Ahsay Backup

A-Click Backup Manager v8

Office 365 Backup & Restore Guide for MacOS

Ahsay Systems Corporation Limited

11 October 2021

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

Copyright Notice

© 2021 Ahsay Systems Corporation Limited. All rights reserved.

The use and copying of this product is subject to a license agreement. Any other use is prohibited. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form by any means without prior written consent of Ahsay Systems Corporation Limited. Information in this manual is subject to change without notice and does not represent a commitment on the part of the vendor, Ahsay Systems Corporation Limited does not warrant that this document is error free. If you find any errors in this document, please report to Ahsay Systems Corporation Limited in writing.

This product includes software developed by the Apache Software Foundation (https://www.apache.org/).

Trademarks

Ahsay, Ahsay Cloud Backup Suite, Ahsay Online Backup Suite, Ahsay Offsite Backup Server, Ahsay Online Backup Manager, Ahsay A-Click Backup, Ahsay Replication Server, Ahsay BackupBox Firmware, Ahsay Universal Backup System and Ahsay NAS Client Utility, Ahsay Mobile are trademarks of Ahsay Systems Corporation Limited.

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

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

Dropbox is a registered trademark of Dropbox Inc.

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

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

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

MariaDB is a registered trademark of MariaDB Corporation AB.

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

Microsoft Windows, Microsoft Exchange Server, Microsoft SQL Server, Microsoft Hyper-V, Microsoft Azure, OneDrive, OneDrive for Business, Microsoft Authenticator, and Microsoft Office 365 are registered trademarks of Microsoft Corporation.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Oracle 11g, Oracle 12c, Oracle 18c, Oracle 19c, and MySQL are registered trademarks of Oracle Corporation.

Rackspace and OpenStack are registered trademarks of Rackspace US, Inc.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo and JBoss are registered trademarks of Red Hat, Inc. www.redhat.com in the U.S. and other countries.

Linux is a registered trademark of Linus Torvalds in the U.S. and other countries.

Ubuntu is a registered trademark of Canonical Ltd.

ShadowProtect is a registered trademark of StorageCraft Technology Corporation.

VMware ESXi, vCenter, and vSAN are registered trademarks of VMware, Inc.

All other product names are registered trademarks of their respective owners.

Disclaimer

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

Revision History

Date	Descriptions	Type of modification
6 October 2020	Added Appendix H	New
9 October 2020	Updated screenshots in Ch. 7 and Appendix F	Modifications
25 January 2021	Updated PDIC diagram in Ch. 5; Reorganized Permission Requirements in Ch. 2.12; Added Ch. 2.16; Modified Limitations in Ch. 2.17	Modifications
29 January 2021	Updated screenshots in Chapters 2, 7 and Appendix F	Modifications
7 April 2021	Updated Ch. 5; added sub-chapters for the detailed process diagrams in Ch. 5.1, 5.2, 5.2.1, 5.2.2 and 5.3	New / Modifications
23 July 2021	Updated Ch. 2.17.1 Ahsay Limitations;	Modifications
11 October 2021	Updated login instructions in Ch. 3	Modifications

Table of Contents

1 Overview 1

1.1 What is this software? 1
1.2 System Architecture 1
1.3 Why should I use AhsayACB or AhsayCBS User Web Console? 2
1.4 About This Document 7

2 Preparing for Backup and Restore 8

2.1 Hardware Requirement 8
2.2 Software Requirement 8
2.3 AhsayACB Installation Requirements 8
2.4 AhsayACB License Requirements 8
2.5 Add-on Module Requirements 8
2.6 Access for AhsayCBS User Web Console 9
2.7 Backup Quota Requirement 9
2.8 Public Folder Backup 9
2.9 SharePoint Personal Site Backup 9
2.10 Java Heap Size 9
2.11 Office 365 License Requirements 10
2.12 Office 365 Permission Requirements 11
2.12.1 Assigning Global Admin Role to Accounts 12
2.12.2 Granting Permission to Discovery Management Group 14
2.12.3 Granting Permission to Accounts for Creating Backup Set 16
2.13 Data Synchronization Check (DSC) 19
2.14 Authentication 21
2.15 Supported Services 25
2.16 Maximum Supported File Size 30
2.17 Limitations 31
2.17.1 Ahsay Limitations 31
2.17.2 Microsoft Limitations 32
2.18 Best Practices and Recommendations 33

3 Logging in to AhsayACB 36

3.1 Login to AhsayACB without 2FA 36
3.2 Login to AhsayACB with 2FA using authenticator app 38
3.3 Login to AhsayACB with 2FA using Twilio 41

4 Creating an Office 365 Backup Set 43

4.1 Modern Authentication 43
4.2 Hybrid Authentication 60

5 Overview of Office 365 Backup Process 80
5.1 Periodic Data Integrity Check (PDIC) Process 81
5.2 Backup Set Index Handling Process 83
5.2.1 Start Backup Job 83
5.2.2 Completed Backup Job 84
5.3 Data Validation Check Process 85

6 Running Backup Job 86

7 Restoring Office 365 Backup Set 88
7.1 Restore Backup with AhsayACB 88
7.1.1 Local machine 89
7.1.2 Original Location 89
7.1.3 Alternate Office 365 Account 90
7.2 Restore Filter with AhsayACB 91

8 Contacting Ahsay 102
8.1 Technical Assistance 102
8.2 Documentation 102

Appendix 103
Appendix A Example Scenarios for Office 365 License Requirement and Usage 103
Appendix B Example Scenarios for Restore Filter using AhsayACB 106
Appendix C Setting Multi-Factor Authentication (MFA) in Microsoft 365 Admin Center 118
Appendix D Example Scenario for Data Synchronization Check (DSC) with backup logs 131
Appendix E Setting the Data Synchronization Check (DSC) 135
Appendix F Steps on How to view Item count and Storage used in Microsoft 365 Admin Center 140
Appendix G Migrating Authentication of Office 365 Backup Set 144
Appendix H Steps on How to Change the Office 365 Authentication 150

1 Overview

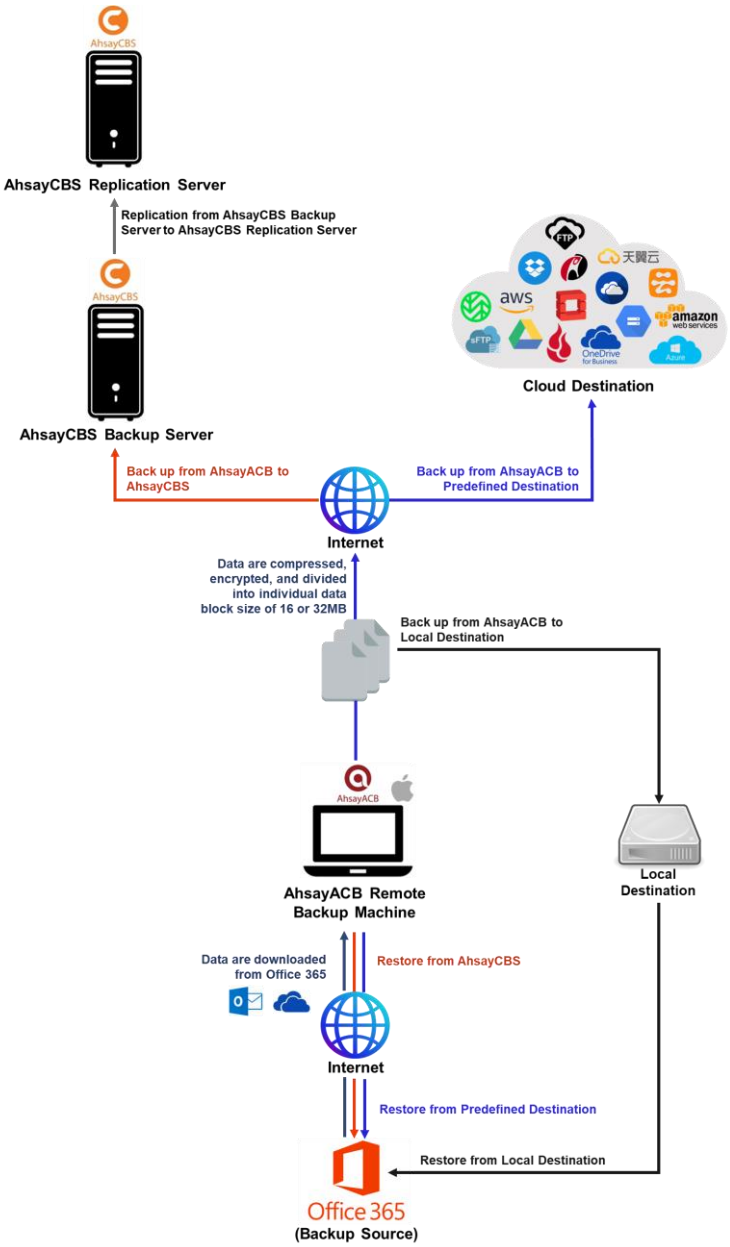
1.1 What is this software?

Ahsay brings you specialized client backup software, namely AhsayACB, to provide a set of tools to protect your Office 365 user accounts. This includes backup and recovery of individual emails, contacts, calendars and other mail items in your Office 365 Outlook, files on OneDrive and SharePoint, with snapshots / versioning, and retention policy to protect even items that you may have accidentally deleted from your Office 365 user account.

1.2 System Architecture

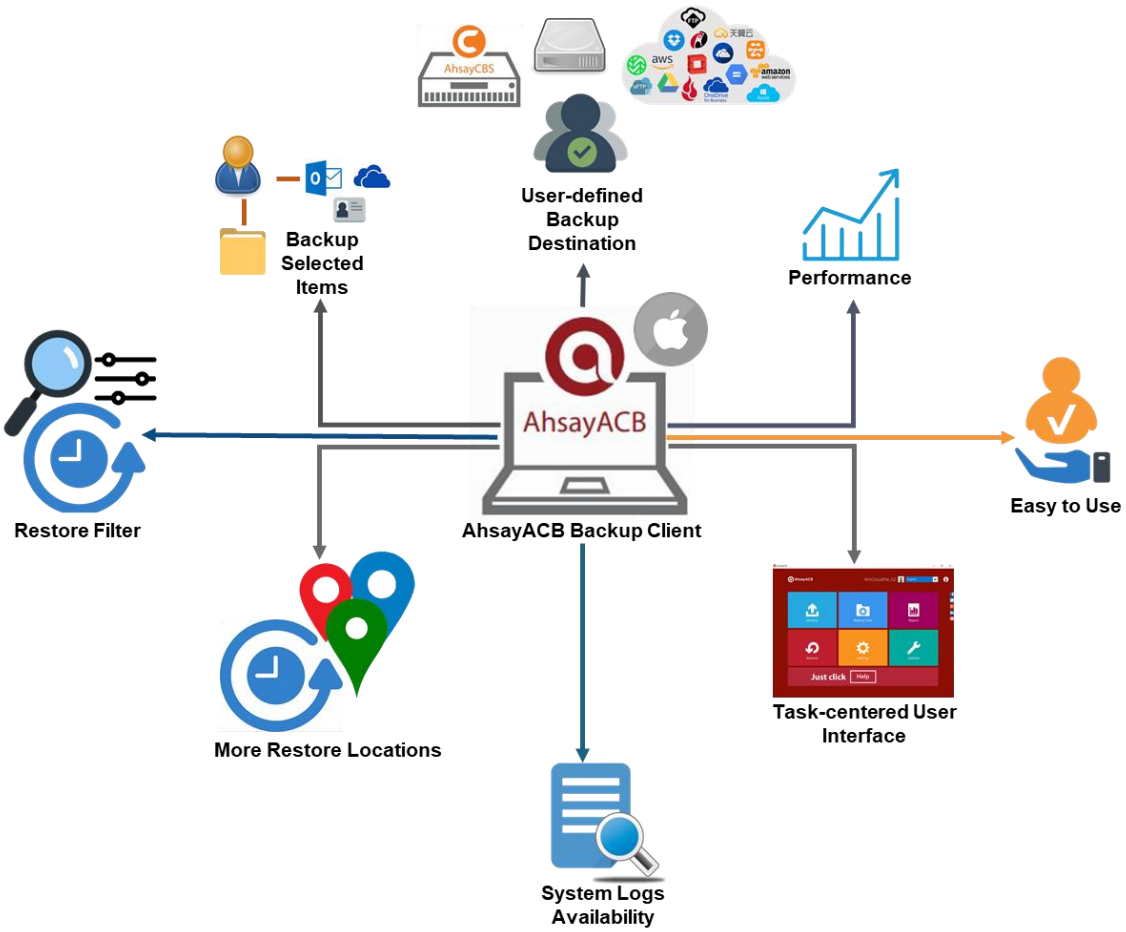
Below is the system architecture diagram illustrating the major elements involved in the backup process among the Office 365 service, AhsayACB and AhsayCBS.

In this user guide, we will focus on the software installation, as well as the end-to-end backup and restore process using the AhsayACB (Agent-based).



1.3 Why should I use AhsayACB or AhsayCBS User Web Console?

We are committed to bringing you a comprehensive Office 365 backup solution with AhsayACB. Below are some key areas that we can help making your backup experience a better one.



User-defined Backup Destination

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

Performance

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

The introduction of the Change Key API in v8.3.4.0 has significantly improved backup performance for both Full and Incremental backup jobs, which means Office 365 user accounts with a large number of items, each incremental backup can be completed within hours.

Easy to Use

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

Task-centered User Interface

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

System Logs Availability

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

More Restore Locations

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

Flexible restore option: Restore items to the original location or an alternate location.

Restore Filter

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

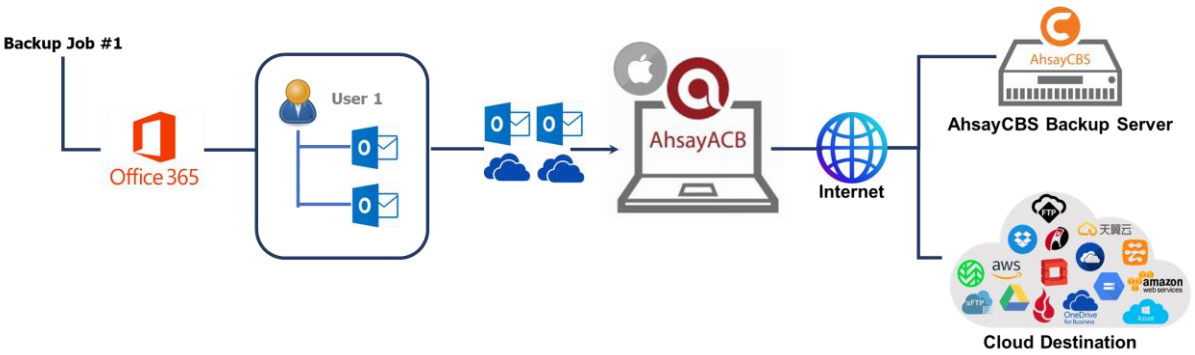
Fast and Efficient

We understand that backup could be a time and resources consuming process, which is why AhsayACB is designed with advanced technologies to make backup a fast and efficient process.

We also understand that 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.

- **Multi-threading** – this technology utilizes the computing power of multiple CPU cores for creating multiple backup and restore threads to produce fast backup and restore performance.

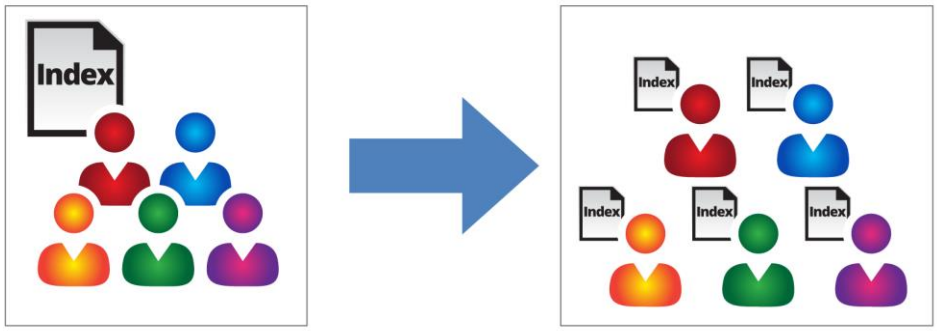
  Backup job uses a maximum of 4 concurrent threads.



As shown the technology translate into a total of 4 concurrent threads.

- **Index File Structure** – The index file structure has been re-designed to improve the backup and restore performance.

  Each Office 365 user will have its own individual index file instead of a single index file for all users within the backup set.



  This new design eliminates any potential I/O performance bottlenecks when the index files are updated during each backup job, which can occur when using single index file structure for multi-thread concurrent 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.

Backup of Selected Items

To back up the Office 365 user accounts, the backup source can be user level, and even item level.

Flexible backup options: Can select all components in the Office 365 user account, individual components such as Outlook, OneDrive, or Personal SharePoint or specific items within Outlook, OneDrive, Personal SharePoint.

High Level of Security

We understand your Office 365 users 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.

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

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
- Restore backup set
- Configure user settings
- Configure backup settings
- View and download backup and restore reports
- Monitor backup and restore live activities
- Monitor storage statistic

Cloud Destinations Backup

To offer you with the highest flexibility of backup destination, you can now back up Office 365 user 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.

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

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

The following table summarizes the differences in backup options available between a Run-on Server and Run-on Client Office 365 backup set, and the tool to use (web console or client agent) when performing a backup and restore:

Features/Functions	Run on Client Office 365 Backup Set	Run on Server Office 365 Backup Set
General Settings	✓	✓
Backup Source	✓	✓
Backup Schedule	✓	✓
Destination	AhsayCBS, Predefined Destinations, Standard and Local	AhsayCBS and Predefined Destinations only
Multiple Destinations	✘	✓
In-File Delta	✓	✓
Retention Policy	✓	✓
Command Line Tool	AhsayOBM for Windows only	✘
Reminder	AhsayOBM / AhsayACB for Windows only	✘
Bandwidth Control	✓	✓
IP Allowed for Restore	✓	✘
System Logs of Data Integrity Check and Space Freeing Up	✓	✘
Others	✓	✓
To Run a Backup	AhsayOBM / AhsayACB	AhsayCBS User Web Console only
To Run a Restore	AhsayOBM / AhsayACB / AhsayOBR	AhsayCBS User Web Console only

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

Features/Functions	Run on Server Office 365 Backup Set	Run on Client Office 365 Backup Set
Data Integrity Check	✓	✓
Space Freeing Up	✓	✓
Delete Backup Data	✓	✓
Decrypt Backup Data	✘	✓

NOTE:

For more details on the Run-on Server backup option, please refer to the following guides:
AhsayCBS v8 User Guide – Office 365 Run on Server (Agentless) Backup and Restore Guide

1.4 About This Document

What is the purpose of this document?

This document aims at providing all necessary information for you to get started with setting up your system for Office 365 backup and restore, followed by step-by-step instructions on creating backup set, running backup job, and restoring backed up data, using the AhsayACB.

The document can be divided into 3 main parts.

Part 1: Preparing for Office 365 Backup & Restore

Requirements
Requirements on hardware & software for installation

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

Part 2: Performing Office 365 Backup

Logging in to Client Agent
Log in to AhsayACB

Creating a Backup Set
Create a backup set using AhsayACB

Running a Backup Set
Run a backup set using AhsayACB

Part 3: Restoring Office 365 Backup

Restoring a Backup Set using AhsayACB
Restore a backup using AhsayACB

What should I expect from this document?

After reading through this documentation, you can expect to have sufficient knowledge to set up your system to backup Office 365 on AhsayACB, as well as to carry out an end-to-end backup and restore process.

Who should read this document?

This documentation is intended for backup administrators and IT professionals who are responsible for the Office 365 backup and restore.

2 Preparing for Backup and Restore

2.1 Hardware Requirement

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

2.2 Software Requirement

Make sure the operating system where you have the Office 365 installed is compatible with the AhsayACB. 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

2.3 AhsayACB Installation Requirements

For agent-based backup and restore, make sure that the latest version of AhsayACB is installed on your computer with Internet access for connection to your Office 365 account.

User should also stay up-to-date when newer version of AhsayACB is released. To get our latest product and company news through email, please subscribe to our mailing list. http://www.ahsay.com/jsp/en/home/subscribe_mail_list.jsp

2.4 AhsayACB License Requirements

AhsayACB licenses are calculated on a per device basis:

i. To backup users with one (1) backup client computer

   Example: If one AhsayACB is installed then, one AhsayACB license is required.

ii. To backup users with multiple backup client computers, the number of AhsayACB licenses required is equal to the number of devices.

Please contact your backup service provider for more details.

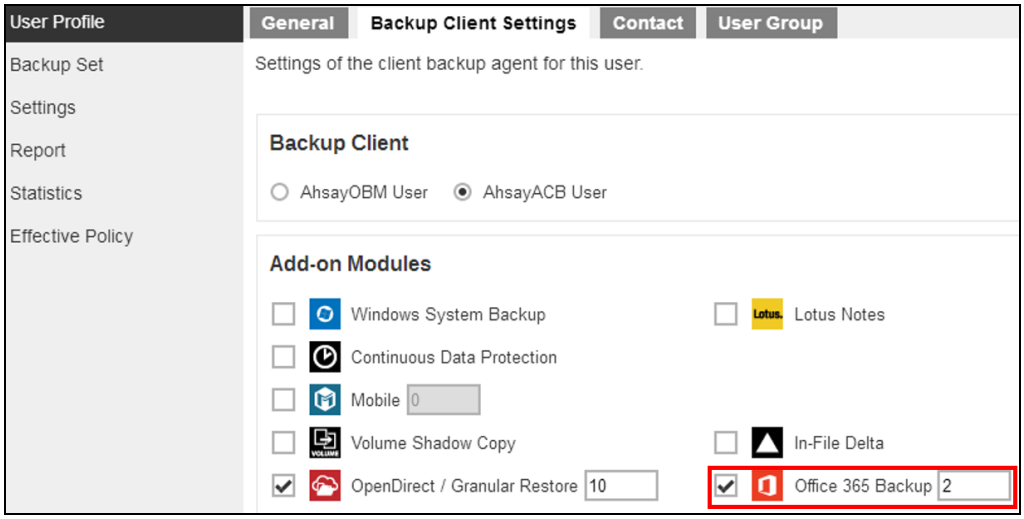
2.5 Add-on Module Requirements

Make sure that the Office 365 Backup feature has been enabled as an add-on module in your AhsayACB user account and there is enough Office 365 Backup license quota to cover the backup of your users.

Please contact your backup service provider for more details. Below is a sample screen shot of an AhsayACB User with an add-on module of Office 365 with two (2) licenses.

NOTE

- Please be reminded that a maximum of two modules is allowed for Office 365 Backup on AhsayACB. If you wish to add extra module, consider using AhsayOBM instead. Please contact your backup service provider for more details.
- Each AhsayACB Office 365 backup set is limited to one Office 365 user account. Therefore, when you backup two Office 365 user accounts it will require two separate backup sets.



For more information, refer to Appendix A: Example Scenarios for Office 365 License Requirement and Usage.

2.6 Access for AhsayCBS User Web Console

It is now possible to perform agentless backup and restore, which can be done via the AhsayCBS User Web Console without using the AhsayACB client agent. In order to access the User Web Console, make sure you have Internet connection and a web browser installed on your computer or mobile device.

2.7 Backup Quota Requirement

Make sure that your AhsayACB user account has sufficient quota assigned to accommodate the storage of the Office 365 users for the new backup set and retention policy. Please contact your backup service provider for more details.

To get an accurate estimate of the backup quota requirement, it is recommended to check the actual usage of the Office 365 Organization in the Microsoft 365 Admin Centre. Please refer to this link: Appendix F: Steps on How to view Item count and Storage used in Microsoft 365 Admin Center

2.8 Public Folder Backup

A licensed Exchange Administrator or a licensed user with Public Folder permission is required otherwise you will not be able to access the public folder to select items and for backup or restore.

2.9 SharePoint Personal Site Backup

To be able to backup SharePoint Personal Sites, ensure that you use Hybrid Authentication when creating a backup set. Due to the current limitation with Microsoft API, Modern Authentication is currently not suitable for backup sets with Personal Sites selected. As backup and restore of SharePoint metadata are not fully supported.

2.10 Java Heap Size

The default Java setting heap 2048M, is sufficient for Office 365 backups.

2.11 Office 365 License Requirements

- **Office 365 Subscription Plan**

  The following subscription plans with Office 365 email services are supported to run backup and restore on AhsayACB or AhsayCBS User Web Console.

