Integrity check is completed.

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

f The backup job process will continue.

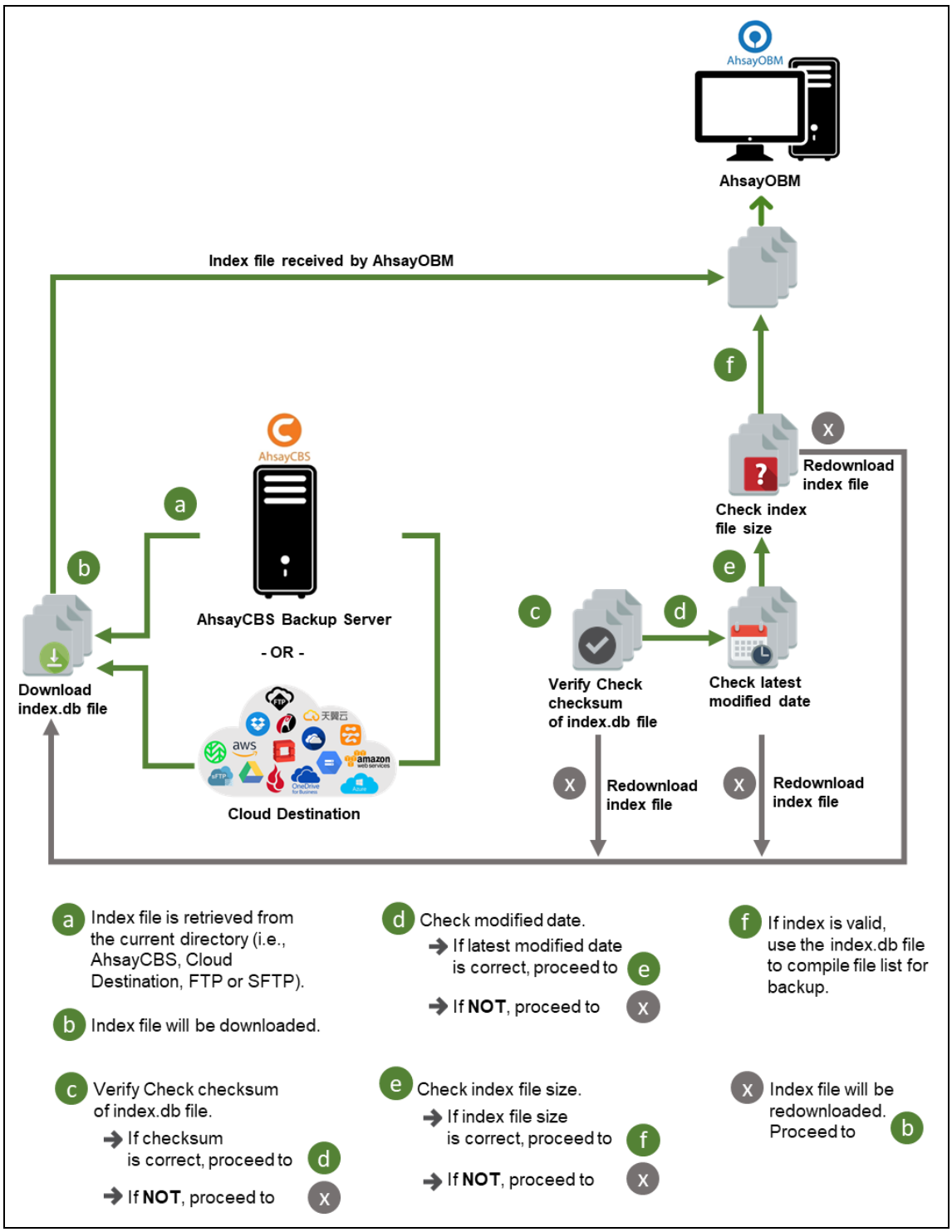
y Index files which are more than 90 days old will be removed from the backup destination(s).

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

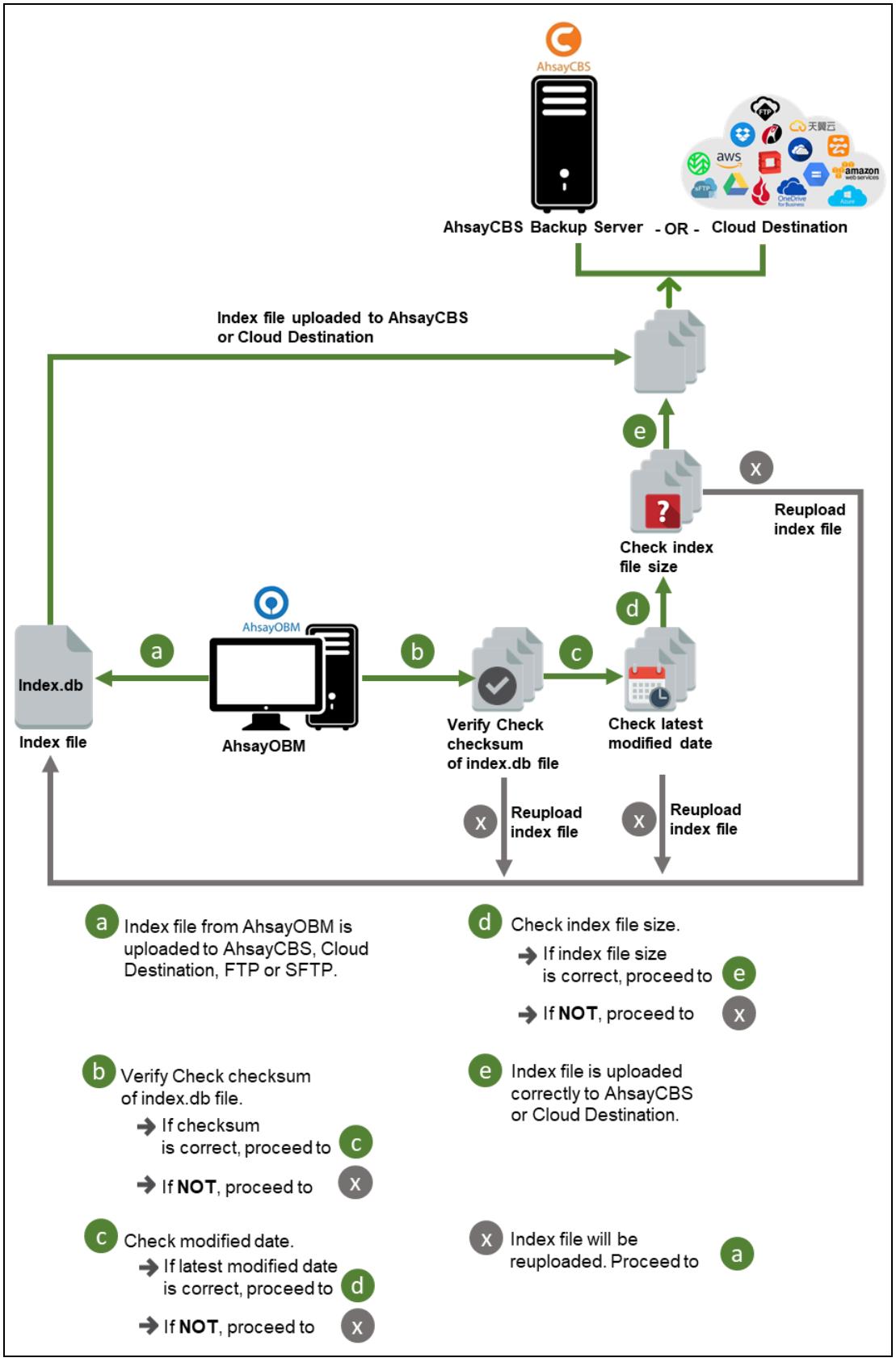
3.2 Backup Set Index Handling Process

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.

3.2.1 Start Backup Job

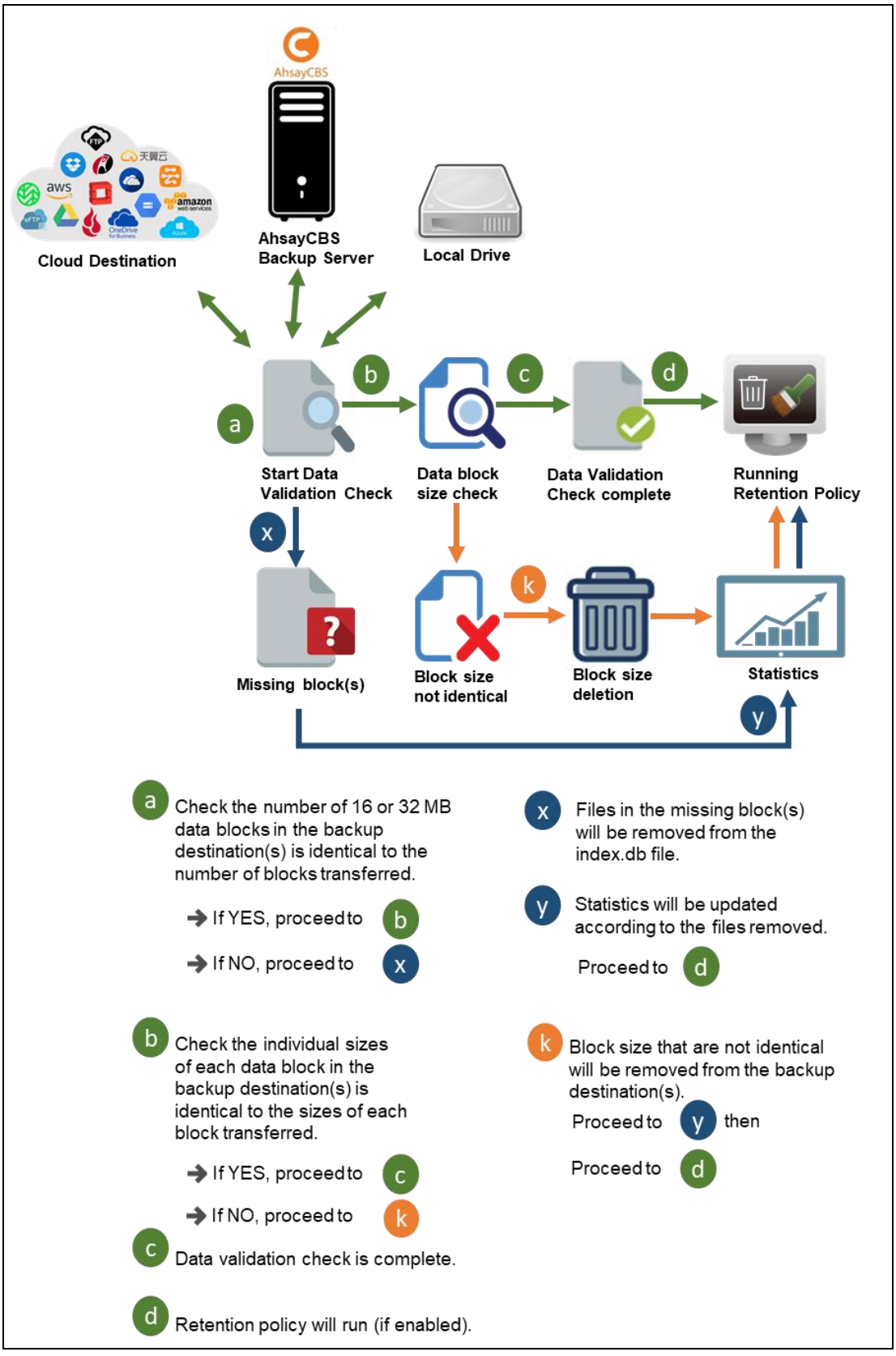


3.2.2 Completed Backup Job



3.3 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.



4 Logging in to AhsayOBM

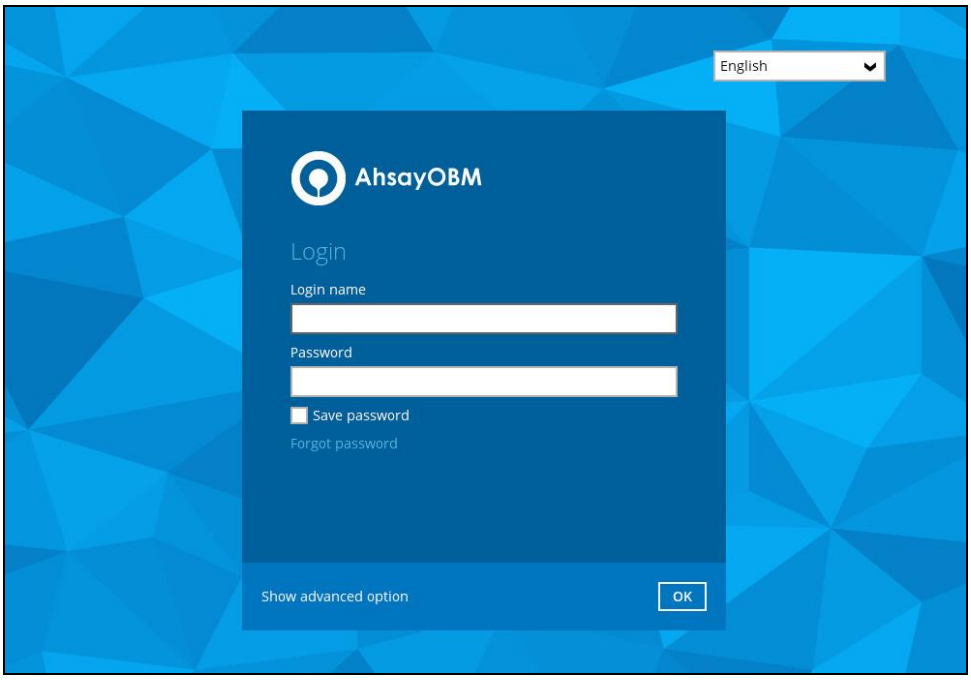
Starting with AhsayOBM v8.5.0.0 there are several login scenarios depending on the setting of the account you are using. The different scenarios will be discussed below:

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

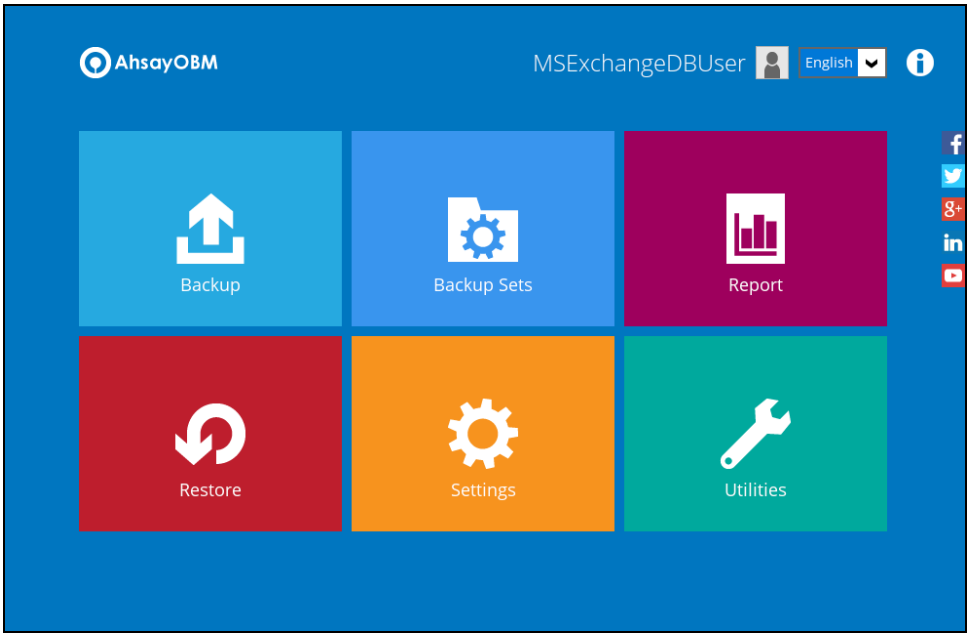
4.1 Login to AhsayOBM without 2FA

1. A shortcut icon of AhsayOBM should have been created on your Windows desktop after installation. Double click the icon to launch the application.

2. Enter the **Login name** and **Password** of your AhsayOBM account provided by your backup service provider, then click **OK** to login.



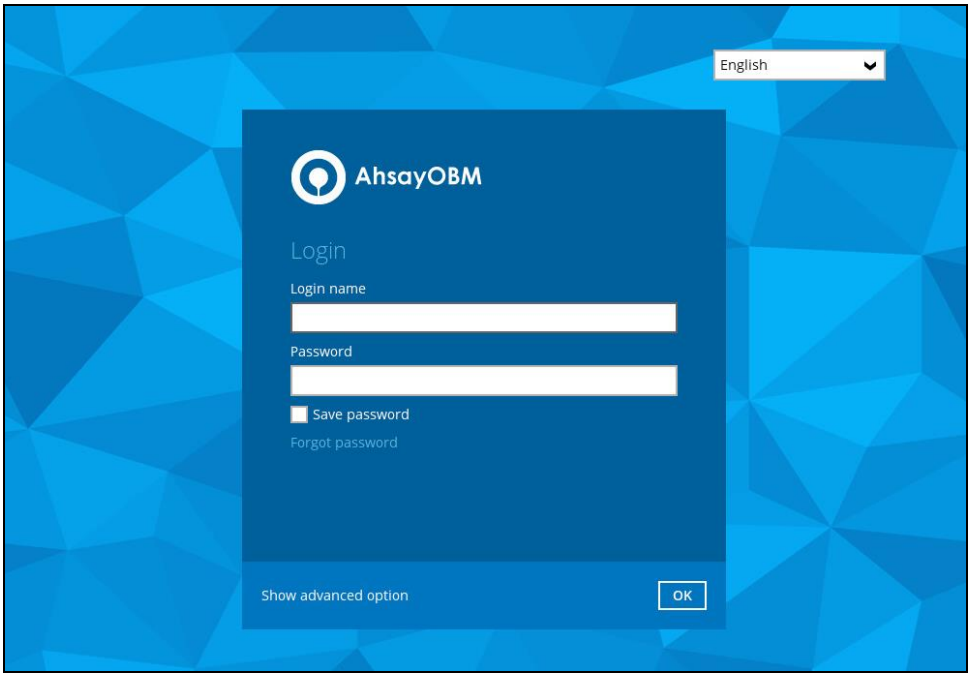
3. After successful login, the following screen will appear.



4.2 Login to AhsayOBM with 2FA using authenticator app

1. A shortcut icon of AhsayOBM should have been created on your Windows desktop after installation. Double click the icon to launch the application.

2. Enter the **Login name** and **Password** of your AhsayOBM account provided by your backup service provider, then click **OK** to login.



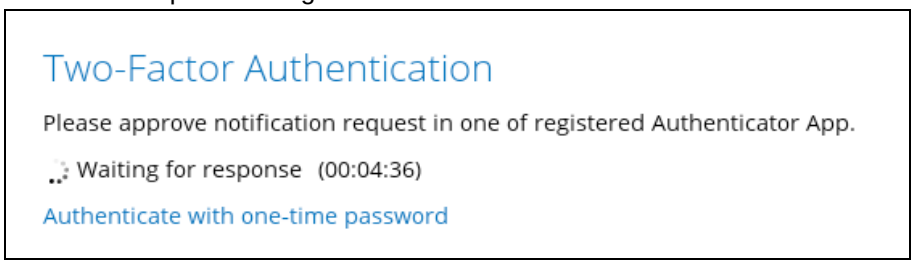
3. One of the two authentication methods will be displayed to continue with the login:

   - Push Notification and TOTP when using Ahsay Mobile app
   - TOTP only

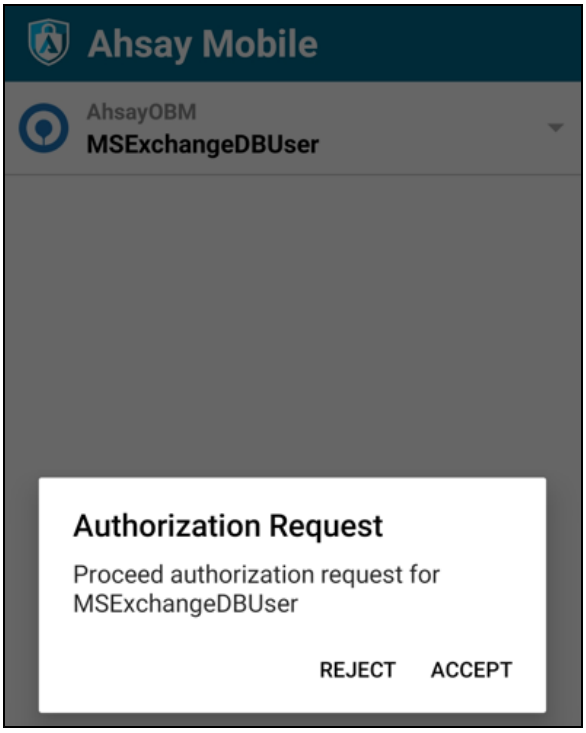
     - If **Ahsay Mobile app** was configured to use Push Notification and TOTP then there are two 2FA modes that can be used:

       - Push Notification (default)

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

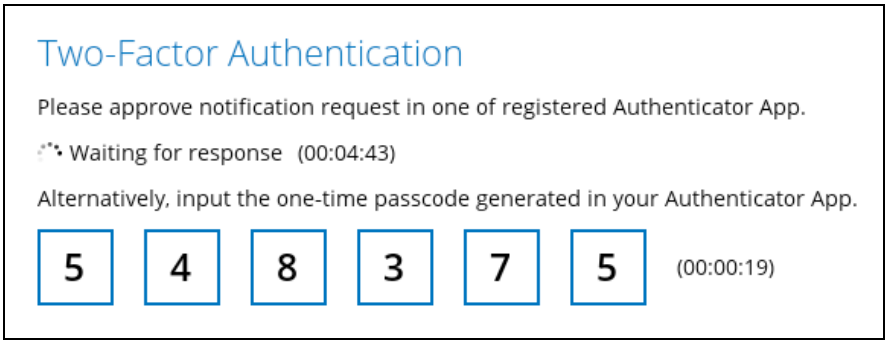


Example of the login request sent to the Ahsay Mobile app.

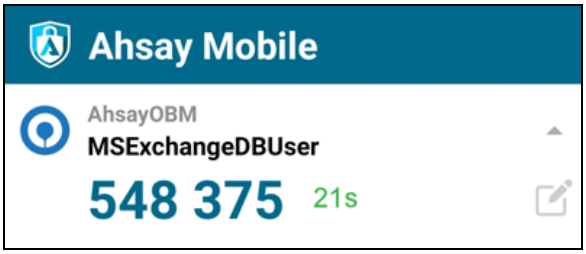


- TOTP

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.