Office 365 Business Essentials	Office 365 Business Premium
Office 365 Education	Office 365 Enterprise E1
Office 365 Enterprise E3	Office 365 Enterprise E4
Office 365 Enterprise E5	Office 365 Education

- **Office 365 Subscription Status**

  Make sure your Office 365 subscription with Microsoft is active in order to enjoy all privileges that come along with our backup services. If your account has expired, renew it with Microsoft as soon as possible so that you can continue enjoy the Office 365 backup services provided by Ahsay.

  When your account is expired, depending on your role, certain access restrictions will be applied to your account. Refer to the URL below for more details.

  Microsoft Office 365 Subscription Status

2.12 Office 365 Permission Requirements

The basic permissions required by an Office user account for authentication of an Office 365 backup set is as follows:

- **Global Admin Role**

  Starting with AhsayACB v8.3.6.0 or above, the Office 365 account used for authentication must have Global Admin Role, since Modern Authentication will be used.

  This is to ensure that the authorization configuration requirements will be fulfilled (e.g. connect to Microsoft Azure AD to obtain the App Access Token). To assign the role, please refer to Ch. 2.12.1.

- A member of **Discovery Management** security group

  The **Discovery Management** security group must be assigned the following roles. To assign the role, please refer to Ch. 2.12.2.

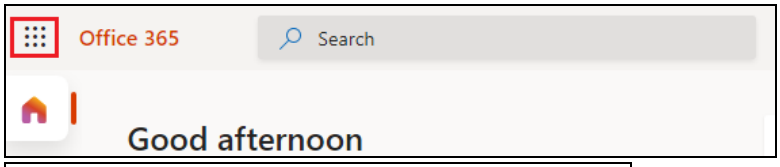
  - Mailbox Search
  - Public Folders

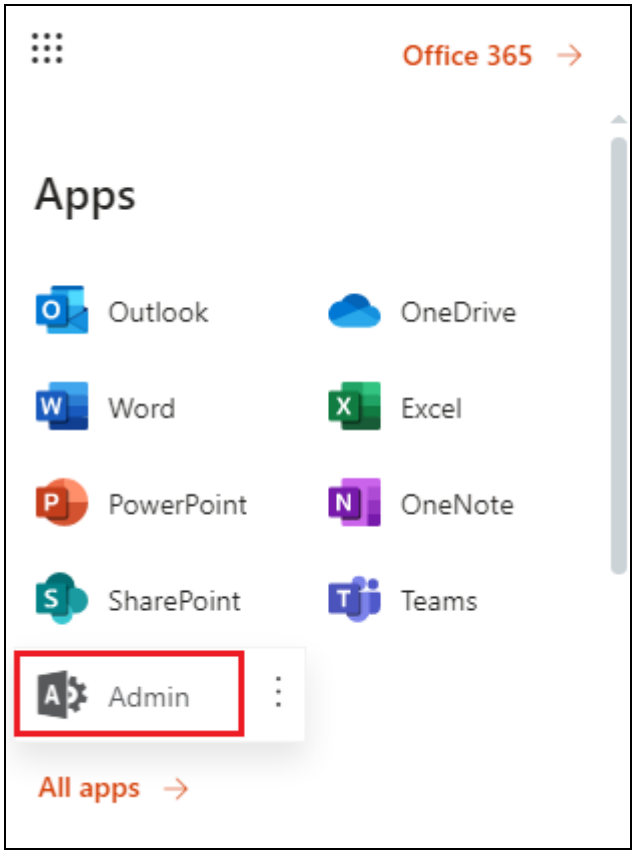
Otherwise, proceed to grant all necessary permissions to the Office user account as shown in the following chapters 2.12.1, 2.12.2 and 2.12.3.

2.12.1 Assigning Global Admin Role to Accounts

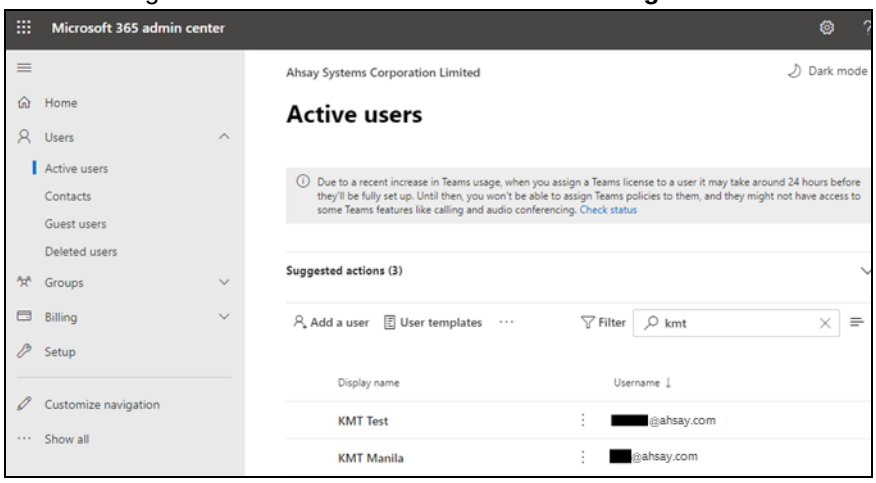
To assign the Global Admin role to accounts, follow the steps below:

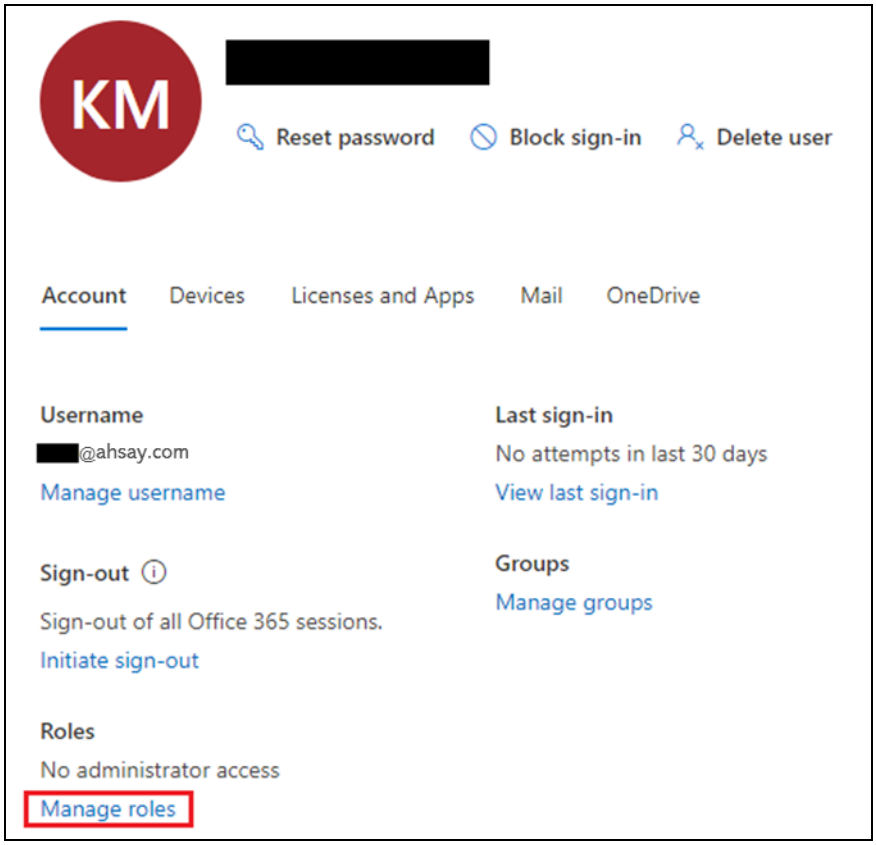
i. Click the App launcher in the upper left side then click **Admin** to go to the Microsoft 365 admin center.



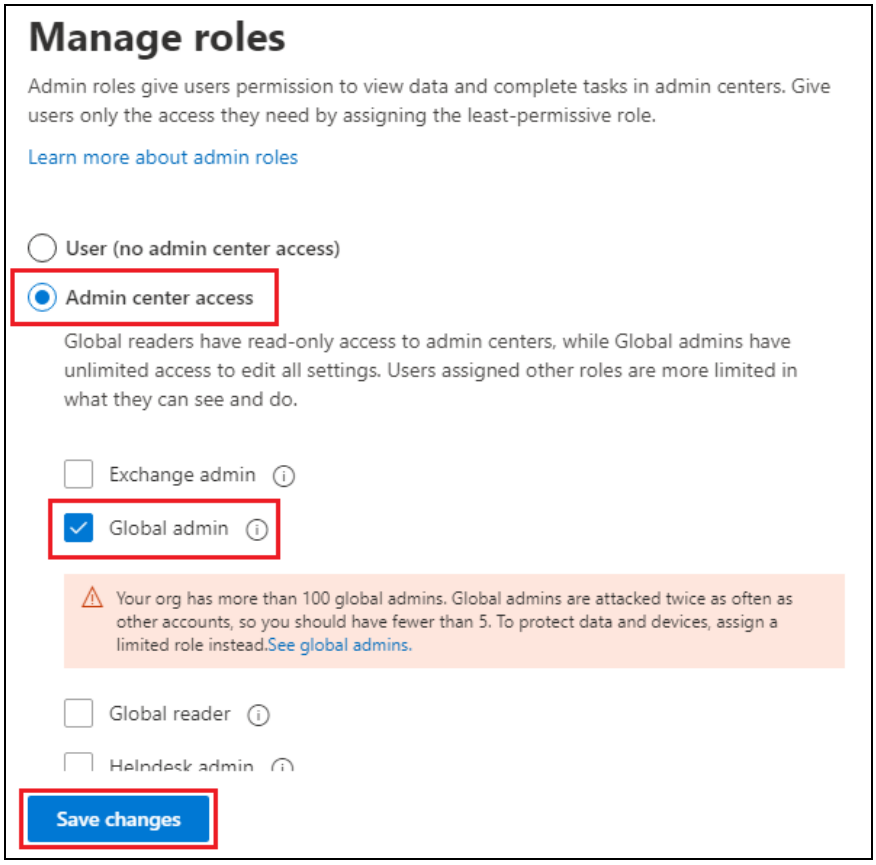


ii. In the Microsoft 365 admin center, on the left panel click **Users**. Find the user you want to assign the Global Admin role and select **Manage roles**.





iii. In the Manage roles window, select **Admin center access** then check the box beside **Global admin**. Click **Save Changes** to save the role you assigned.

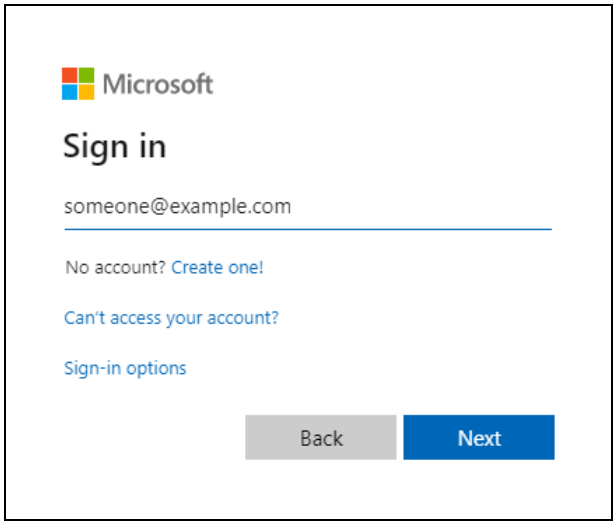


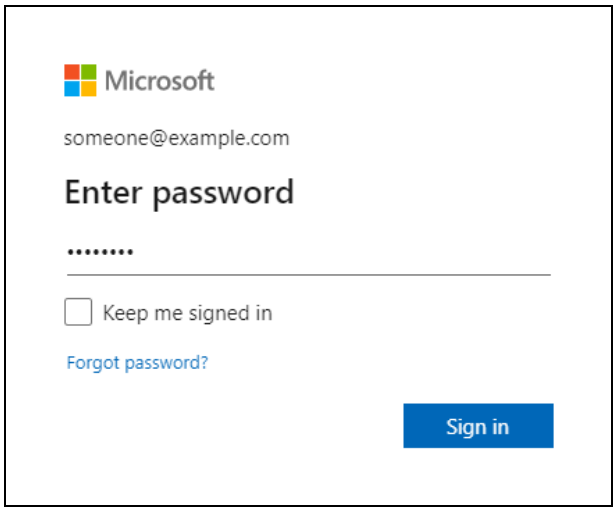
2.12.2 Granting Permission to Discovery Management Group

This permission allows users added under the **Members** section of the **Discovery Management** group (refer to Ch. 2.12.3 for setup) to back up and/or restore user item(s) not only for their own account, but also the accounts of other users in the same **Members** section.

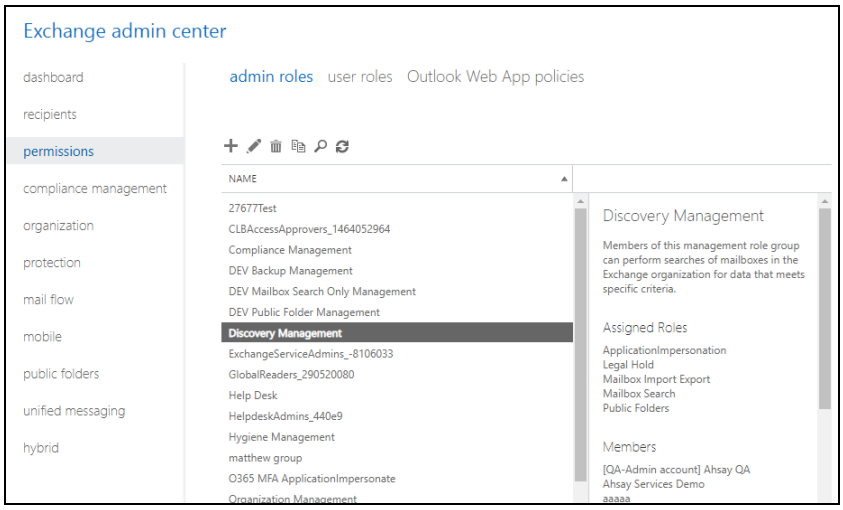
i. Open https://outlook.office365.com/ecp

ii. Log in to the **Office 365** as an account administrator.



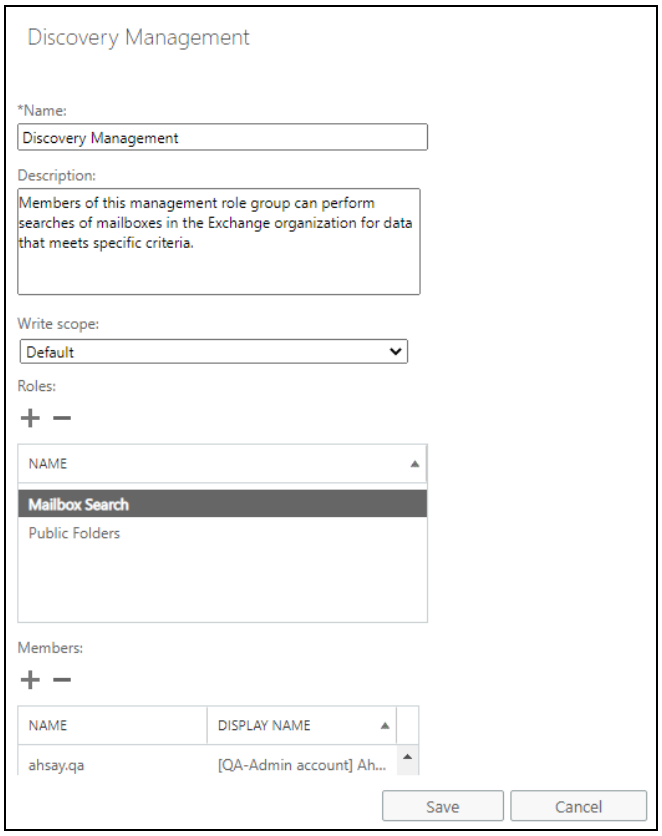


iii. Select the **permissions** menu on the left, then double click on **Discovery Management** on the right.



iv. Click the **+** icon under the **Roles** section. These are the following roles:

- Mailbox Search
- Public Folders

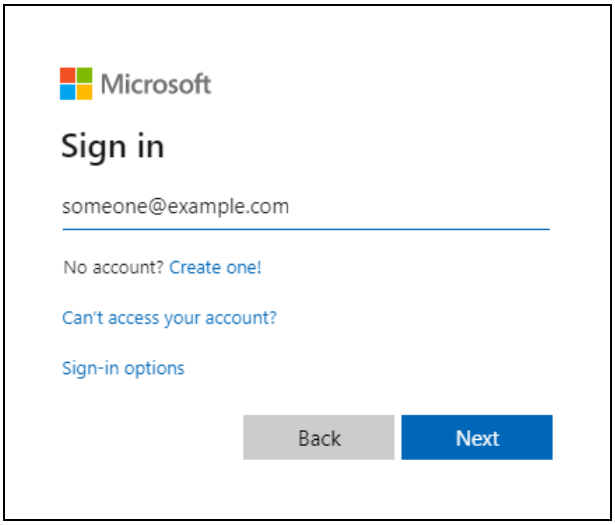


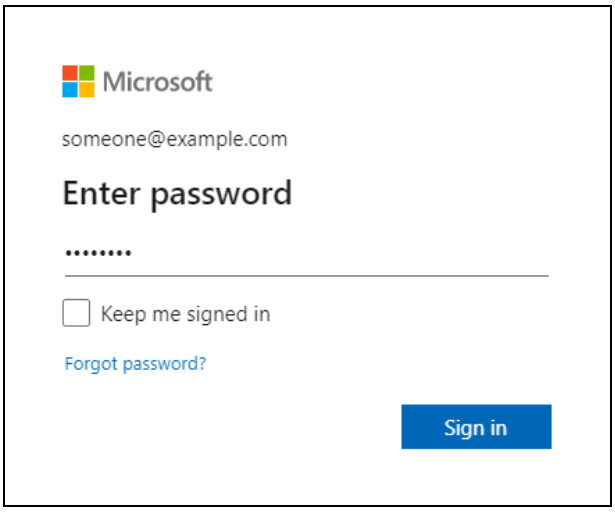
v. Click **Save** to confirm and exit the setting.

2.12.3 Granting Permission to Accounts for Creating Backup Set

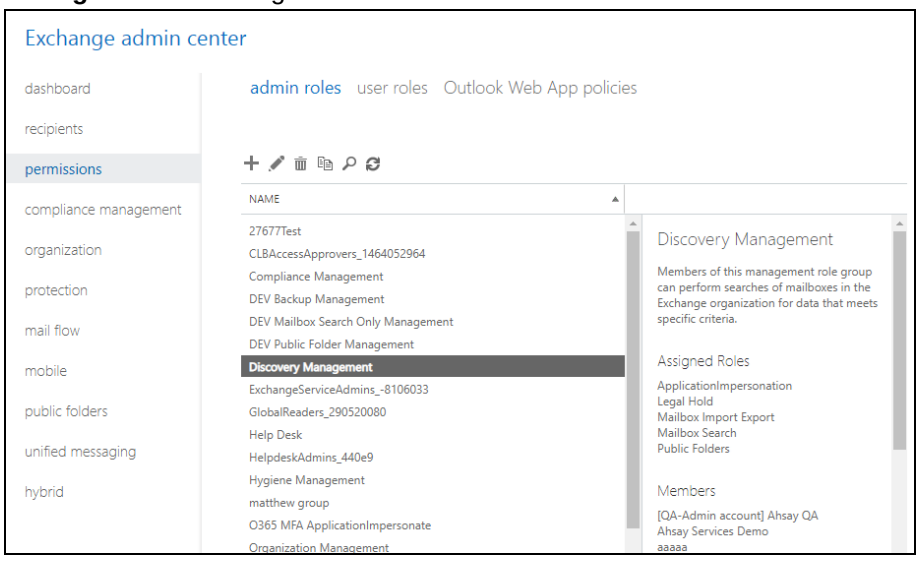
i. Open https://outlook.office365.com/ecp

ii. Log in to the **Office 365** as an account administrator.



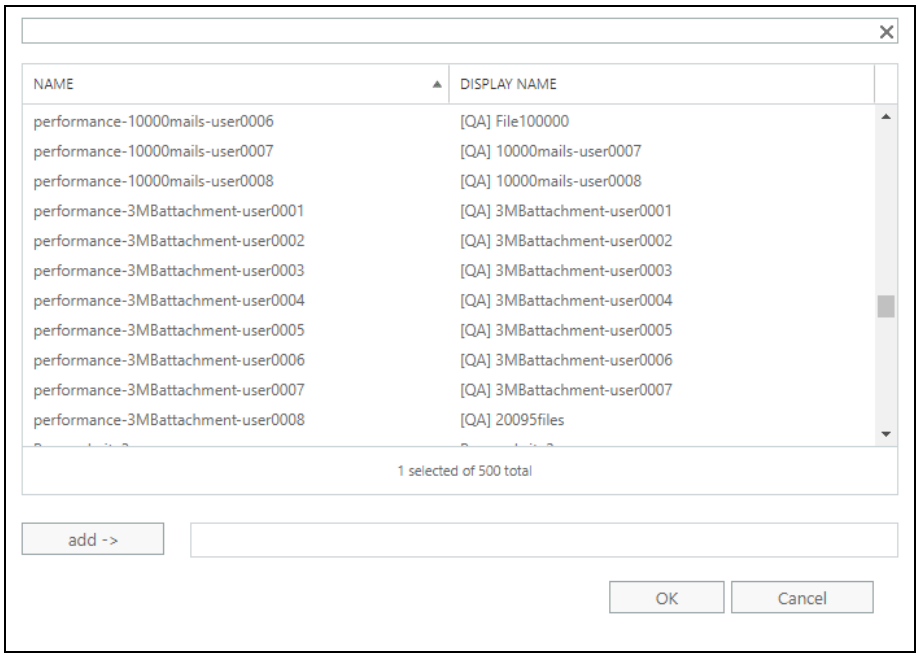


iii. Select the **permissions** menu on the left, then double click on **Discovery Management** on the right.



iv. You can now add users to this group. Click the **+** icon under the **Members** section.

v. Look for the username(s) of the account that you would like to add permission for, then click **add** > **OK** to add the corresponding user(s) to the permission group.



vi. Click **Save** to confirm and exit the setting.

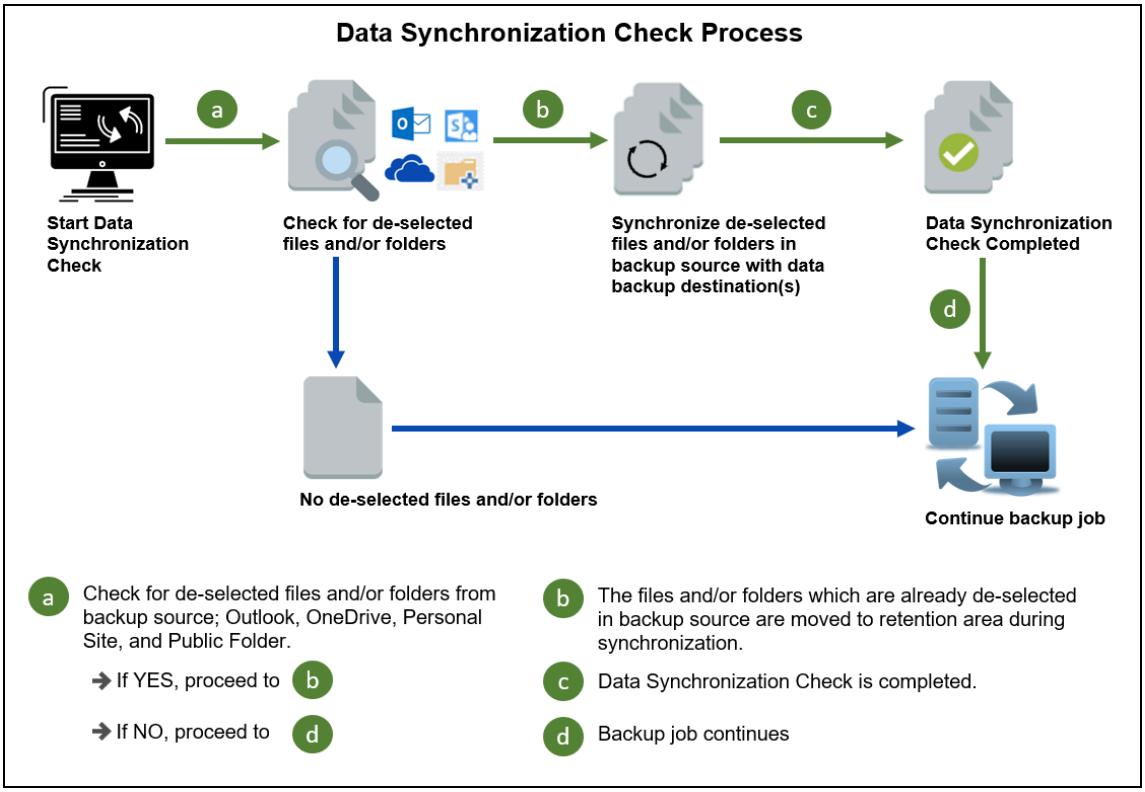
2.13 Data Synchronization Check (DSC)

To compensate for the significant backup performance increase, there is a tradeoff made by the Change Key API, which skips the checking of de-selected files in the backup source, which over time can result in a discrepancy between the items or files/folders selected in the backup sources and the those in the backup destination(s). However, the Change Key API will continue to check for de-selected Office 365 user accounts. Un-selected individual Office 365 user accounts detected during a backup job and will be automatically moved to retention area.

To overcome this, it is necessary in some cases to run a Data Synchronization Check (DSC) periodically. The DSC is similar to a regular Office 365 Change Key API backup job but with the additional checking and handling of de-selected files and/or folders in the backup source. So that it will synchronize the data in the backup source and backup destination(s) to avoid data build-up and the freeing up of storage quota.

Here are the pros and cons of performing the data synchronization check.

	Enabled	Disabled
Backup time	Since data synchronization check is enabled, it will only run on the set interval. For example, the default number of interval is 60 days. The backup time for the data synchronization job will take longer than the usual backup as it is checking the de-selected files and/or folders in the backup source and data in backup destination(s).	As data synchronization check is disabled, the backup time will not be affected.
Storage	Management of storage quota will be more efficient as it will detect items that are de-selected and moved it to retention and will be removed after it exceeds the retention policy freeing up the storage quota.	Management of storage quota will be less efficient even though files and/or folders are already de-selected from the backup source, these files will remain in the data area of backup destination(s).



NOTE

To setup the Data Synchronization Check (DSC), refer to this Appendix E Setting the Data Synchronization Check (DSC).

2.14 Authentication

To comply with Microsoft's product roadmap for Office 365, from AhsayACB v8.3.6.0 or above, Basic Authentication (Authentication using Office 365 login credentials) will no longer be utilized. Instead all new Office 365 backup sets created will use either Modern Authentication or Hybrid Authentication.

By second half of 2021, it will be a mandatory requirement for organizations still using Basic Authentication or Hybrid Authentication to migrate to Modern Authentication.

Modern Authentication provides a more secure user authentication by using app token for authentication aside from using the Office 365 login credentials. In order to use Modern Authentication, the Office 365 account is registered under Global region and the Office 365 backup is configured to use Global region. As both Germany and China region do not support Modern Authentication.

Existing backup sets using Basic Authentication created prior to AhsayACB v8.3.6.0 can be migrated to Hybrid Authentication or Modern Authentication. However, once the authentication process is completed, the authentication can never be reverted back to Basic Authentication. For more information on how to migrate to Hybrid Authentication or Modern Authentication please refer to Appendix G Migrating Authentication of Office 365 Backup Set. After the upgrade to AhsayACB v8.3.6.0 or above, the backup and restore process of existing Office 365 backup sets still using Basic Authentication will not be affected during this transition period since Modern Authentication is not yet enforced by Microsoft.

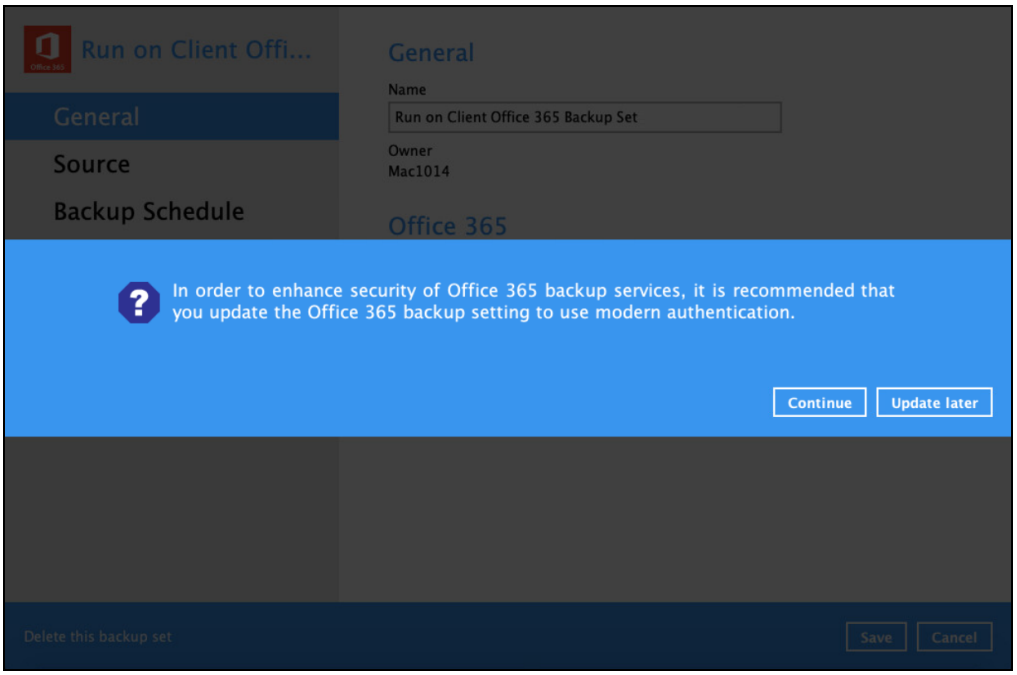
NOTE

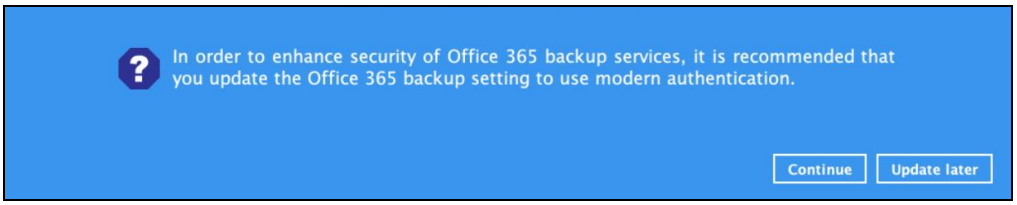
Please note that Modern Authentication with enabled security in Azure Active Directory (AD) will be made default if there is zero-usage on any Office 365 organization by October 2020.

To check the current authentication being used in your Office 365 backup set, see criteria below:

- **Basic Authentication**

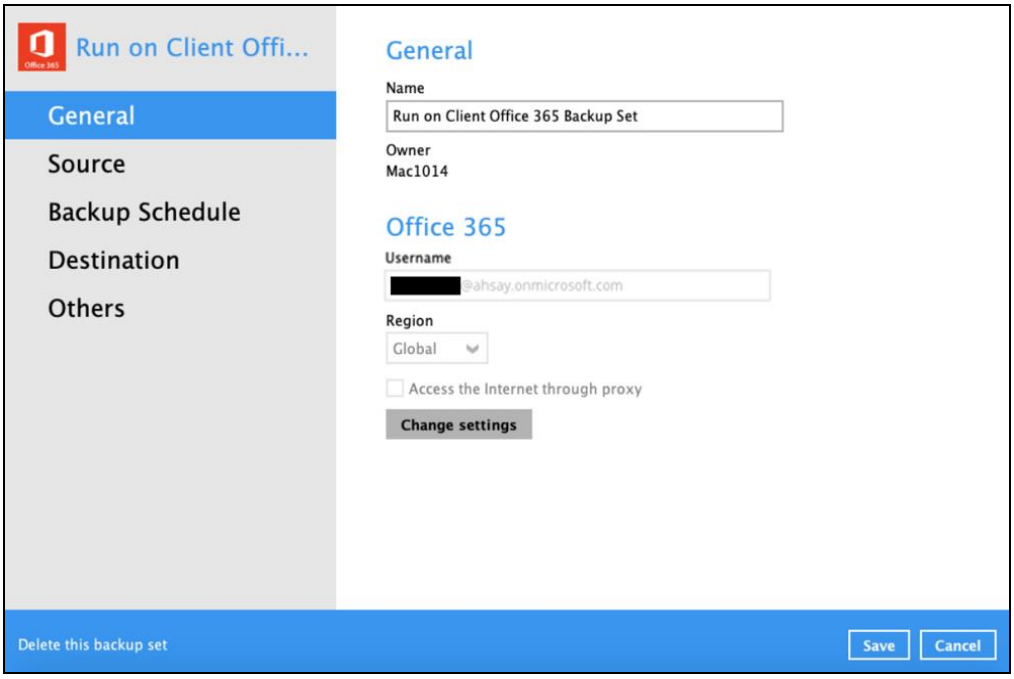
  If you click on the backup set and the following pop-up message is displayed, then the backup set is using Basic Authentication.



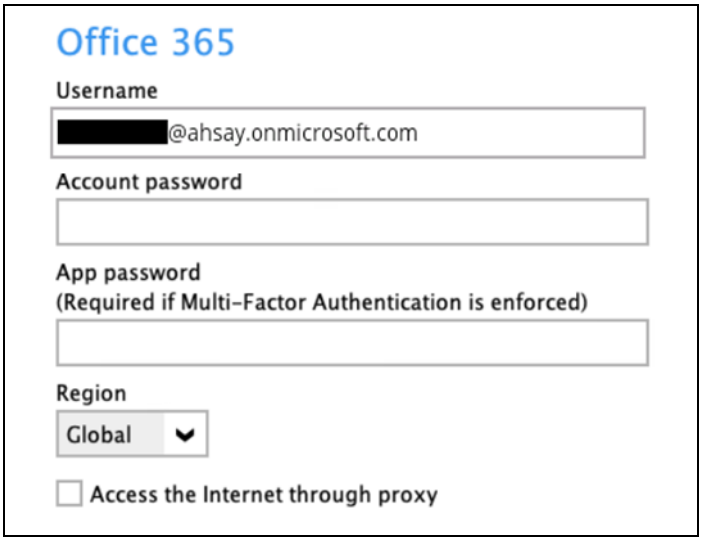


- **Modern Authentication**

Go to **Backup Sets** > **backup set name** > **General** > **Change settings**.

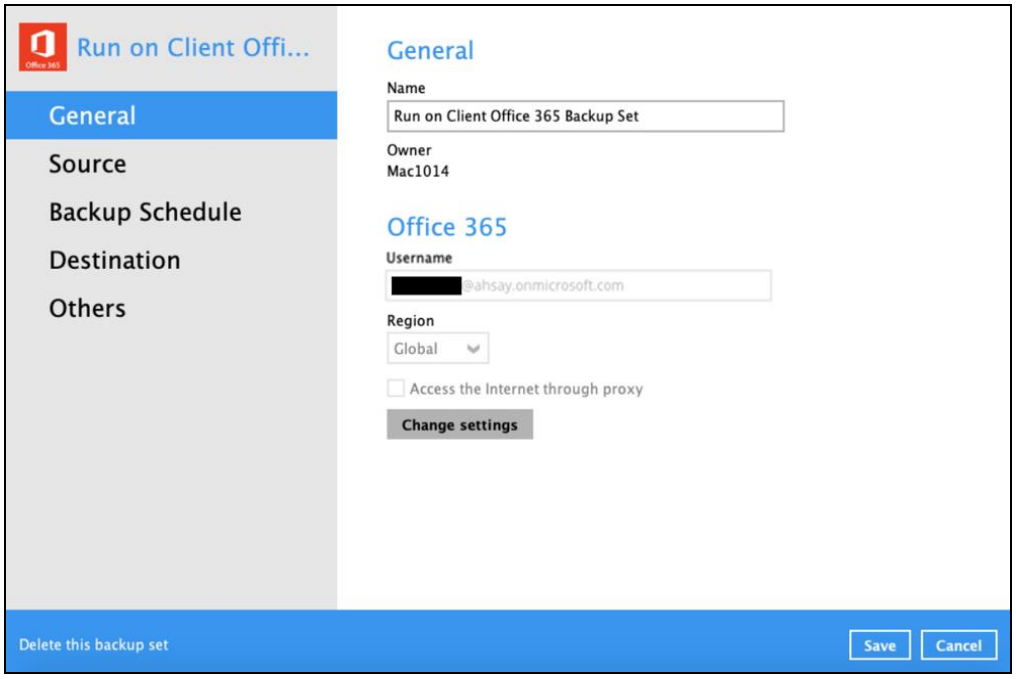


In the Office 365 credentials page, the region is Global and the Username exists but has no password, then the backup set is using Modern Authentication.

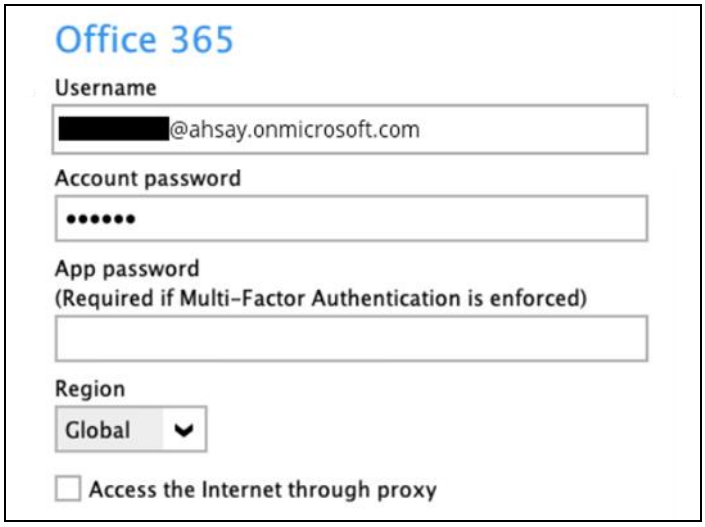


- **Hybrid Authentication**

1. There is no pop up authentication alert.



2. In the Office 365 credentials page, the region is Global and there is a Username and Account password then the backup set is using Hybrid Authentication.

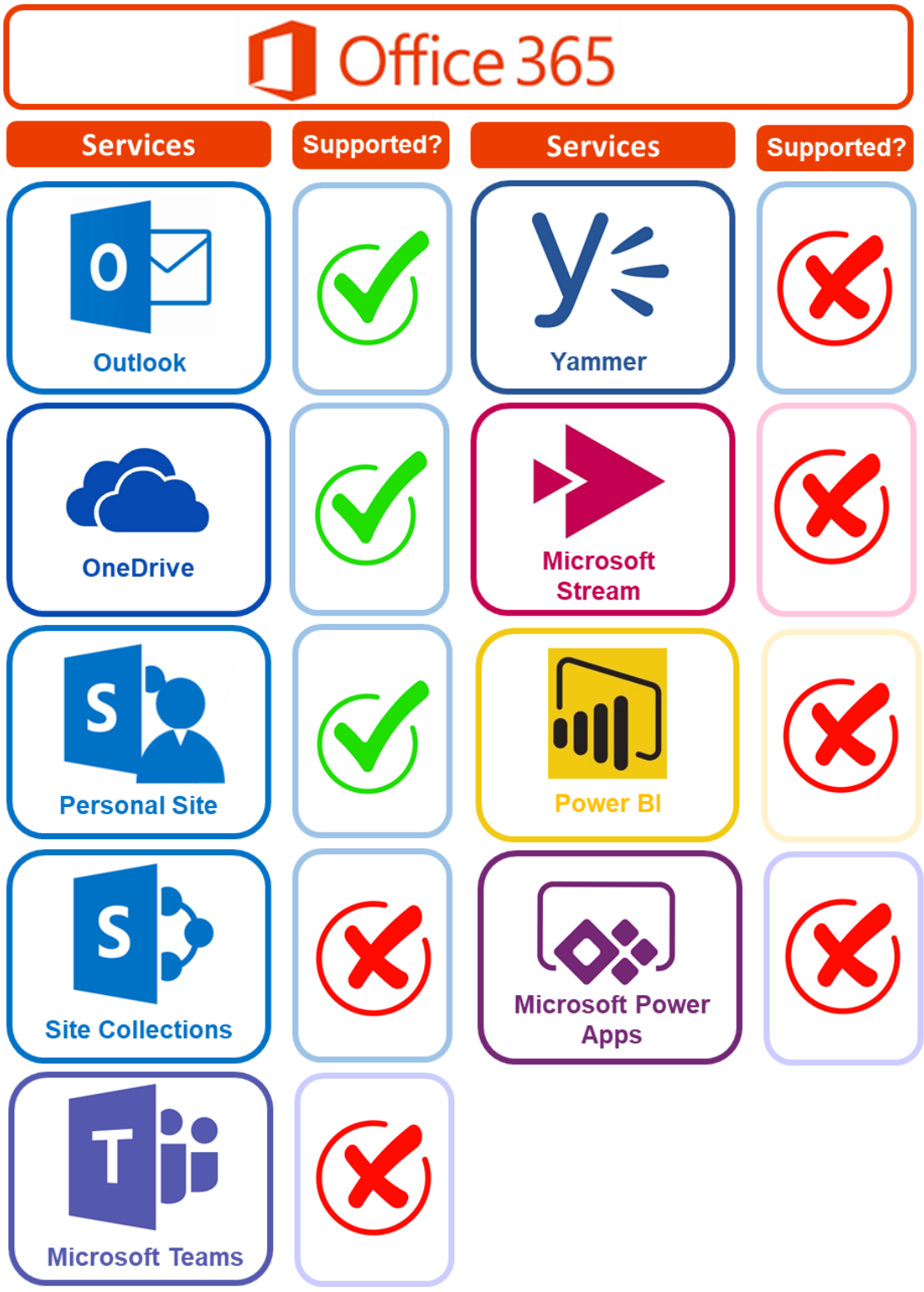


2.15 Supported Services

Below are the supported services of Office 365 Backup module. It is also specified in the table some services that are currently not yet supported by the Office 365 Backup module.

Note: If you wish to backup SharePoint Sites you have to use the AhsayOBM.

Refer to this link for the AhsayOBM v8 User Guide - Office365 Backup & Restore for Mac.

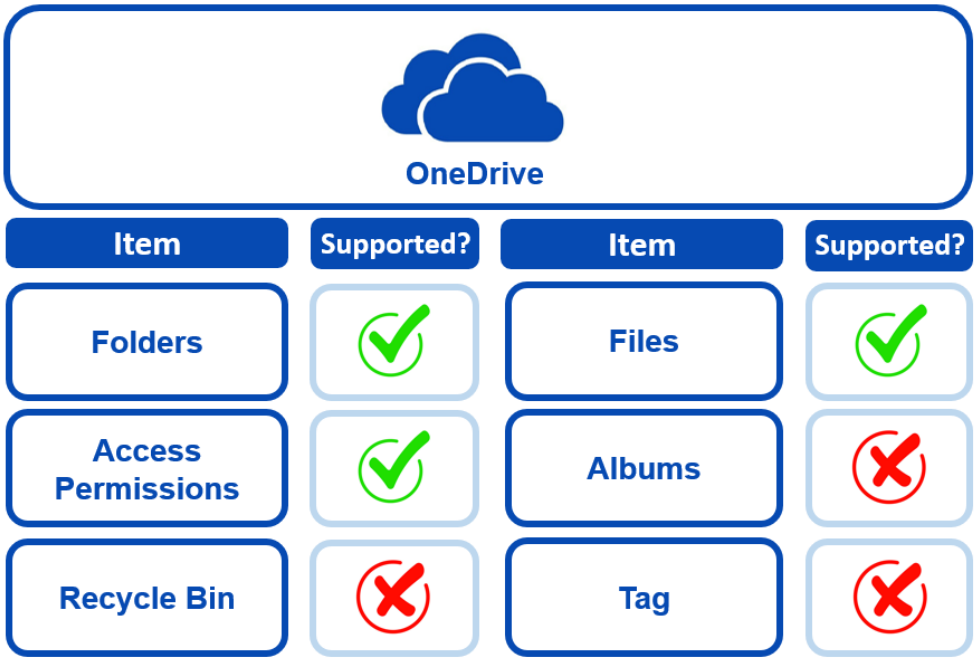


Below are the supported Outlook Mailbox types of Office 365 Backup.

Below are the items that you can backup or restore from an Outlook mailbox.

Item	Supported?	Item	Supported?
Archive	✓	Calendar	✓
Clutter	✓	Companies	✗
Contacts	✓	Conversation History	✗
Deleted Items	✓	Drafts	✓
External Contacts	✗	GAL Contacts	✗
Inbox	✓	Journal	✗
Junk Emails	✓	Notes	✓
Organizational Contacts	✗	Outbox	✗
PeopleCentricConversation Buddies	✗	PersonMetaData	✗
Recipient Cache	✗	RS Feeds	✓
Search Folders	✗	Sent Items	✓
Social Activity Notifications	✗	Sync Issues	✗
Tasks	✓	Trash	✓

Below are the items that you can backup or restore from OneDrive.



Below are the Personal Site items that you can back up or restore from an Office 365 backup set.

Below are the items from the Public Folder that you can backup and restore from an Office 365 backup set.

Public Folders			
Item	Supported?	Item	Supported?
Folders	✓	Files	✓

2.16 Maximum Supported File Size

The following table shows the maximum supported file size per item for backup and restore of each service.

Service	Maximum File Size
Outlook with or without attachments (applies to User mailbox, Room mailbox, Shared mailbox, Equipment mailbox)	150 MB
Public Folders with or without attachments	150 MB
OneDrive	8 GB
Personal Site	8 GB

2.17 Limitations

2.17.1 Ahsay Limitations

- **Supports Backup up to 2 Office 365 User Accounts**

  Each AhsayACB Office 365 backup set is limited to one Office 365 user account. Therefore, when you backup two Office 365 user accounts it will require two separate backup sets.

  Supported backup set configurations:

  Example 1 shows one (1) backup set with one (1) Office 365 user account.

  Example 2 shows two (2) separate backup sets, each with one (1) Office 365 user account

#	Backup Set	Office 365 User Account
1	Sample Backup Set 01	user01@company-office365.com
2	Sample Backup Set 01	user01@company-office365.com
	Sample Backup Set 02	user02@company-office365.com

  Consider using AhsayOBM instead if you wish to back up two or more Office 365 user accounts per backup set.

  Contact your backup service provider for more details and refer to AhsayOBM v8 User Guide - Office365 Backup & Restore for Mac.

- **Modern Authentication**

  - Modern Authentication is only supported for Office 365 account that is registered in Global region and the Office 365 backup is configured to use Global region.
  - Migration to Modern Authentication is not supported on an Office 365 account without a Global Admin role; or during the migration process, the Office 365 account used to authenticate the migration does not have Global Admin role.
  - Due to limitations in Microsoft API, when using Modern Authentication, backup and restore of SharePoint Web Parts and Metadata are not fully supported.
  - Backup sets using Modern Authentication do not support backup of external content types (through the linkage from selected lists).
  - Backup sets using Modern Authentication do not support backup and restore of the following:
    - Some list settings, currently known as Survey Options on survey list.
    - Feature setting for Personal Site.

- **OneDrive**

  - Backup and restore of file share links will be supported for OneDrive and SharePoint Documents only, and only for restore to the same Office 365 organization.
  - Backup and restore of all versions will be supported for **OneDrive and SharePoint Documents** only, except for ".aspx" files.

- **Outlook**
  - For Outlook mail item, after using restore to original location to overwrite a mail item (and hence id of the mail id is changed), then

    In the backup source tree of the same backup set:
    - the original ticked item still uses the old mail id to reference and becomes red item.
    - there is another item (with the latest mail id) created for that mail item
  - User will need to deselect the red item and tick the mail item again in the backup source tree in order to do the next backup properly. As per development team, the issue will not be handled as user's selected source should not be modified by system.

2.17.2 Microsoft Limitations

- **OneDrive**

  For more detailed information on the limitations of OneDrive, please refer to this Microsoft article, OneDrive Limits. These are some of the limitations that will be discussed in the OneDrive Limits article:
  - File upload size which is 15GB for OneDrive
  - File name and path lengths
  - Thumbnails and previews
  - Number of items to be synced
  - Information rights management
  - Differential sync
  - Libraries with specific columns
  - Windows specific limitations

2.18 Best Practices and Recommendations

The following are some best practices or recommendations we strongly recommend you follow before you start any Office 365 backup and restore.