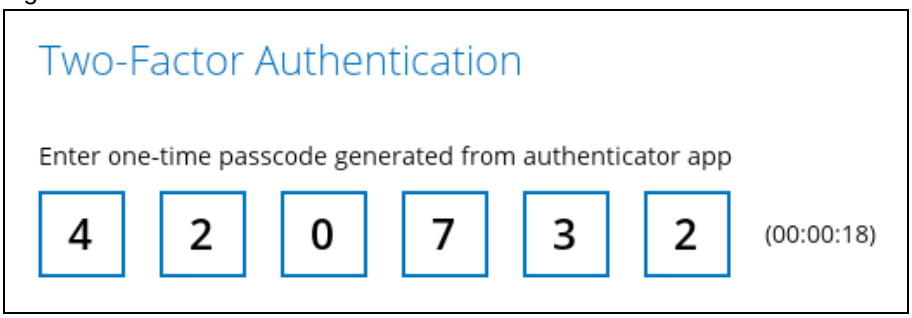


Example of the one-time passcode generated in Ahsay Mobile.

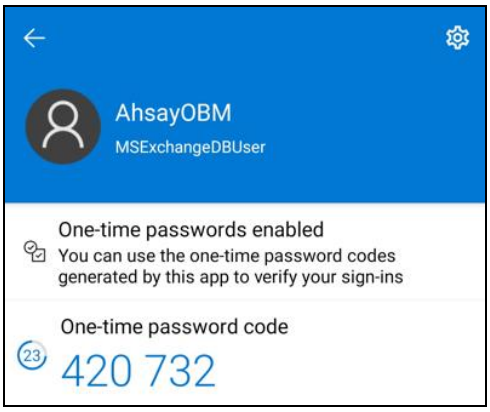


- TOTP only

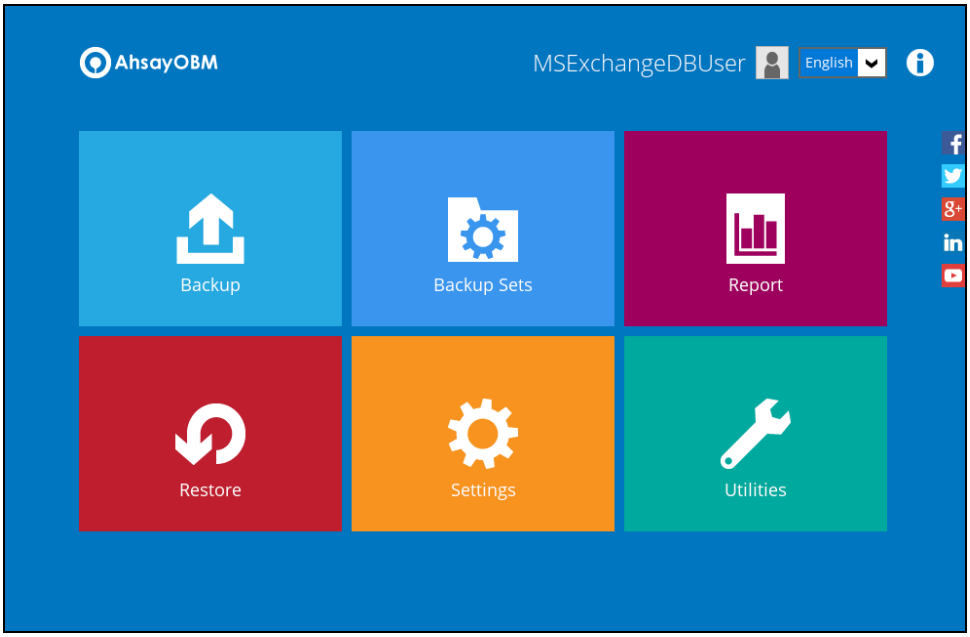
  Enter the one-time passcode generated by the authenticator app to complete the login.



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



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



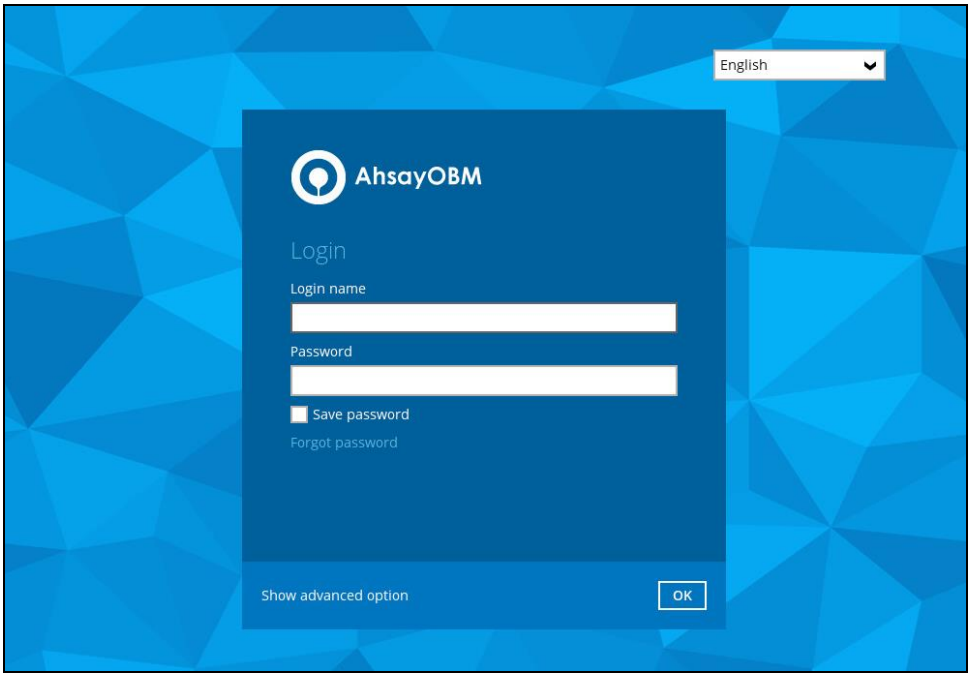
NOTE

If you have trouble logging in using the authenticator app please refer to Chapter 9 of the AhsayOBM Quick Start Guide for Windows for more information.

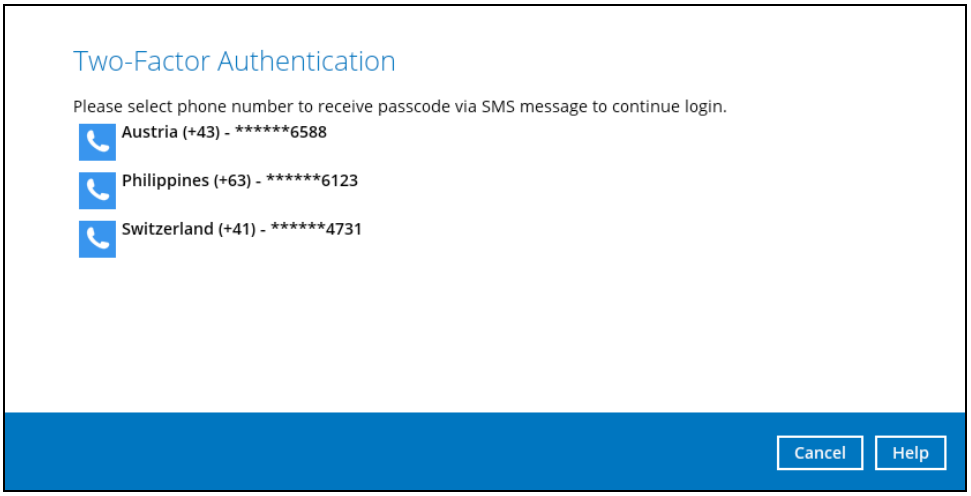
4.3 Login to AhsayOBM with 2FA using Twilio

1. A shortcut icon of AhsayOBM should have been created on your Windows desktop after installation. Double click the icon to launch the application.

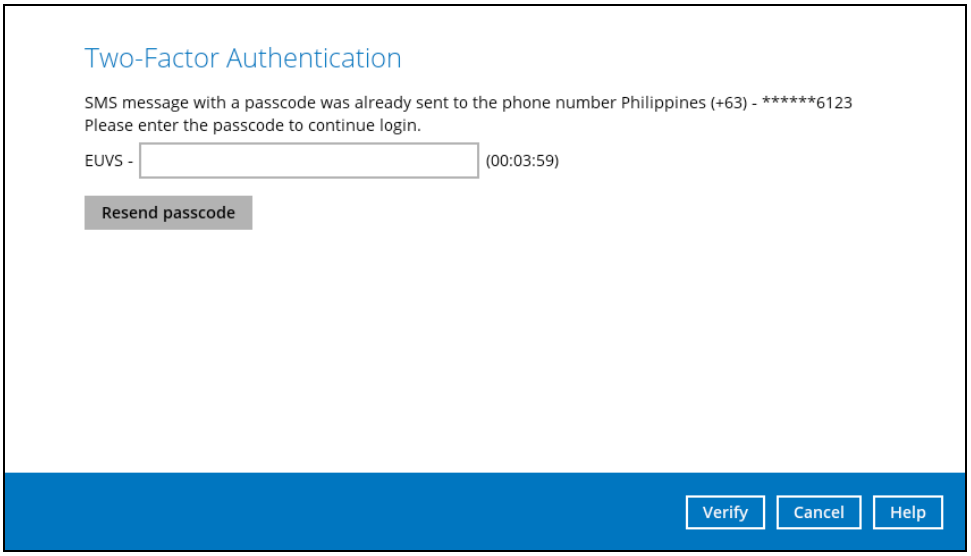
2. Enter the **Login name** and **Password** of your AhsayOBM account provided by your backup service provider, then click **OK** to login.



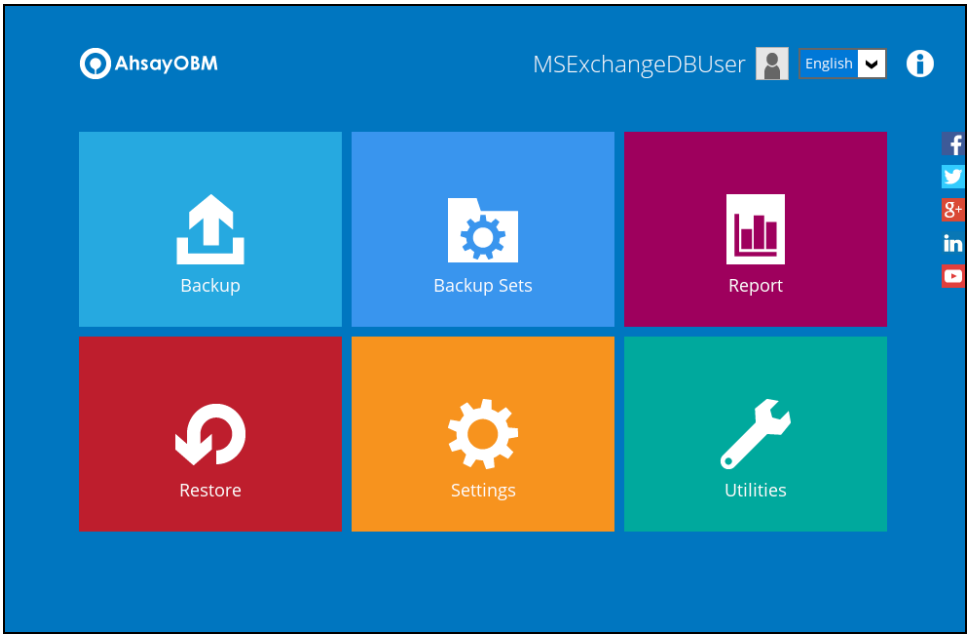
3. Select your phone number.



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



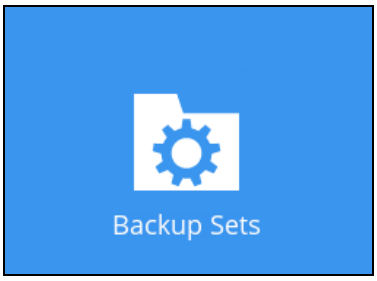
5. After successful login, the following screen will appear.



5 Backing up Microsoft Exchange Database 2007/2010/2013/2016/2019

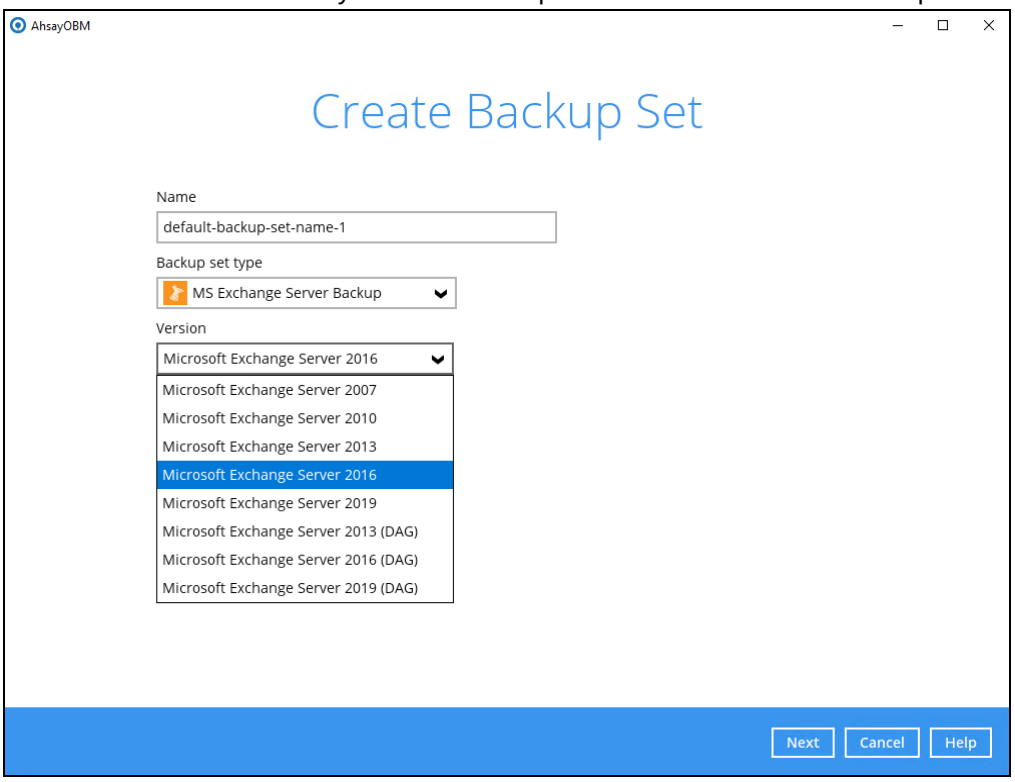
5.1 Creating a MS Exchange Server Backup Set for Exchange Server 2007/2010/2013/2016/2019

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

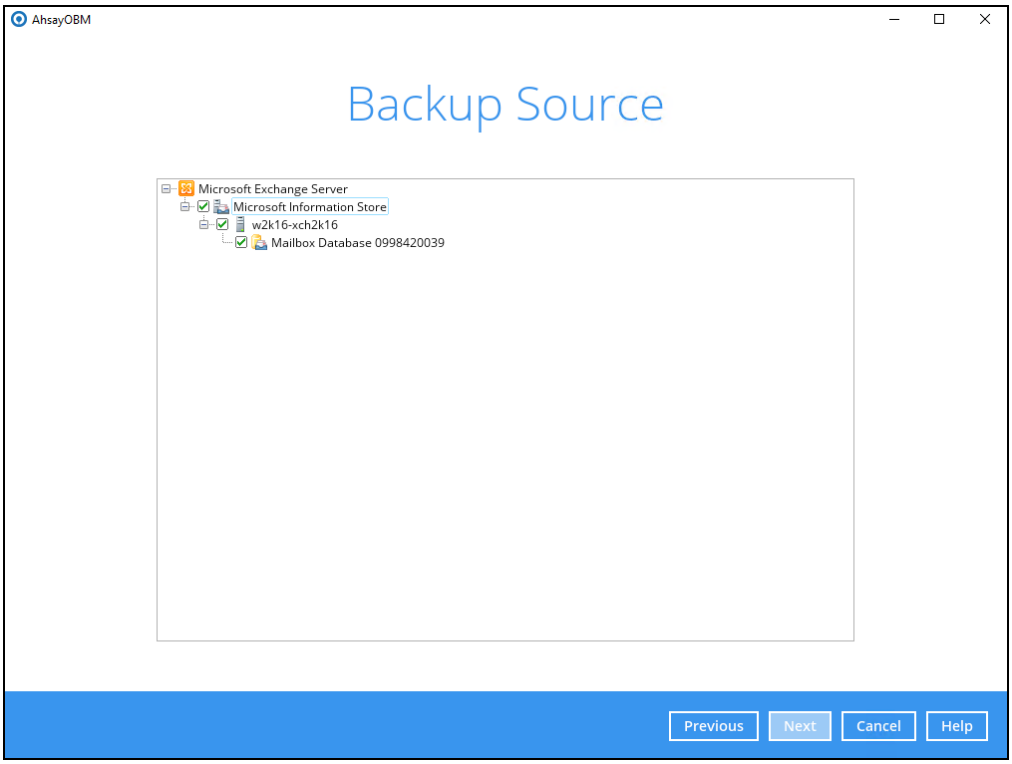


2. Create a new backup set by clicking the "**+**" icon next to **Add new backup set**.

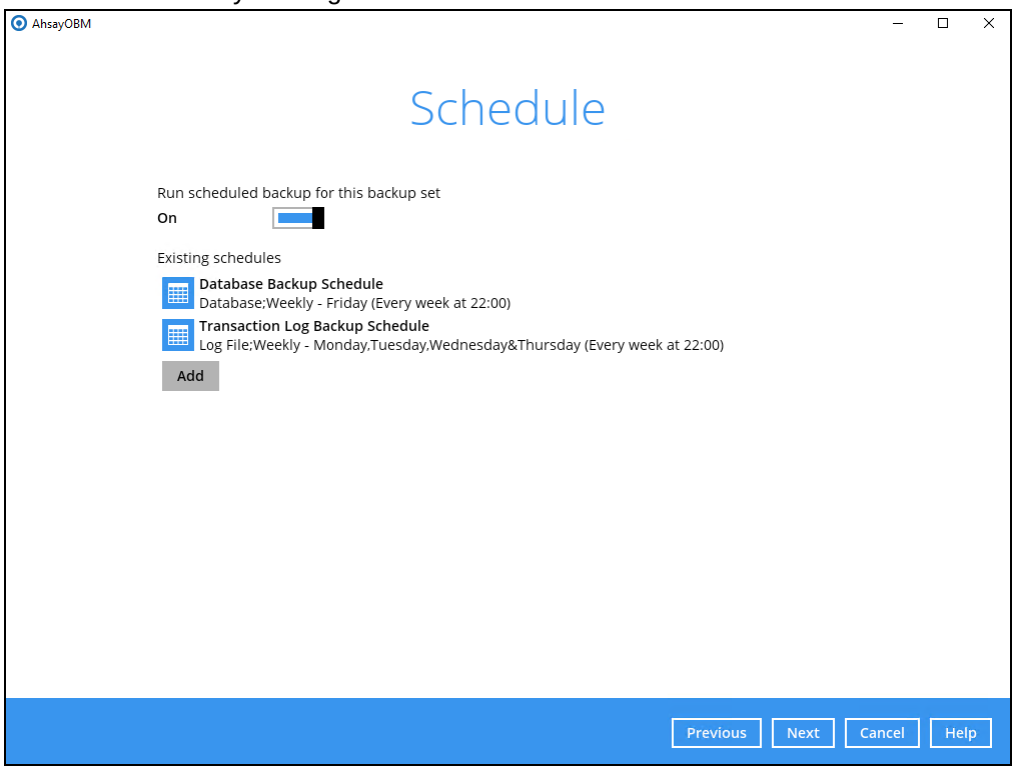
3. Select the Backup set type as **MS Exchange Server Backup.** The system will automatically detect and select the Exchange Server version, make sure the version selected is correct. Name your new backup set and then click **Next** to proceed.



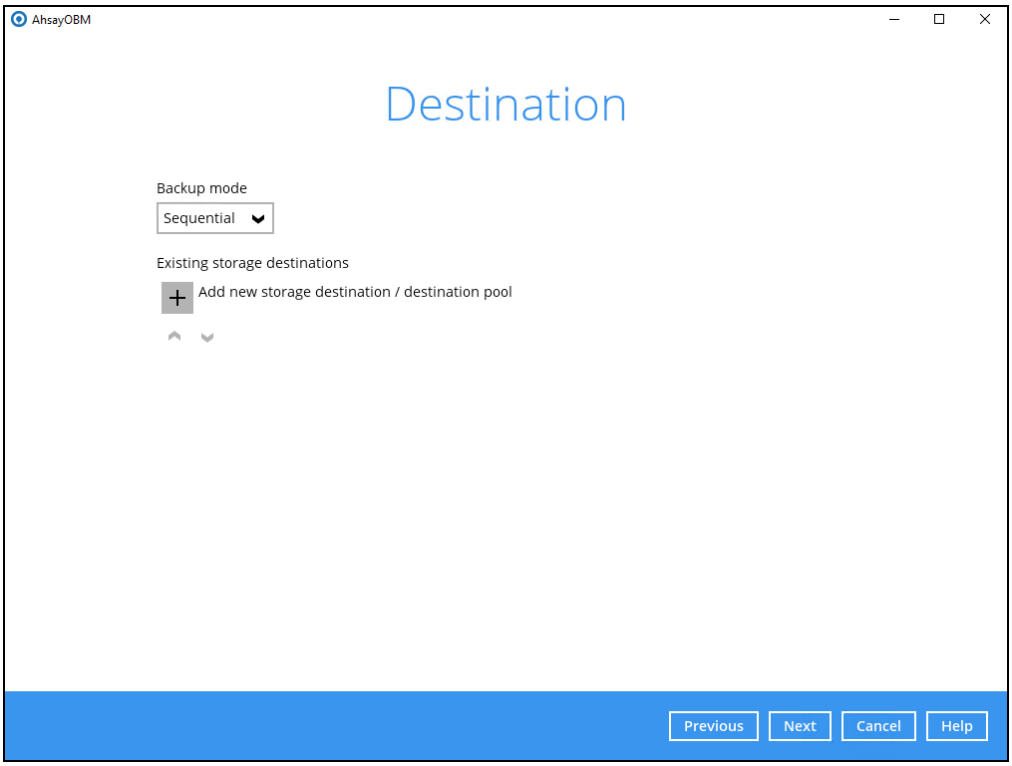
4. In the **Backup Source** menu, select the Information Store for backup. Click **Next** to proceed.