- **Temporary Directory Folder Location (For backup and restore running on AhsayACB only)**

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

- **Performance Recommendations**

  Consider the following best practices for optimized performance of the backup operations:

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

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

- **Set Backup Destination**

  After creating the backup set-in Run-on **Client** mode on AhsayCBS user web console, please remember to login AhsayACB to set the backup destination if you want the backup destination to be Local/ Mapped Drive/ Removable Drive.

- **Backup Destination**

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

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

- **Login AhsayACB**

  After modifying the backup schedule of the **Run-on Client** backup set on AhsayCBS user web console, please remember to login to the AhsayACB client once to synchronize the changes immediately.

- **Periodic Backup Schedule**

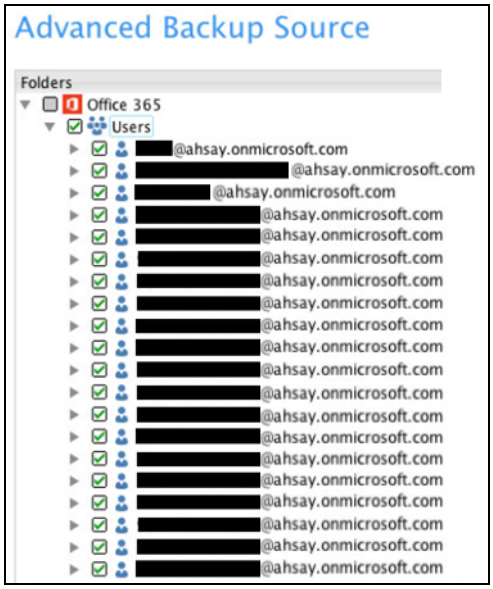
  Consider the following key points to efficiently handle backup sets with periodic backup schedule.

  - 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.

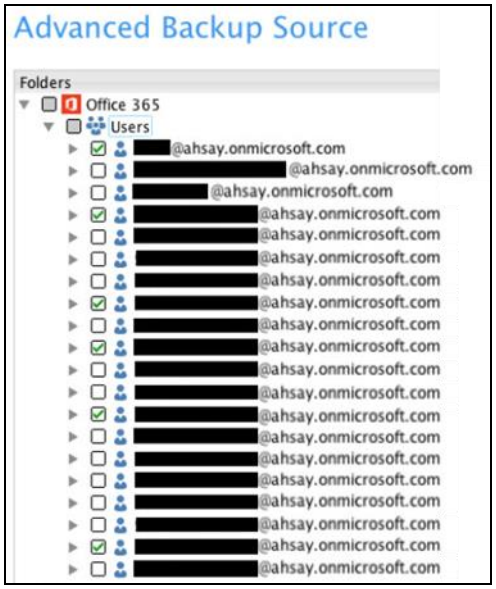
- **Backup Source**

  For Office 365 backup sets there are two approaches for backup source selection. Below are the sample screenshots of the selection All Items and Selective Items.

  All Items

  Selective Items

  - **All Items**

    If you tick the "Users" checkbox, all of the Items of the Office 365 user account will automatically be selected.

  - **Selective Items**

    If you tick selective Items from Outlook or OneDrive, you will notice that the "Users" checkbox is highlighted with gray color. This indicates that not all the users are selected.

  These are the Pros and Cons when selecting a backup source from All Items and Selective Items.

	All Items	Selective Items
User Maintenance	The Admin does not need to manage the backup set, i.e. to select or unselect items, the changes are automatically updated in the backup source	The Admin will have to select or unselect items manually as the changes are not automatically updated in the backup source.
Backup Time	All Items of the Office 365 user account will be backed up. This means the initial of full backup job will take longer, any subsequent incremental backup will take longer.	Only selective Items of the Office 365 user account will be backed up. This will mean the initial of full backup job will be faster, any subsequent incremental backup will be faster.
Storage	As all Items of the Office 365 user account are backed up, more storage will be required.	As only selective Office 365 user accounts will be backed up, the backup set will require relatively less storage.

- **Authentication**

Although Microsoft has moved the enforcement date for Modern Authentication from end of 2020 to the second half of 2021, since this new authentication is already available starting with AhsayACB v8.3.6.0 or above, it is recommended that backup sets are migrated to Modern Authentication. All newly created Office 365 backup sets on AhsayACB v8.3.6.0 or above automatically use Modern Authentication.

However, due to the current limitation with Microsoft API, Modern Authentication is currently not suitable for backup sets with Personal Sites selected. As a temporary workaround for Office 365 backup sets which require backup of Personal Sites selected, the backup set should be migrated to Hybrid Authentication until the issue has been resolved by Microsoft.

3 Logging in to AhsayACB

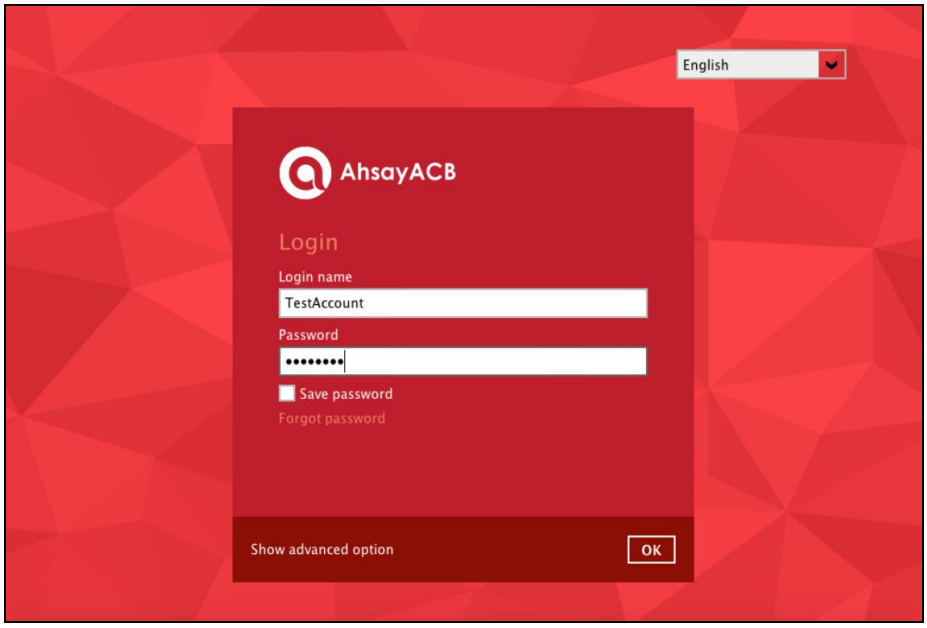
Starting with AhsayACB v8.5.0.0, there are several login scenarios depending on the setting of the account you are using. The different scenarios will be discussed below:

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

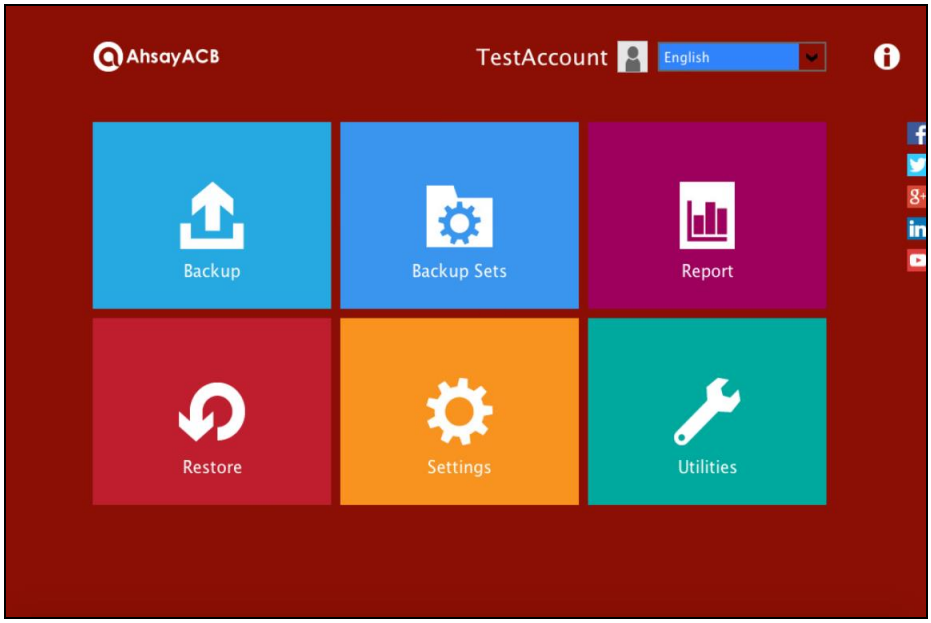
3.1 Login to AhsayACB without 2FA

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

2. Enter the **Login name** and **Password** of your AhsayACB account then click **OK** to log in.



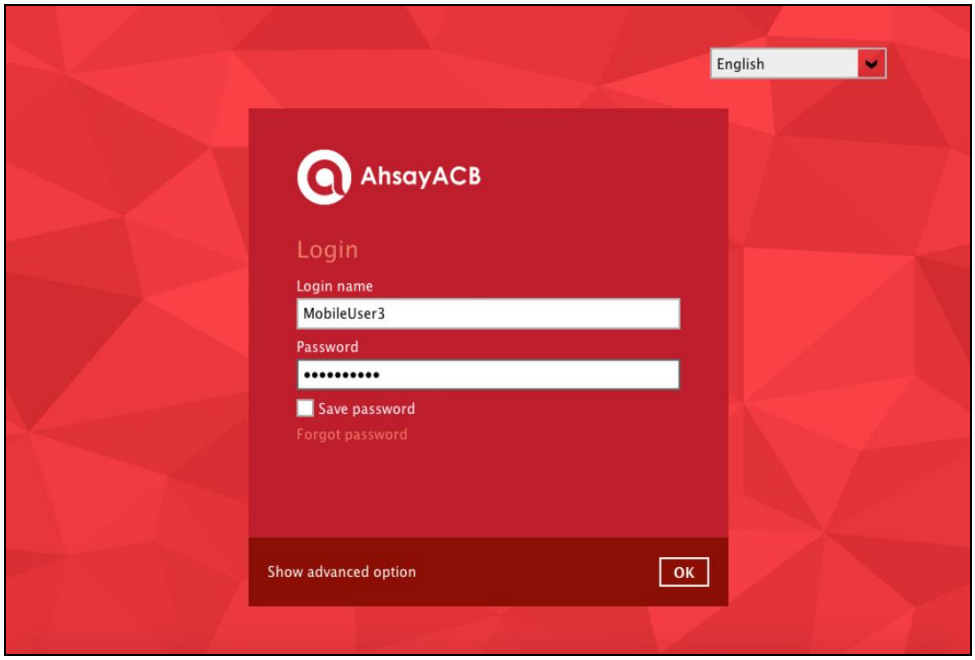
3. After successful login, the following screen will appear.



3.2 Login to AhsayACB with 2FA using authenticator app

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

2. Enter the **Login name** and **Password** of your AhsayACB account then click **OK** to log in.



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

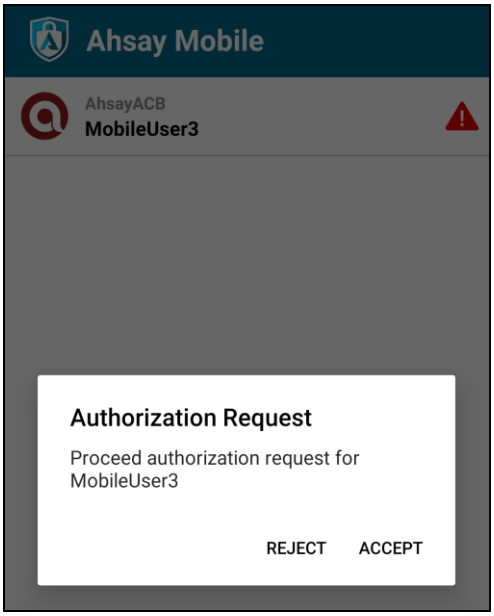
   - Push Notification and TOTP when using Ahsay Mobile app
   - TOTP only

   ➢ 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.

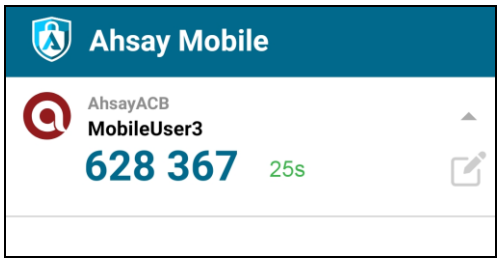
Example of the login request sent to the Ahsay Mobile app.



- 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.

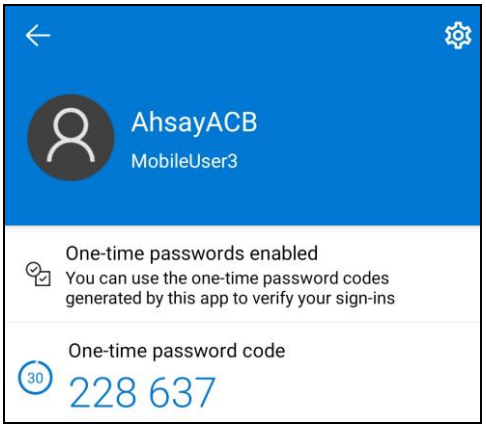
Example of the one-time password generated in the Ahsay Mobile app.



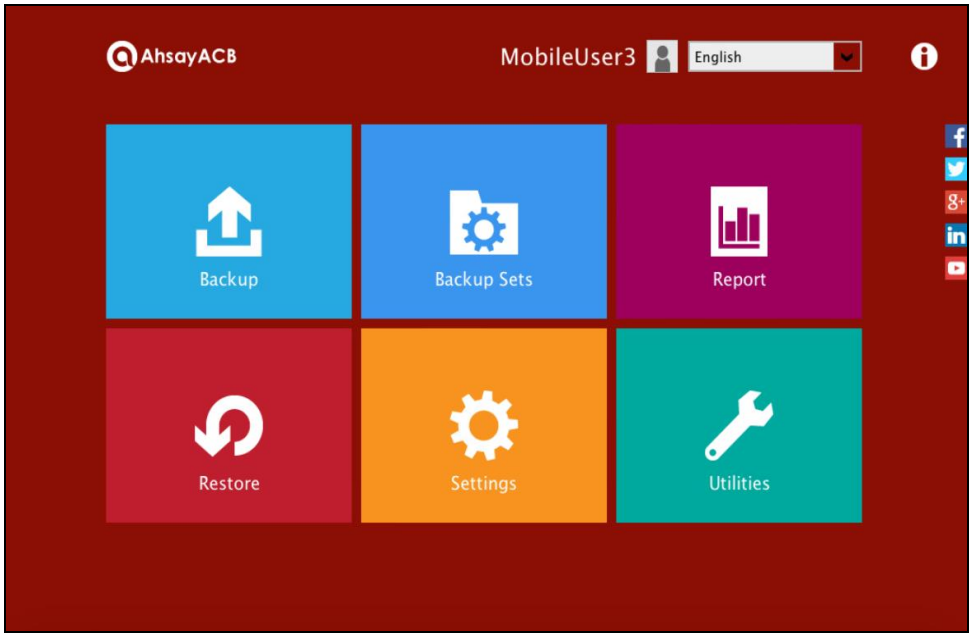
➢ TOTP only

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.



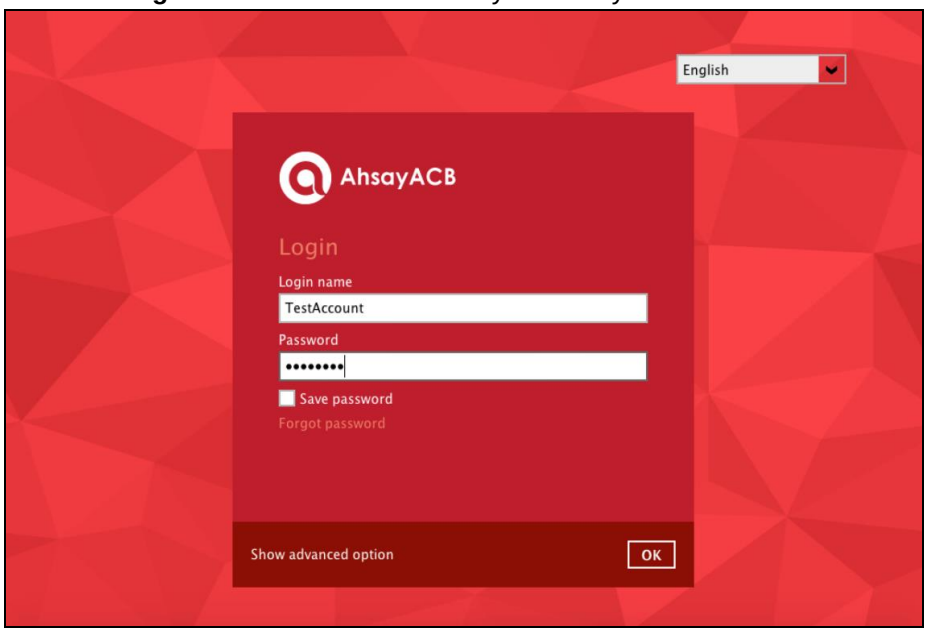
NOTE

If you have trouble logging in using the authenticator app, please refer to Chapter 8 of the AhsayACB Quick Start Guide for Mac for more information.

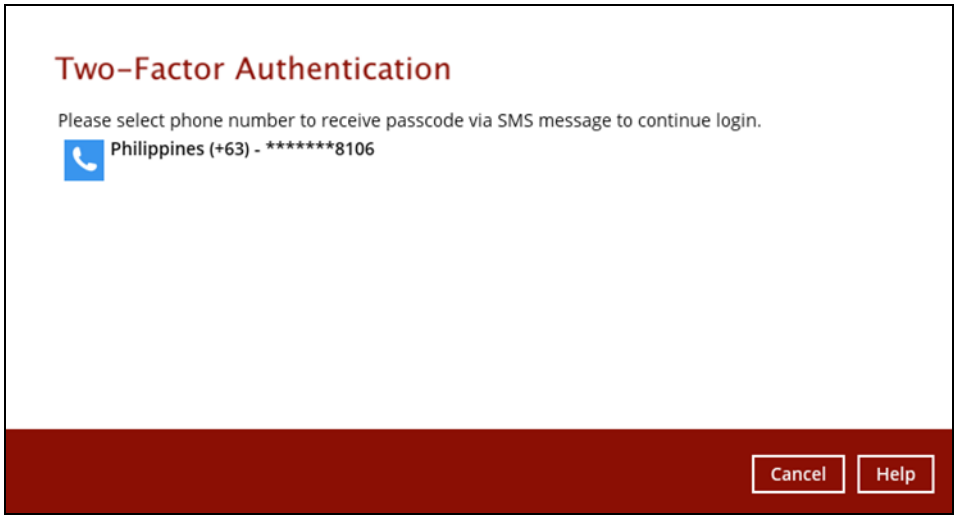
3.3 Login to AhsayACB with 2FA using Twilio

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

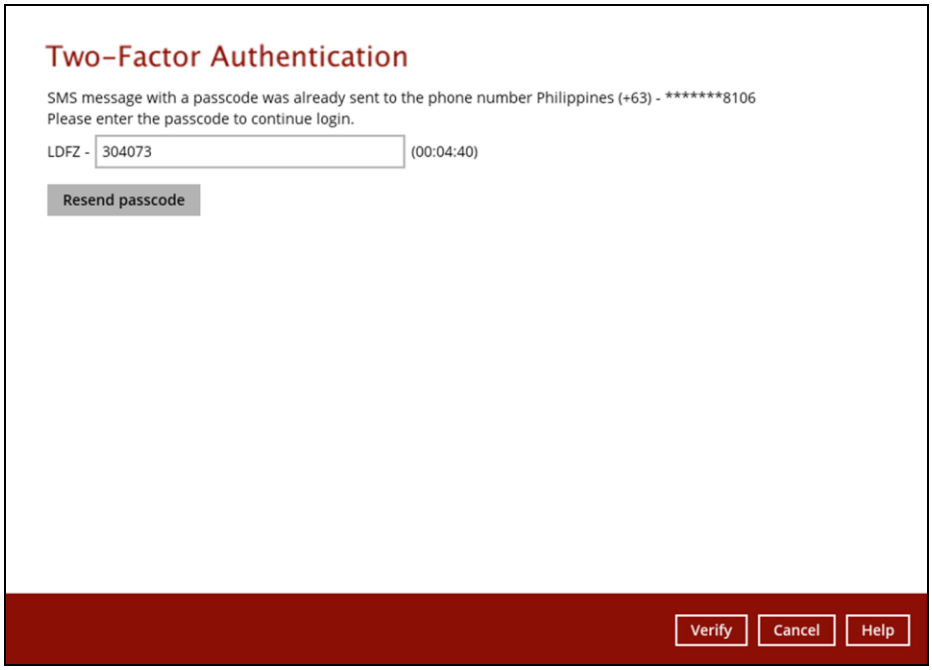
2. Enter the **Login name** and **Password** of your AhsayACB account then click **OK** to log in.



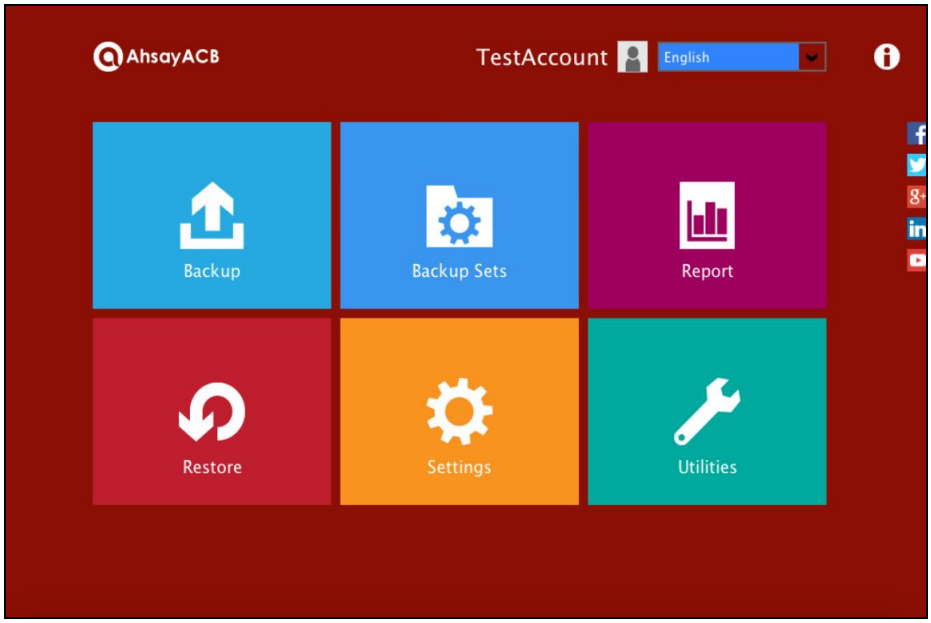
3. Select your phone number.



4. Enter the passcode and click **Verify** to log in.



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

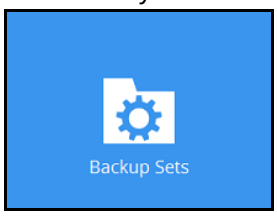


4 Creating an Office 365 Backup Set

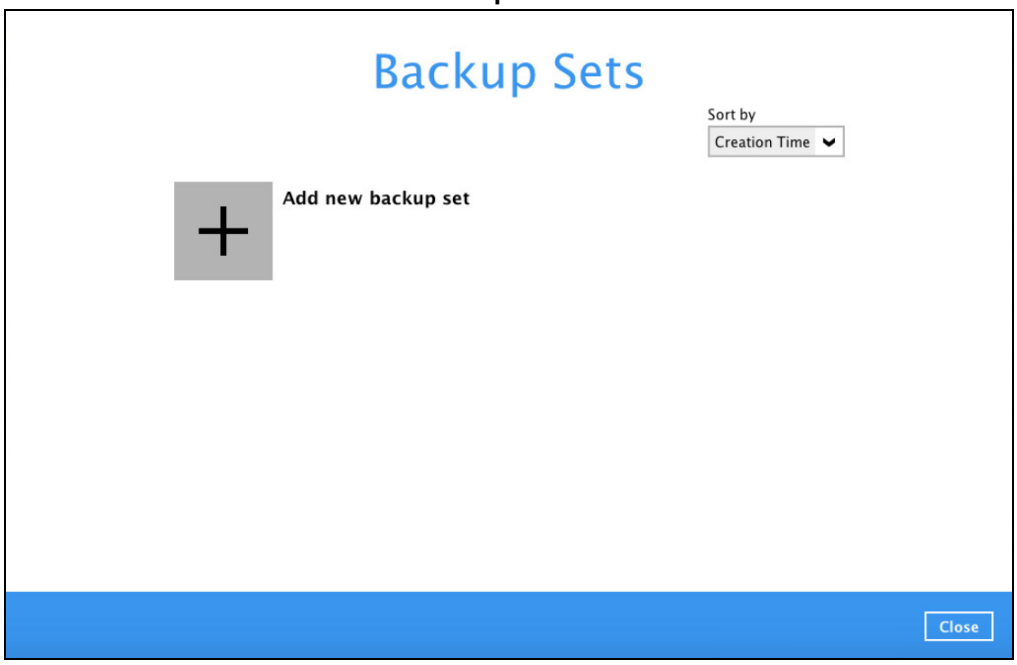
Starting with AhsayACB v8.3.6.0, Basic Authentication will not be utilized anymore, but instead there are two types of authentication that can be used in creating a backup set namely Modern Authentication or Hybrid Authentication.