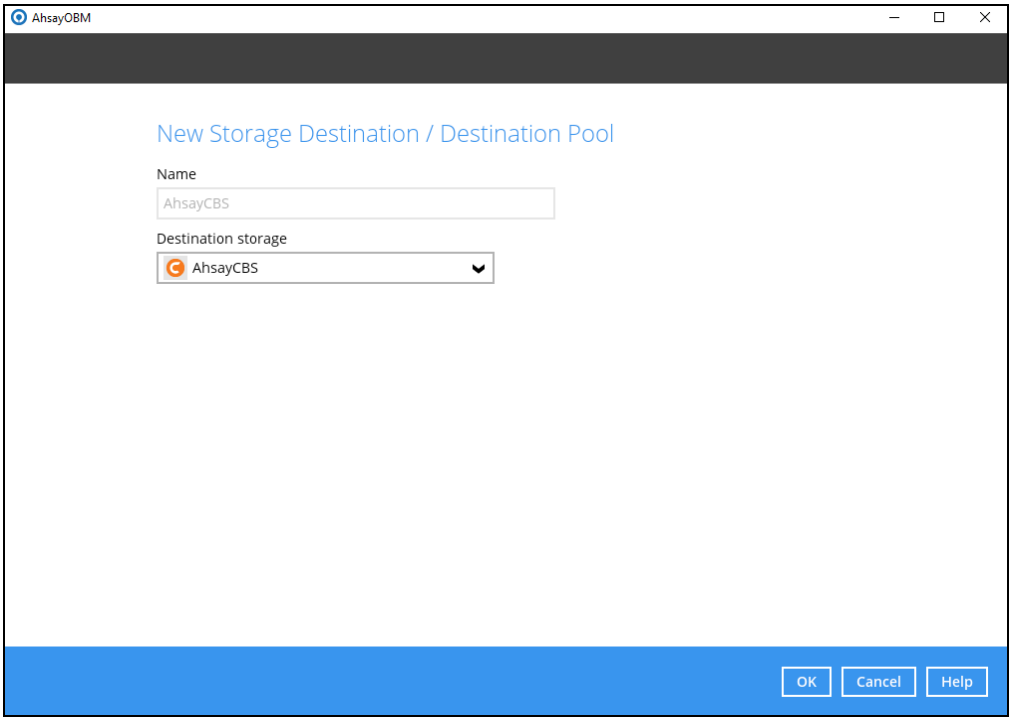
5. In the **Schedule** menu, you can configure a backup schedule for backup job to run automatically at your specified time interval. By default, the **Run scheduled backup for this backup set** option is enabled. You can modify the existing schedules, or you can create a new one by clicking the “Add” button**.**



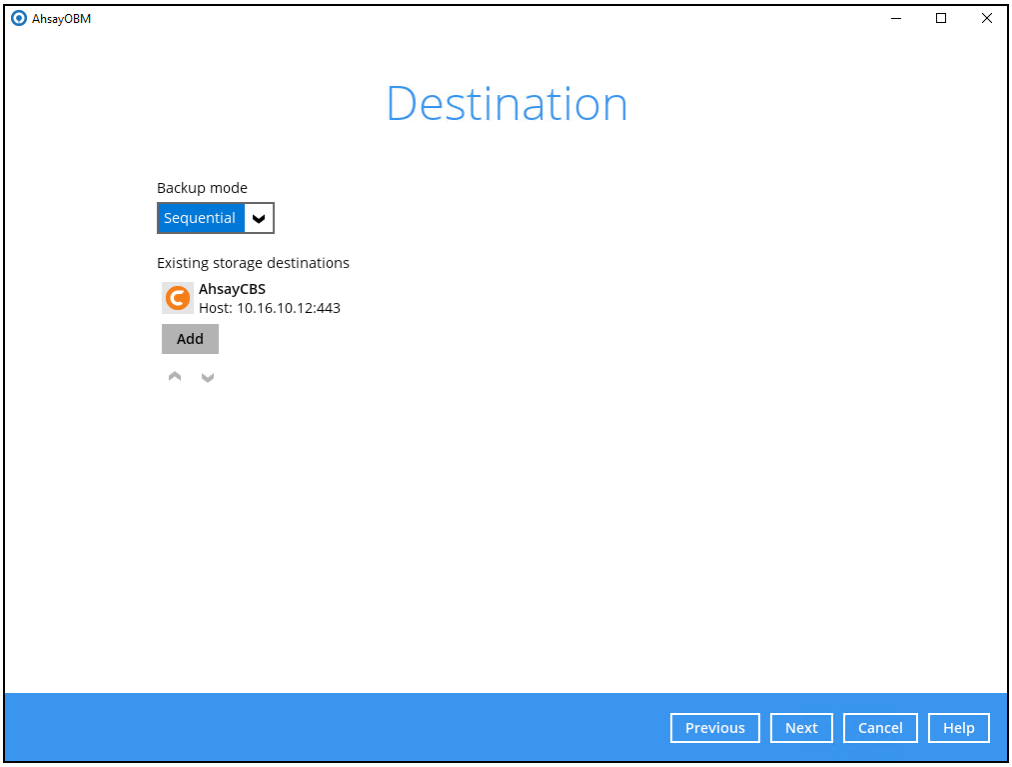
6. In the **Destination** menu, select a backup destination where the backup data will be stored. Click the "**+**" icon next to **Add new storage destination / destination pool**.



7. Select the destination storage, then click **OK** to proceed.



8. When you are done with settings, click **Next** on the **Destination** menu page to proceed.

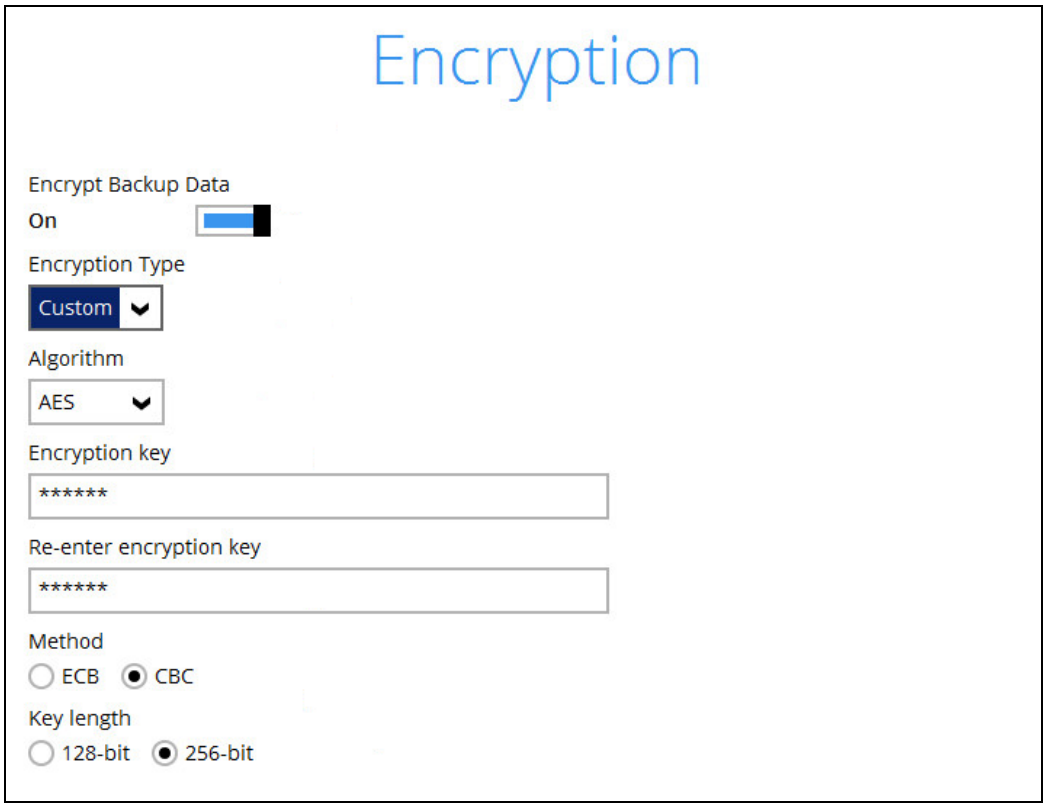


9. In the Encryption window, the default **Encrypt Backup Data** option is enabled with an encryption key preset by the system which provides the most secure protection.

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

- **Default** – an encryption key with 44 alpha numeric characters will be randomly generated by the system
- **User password** – the encryption key will be the same as the login password of your AhsayOBM at the time when this backup set is created. Please be reminded that if you change the AhsayOBM login password later, the encryption keys of the backup sets previously created with this encryption type will remain unchanged.

- **Custom** – you can customize your encryption key, where you can set your own algorithm, encryption key, method and key length.

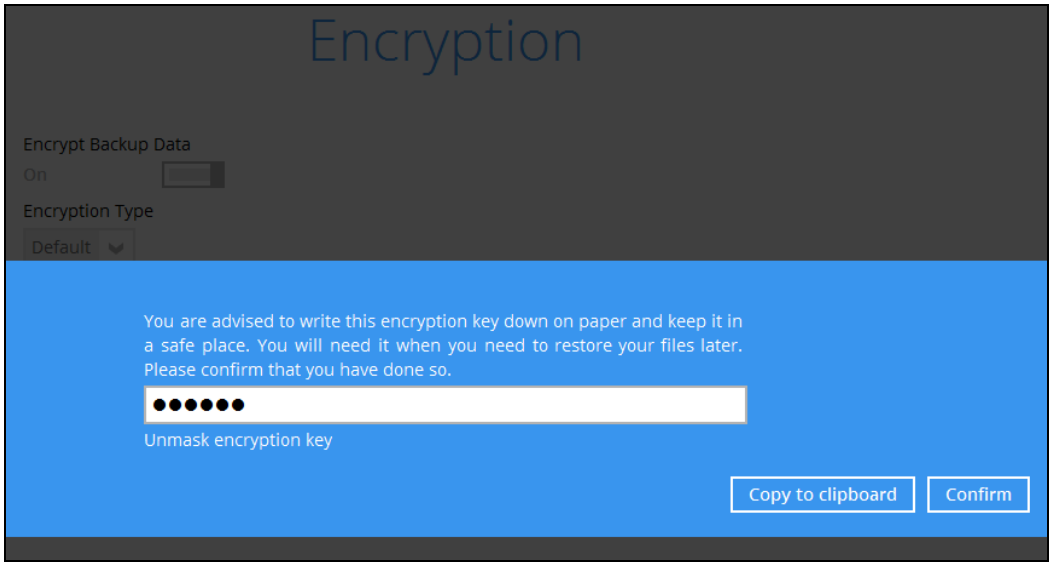


NOTE

For best practice on managing your encryption key, refer to the following article. https://wiki.ahsay.com/doku.php?id=public:8015_faq:best_practices_for_managing_encryption_key&s%5b%5d.

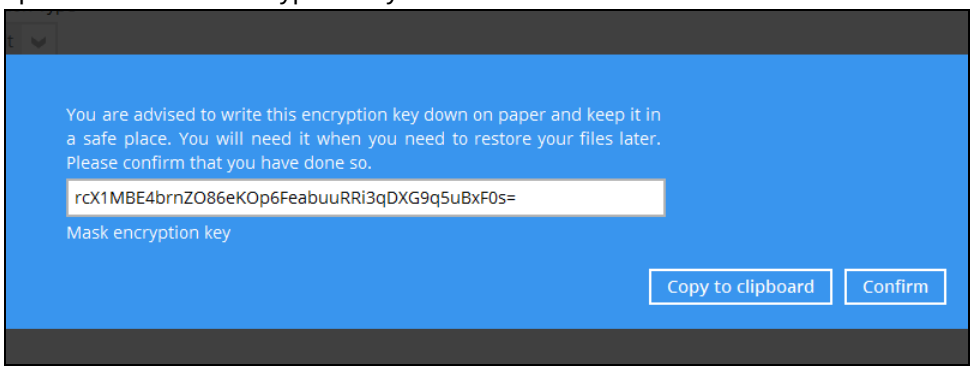
Click **Next** when you are done setting.

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



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

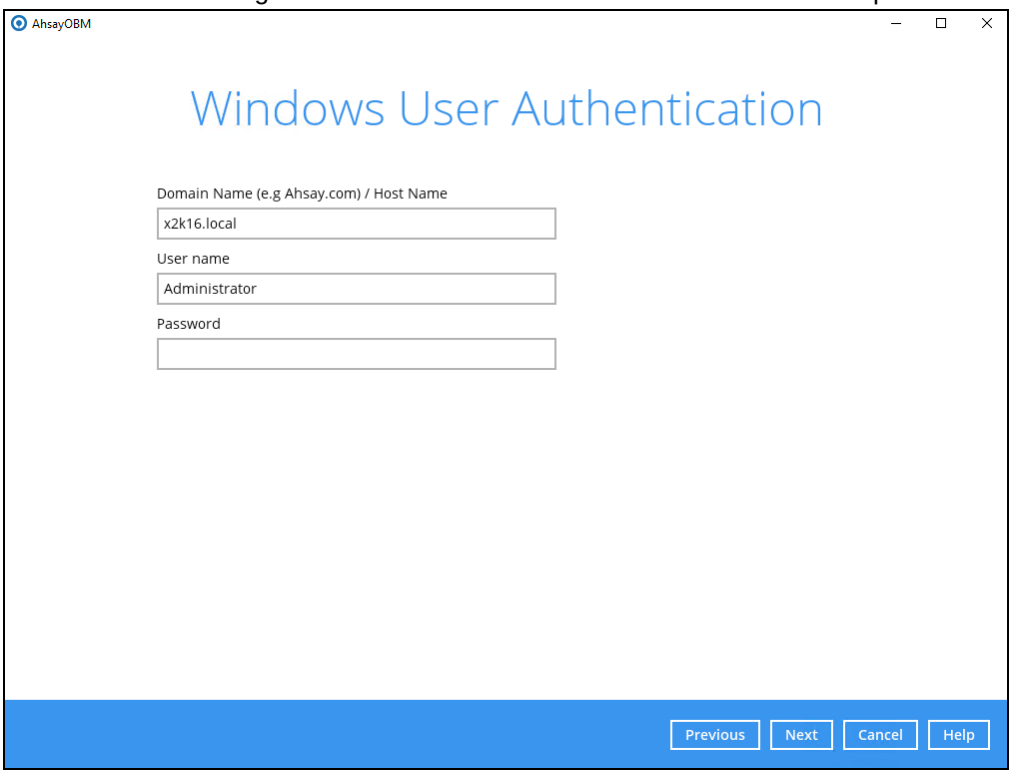
- **Unmask encryption key** – The encryption key is masked by default. Click this option to show the encryption key.



- **Copy to clipboard** – Click to copy the encryption key, then you can paste it in another location of your choice.

- **Confirm** – Click to exit this pop-up window and proceed to the next step

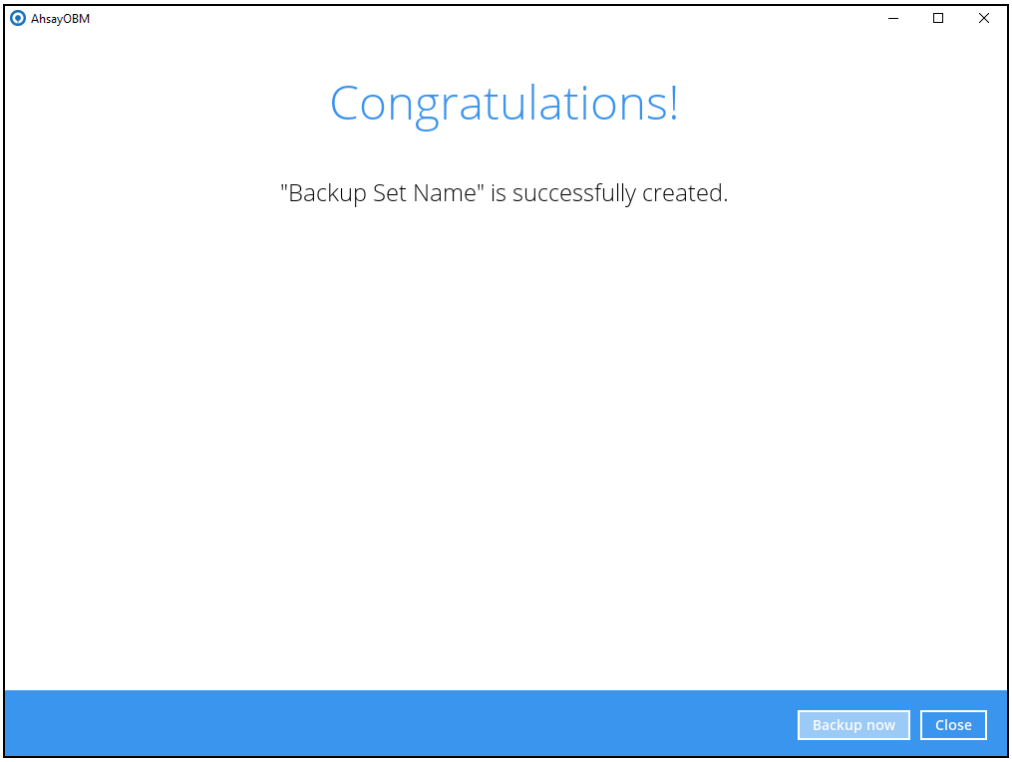
11. Enter the Windows login credentials for user authentication. Click **Next** to proceed.



NOTE

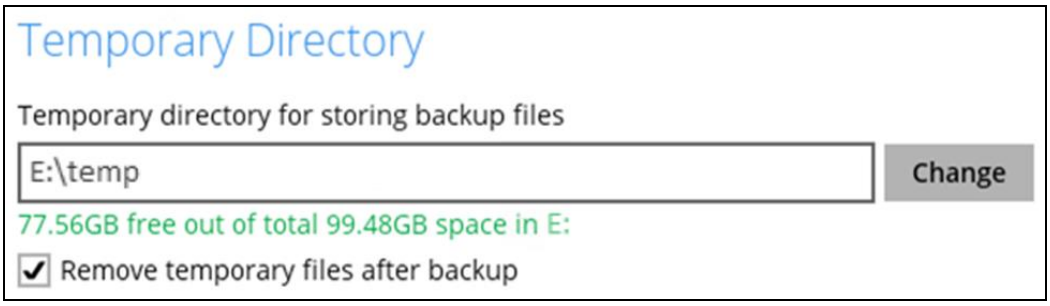
The Windows User Authentication interface will show only if scheduled backup is enabled and set successfully.

12. The following screen shows when the new backup set is created successfully.



13. You can click **Backup now** to start a backup immediately, or you can run a backup job later by following the instructions in Running Backup Job for Microsoft Exchange Server 2007/2010/2013/2016/2019.

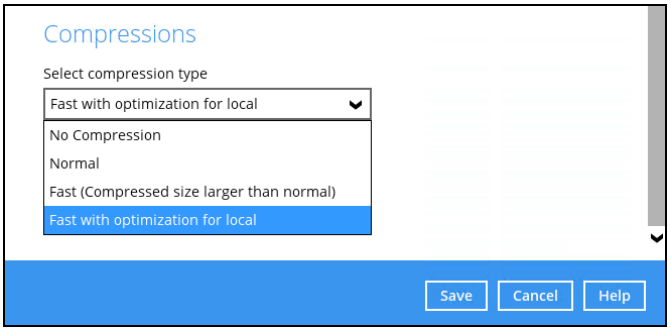
14. Based on Best Practices and Recommendations, it is highly recommended to set the **temporary directory** to another location other Drive C: (e.g. Drive E:). To do this, go to **Backup Sets > Others > Temporary Directory** and click the **Change** button to browse for another location.



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

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

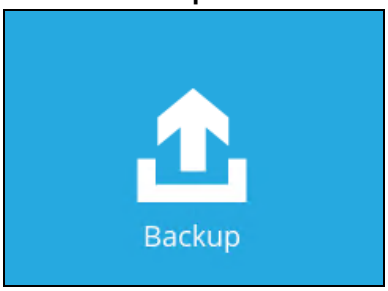
    - No Compression
    - Normal
    - Fast (Compressed size larger than normal)
    - Fast with optimization for local



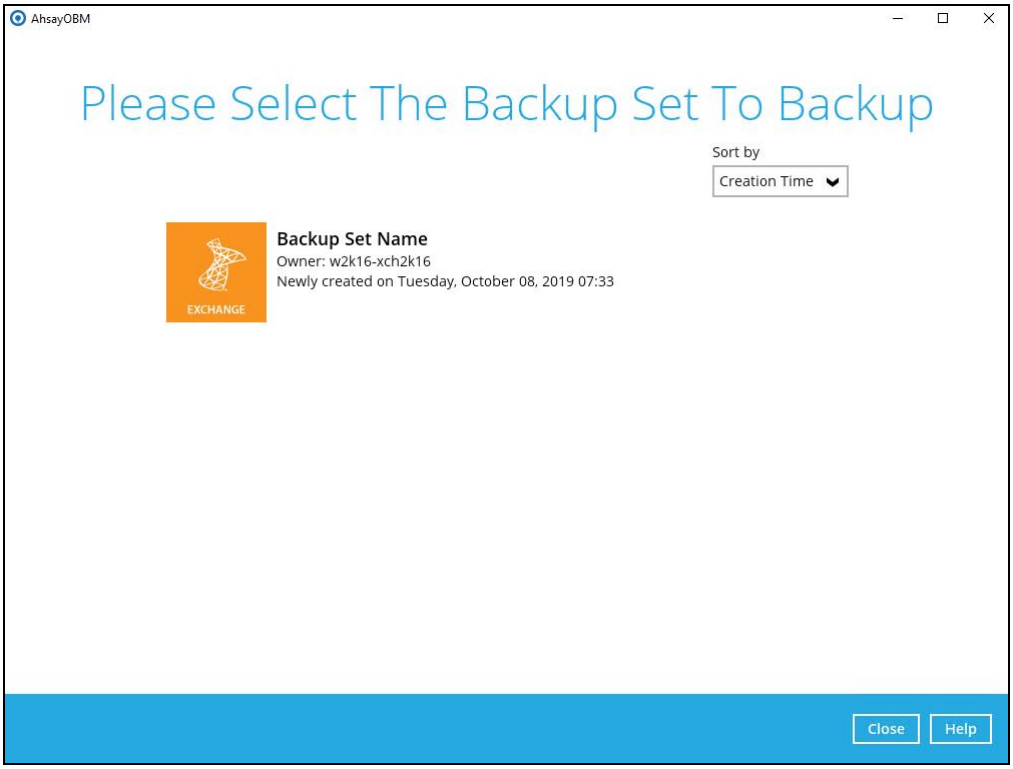
5.2 Running Backup Job for Microsoft Exchange Server 2007/2010/2013/2016/2019

1. Log in to AhsayOBM according to the instructions in Logging in to AhsayOBM.

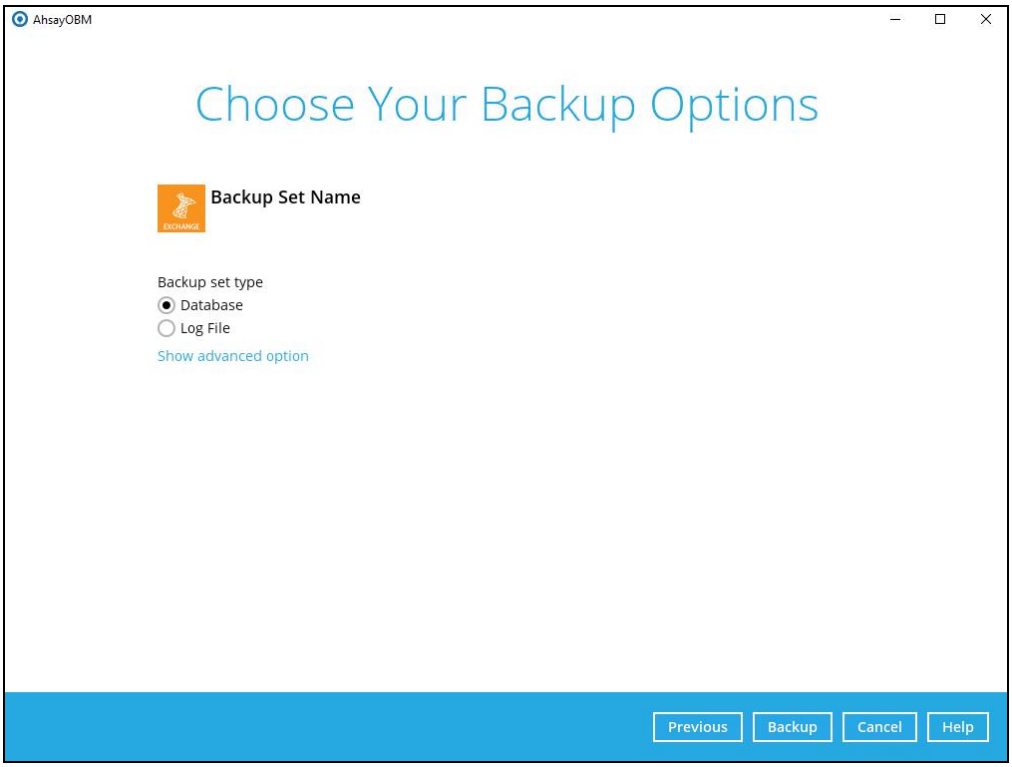
2. Click the **Backup** icon on the main interface of AhsayOBM.