4.1 Modern Authentication

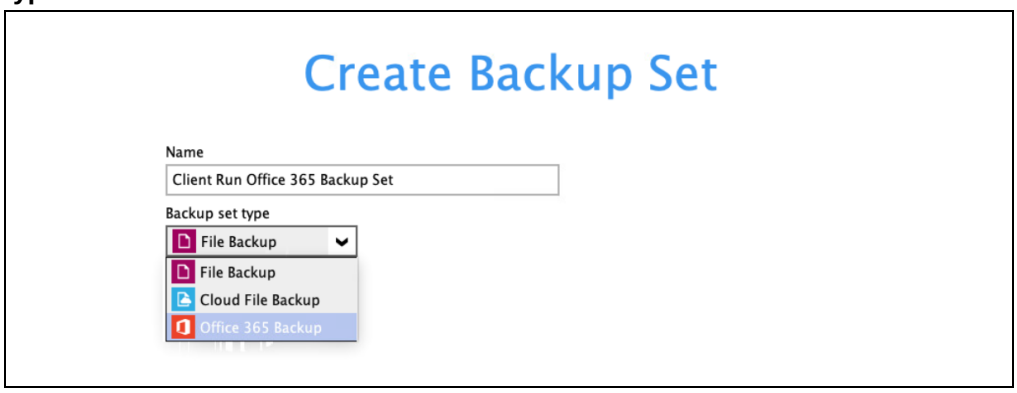
1. In the AhsayACB main interface, click **Backup Sets**.



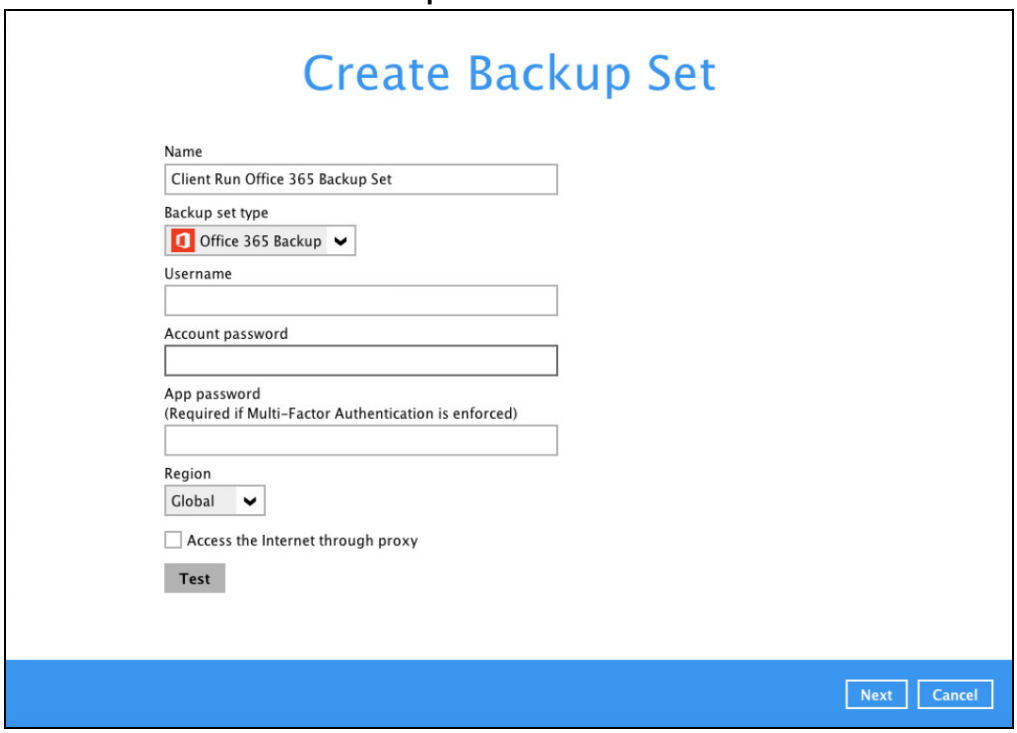
2. Click the "**+**" icon next to **Add new backup set**.



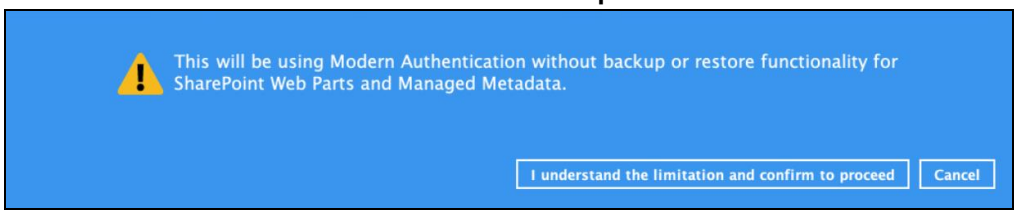
3. Enter a **Name** for your backup set and select **Office 365 Backup** as the **Backup set type**.



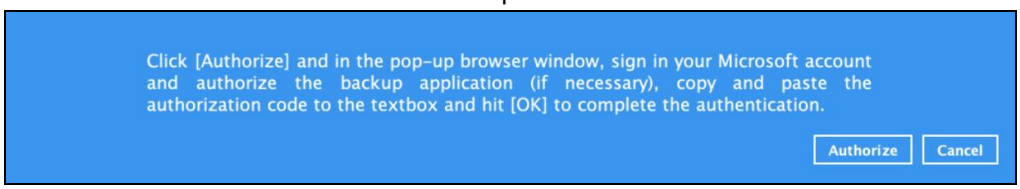
Leave the **Username** and **Account password** blank and click **Test**.



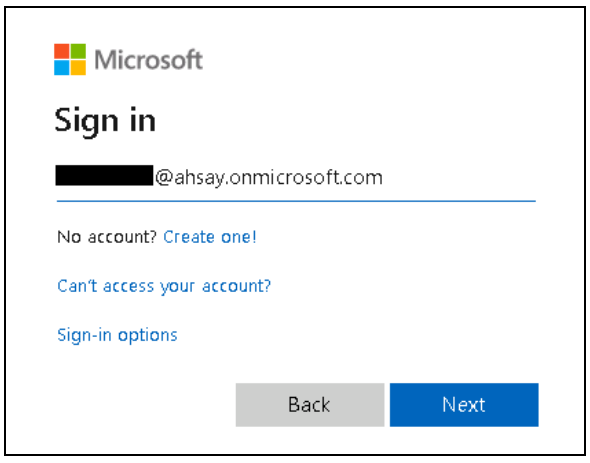
Click **I understand the limitation and confirm to proceed**.

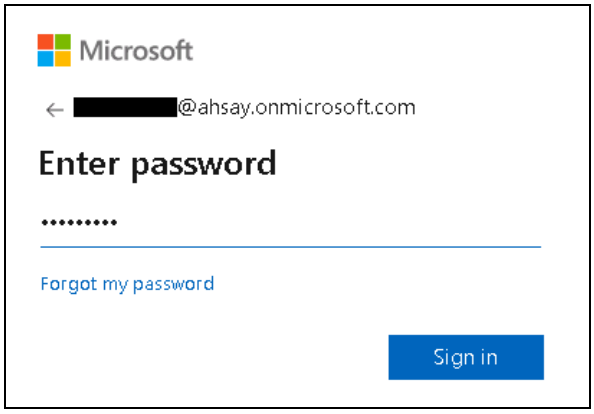


Click **Authorize** to start the authentication process.

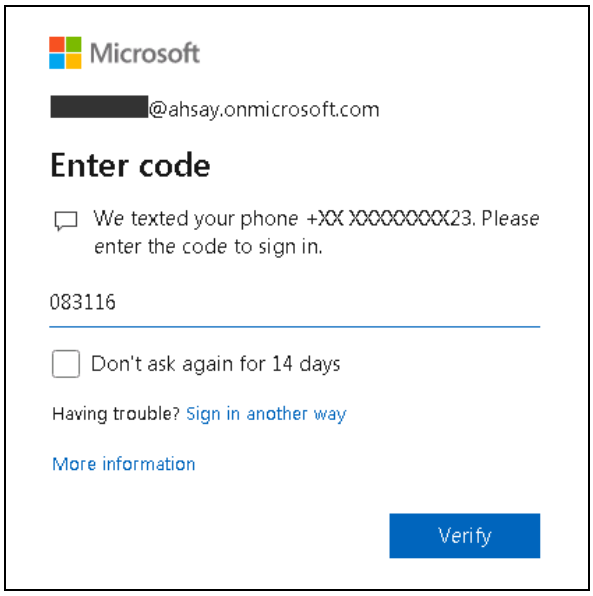


Sign in to your Microsoft account.





If MFA is enforced for the Office 365 user account used to authenticate the backup set, enter the code and click **Verify**.



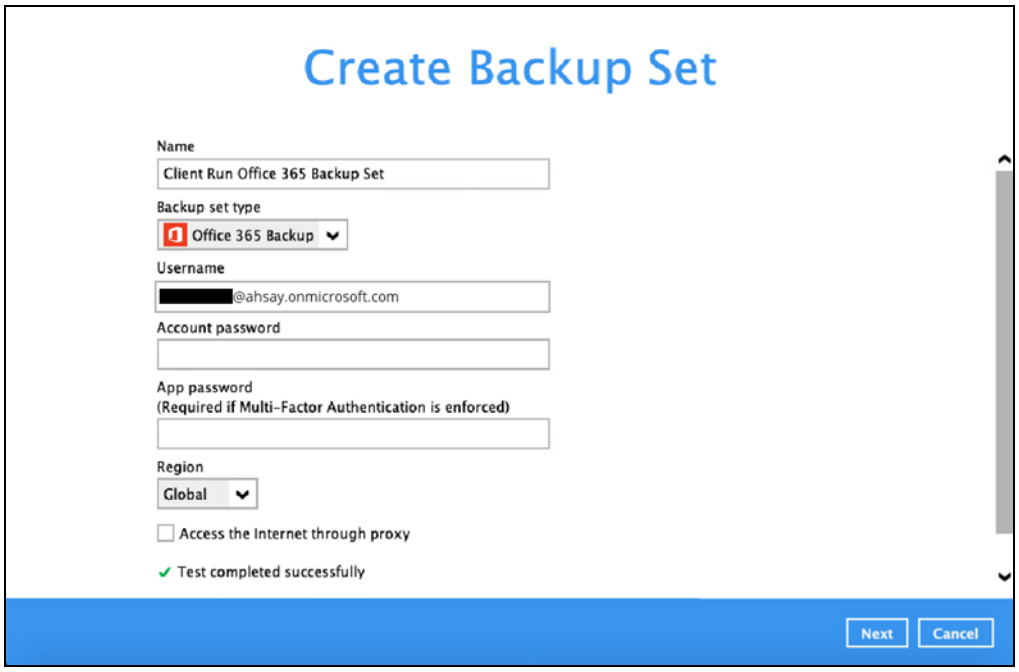
NOTE

The verification code is only required if the MFA status of an Office 365 account is enforced.

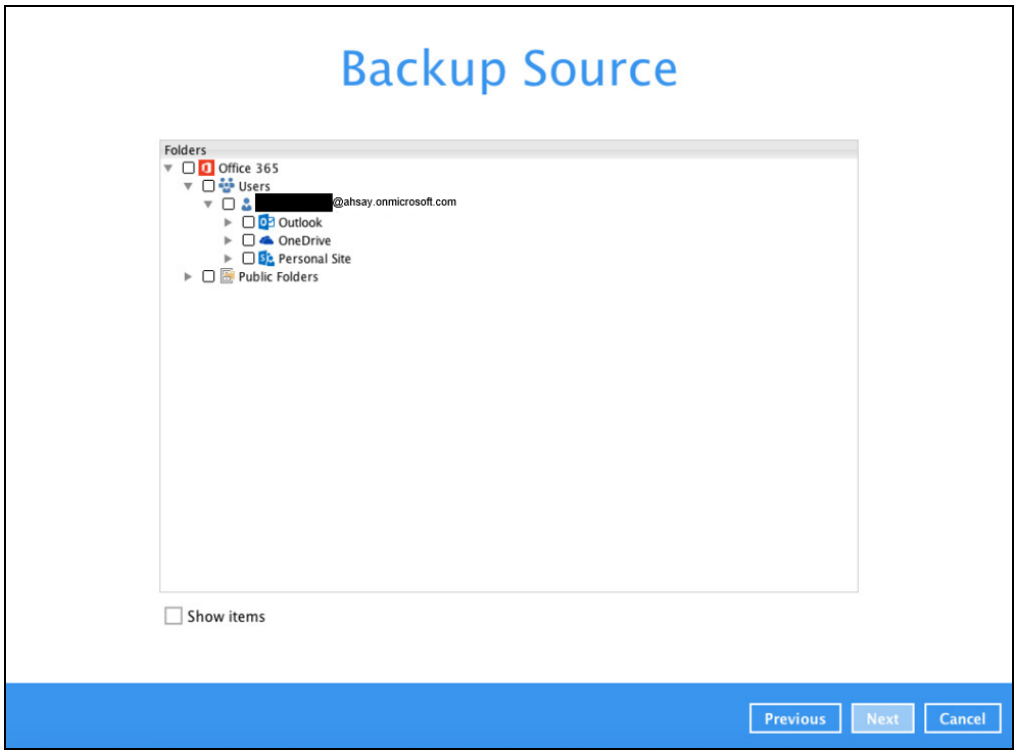
Copy the authorization code.

Go back to AhsayACB and paste the authorization code. Click **OK** to proceed.

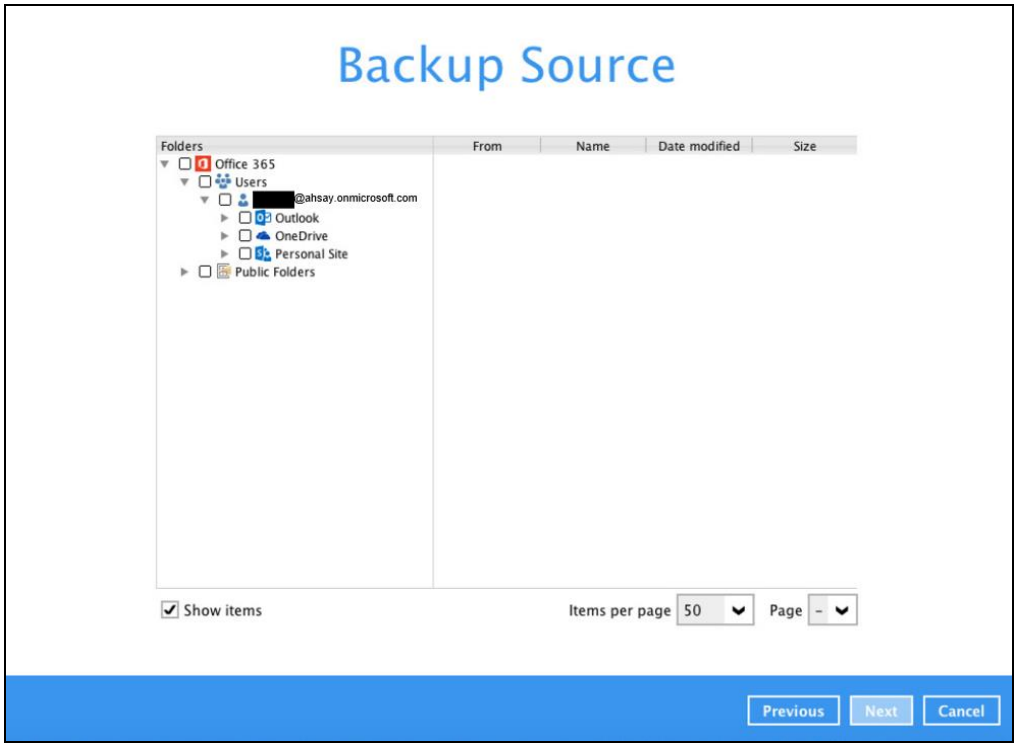
Test completed successfully shows when the validation is successful. Press **Next** to proceed to the next step.



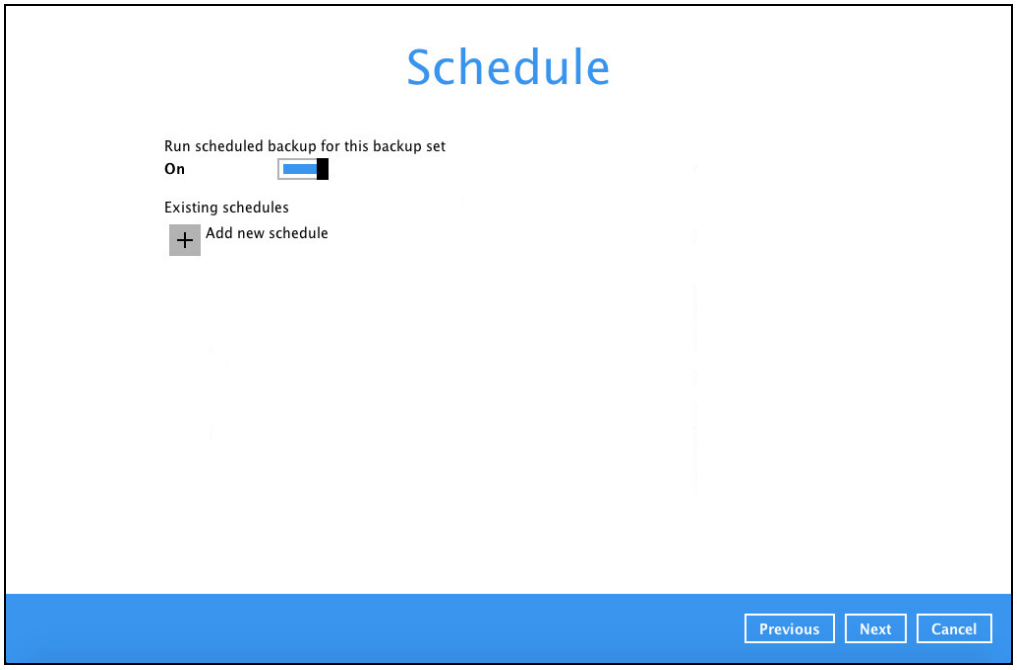
4. In the **Backup Source** menu, select the desired user account and content folder for backup.

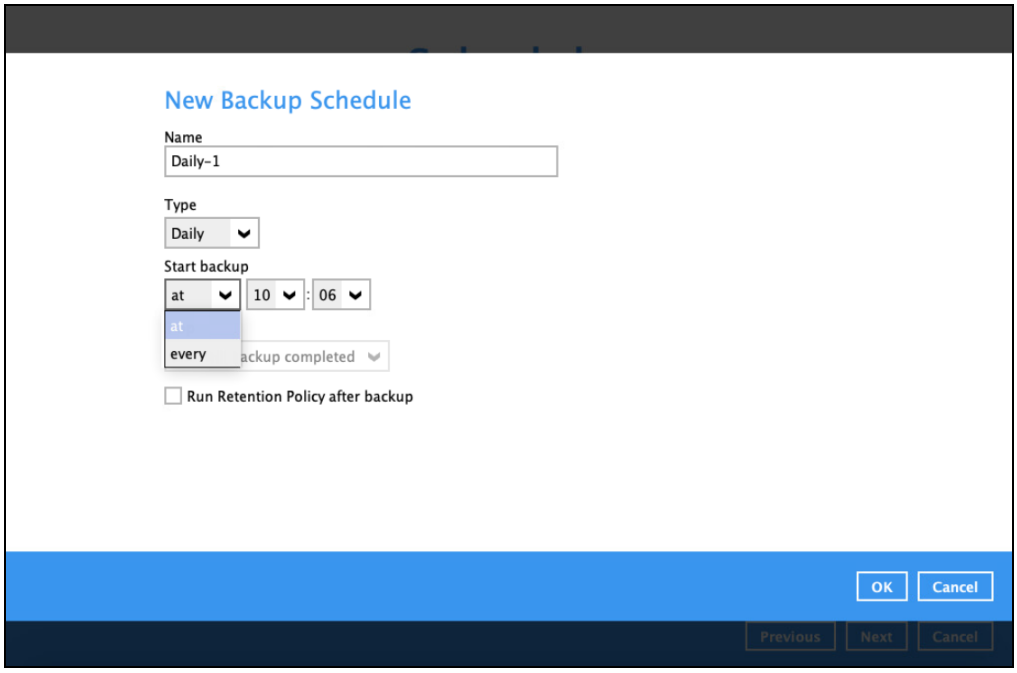


Enable the **Show items** checkbox at the bottom left corner if you would like to choose individual items for backup.



5. In the Schedule menu, configure a backup schedule for backup job to run automatically at your specified time interval. Slide the on/off button to turn on this feature, then click **Add new schedule** to add a new schedule, then click **Next** to proceed afterward.

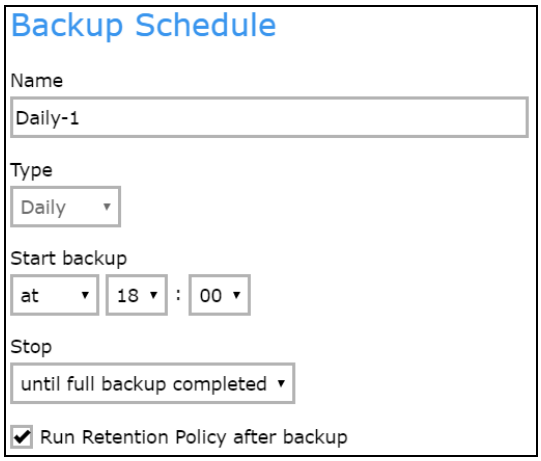




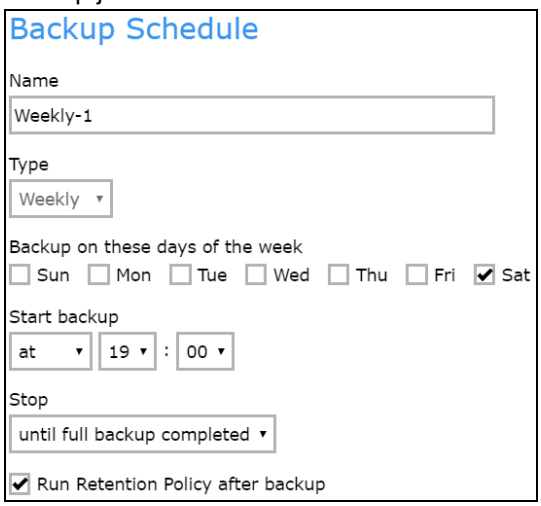
In the New Backup Schedule window, configure the following backup schedule settings.

- **Name** – the name of the backup schedule.
- **Type** – the type of the backup schedule. There are four (4) different types of backup schedule: Daily, Weekly, Monthly and Custom.

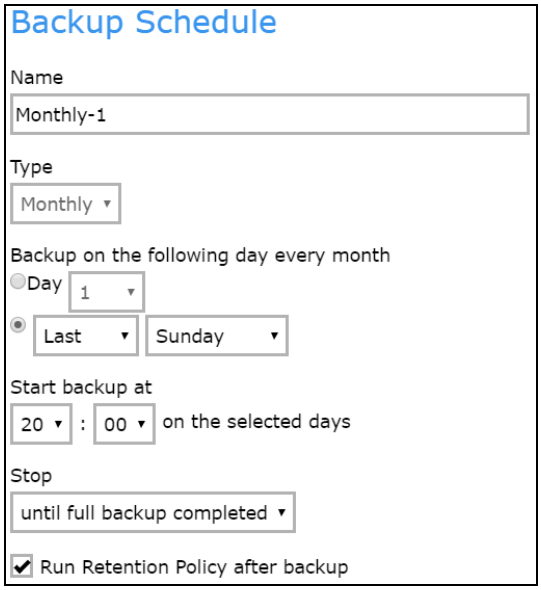
- **Daily** – the time of the day when the backup job will run.