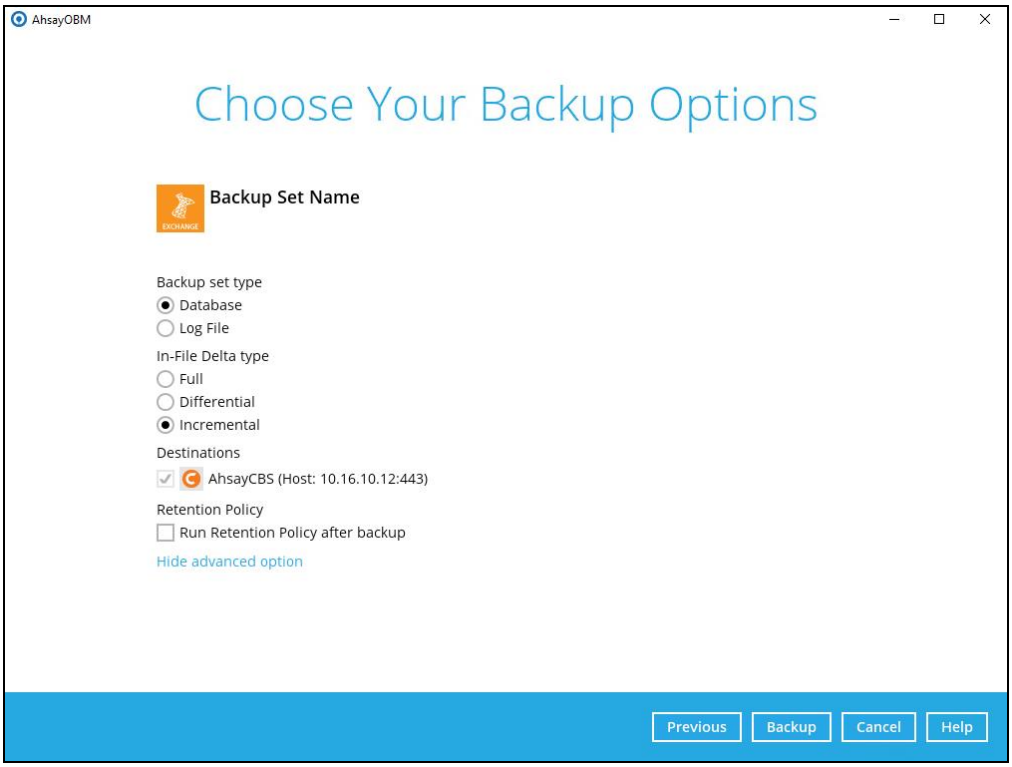


3. Select the backup set which you would like to start a backup for.



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





Refer to Appendix A Exchange Server Backup Type for more information regarding the backup set type.

5. Click **Backup** to start the backup job.

6 Restoring Microsoft Exchange Server 2007/2010/2013/2016/2019

6.1 Pre-restoration Requirements

Before you get started with restoring your database using the AhsayOBM, there are a couple of steps you may need to perform first.

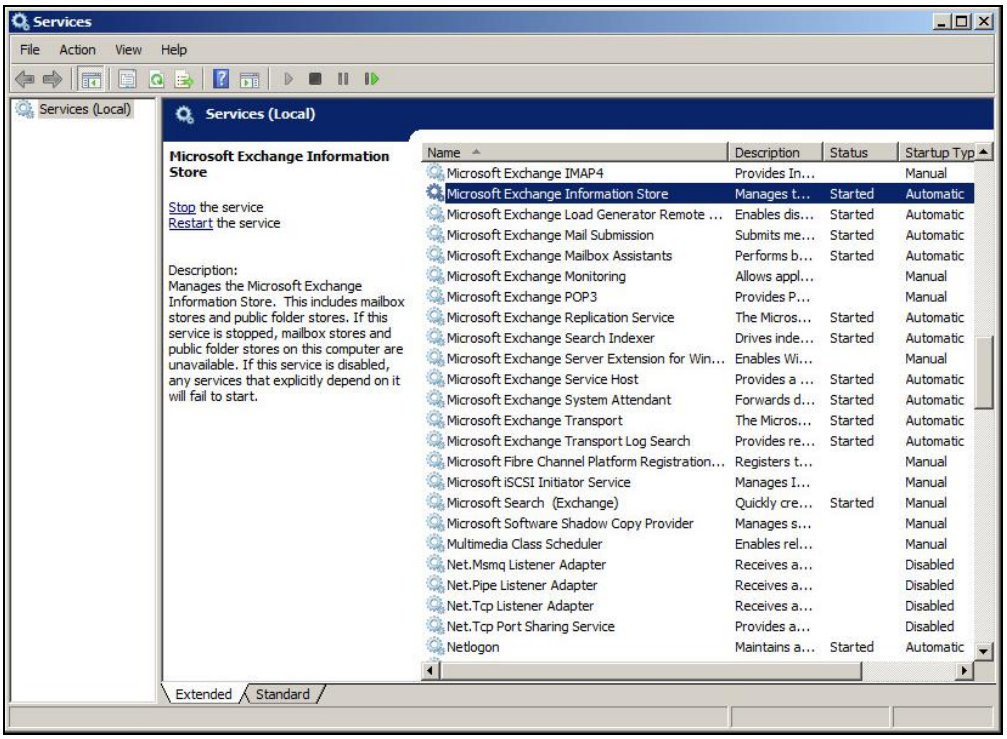
1. Prepare the operating system for the Exchange Server restore (if required). Install the original version of Windows and Exchange Server (with the same level of service pack installed as in the original system).

2. Restore Windows Active Directory (if required). Restore the System State data from the backup server, and then restore the System State using WBAdmin.exe.

3. Install AhsayOBM (if required). Refer to the Ahsay Online Backup Manager v8 Quick Start Guide for Windows via the URL below.
   https://www.ahsay.com/download/download_document_v8_obm-quickstart-windows.jsp

4. Make sure the **Microsoft Exchange Information Store** services from Windows Services is started.

   Launch **Services** in Windows by clicking **Start** then typing “Services” in the search box. After launching the Services window, look for **Microsoft Exchange Information Store** and check the Status column to confirm if it is started. If it is not, right-click the item then select **Start**.

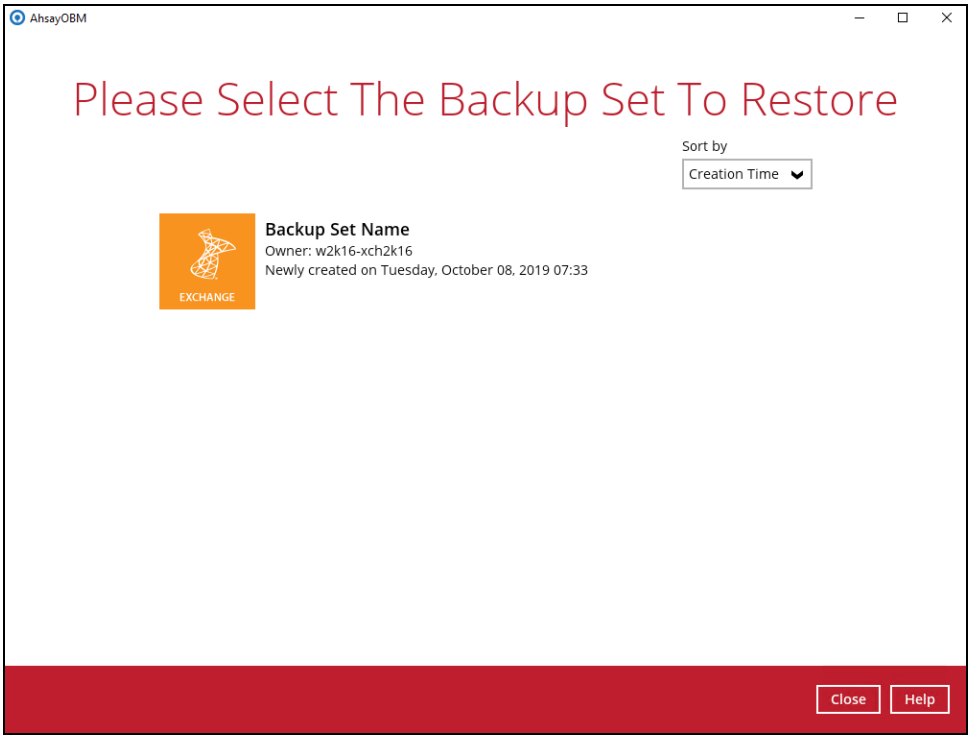


6.2 Restoring Exchange Database for Microsoft Exchange Server 2007/2010/2013/2016/2019

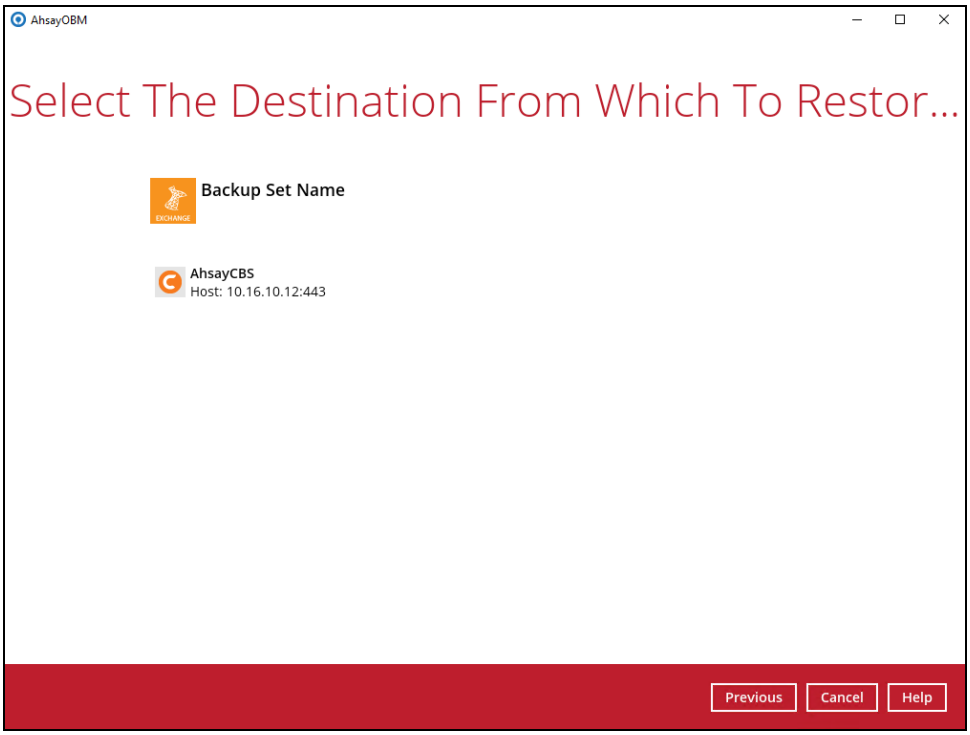
1. Make sure you have followed the steps in Section 3.1 before proceeding to this section.

2. In the AhsayOBM main interface, click the **Restore** icon.

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

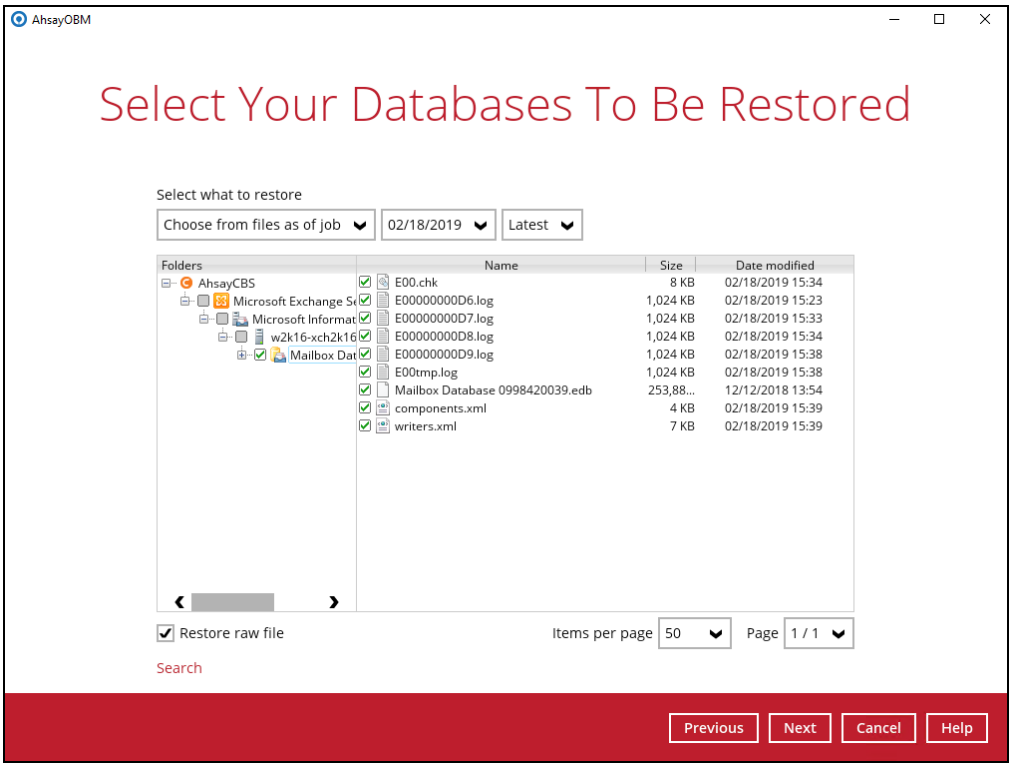


4. Select the backup destination that contains the database you would like to restore.



5. Click to expand the menu tree to select which Information Store to restore. You can also select individual database file to restore by clicking the **Restore raw file** checkbox at the bottom left corner.

   In addition, you can also choose to restore backup item(s) from a specific backup job using the drop-down menu at the top. Click **Next** to proceed when you are done with the selection.

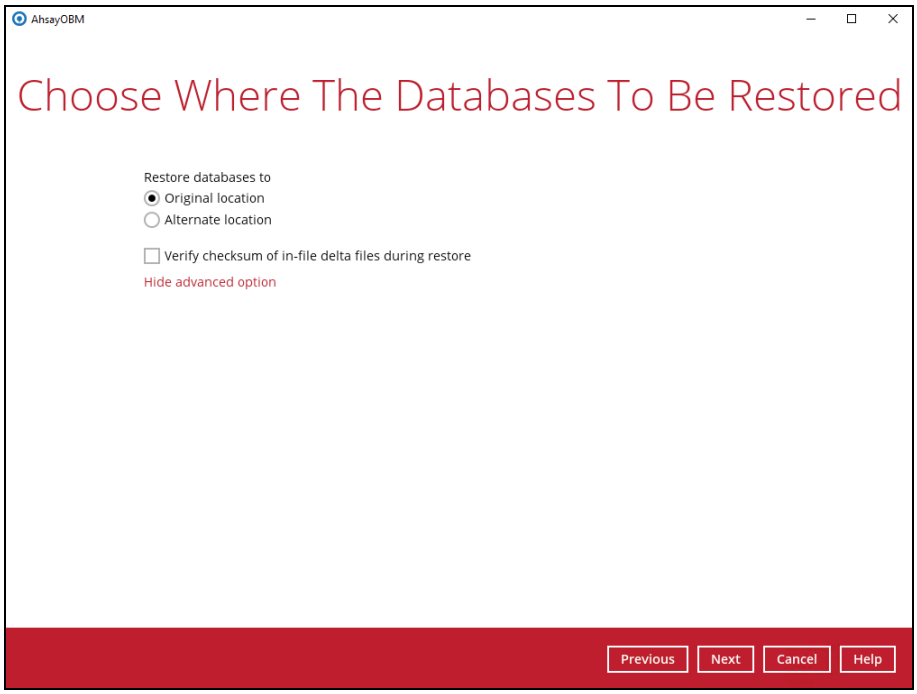


6. Select to restore the database to its Original location, or to an Alternate location.

Restore to Original location

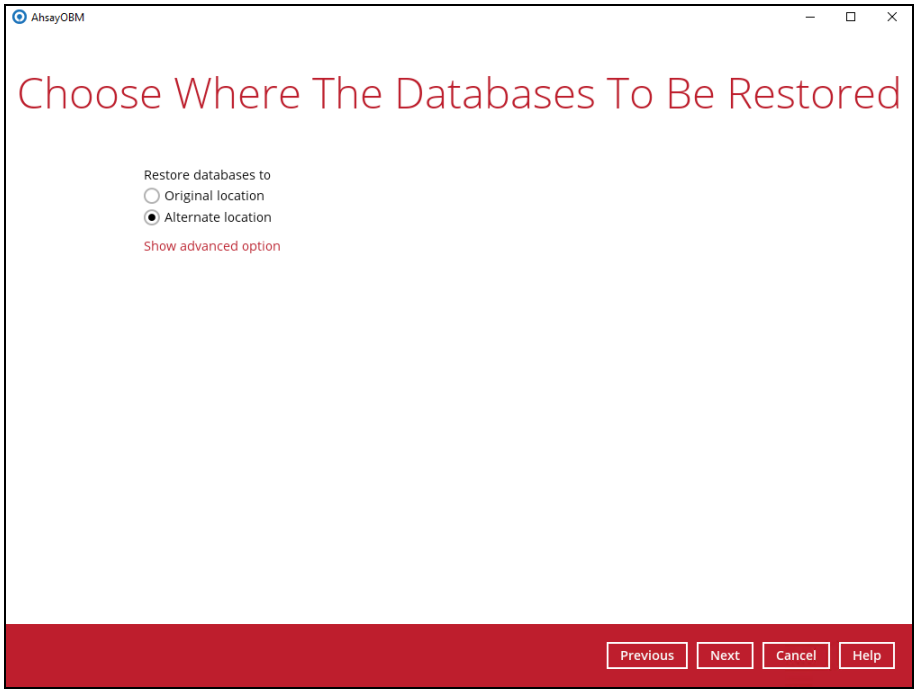
Select the **Original location** option, then press **Next** to proceed.

If you would like to modify the Verify checksum settings, click **Show advanced option**.

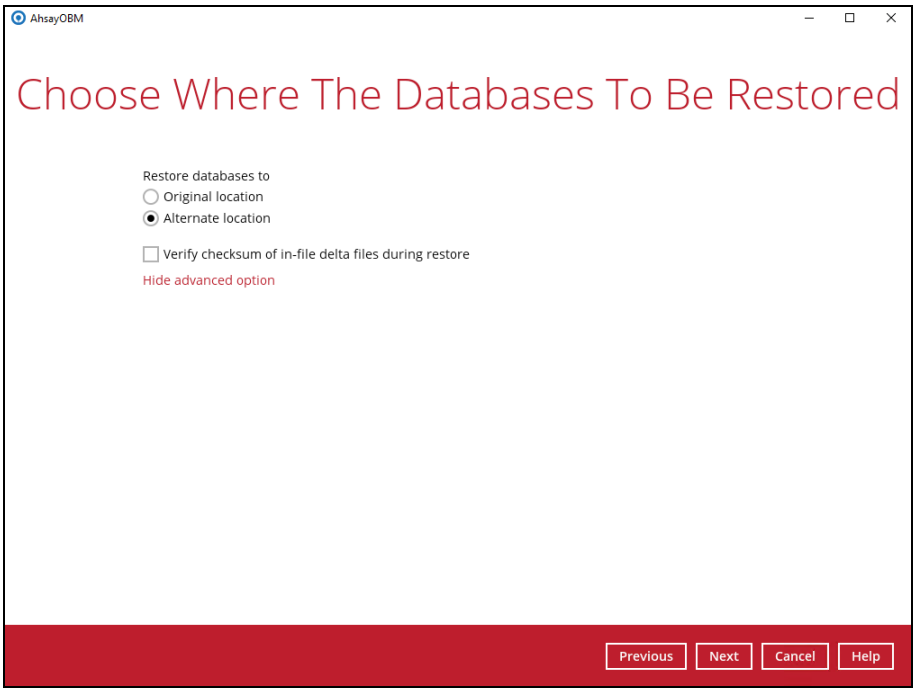


Restore to Alternate location

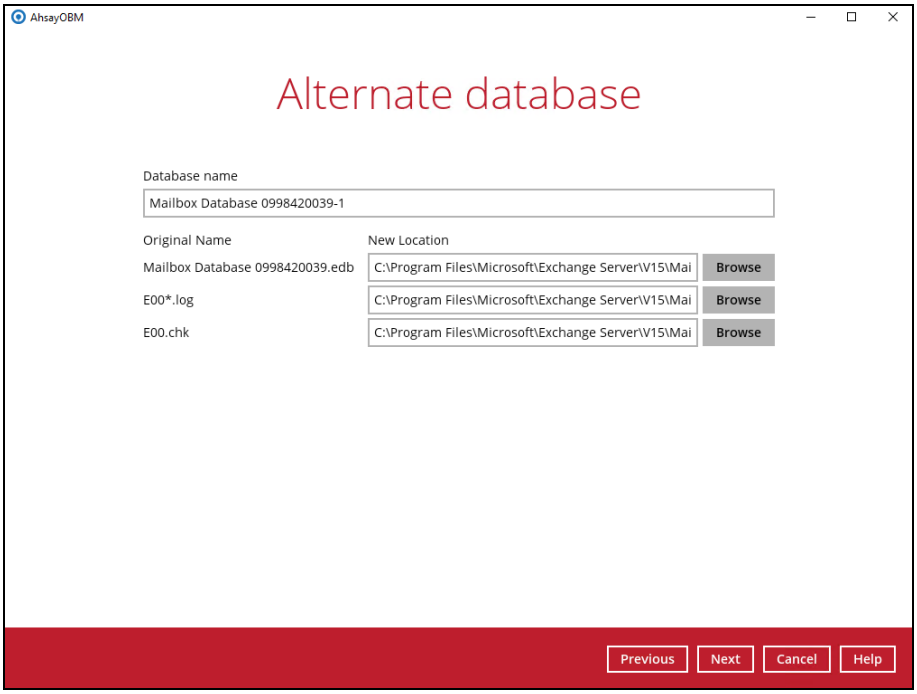
a) Select the **Alternate location** option, then press **Next** to proceed.



b) If you would like to modify the Verify checksum settings, click **Show advanced option**.

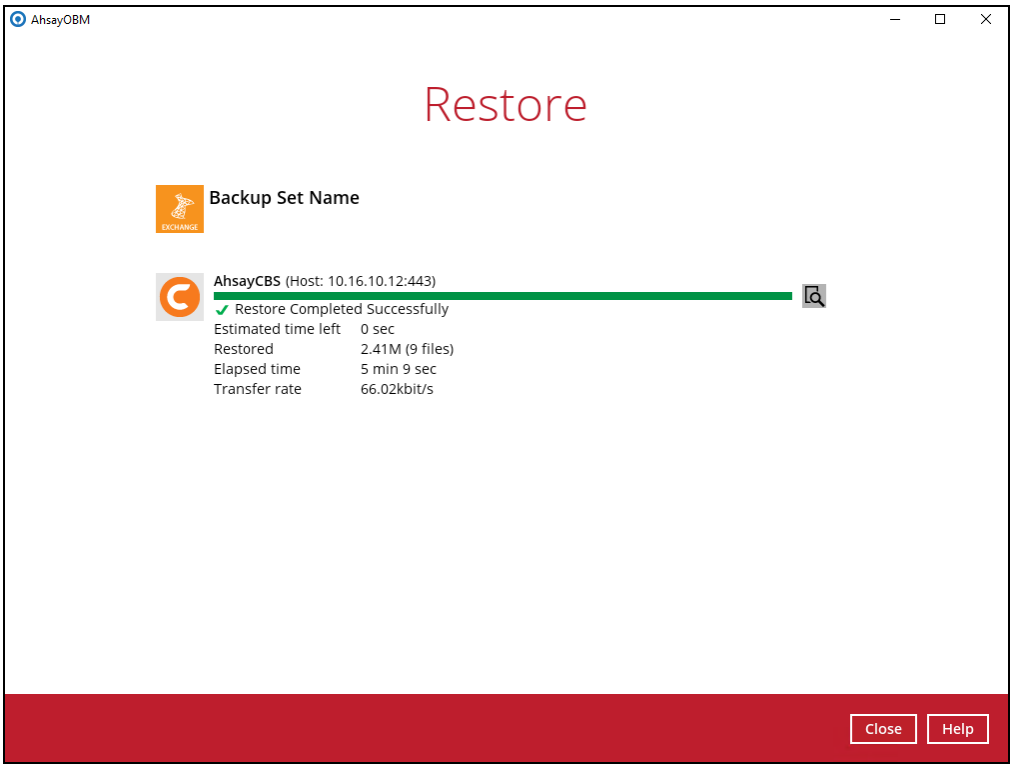


c) Select the locations where you would like to restore the database to. Name the new mailbox store, then click **Browse** to modify the database, log and checksum file location if necessary. Click **Next** to proceed when you are done with the settings.



7. Select the temporary directory for storing temporary files, such as delta files when they are being merged, click **Restore** to start the restoration.

8. The following screen with the text **Restore Completed Successfully** shows when the restoration is completed.



For details regarding verifying the restoration activities log between AhsayOBM and the Exchange Server, refer to Appendix B Restore Activities Log.

7 Backing up Microsoft Exchange Server in Database Availability Group (DAG)

7.1 License Requirement to Back up all Exchange Server 2013/2016/2019 in DAG environment

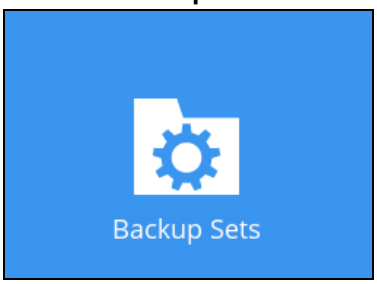
One AhsayOBM license CAL with one Exchange Server Add-on Module is deducted from each installation of the AhsayOBM on the DAG environment. Please check with your backup service provider if more AhsayOBM with Exchange backup is required.

7.2 Creating Backup Set for Microsoft Exchange Server 2013/2016/2019 (DAG)

NOTE

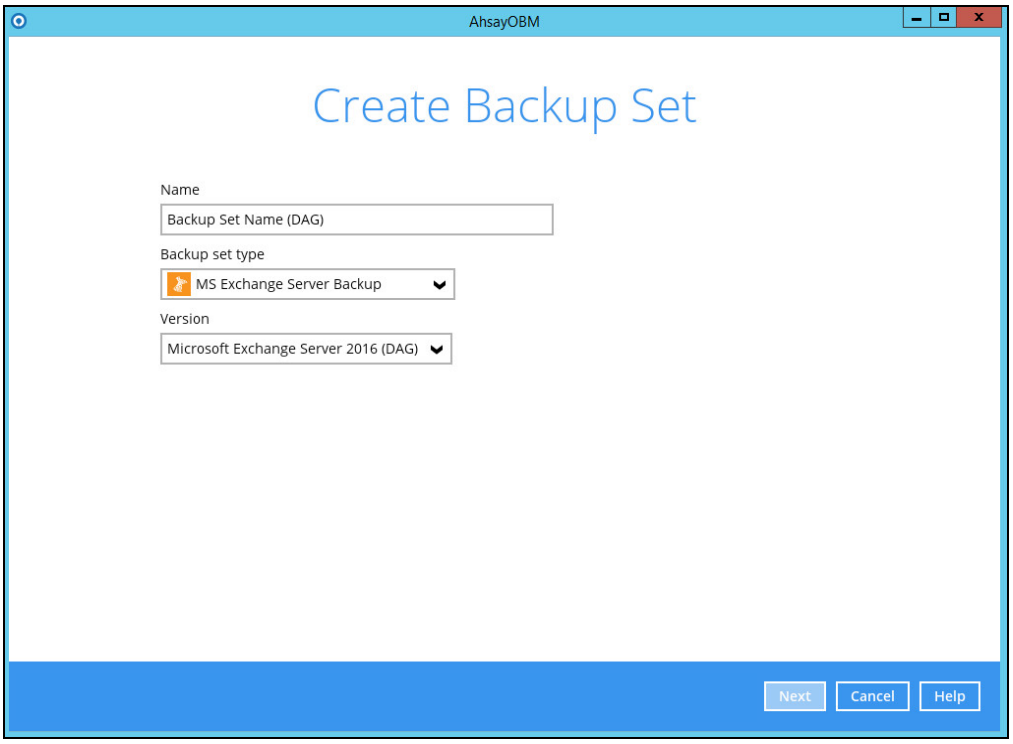
From AhsayOBM v8.5.4.x or later, creation of backup set for Microsoft Exchange Server 2010 in Database Availability Group (DAG) has been desupported. However, if there are existing backup sets created prior to upgrading to AhsayOBM v8.5.4.x or later, the existing Microsoft Exchange Server 2010 DAG backup set will still be available.

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

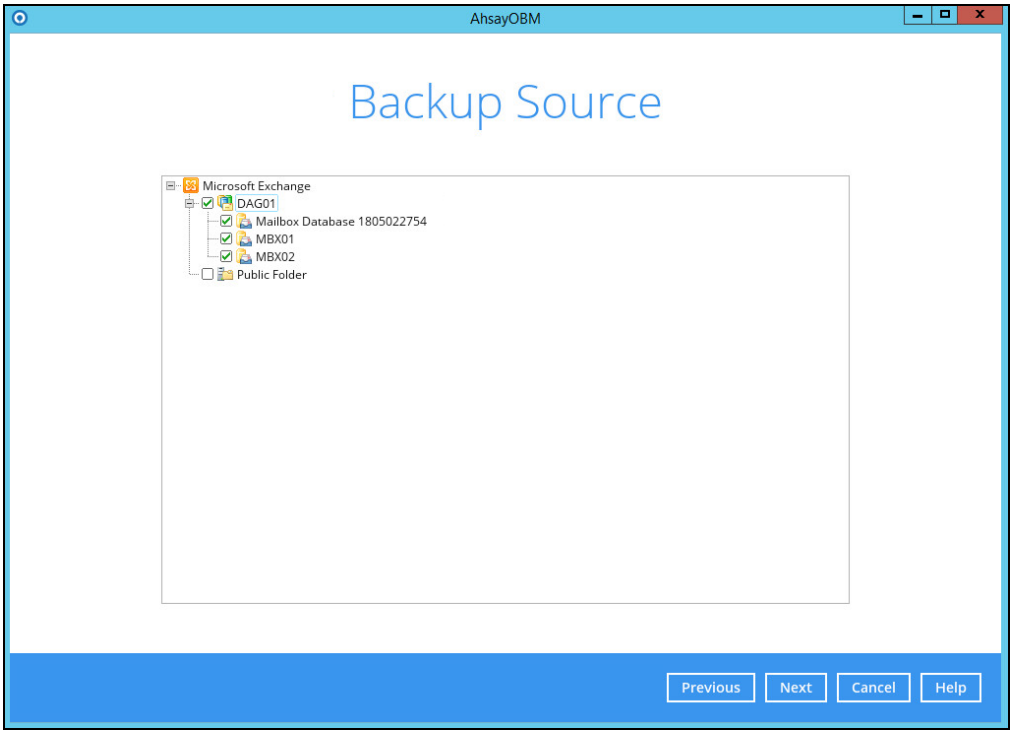


2. Create a new backup set by clicking the **Add** button.

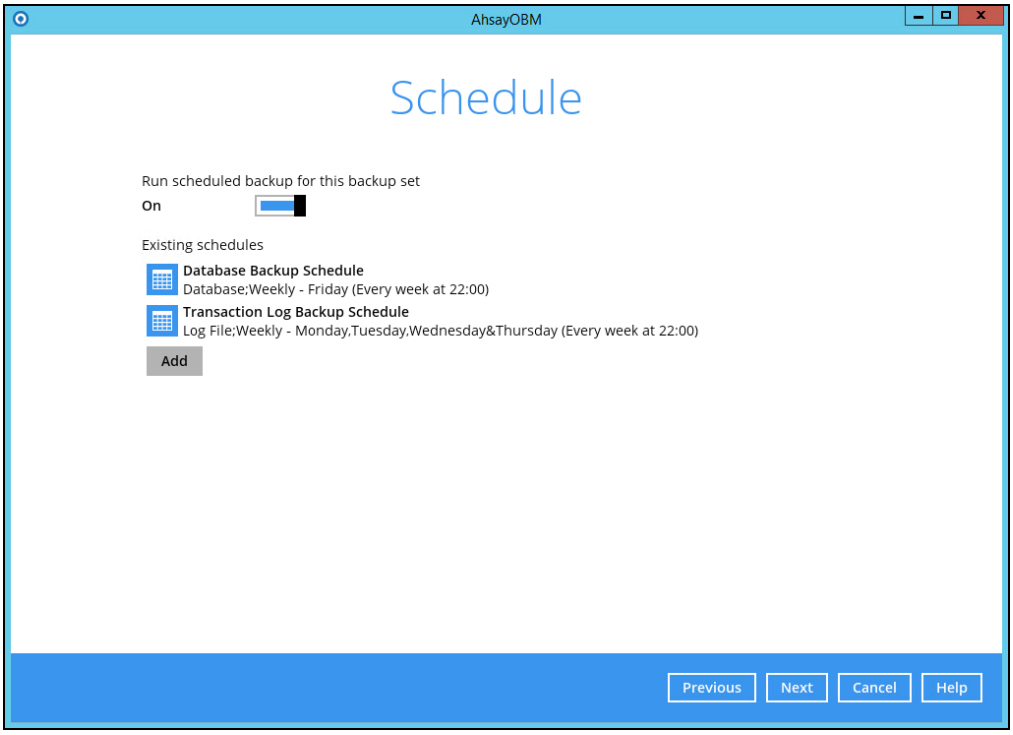
3. Select the Backup set type as **MS Exchange Server Backup**. Make sure you choose the correct Exchange Server version with “Database Availability Group (DAG)”. Name your new backup set, then click **Next** to proceed.



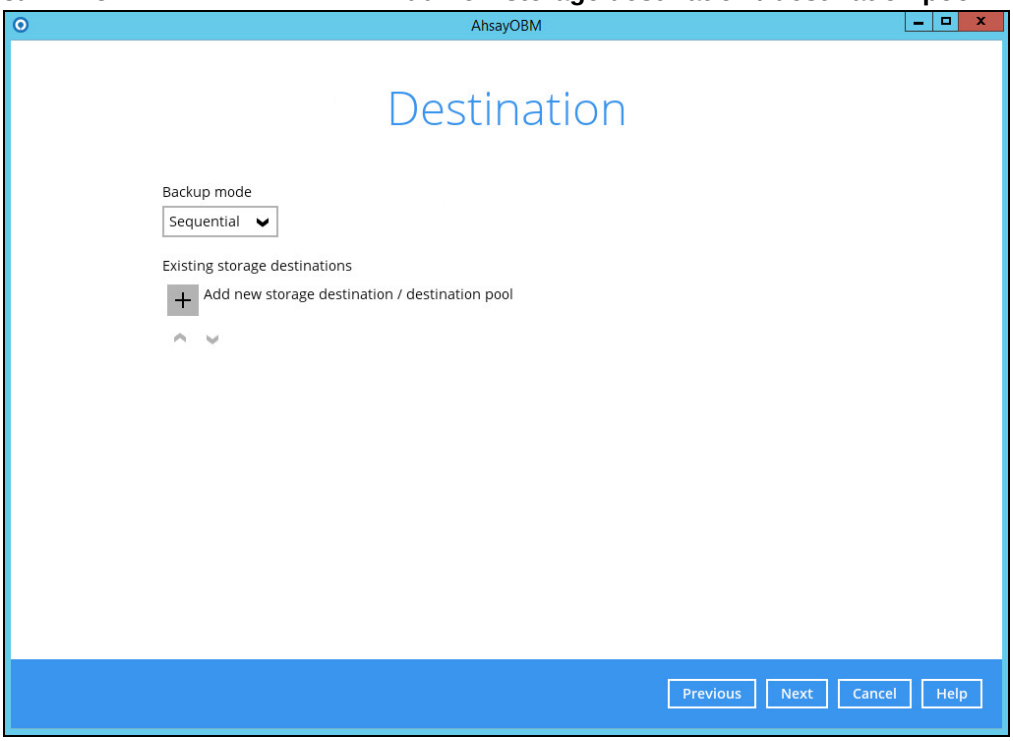
4. In the Backup Source menu, select the DAG / Public Folder for backup. Click **Next** to proceed.



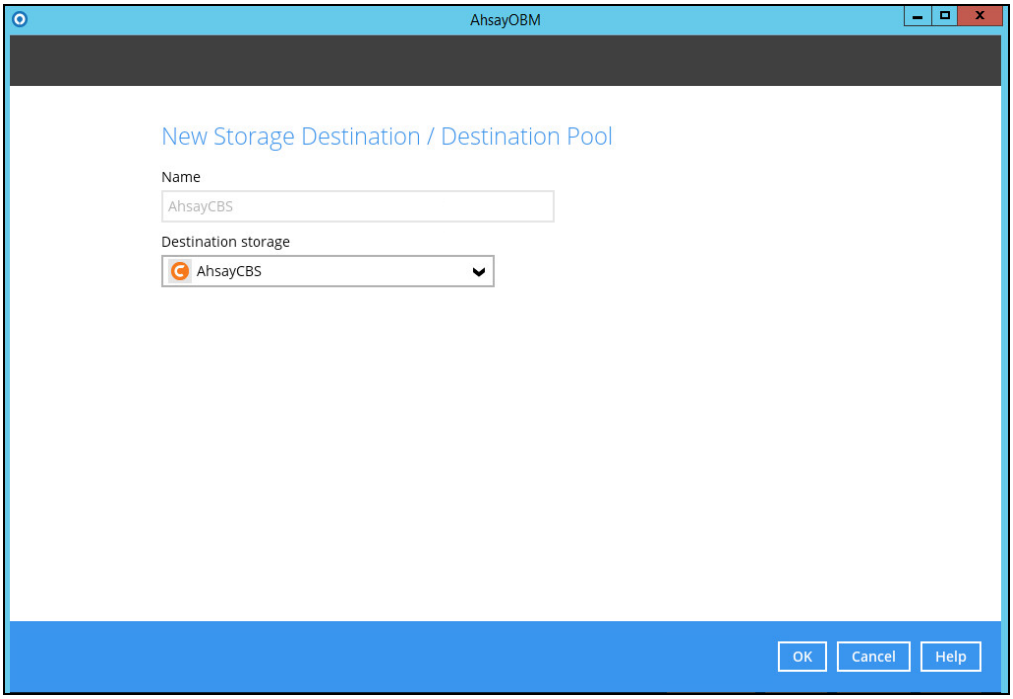
5. In the Schedule menu, you can configure a backup schedule for backup job to run automatically at your specified time interval. By default the **Run scheduled backup for this backup set** option is enabled. You can modify the existing schedules, or you can create a new one by clicking the “Add” button. Click **Next** to proceed when you are done with the settings.



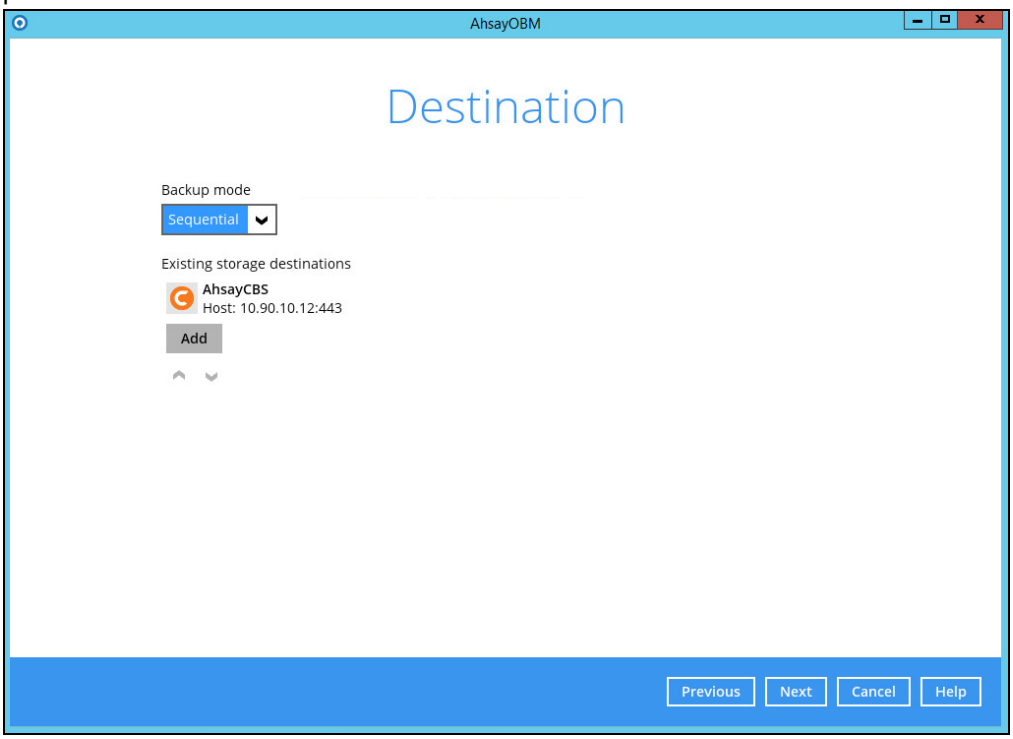
6. In the Destination menu, select a backup destination where the backup data will be stored. Click the "**+**" icon next to **Add new storage destination / destination pool**.