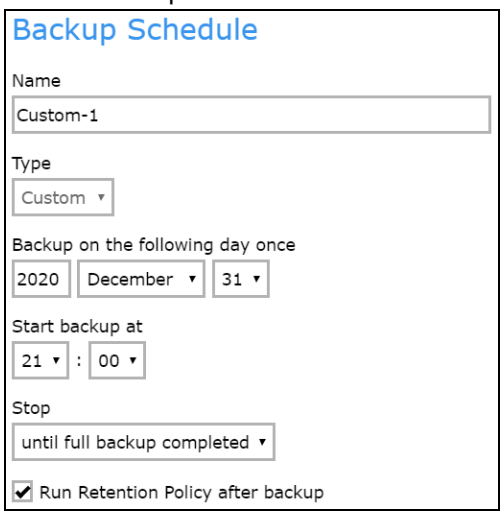
- **Weekly** – the day of the week and the time of the day when the backup job will run.



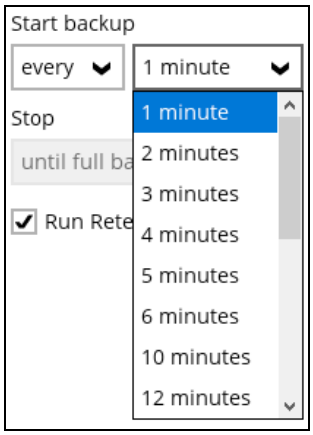
- **Monthly** – the day of the month and the time of the day when the backup job will run.

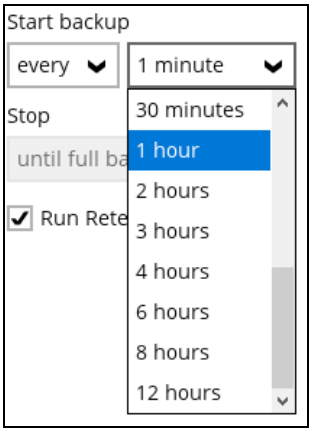


- **Custom** – a specific date and the time when the backup job will run.



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





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

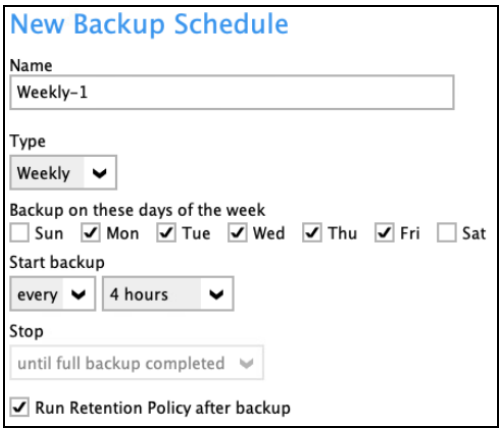


Figure 1.1

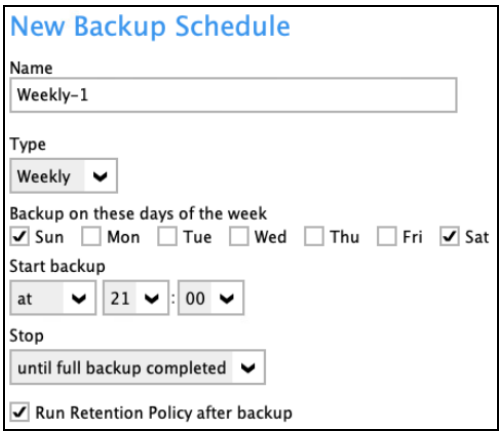


Figure 1.2

Figure 1.1 – Periodic scheduled every 4 hours Monday - Friday for business hours

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

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

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

  For example, if a backup set 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.

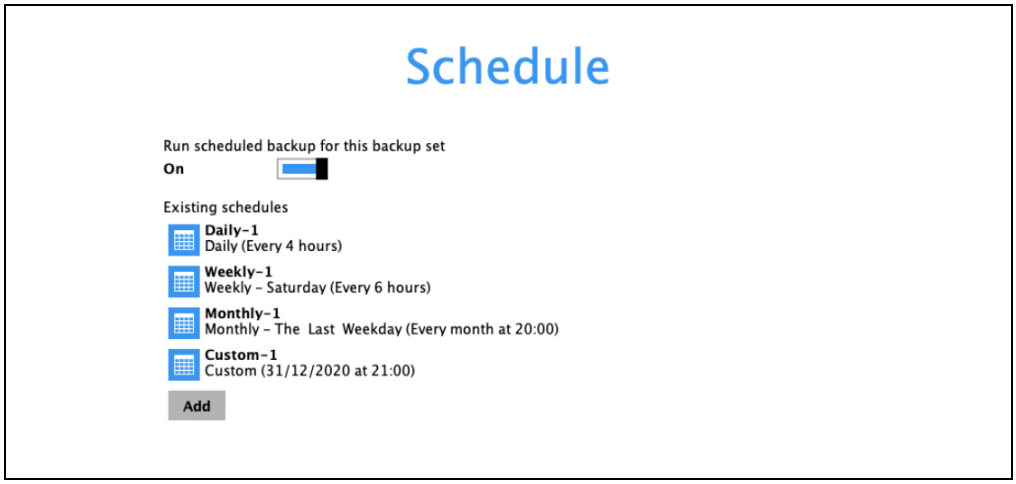
  The partially backed up data will have to be removed by running the data integrity check.

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

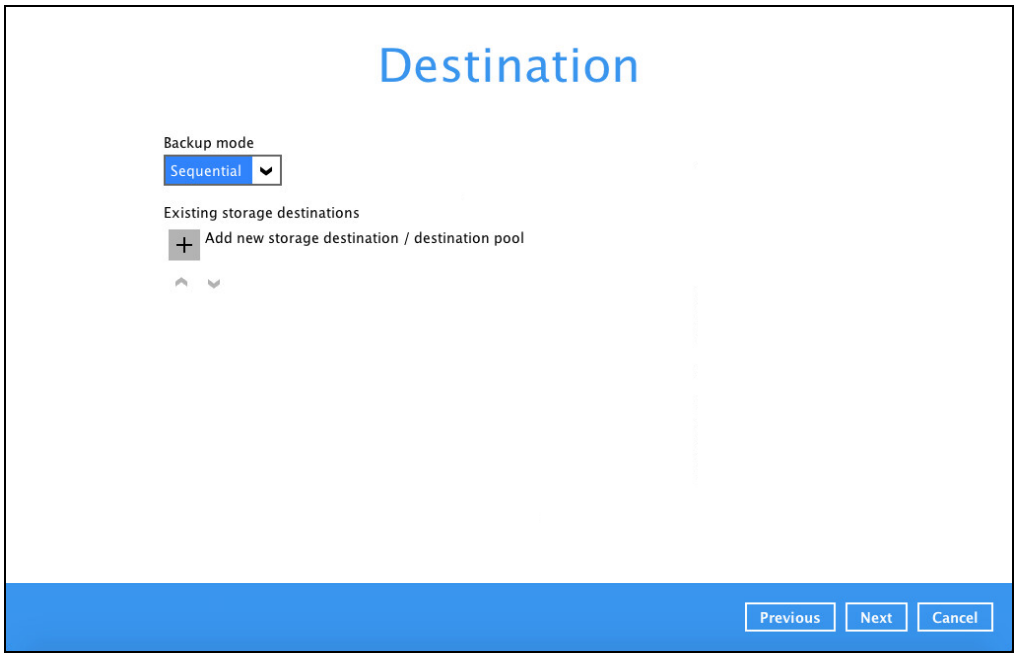
- **Run Retention Policy after backup** – if enabled, the AhsayACB will run a retention policy job to remove files from the backup destination(s) which have exceeded the retention policy after performing a backup job.

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

Click the [Save] button to save settings and multiple backup schedules can be created.



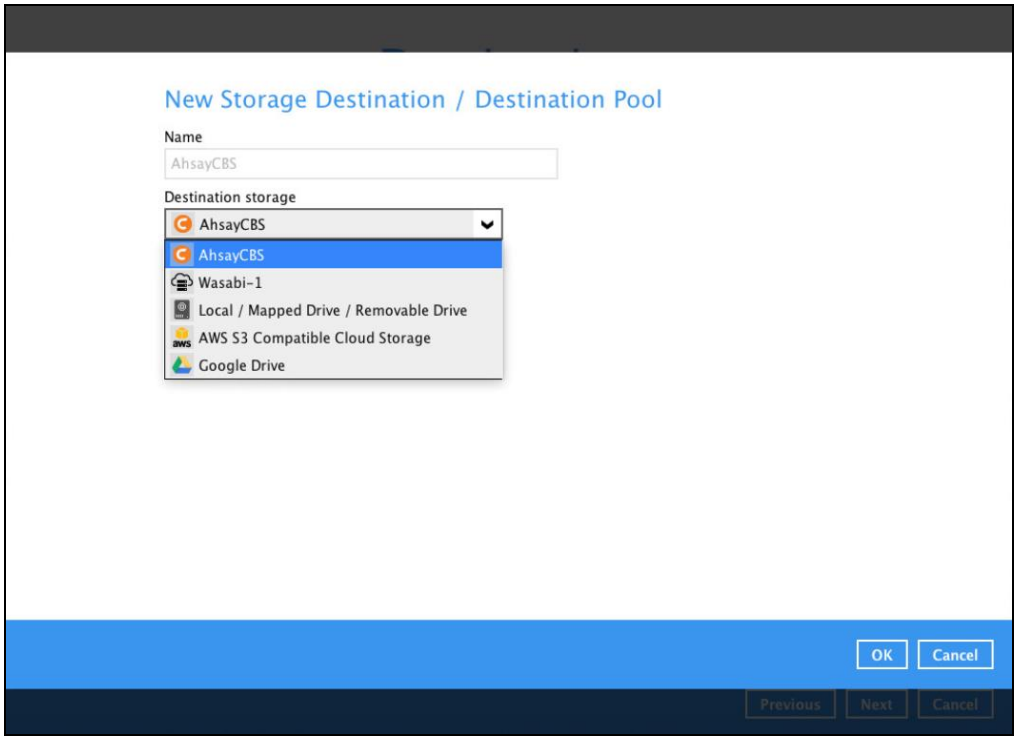
6. In the **Destination** menu, select a backup destination where the backup data will be stored. Click the "**+**" icon next to **Add new storage destination / destination pool**.



NOTE

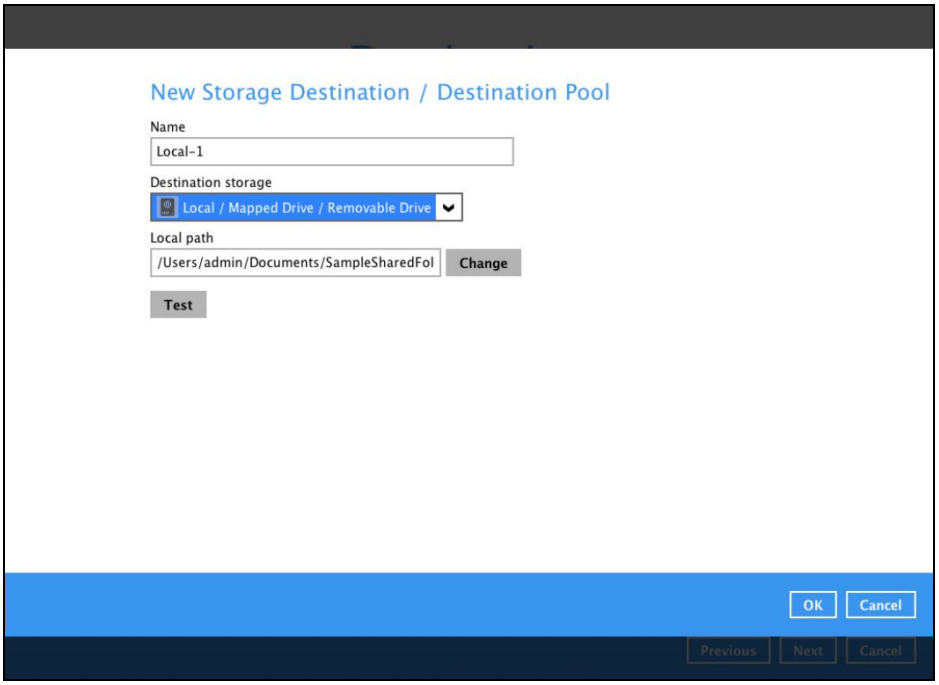
For more details on Backup Destination, refer to the following Wiki article for details:
http://wiki.ahsay.com/doku.php?id=public:8002_faq:faq_on_backup_destination

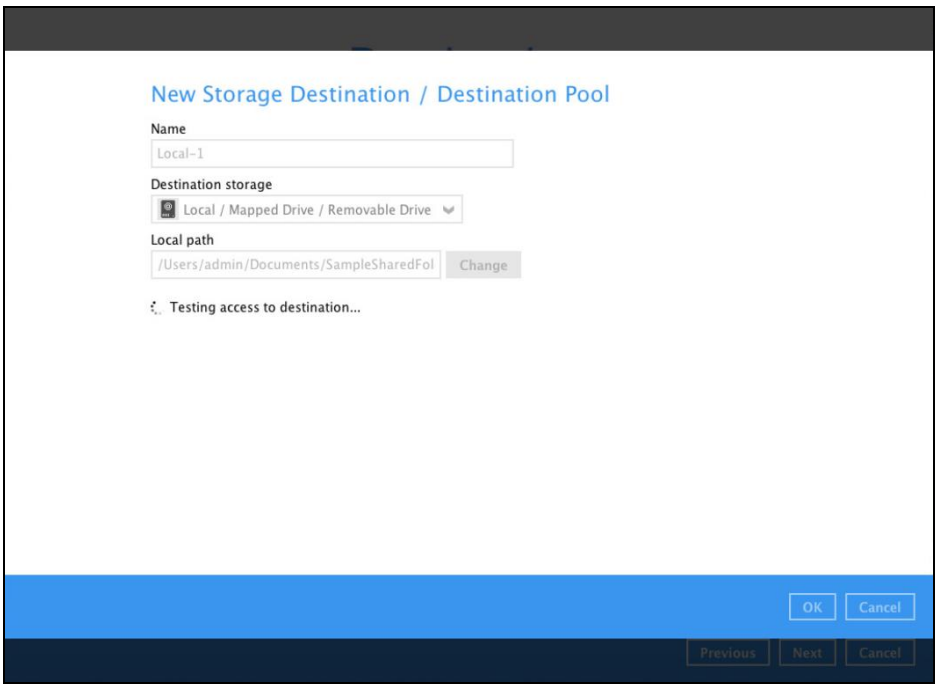
Select storage destinations.

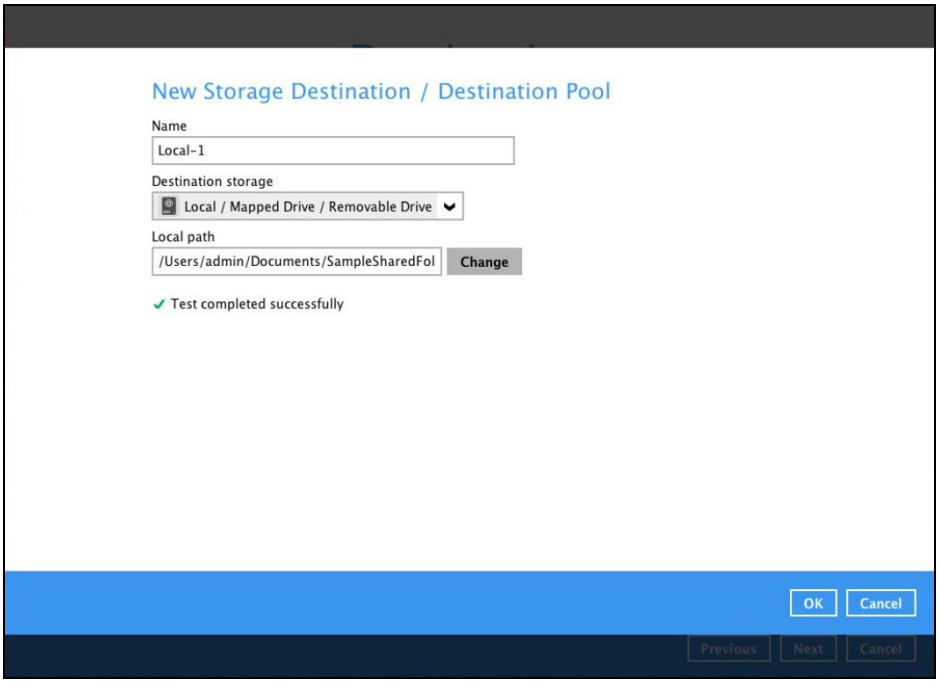


You can choose a storage combination of the Local/Mapped drive/Removable Drive or Cloud storage. Click **OK** to proceed when you are done with the settings.

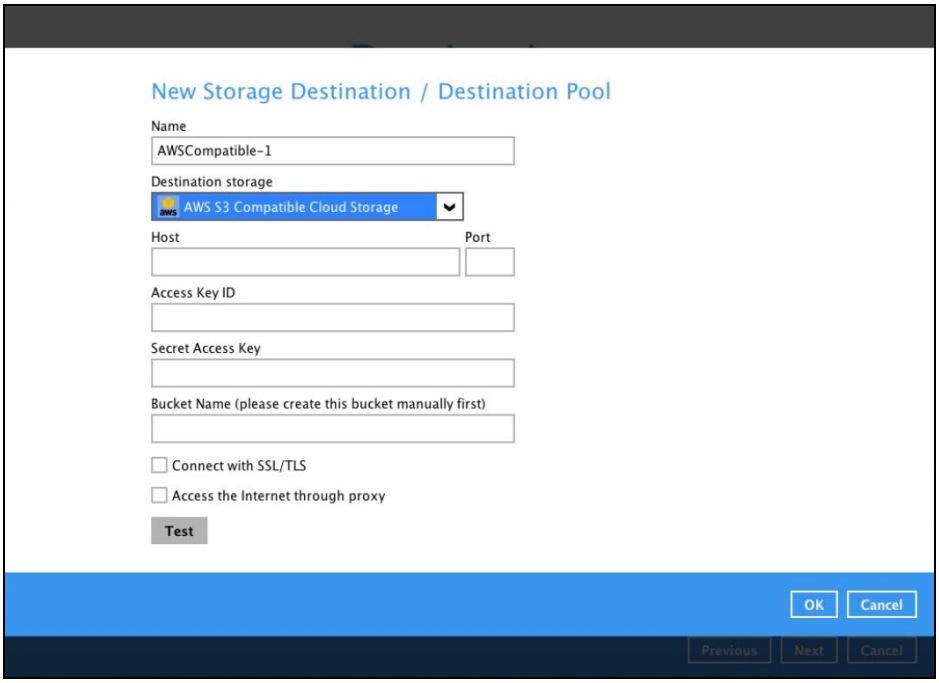
- If you have chosen the **Local / Mapped Drive / Removable Drive** option, click **Change** to browse to a directory path where backup data will be stored, then click **Test** to validate the path. **Test completed successfully** shows when the validation is done.

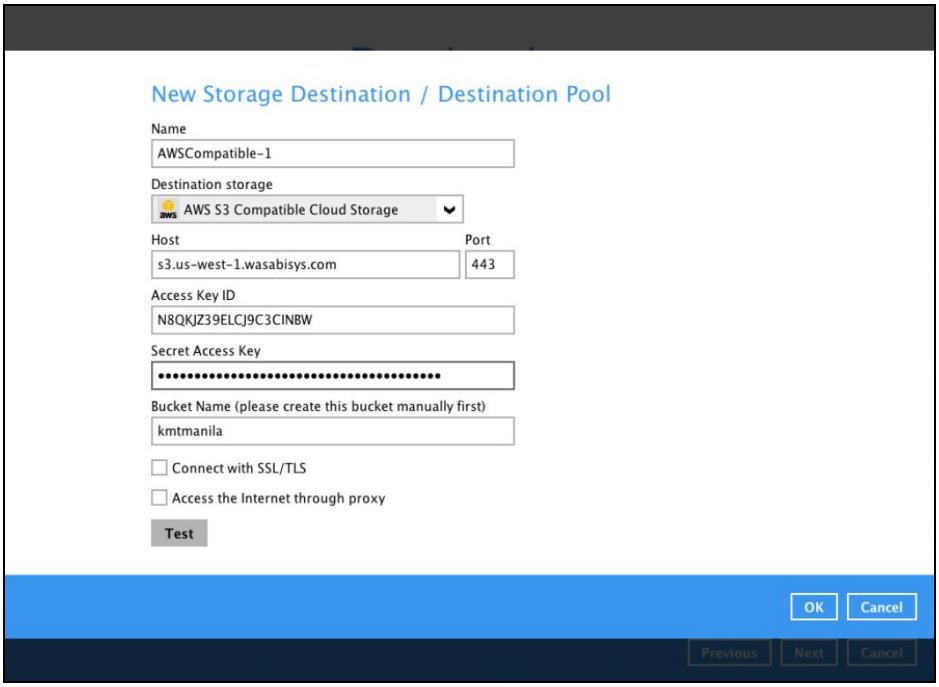


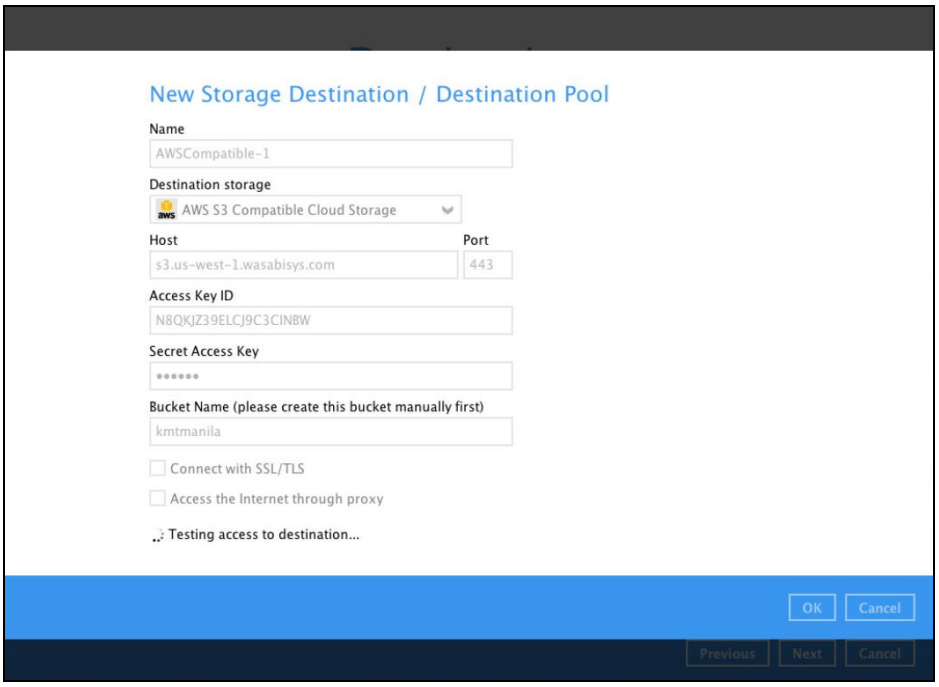


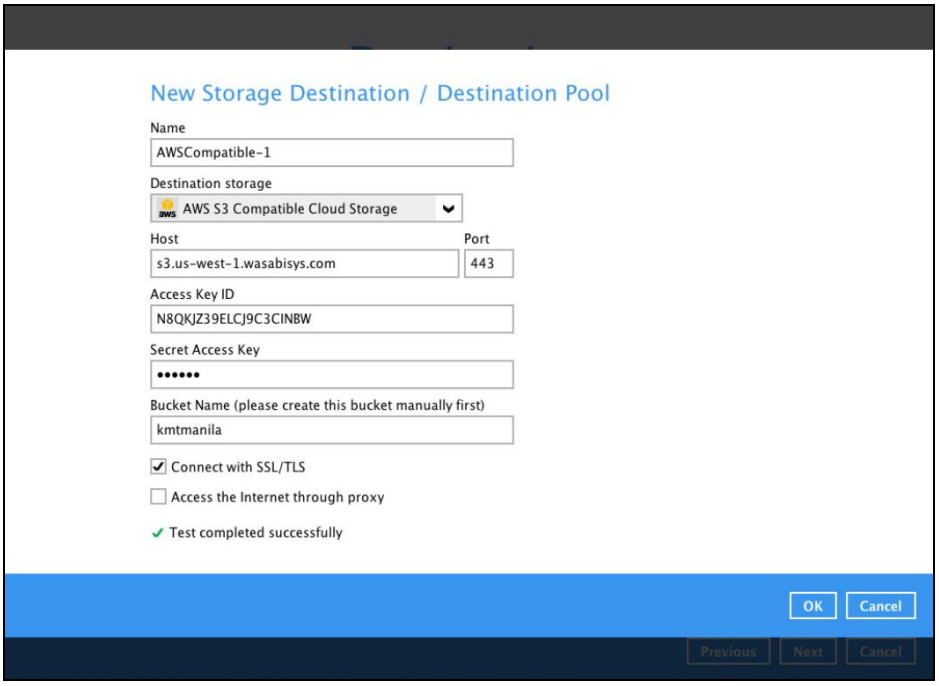


- If you have chosen the **AWS S3 Compatible Cloud Storage**, select from the destination storage then click **OK**. Enter the required details and click **Test** to validate. **Test completed successfully** shows when the validation is done.