7. Select the destination storage, then click **OK** to proceed.



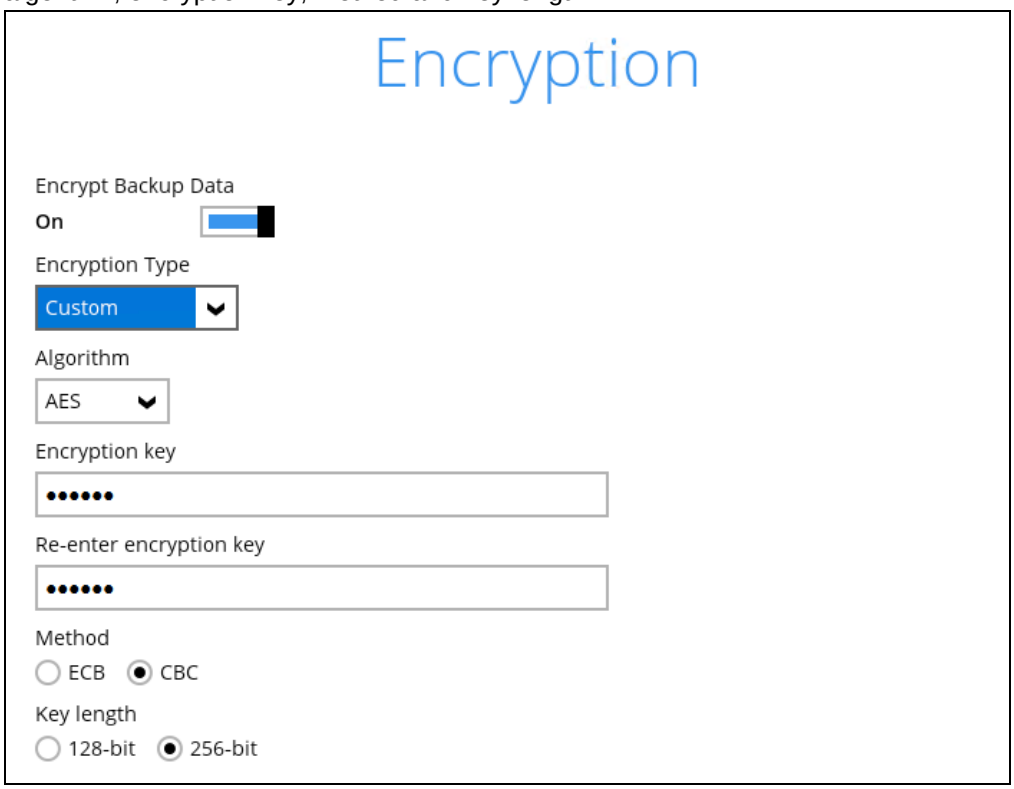
8. When you are done with the settings, click **Next** on the Destination menu page to proceed.



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

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

- **Default** – an encryption key with 44 alpha numeric characters will be randomly generated by the system
- **User password** – the encryption key will be the same as the login password of your AhsayOBM at the time when this backup set is created. Please be reminded that if you change the AhsayOBM login password later, the encryption keys of the backup sets previously created with this encryption type will remain unchanged.
- **Custom** – you can customize your encryption key, where you can set your own algorithm, encryption key, method and key length.

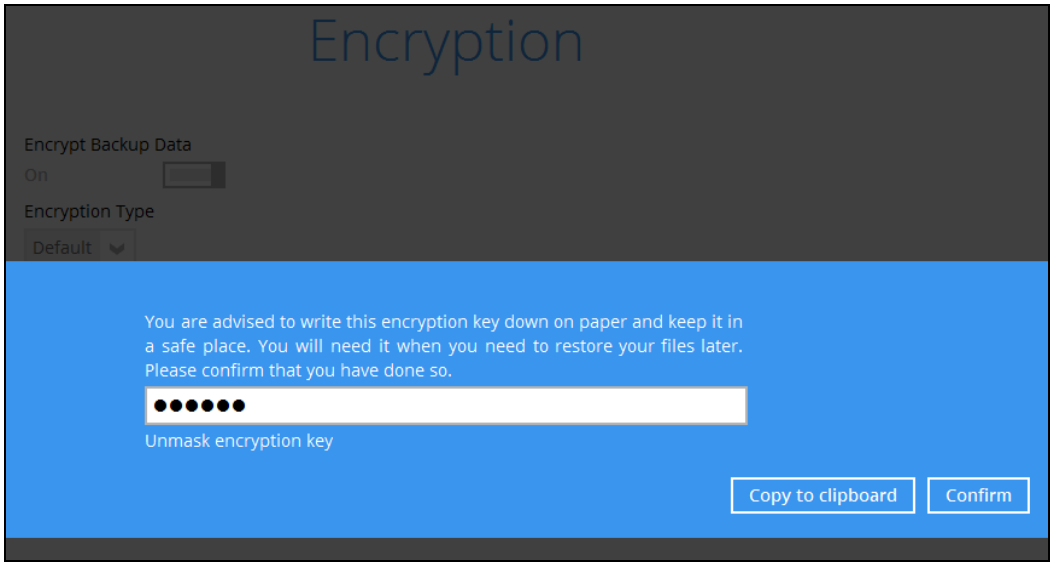


NOTE

For best practice on managing your encryption key, refer to the following article. https://wiki.ahsay.com/doku.php?id=public:8015_faq:best_practices_for_managing_encryption_key&s%5b%5d.

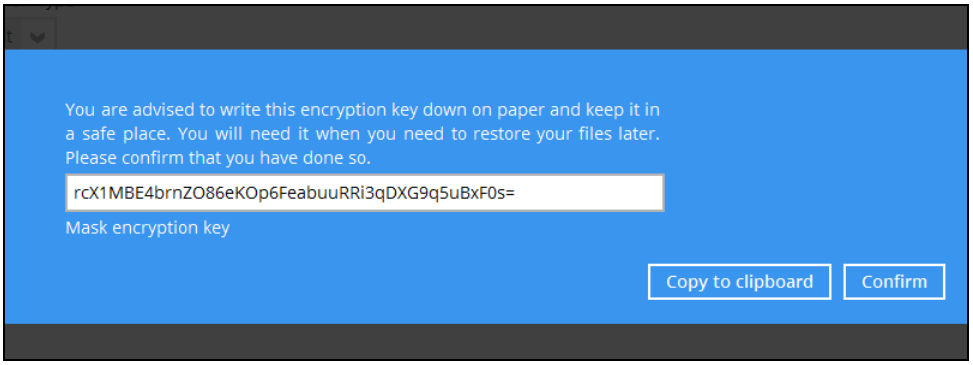
Click **Next** when you are done setting.

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



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

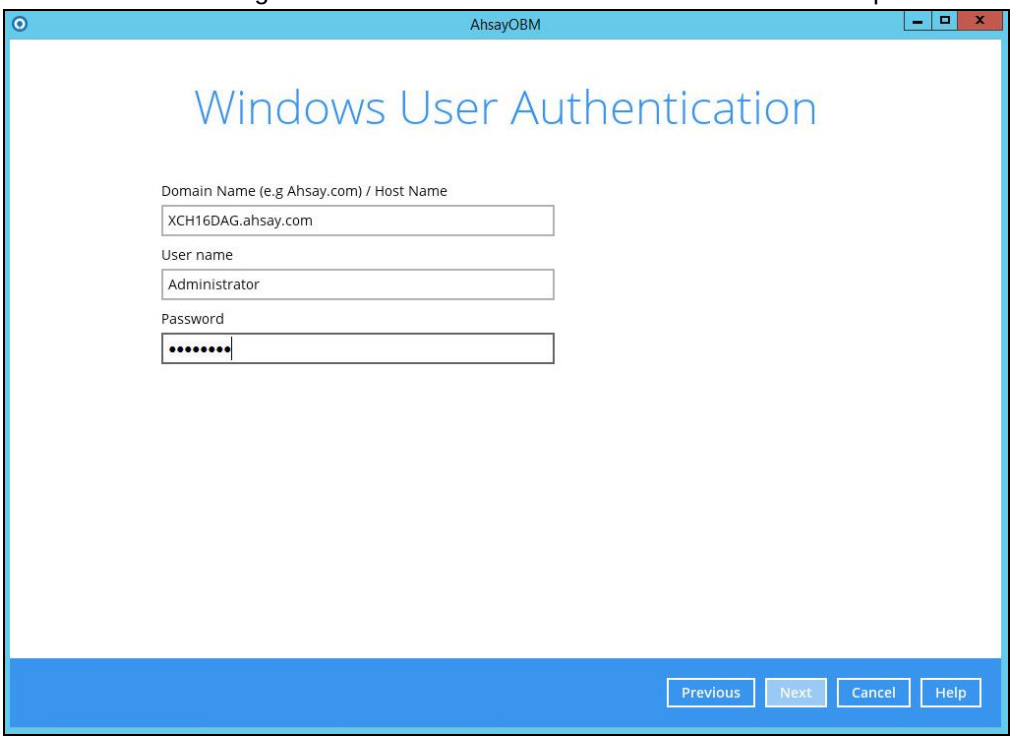
- **Unmask encryption key** – The encryption key is masked by default. Click this option to show the encryption key.



- **Copy to clipboard** – Click to copy the encryption key, then you can paste it in another location of your choice.

- **Confirm** – Click to exit this pop-up window and proceed to the next step

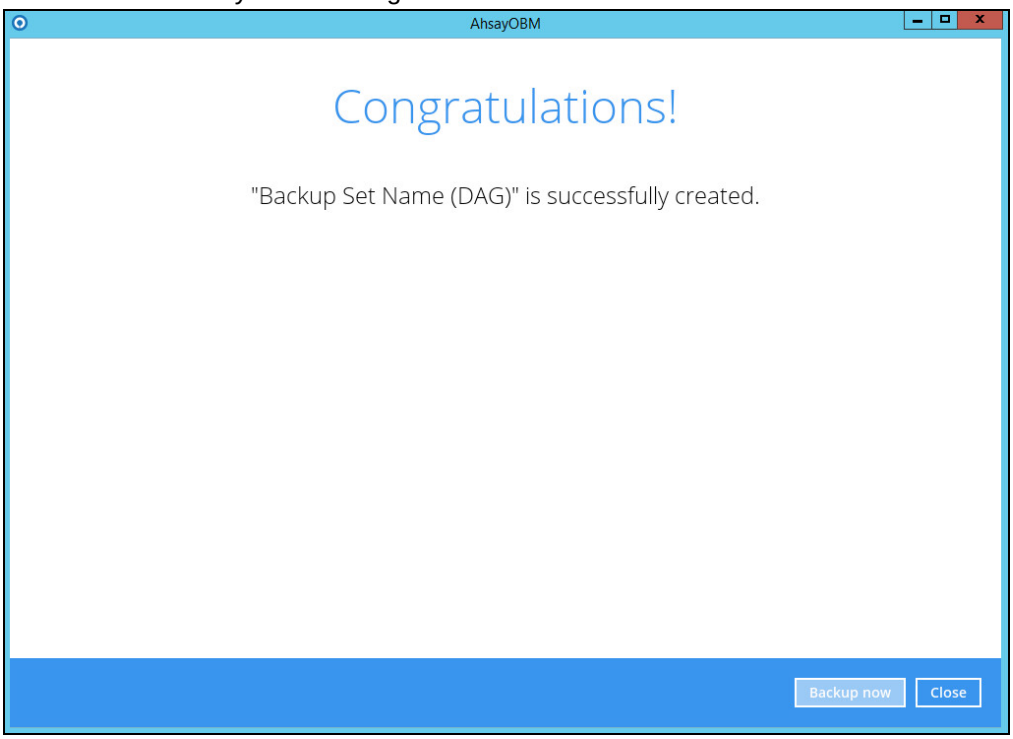
11. Enter the Windows login credentials for user authentication. Click **Next** to proceed.



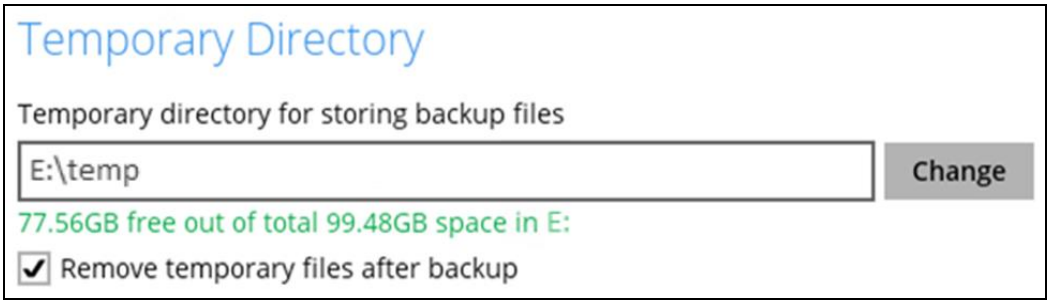
NOTE

The Windows User Authentication interface will show only if scheduled backup is enabled and set successfully.

12. The following screen shows when the new backup set is created successfully. Backup will run automatically at the configured scheduled time.



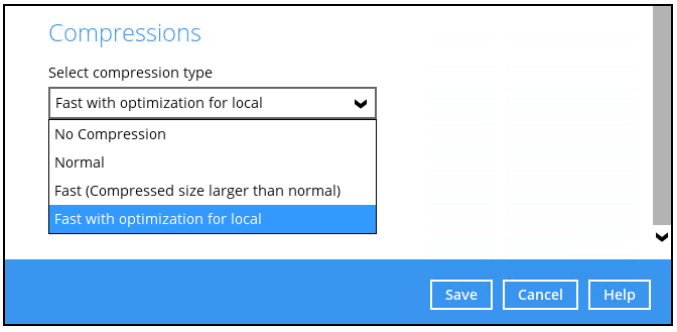
13. Based on Best Practices and Recommendations, it is highly recommended to set the **temporary directory** to another location other Drive C: (e.g. Drive E:). To do this, go to **Backup Sets > Others > Temporary Directory** and click the **Change** button to browse for another location.



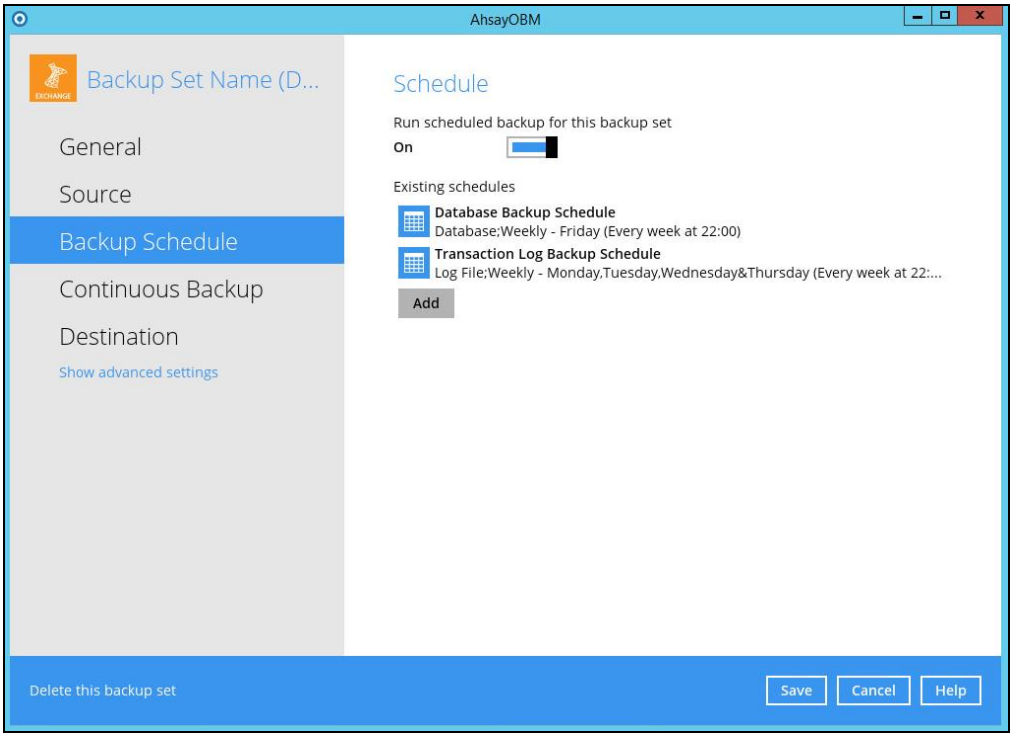
14. Optional: Select your preferred **Compression** type. By default, the compression type is Fast with optimization for local.

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

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

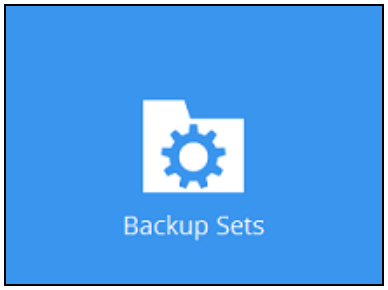


15. On all other Exchange Servers within the same DAG, logon to AhsayOBM using the same login account. Click the same backup set, and make sure the **Run scheduled backup for this backup set** is turned on the **Backup Schedule** menu page. Make sure you save the setting before exiting the application.



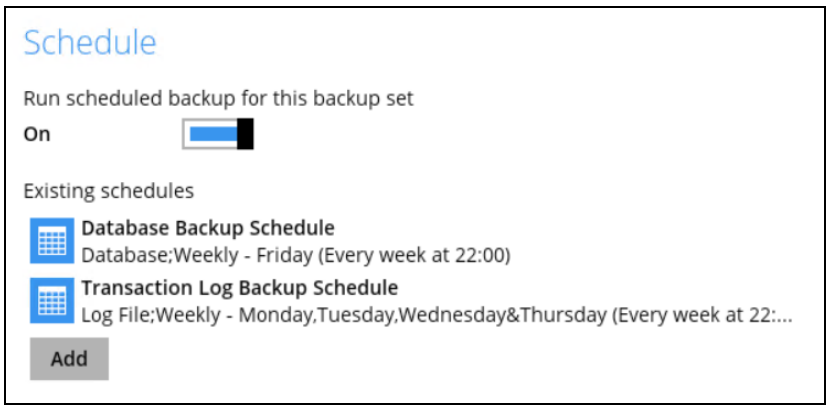
7.3 Configure Backup Schedule for Automated Backup

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

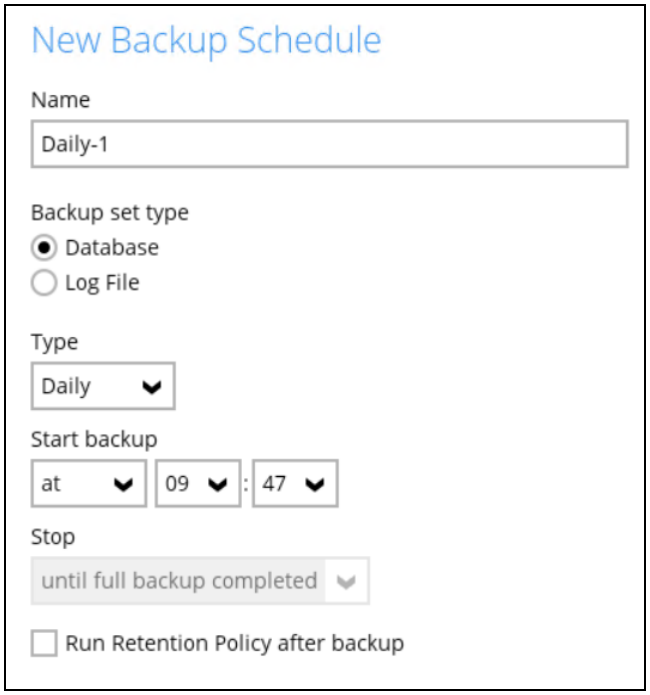


2. All backup sets will be listed. Select the backup set that you would like to create a backup schedule for.

3. Go to the **Backup Schedule** tab. If the **Run scheduled backup for this backup set** option is off, switch it **On**. Existing schedules will be listed by default. Click the **Add** button to add a new backup schedule.

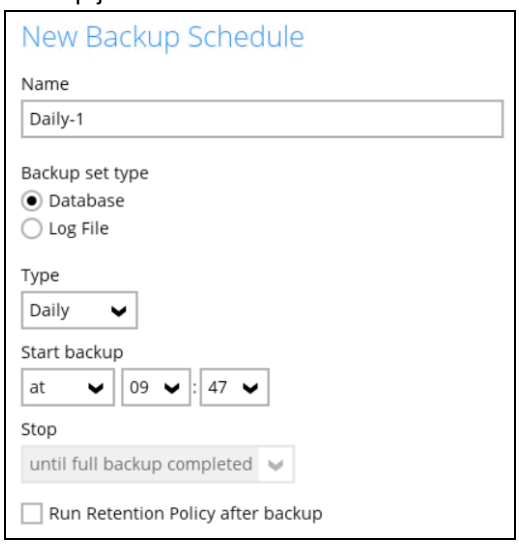


4. The New Backup Schedule window will appear.

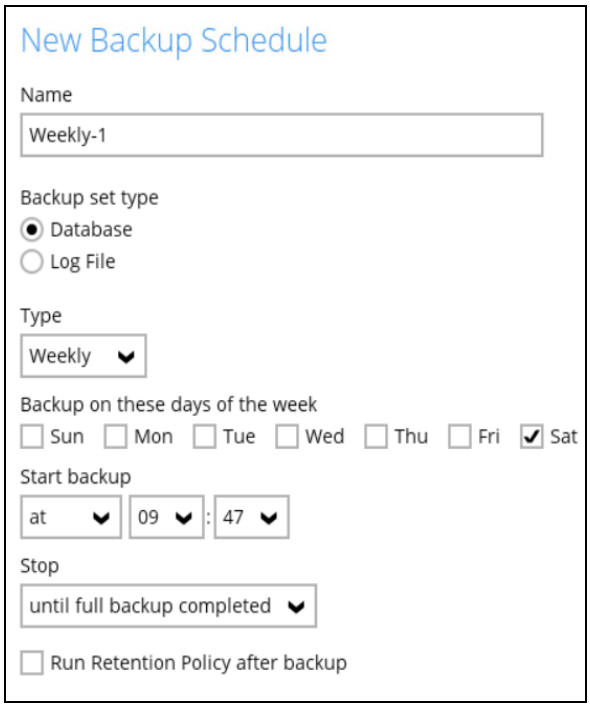


5. In the New Backup Schedule window, configure the following backup schedule settings.

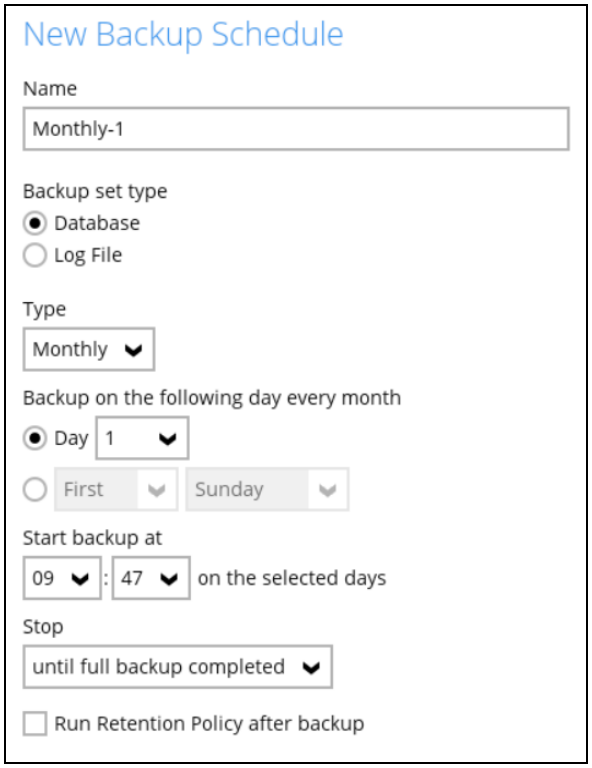
- **Name** – the name of the backup schedule.
- **Backup Set Type** – the type of backup set (i.e. Database or Log File). For more information, refer to Appendix A Exchange Server Backup Type.
- **Type** – the type of backup schedule. There are four (4) different types of backup schedule: Daily, Weekly, Monthly and Custom.
  - **Daily** – the time of the day or interval in minutes/hours which the backup job will run.



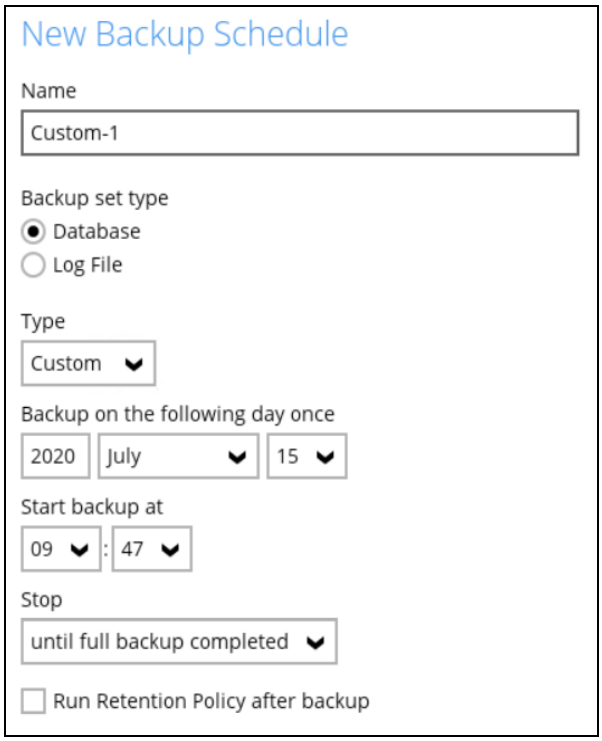
- **Weekly** – the day of the week and the time of the day or interval in minutes/hours which the backup job will run.



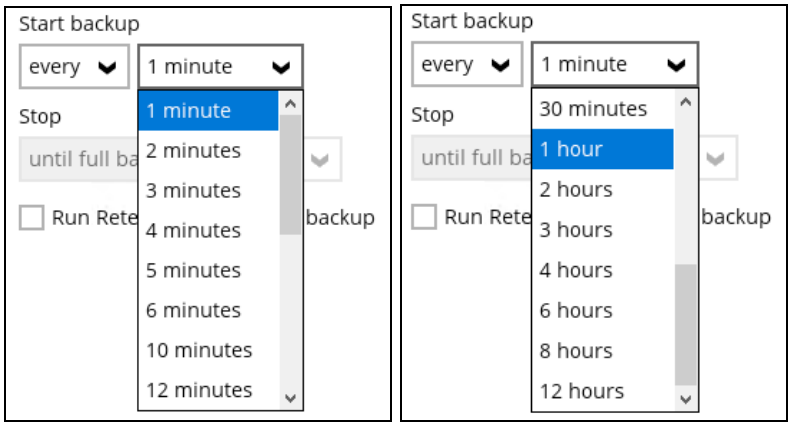
- **Monthly** – the day of the month and the time of that day which the backup job will run.



- **Custom** – a specific date and the time of that date which the backup job will run.



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



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

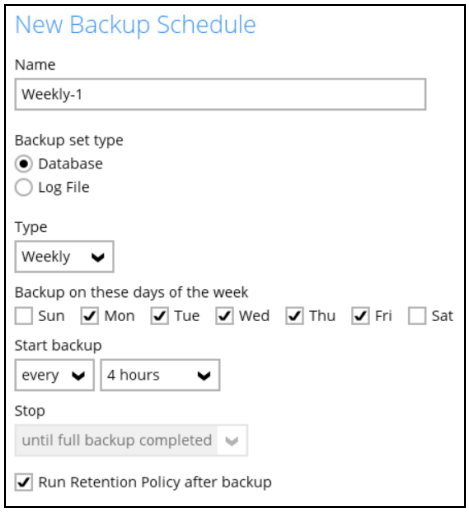


Figure 1.1

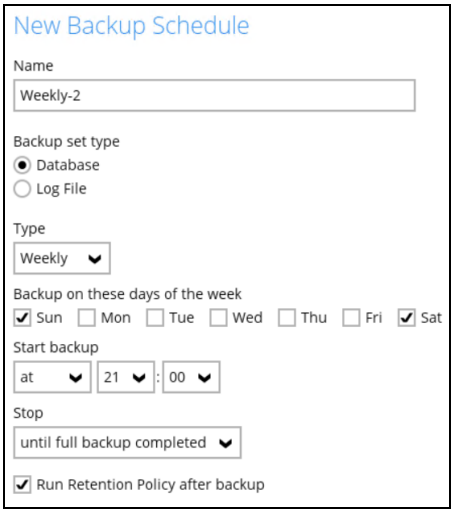


Figure 1.2

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

Figure 1.2 – Normal backup schedule runs at 21:00 or 9:00 PM on Saturday and Sunday on weekend non-business hours

- **Stop** – the stop time of the backup job. This only applies to schedules with start backup "at" and is not supported for periodic backup schedule (start backup "every")
  - **until full backup completed** – this option will stop a backup job once it is complete. This is the configured stop time of the backup job by default.
  - **after (defined no. of hrs.)** – this option will stop a backup job after a certain number of hours regardless of whether the backup job has completed or not. This can range from 1 to 24 hrs.

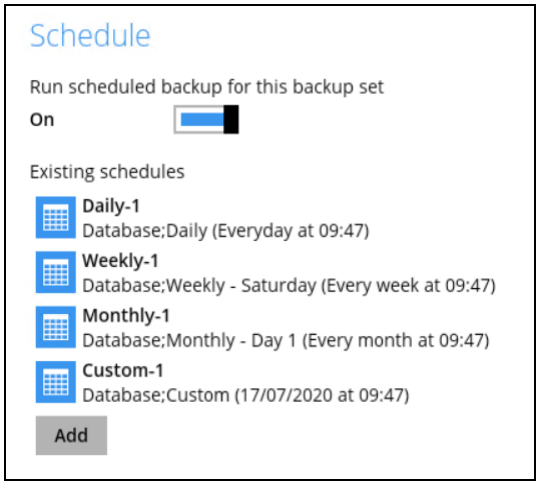
    The number of hours must be enough to complete a backup of all files in the backup set. For small files in a backup, if the number of hours is not enough to back up all files, then the outstanding files will be backed up in the next backup job. However, if the backup set contains large files, this may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

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

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

    As a general rule, it is recommended to review this setting regularly as the data size on the backup machine may grow over time.
- **Run Retention Policy after backup** – if enabled, the AhsayOBM will run a retention policy job to remove files from the backup destination(s) which have exceeded the retention policy after performing a backup job. To save hard disk quote in the long run, it is recommended to enable this option.

As an example, the four types of backup schedules may look like the following:



6. Click **Save** to confirm your settings once done.

8 Restore Microsoft Exchange Server 2013/2016/2019 in Database Availability Group (DAG)

8.1 Pre-restoration requirements

Refer to the following instructions to restore your Exchange database in Database Availability Group (DAG).

The database restoration is required to restore on the active database only. You can identify the Exchange server with the active database from the Exchange Management Shell.

Type the following command in the Exchange Management Shell.

```
Get-MailboxDatabase | ft name, server
```

It will show which Exchange server is hosting the active mailbox database, i.e. Mailbox Database 01 and 03 are hosted on EX1, while Mailbox Database 02 and 04 are hosted on EX2.

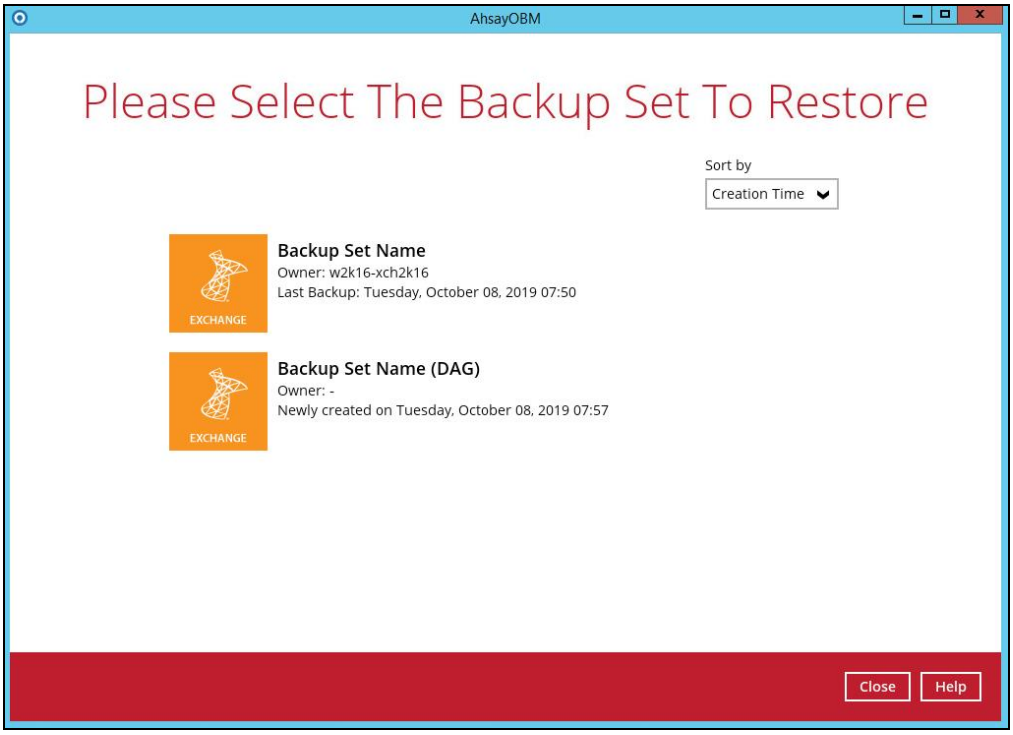
```
[PS] C:\>Get-MailboxDatabase | ft name, server

Name                    Server
----                    ----
Mailbox Database 02     EX2
Mailbox Database 01     EX1
Mailbox Database 03     EX1
Mailbox Database 04     EX2
```

When you can identify which Exchange server is hosting the active database, you can logon to that Exchange server to restore the database.

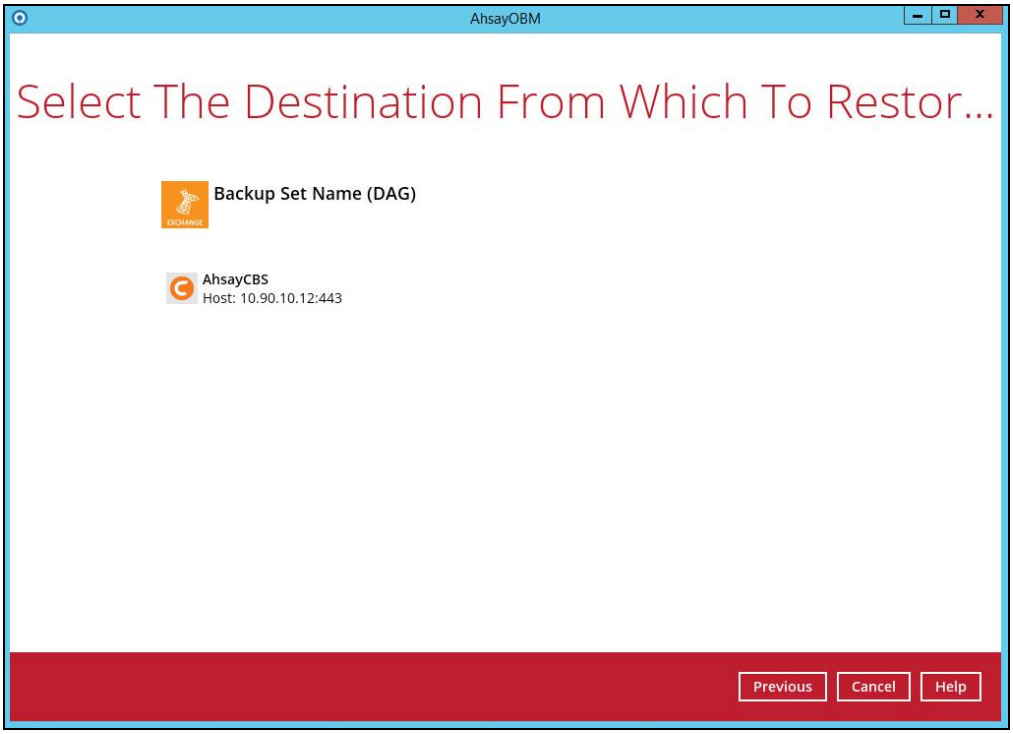
8.2 Restore Exchange Database to the Exchange with the active database

1. In the AhsayOBM main interface, click **Restore**.

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

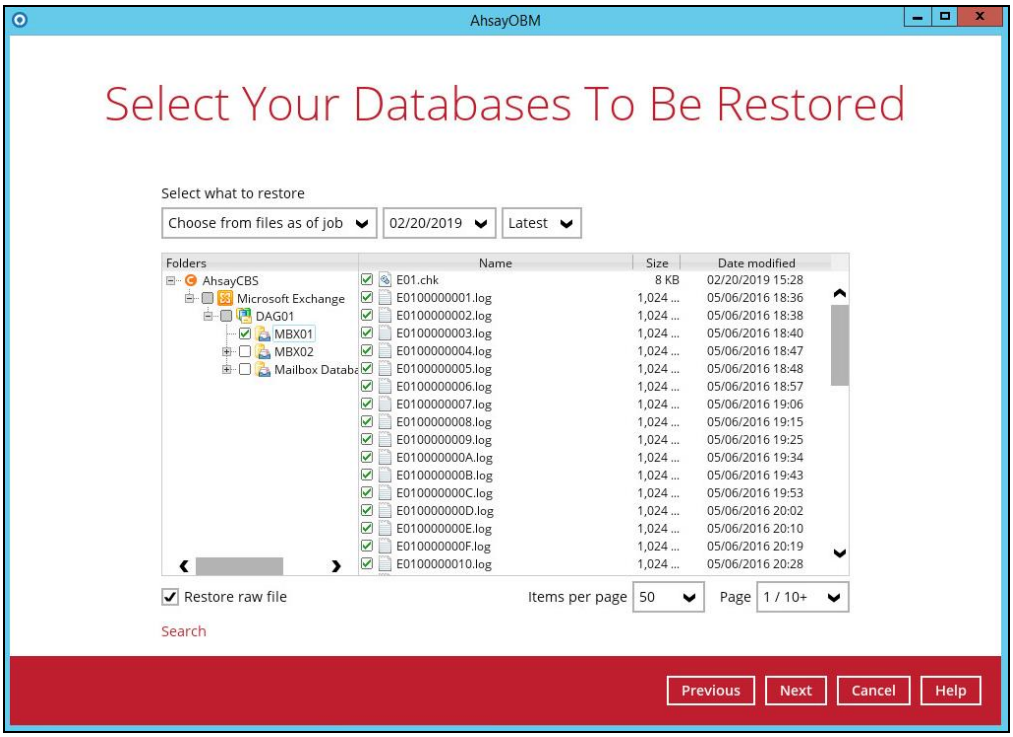


3. Select the backup destination that contains the files or folders that you would like to restore.

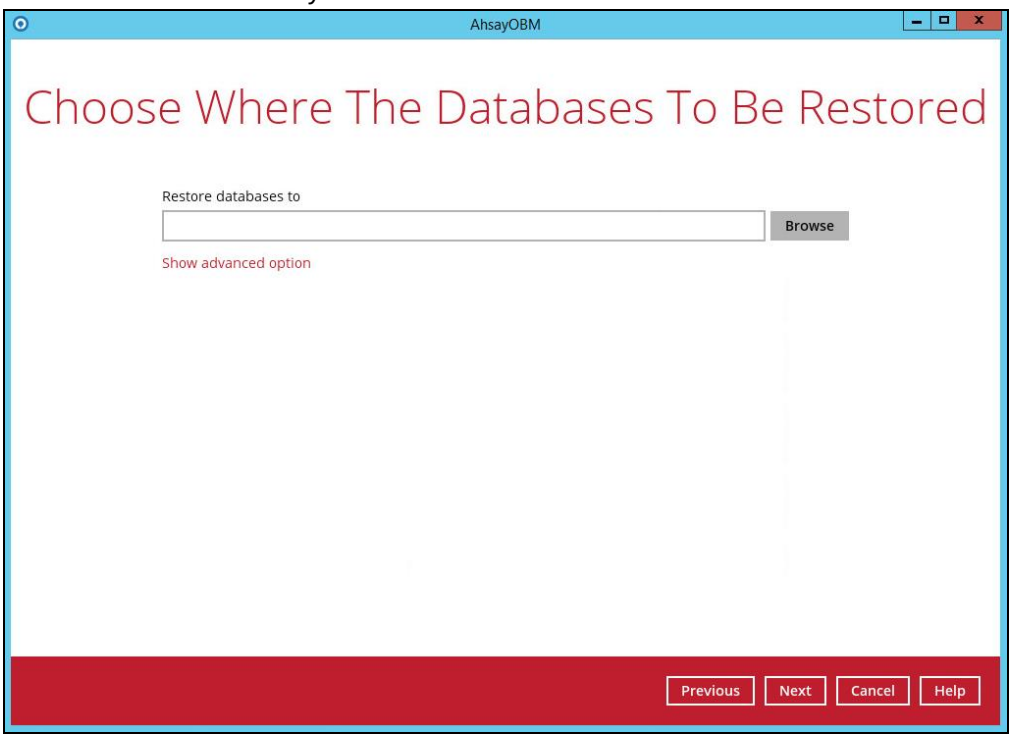


4. Click to expand the menu tree to select which DAG to restore. You can also select individual database file to restore by clicking the **Restore raw file** checkbox at the bottom left corner.

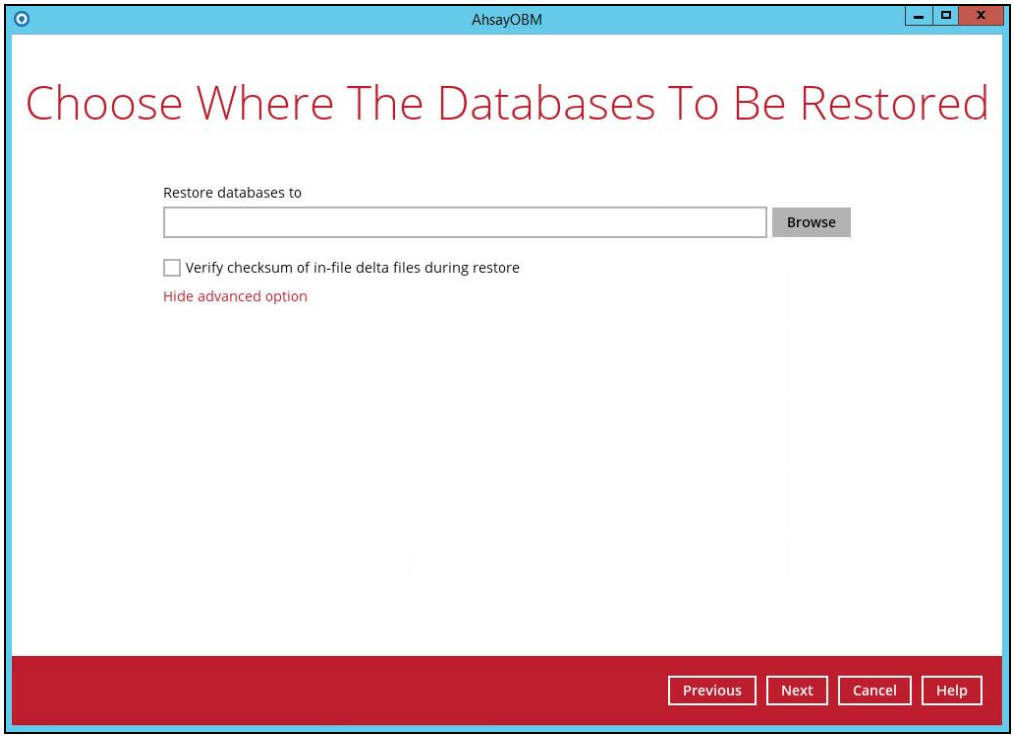
   In addition, you can also choose to restore backup item(s) from a specific backup job using the drop-down menu at the top. Click **Next** to proceed when you are done with the settings.



5. Select the location where you would like to restore the database.

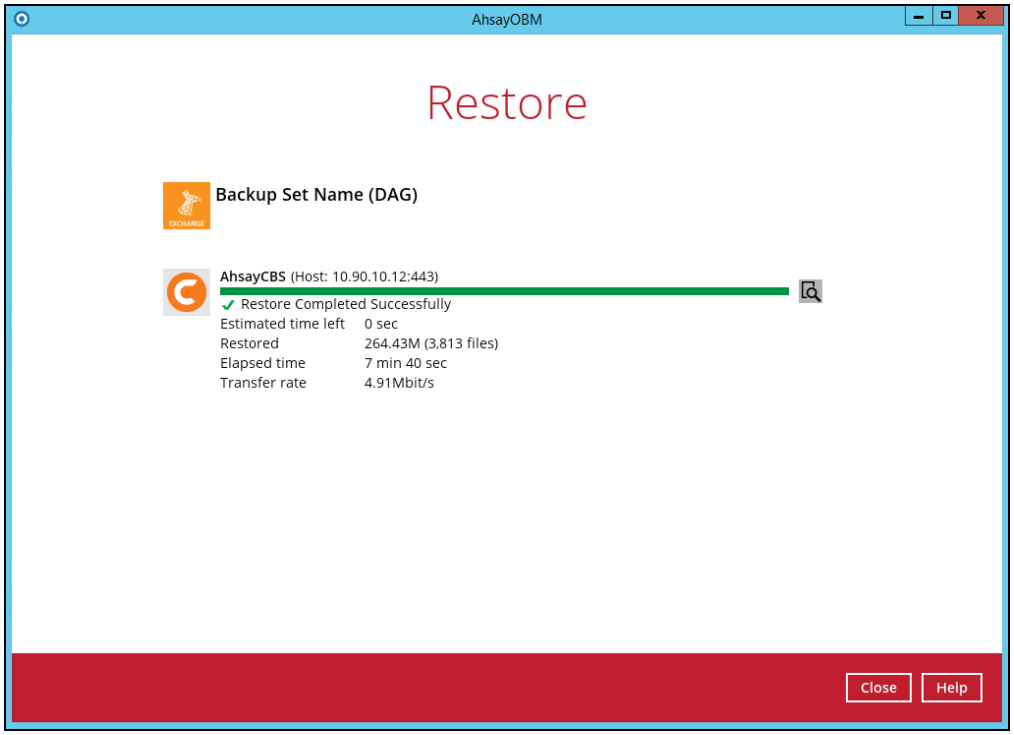


If you would like to modify the Verify checksum settings, click **Show advanced option**.