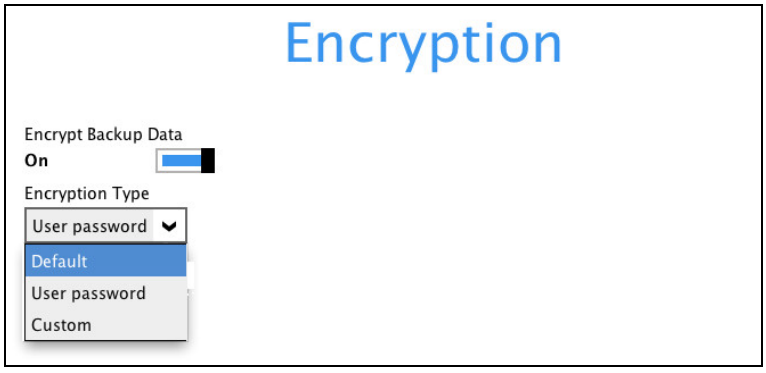

New Storage Destination / Destination Pool
Name
AWSCompatible-1
Destination storage
AWS S3 Compatible Cloud Storage
Host
Port
s3.us-west-1.wasabisys.com
443
Access Key ID
N8QKJZ39ELCJ9C3CINBW
Secret Access Key
Bucket Name (please create this bucket manually first)
kmtmanila
Connect with SSL/TLS
Access the Internet through proxy
Test
OK
Cancel
Previous
Next
Cancel


New Storage Destination / Destination Pool
Name
AWSCompatible-1
Destination storage
AWS S3 Compatible Cloud Storage
Host
Port
s3.us-west-1.wasabisys.com
443
Access Key ID
N8QKJZ39ELCJ9C3CINBW
Secret Access Key
Bucket Name (please create this bucket manually first)
kmtmanila
Connect with SSL/TLS
Access the Internet through proxy
Testing access to destination...
OK
Cancel
Previous
Next
Cancel



You can add multiple storage destinations. The backup data will be uploaded to all the destinations you have selected in the order you added them. Press the icon to alter the order. Click **Next** to proceed when you are done with the selection.

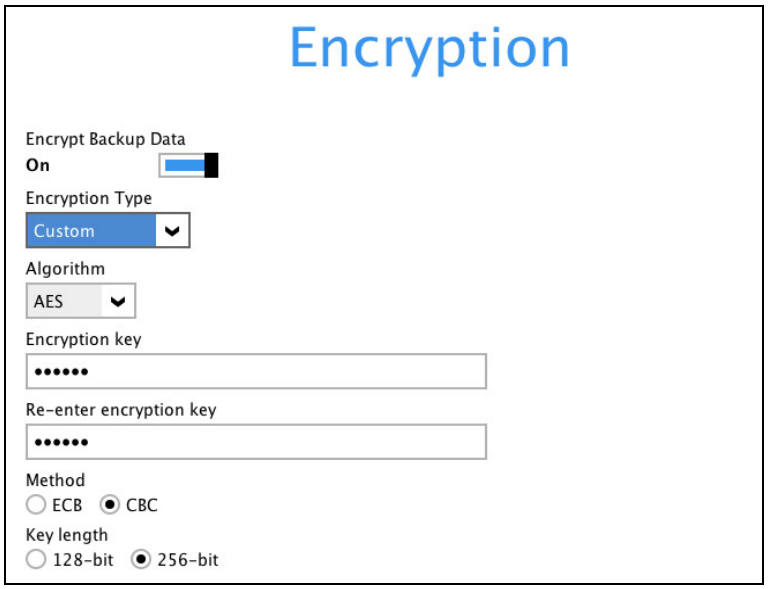
7. In the Encryption window, the default **Encrypt Backup Data** option is enabled with an encryption key preset by the system which provides the most secure protection.



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 AhsayACB at the time when this backup set is created. Please be reminded that if you change the AhsayACB login password later, the encryption keys of the backup sets previously created with this encryption type will remain unchanged.

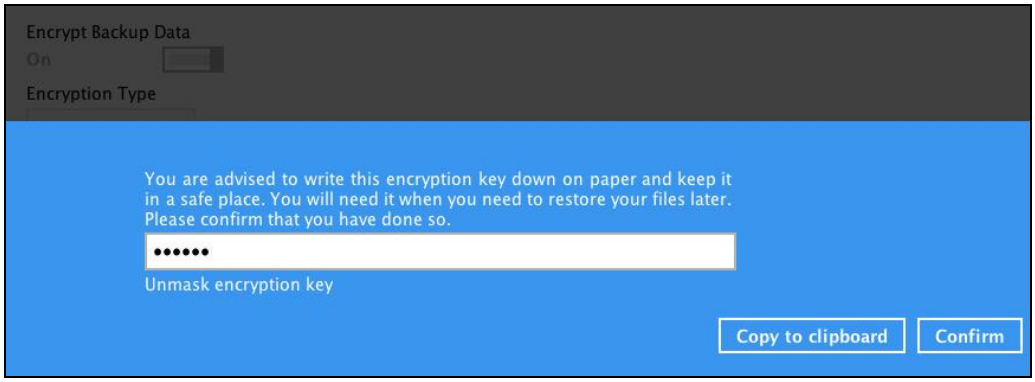
- **Custom** – you can customize your encryption key, where you can set your own algorithm, encryption key, method, and key length.



Note: *For best practice on managing your encryption key, refer to the following Wiki article.*
http://wiki.ahsay.com/doku.php?id=public:5034_best_practices_for_managing_encryption_key

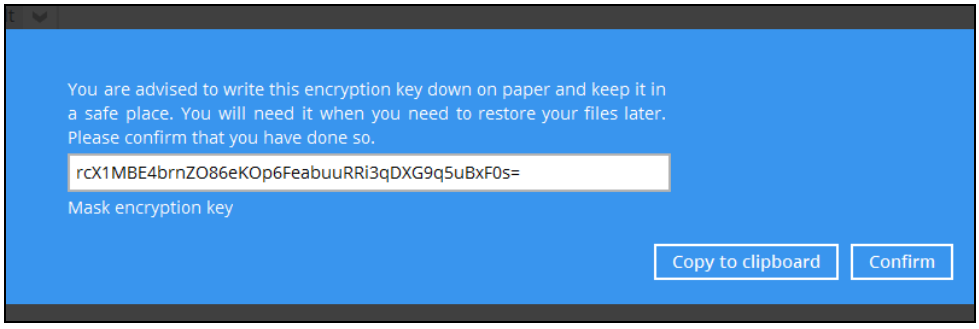
Click **Next** when you are done setting.

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.



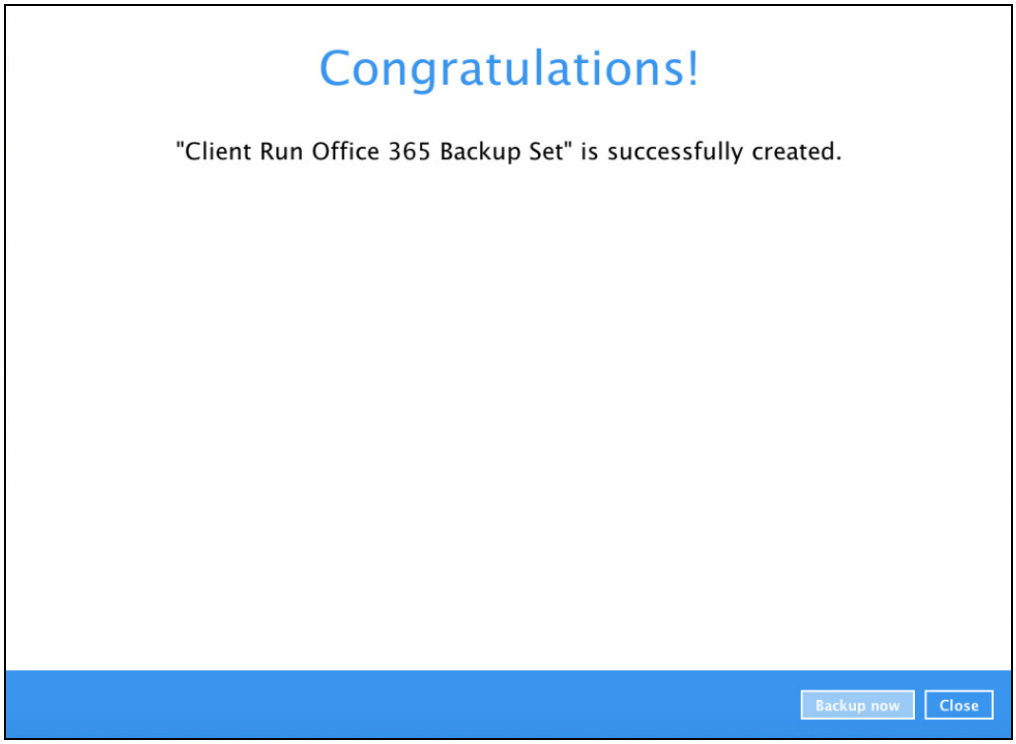
The pop-up window has the following three options to choose from:

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



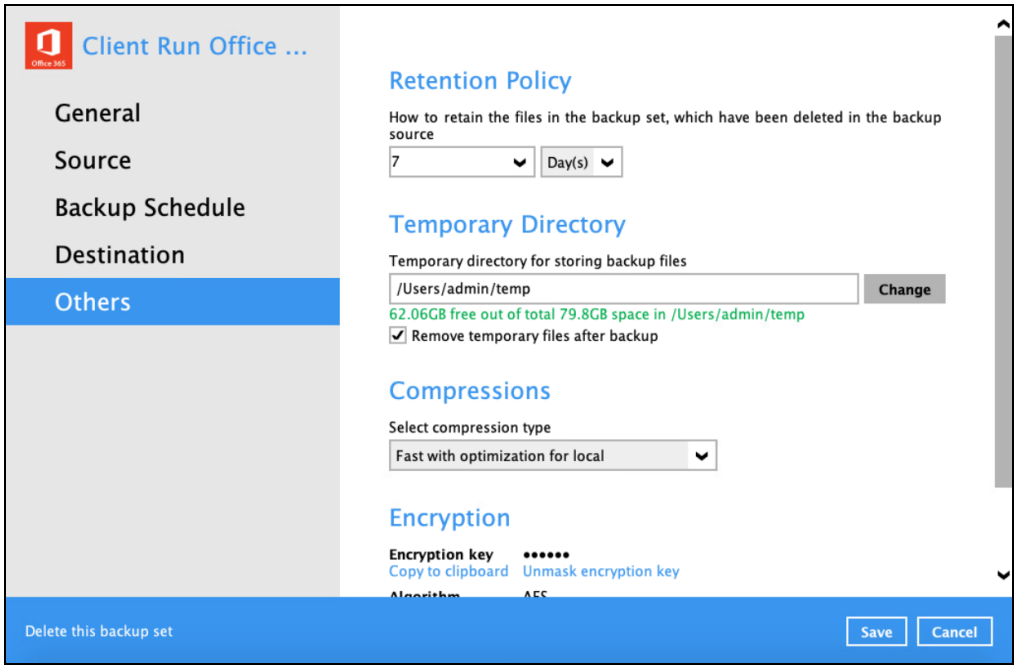
- **Copy to clipboard** – Click to copy the encryption key, then you can paste it in another location of your choice.
- **Confirm** – Click to exit this pop-up window and proceed to the next step.

8. The following screen is displayed when the new Office 365 backup set is created successfully. Click Close to go back to main screen.



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

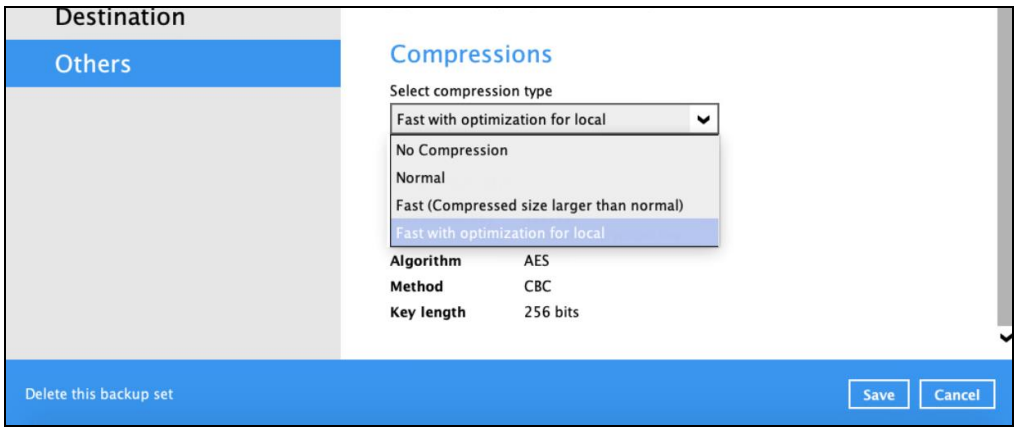
   Go to **Others** > **Temporary Directory**. Click **Change** to browse for another location.



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

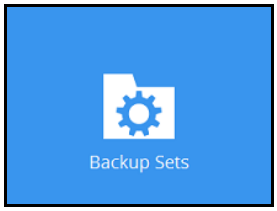
    Go to **Others** > **Compressions**. Select from the following list:

    - No Compression
    - Normal
    - Fast
    - Optimal for Local (Low CPU Usage)

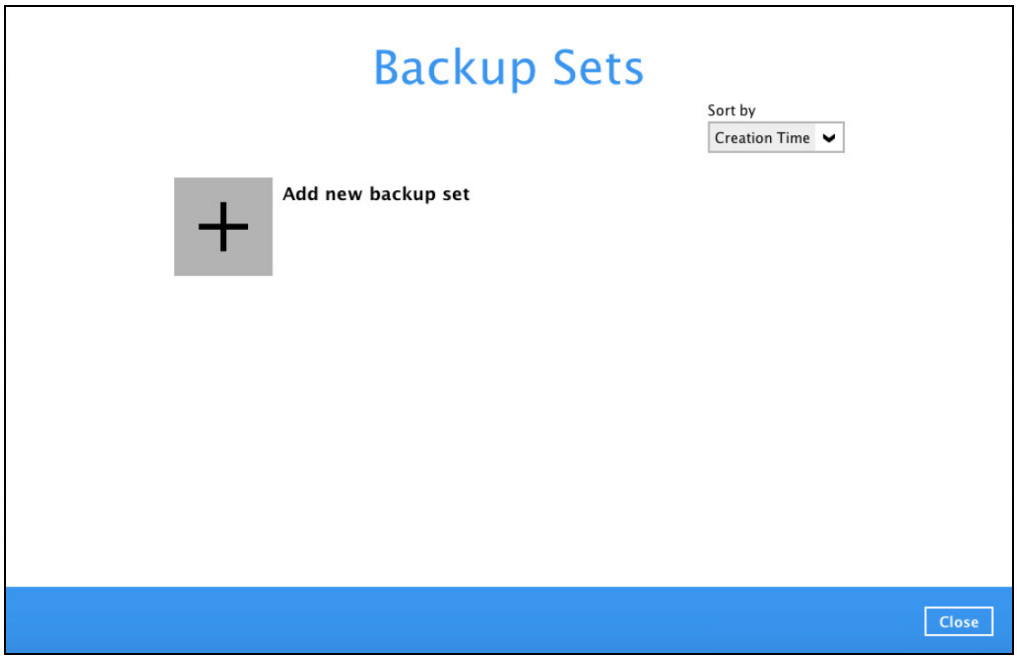


4.2 Hybrid Authentication

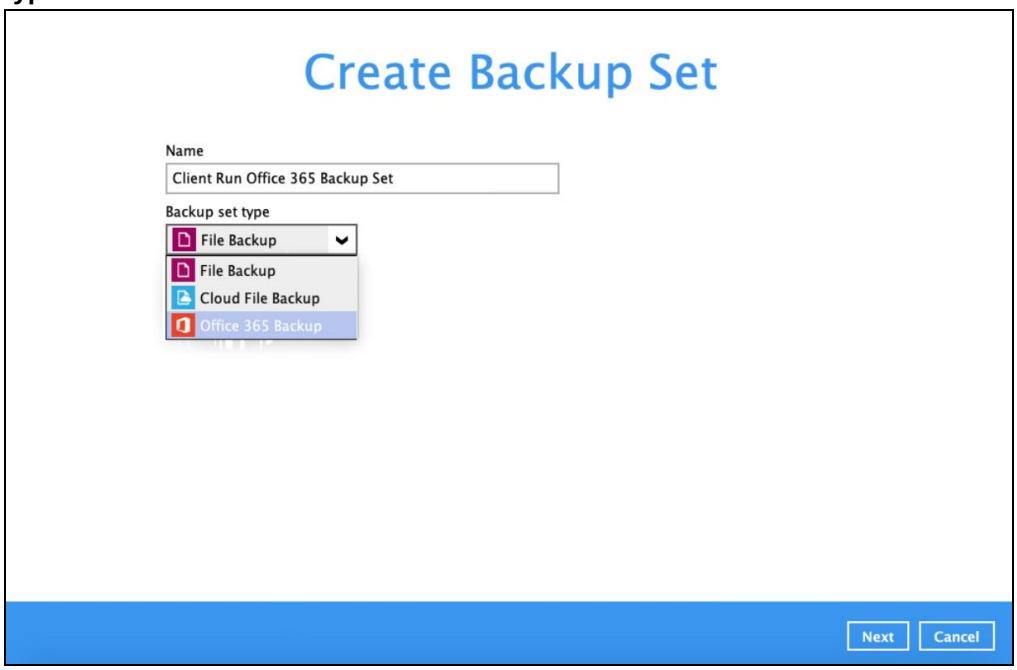
1. In the AhsayACB main interface, click **Backup Sets**.



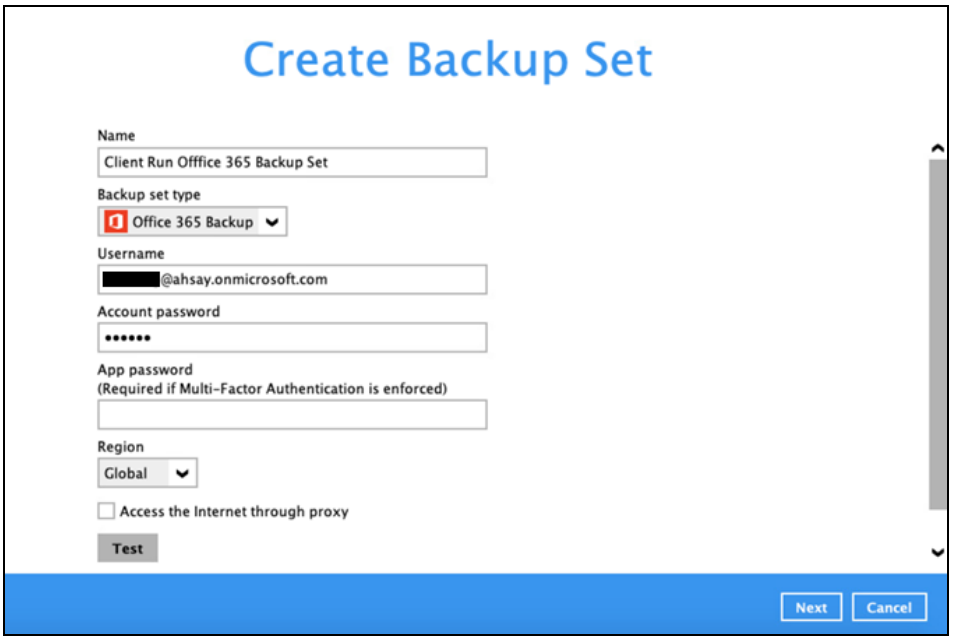
2. Click the "**+**" icon next to **Add new backup set**.



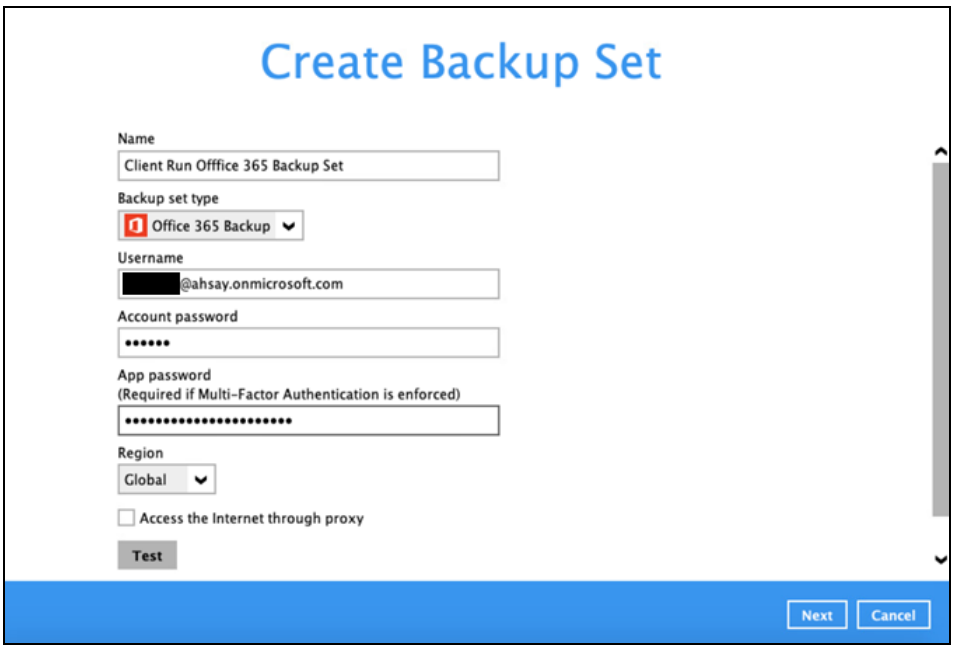
3. Enter a **Name** for your backup set and select **Office 365 Backup** as the **Backup set type**.



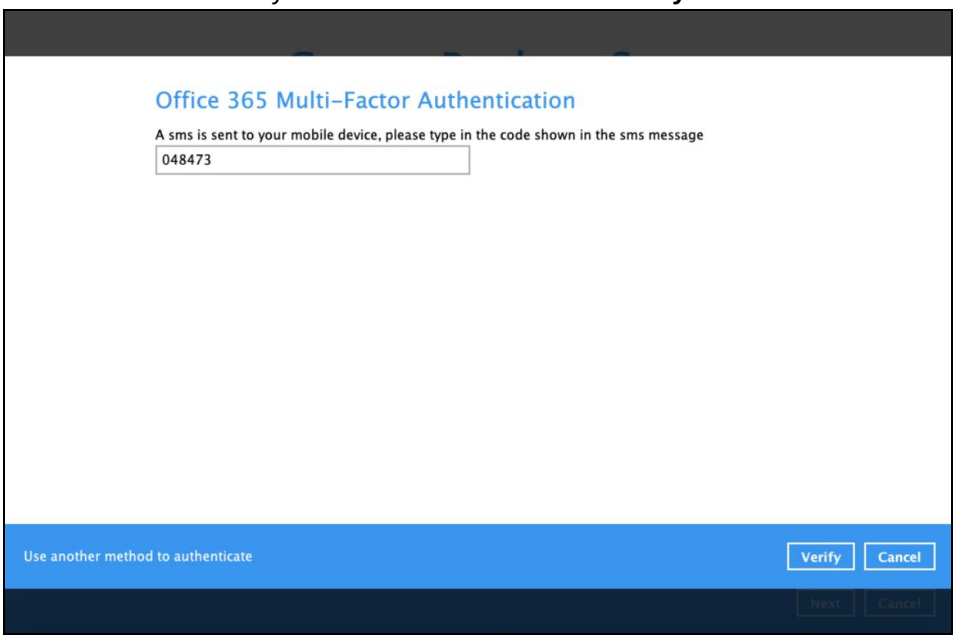
- If MFA is not enforced, enter the Username and Account password. Select the Region and click **Test**.