6. Select the temporary directory for storing temporary files, such as delta files when they are being merged, then click **Restore** to start the restoration.

7. The following screen with the text **Restore Completed Successfully** shows when the restoration is completed.



For details regarding verifying the restoration activities log between AhsayOBM and the Exchange Server, refer to Appendix B Restore Activities Log.

9 Contacting Ahsay

9.1 Technical Assistance

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

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

9.2 Documentation

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

You can send us suggestions for improvements or report on issues in the documentation by contacting us at:
https://www.ahsay.com/partners/

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

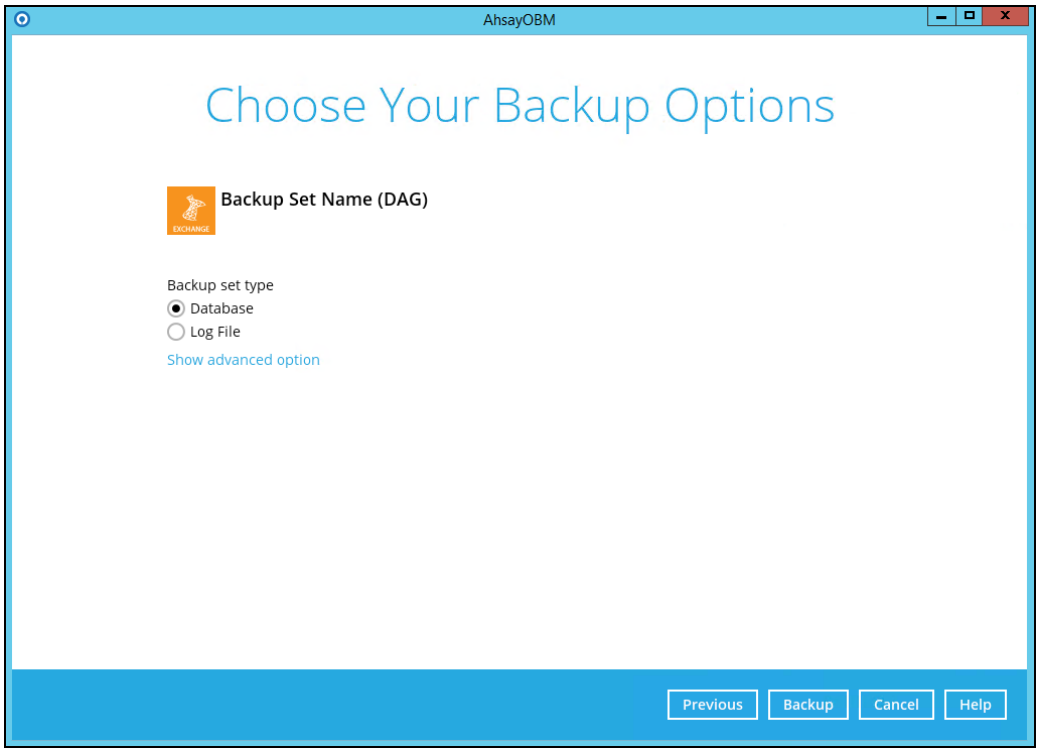
Appendix

Appendix A Exchange Server Backup Type

AhsayOBM utilizes the Volume Shadow Copy Service and the Microsoft Exchange Server 2010 Writers for backup of MS Exchange 2010/2013/2016/2019 databases. It offers the following types of backup options:

- **Database backup**

  Backs up the databases (EDB), transaction logs (LOG), checkpoint files (CHK), and then truncates the transaction logs for a specific database.



A full backup of an Exchange database creates and stores a complete copy of the database file, transaction logs, and checkpoint files. A Microsoft Exchange Server 2010/2013/2016/2019 database has one set of transaction log files dedicated to that one database.

After the database has been backed up, the transaction log files on the disk are truncated so that only database changes that occur after the backup was made will remain. During this process, either the Store Writer or the Replication Service deletes all log entries up to the checkpoint, based on the assumption that the databases have now been backed up in a consistent state that contains all changes up to the most recent checkpoint.

If the database being backed up is dismounted during the backup operation, Exchange Server 2010 will not truncate the transaction logs and the result will be the equivalent of a copy backup operation, not a Full backup operation.

At the completion of Full or Incremental backups, the headers of the active mounted database get updated with the current backup information. A Full backup is required in order

to run Incremental or Differential backups. There is no restriction as to which copy the Full backups are taken from as long as it is a backup.

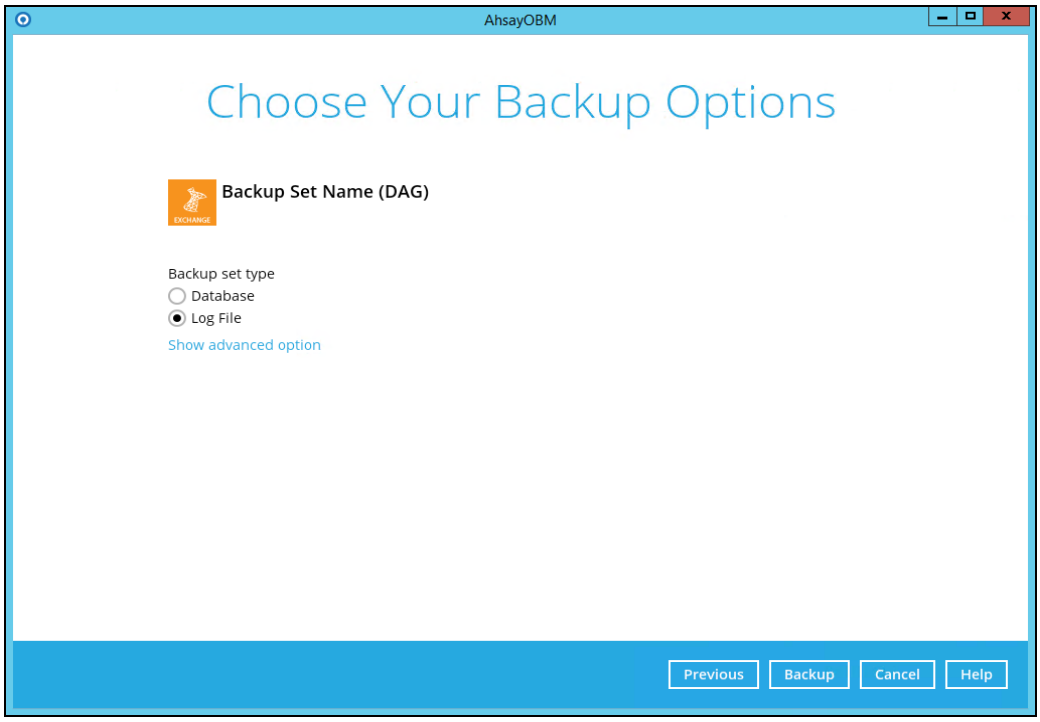
Full backups are used in the following restoration scenarios:

A database becomes corrupted or is lost, but the transaction log files on disk are intact. In this scenario, the affected database files can be restored from the Full backup, and then recovered by replaying the transaction logs that are still on disk.

Transaction log files, as well as the database file on disk, are lost. In this scenario, the transaction log files that were backed up at the time of the Full backup are restored together with the database.

- **Log File backup**

  Backs up the transaction logs (LOG) to record changes since the last full or incremental backup, and then truncates the transaction logs.



An Incremental backup of Microsoft Exchange Server 2010 database saves changes to the database that have occurred since the last Full or Incremental backup. When all the database files and log files are restored to the system, they can be recovered to the state they were in at the time of the last Incremental backup. The data stored in an Incremental backup includes only the transaction log files up to the current time.

When the backup is completed, the Exchange Server truncates the log files and marks the backup time in the database headers. Using an Incremental backup to recover a database requires the restoration of at least two data sets: the last Full backup, and then every Incremental backup taken after the last Full backup. The benefit of using Incremental backup is that an individual Incremental backup is much smaller than a Full backup and an individual Incremental backup is often smaller than an individual Differential backup.

The disadvantage of using Incremental backups is that if there are many Incremental backups made between Full backups, recovering the storage group may involve recovering many Incremental backups. Exchange does not allow an Incremental backup to occur when

there has been no previous Full backup to establish the starting point for the incremental changes.

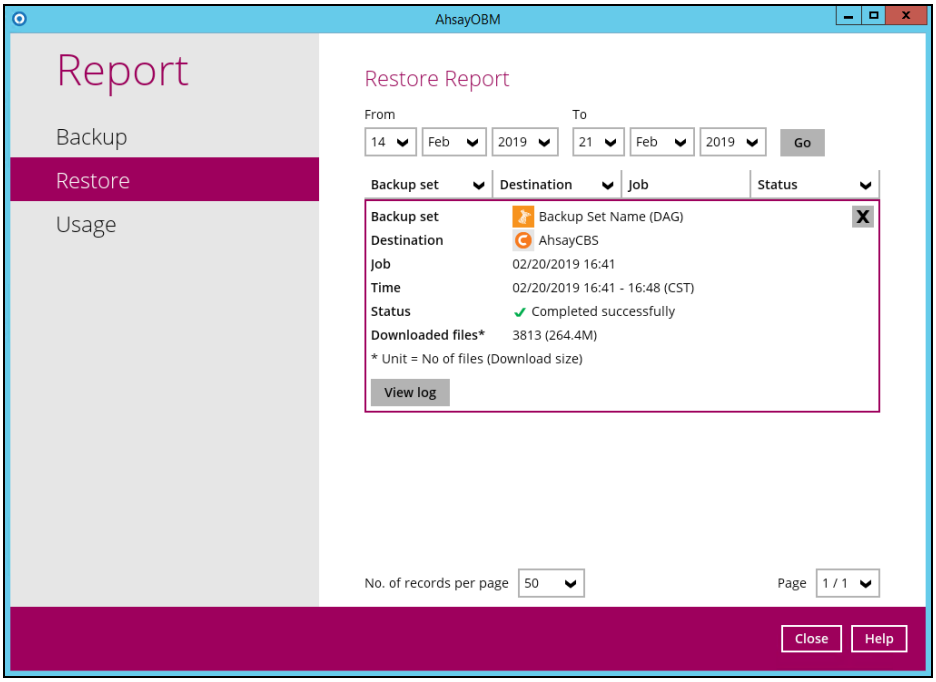
Appendix B Restore Activities Log

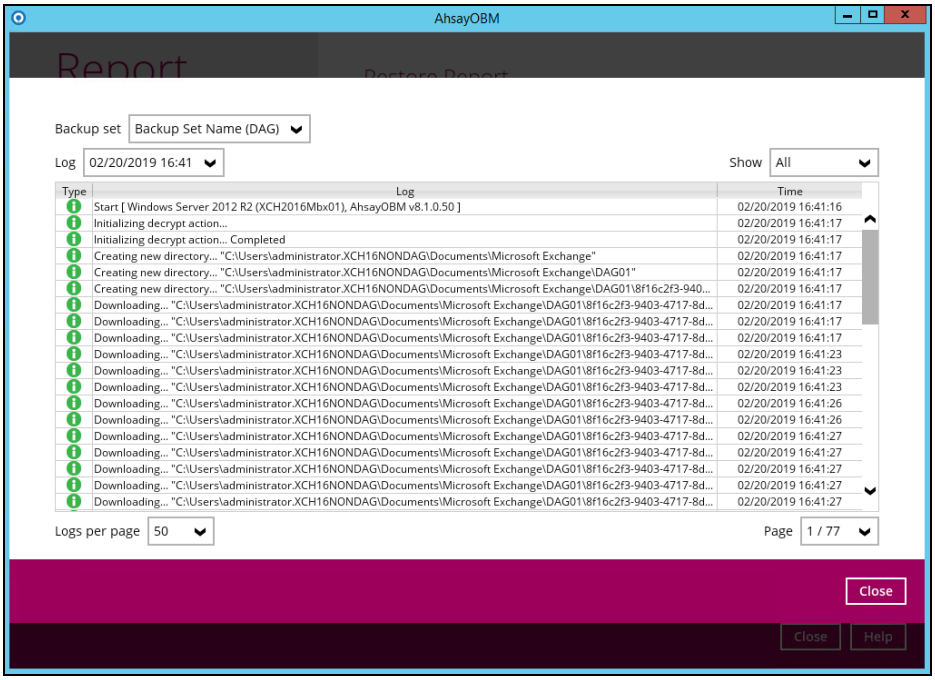
The information below demonstrates how you can verify the restoration activities log between the AhsayOBM and the Microsoft Exchange Server.

To verify the restoration activities log, open both the Restore Report in AhsayOBM and the Event Viewer in the Microsoft Exchange Server.

Opening Restore Report in AhsayOBM

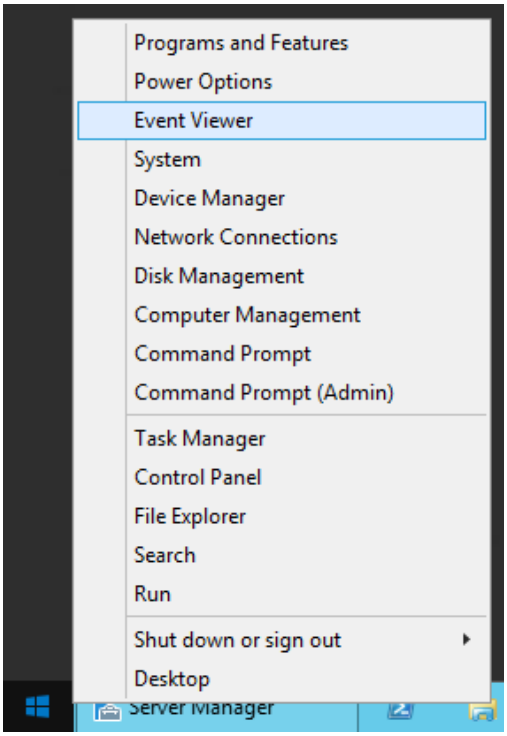
1. Open AhsayOBM, then click the **Report** icon on the main interface page.
2. Click the Restore option on the left, then click the restore report you want to verify on the right. Click the **View Log** button to show all the restoration activities log.



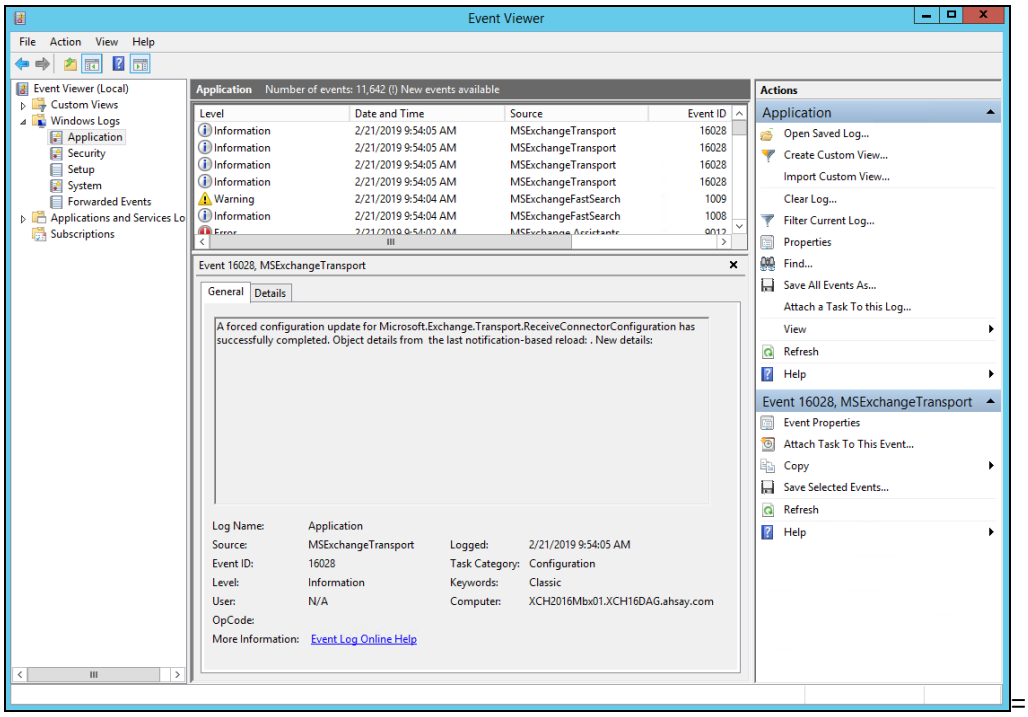


Opening Event Viewer in Microsoft Exchange Server

1. Right-click the Start menu button on the bottom left corner in the Exchange Server, then click on Event Viewer.



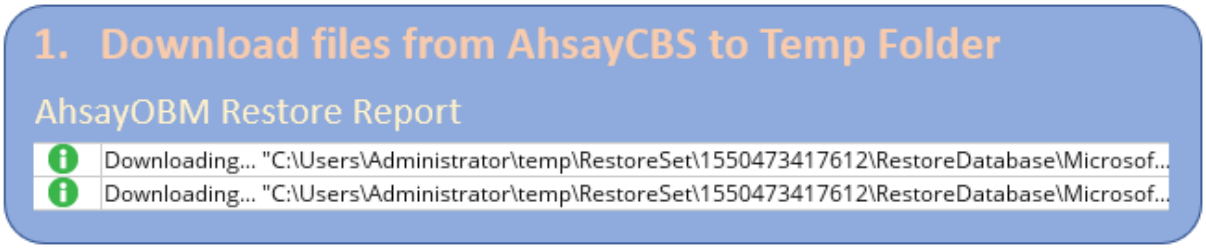
2. When the Event Viewer is opened, click **Windows Log** on the left to expand the menu tree, then select **Application**. All Application activities logs are shown on the right now.

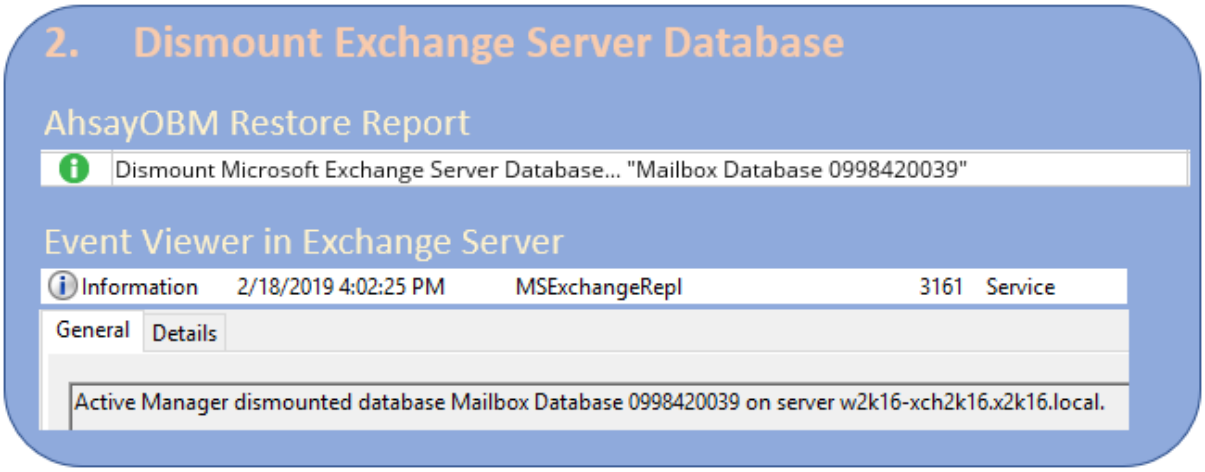


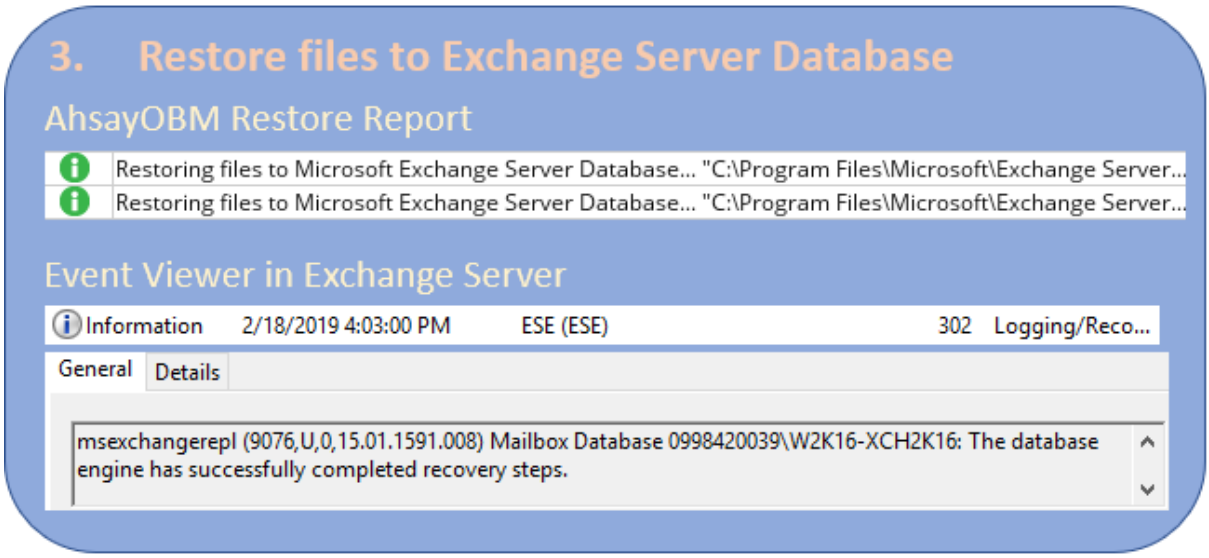
Cross-checking activities log on AhsayOBM Restore Report and Exchange Server Event Viewer

Each restoration action item initiated by AhsayOBM represented by individual activity log in the Restore Report in AhsayOBM, and the corresponding action taken place in the Exchange Server is shown in the Event Viewer as well.

There are 5 major parts to take place during the database restoration progress as shown below.







4. Remount Exchange Server Database

AhsayOBM Restore Report

Re-mount Microsoft Exchange Server Database... "Mailbox Database 0998420039"

Event Viewer in Exchange Server

Information 2/18/2019 4:04:12 PM MSExchangeRepl 3156 Service

General Details

Active Manager successfully mounted database Mailbox Database 0998420039 on server w2k16-xch2k16.x2k16.local.

5. Delete files from Temp Folder

By default, temporary files will be deleted from the temp folder after backup. This feature can be turned on or off by following the steps below:

1. Open AhsayOBM, then click the Backup Set icon on the main interface.
2. Select the backup set you would like to change this setting.
3. Click "Show advanced settings" on the left, then select "Others".
4. Use the "Remove temporary files after backup" checkbox to enable or disable this feature.