- If MFA is enforced, enter the Username, Account password and App password then click **Test**.

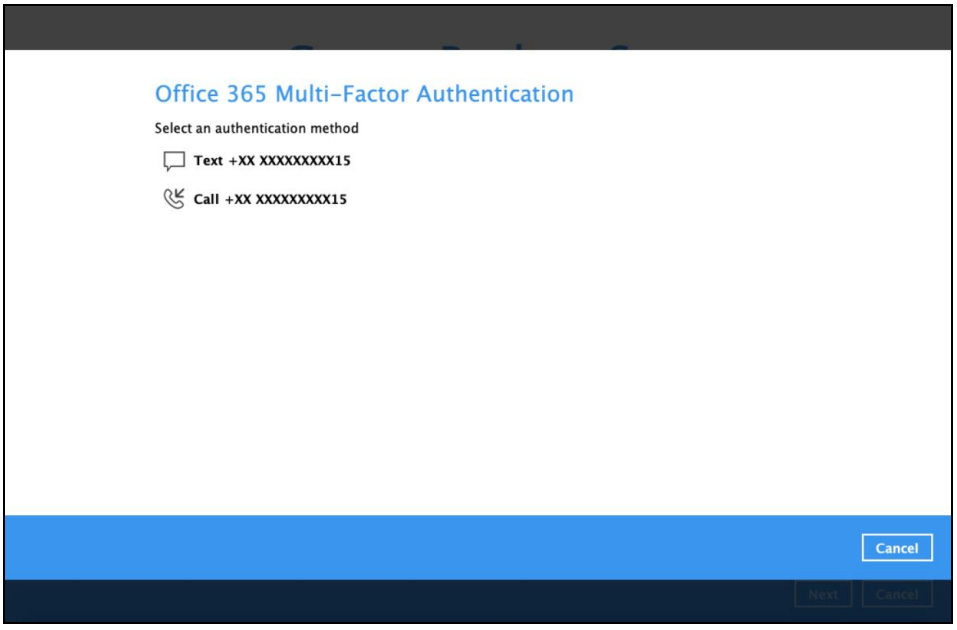


Enter the code sent to your mobile device and click **Verify**.

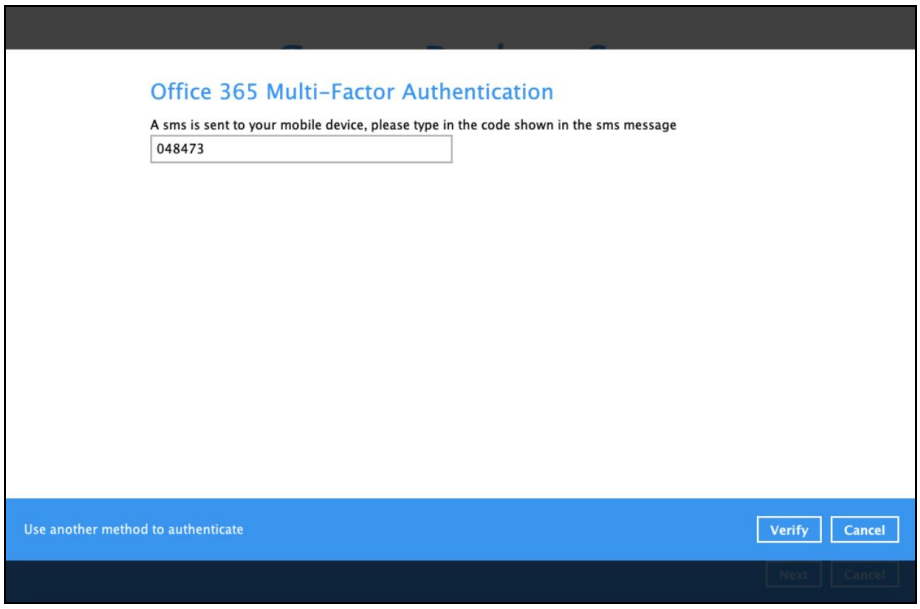


or

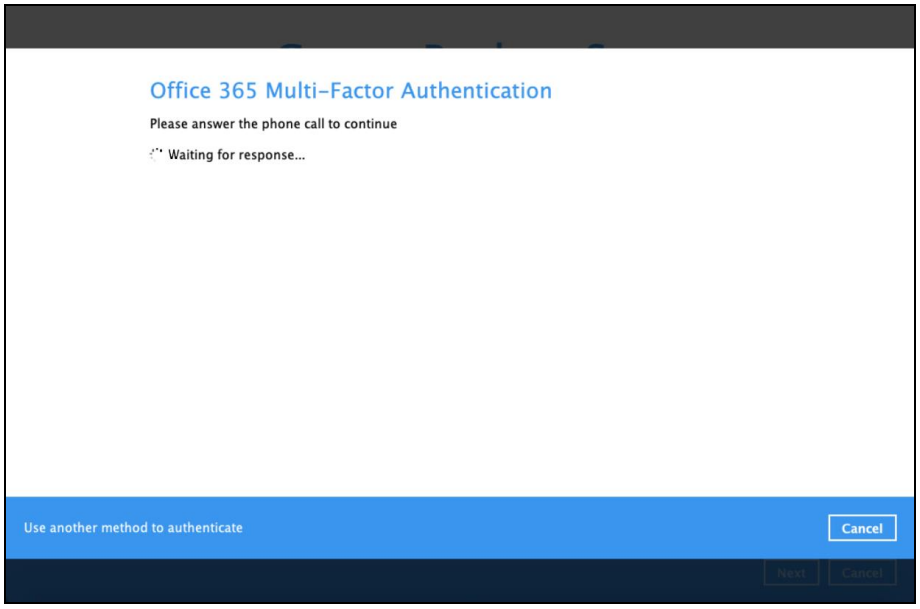
If you click **Use another method to authenticate** link, select between Text or Call.



- If Text is selected, enter the code sent to your mobile device and click **Verify** to proceed.



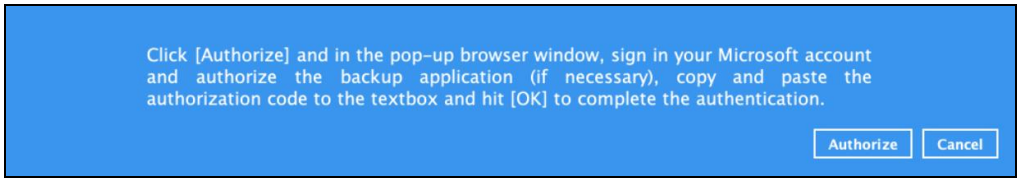
- If Call is selected, you will receive a call from a third-party app. From there follow the instructions to proceed with the authentication.



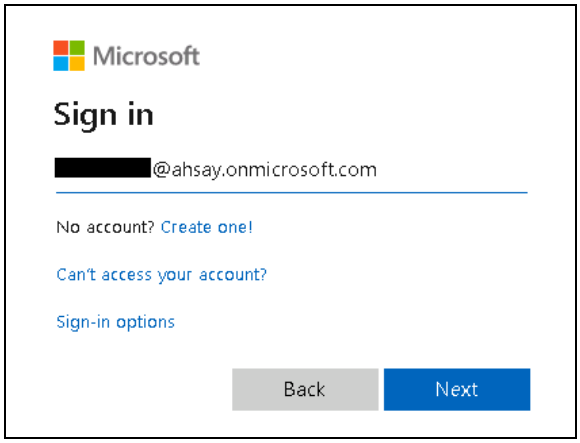
NOTE

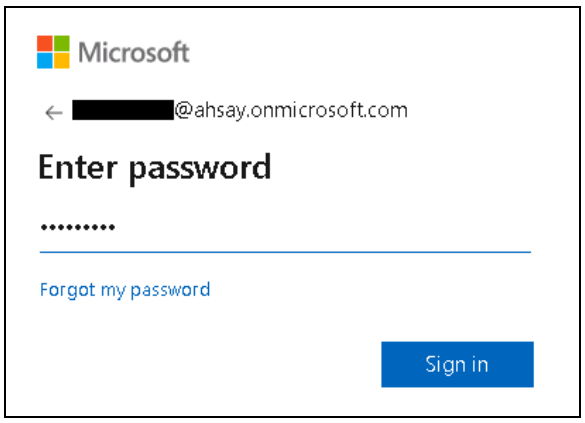
- The App password is only required if the MFA status of an Office 365 account is enforced.
- If the MFA of the Office 365 user account will be enabled later on, it is highly advisable to login to AhsayACB and re-authenticate the Office 365 user account's credential using the MFA App password. Otherwise the scheduled backups of the Office 365 backup set will stop working.

Click **Authorize** to start the authentication process.

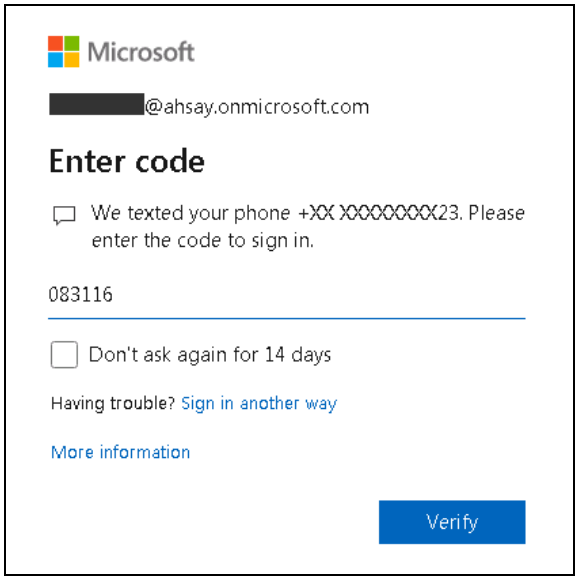


Sign in to your Microsoft account.





If MFA is enforced for the Office 365 user account used to authenticate the backup set, enter the code and click **Verify**.


Microsoft
[redacted]@ahsay.onmicrosoft.com
Enter code
We texted your phone +XX XXXXXXXX23. Please enter the code to sign in.
083116
Don't ask again for 14 days
Having trouble? Sign in another way
More information
Verify

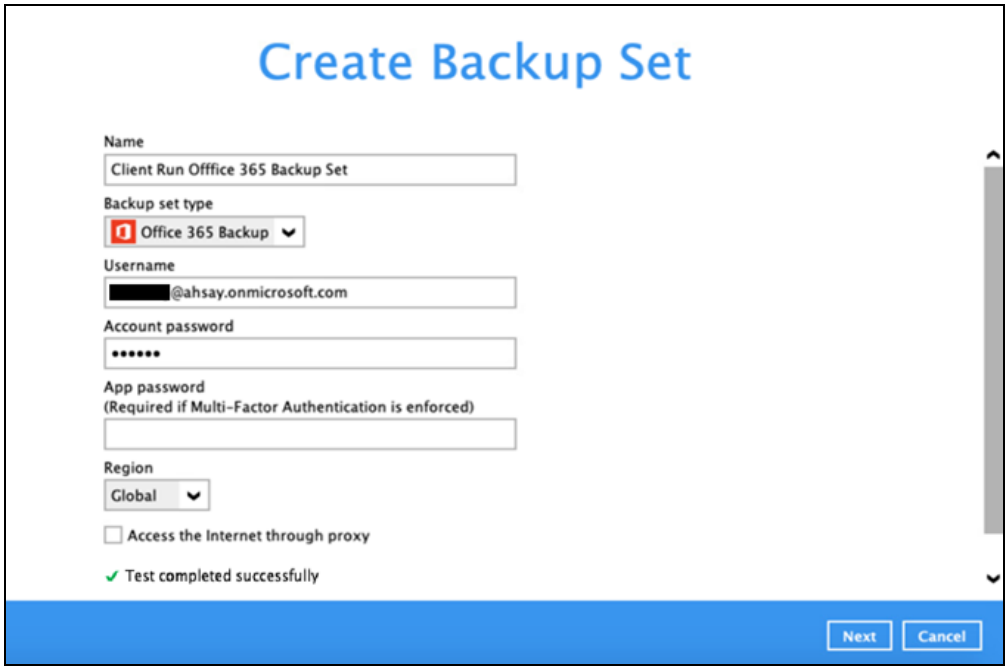
NOTE

The verification code is only required if the MFA status of an Office 365 account is enforced.

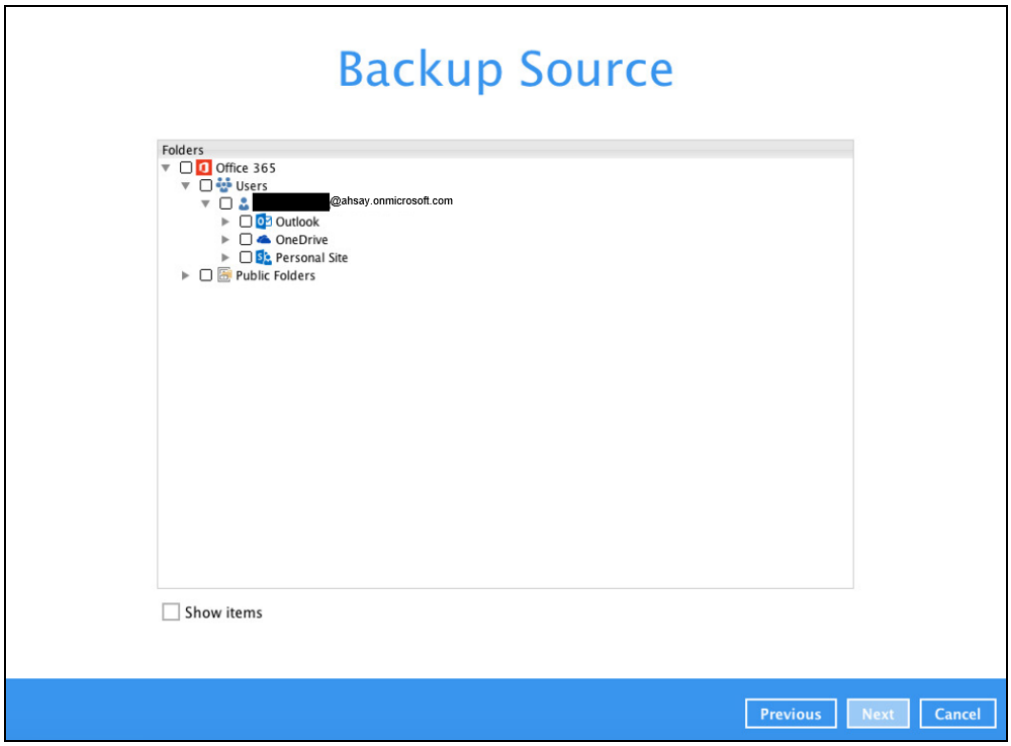
Copy the authorization code.

Go back to AhsayACB and paste the authorization code. Click **OK** to proceed.

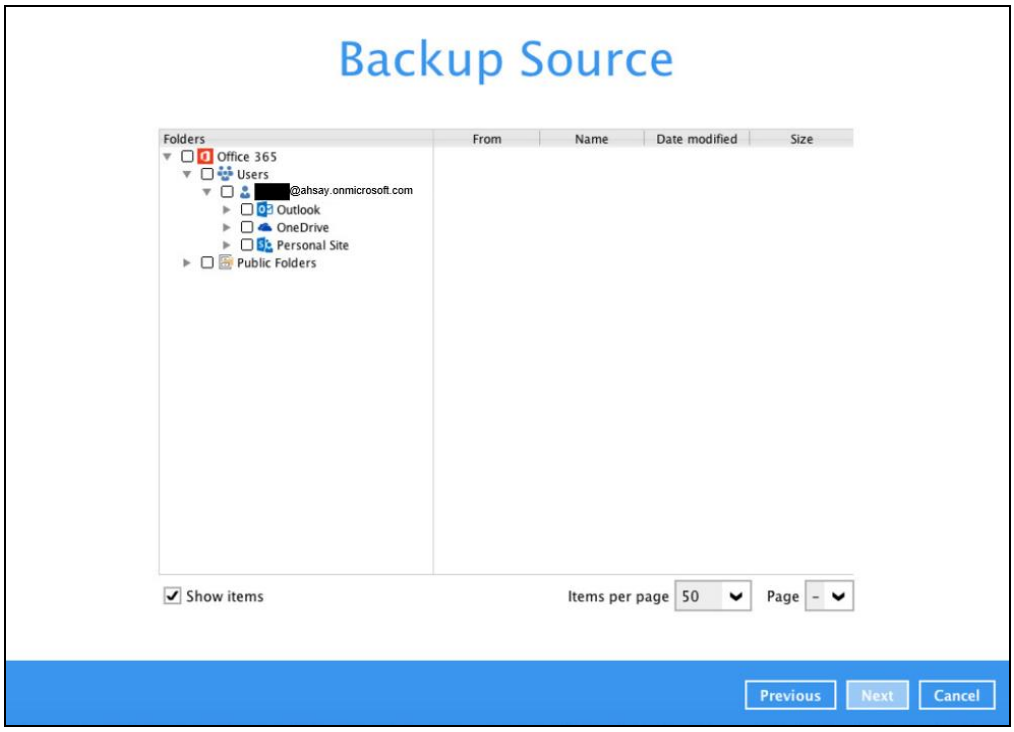
Test completed successfully shows when the validation is successful. Press **Next** to proceed to the next step.



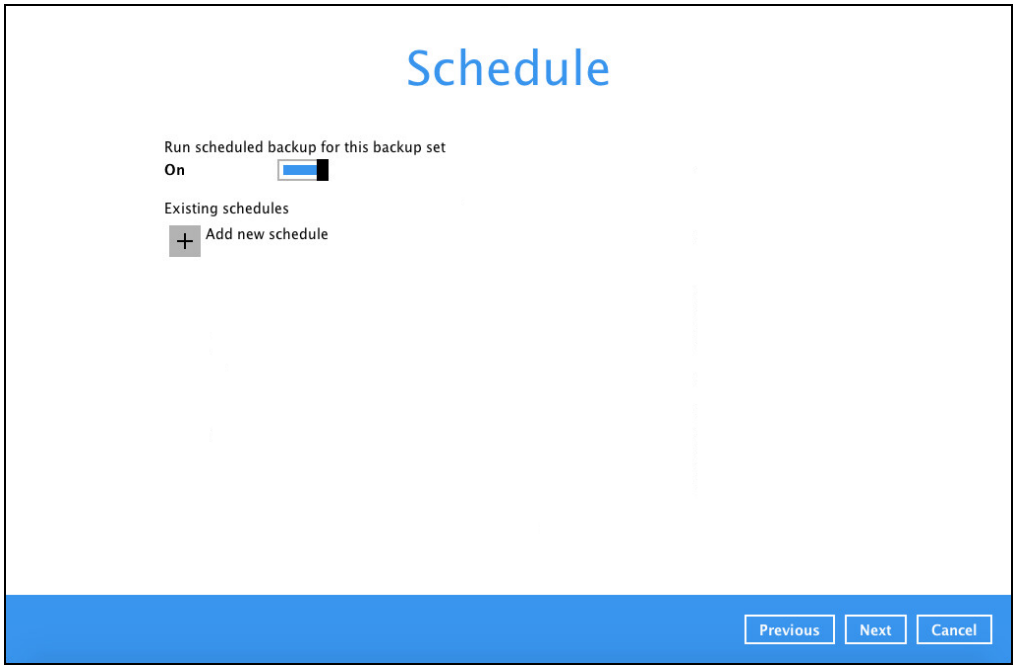
4. In the **Backup Source** menu, select the desired user account and content folder for backup.

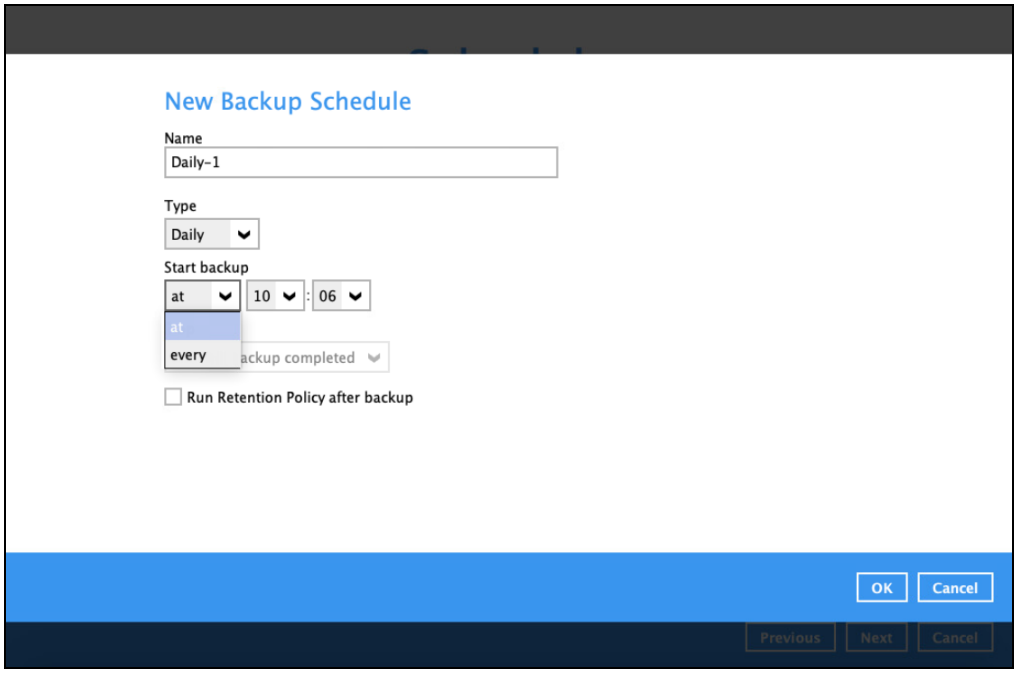


Enable the **Show items** checkbox at the bottom left corner if you would like to choose individual items for backup.



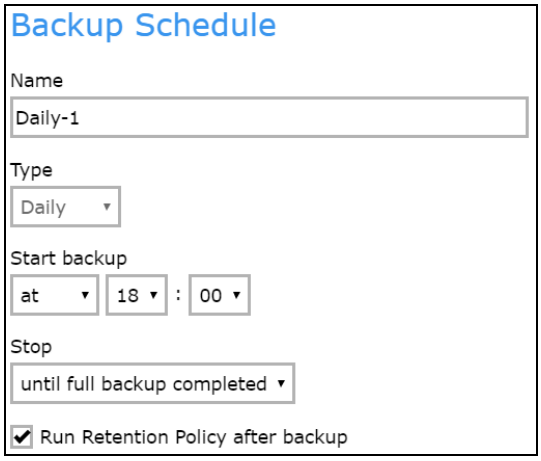
5. In the Schedule menu, configure a backup schedule for backup job to run automatically at your specified time interval. Slide the on/off button to turn on this feature, then click **Add new schedule** to add a new schedule, then click **Next** to proceed afterward.



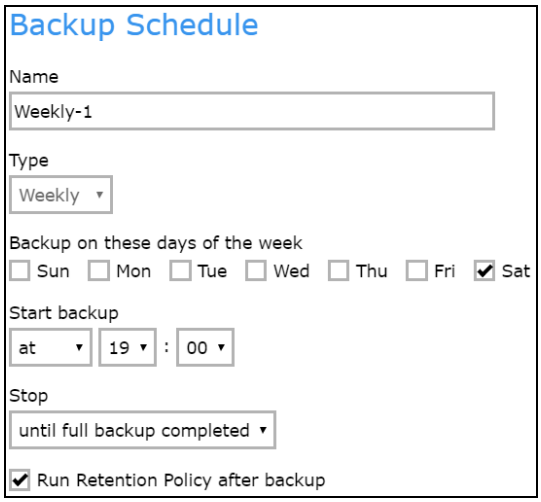


In the New Backup Schedule window, configure the following backup schedule settings.

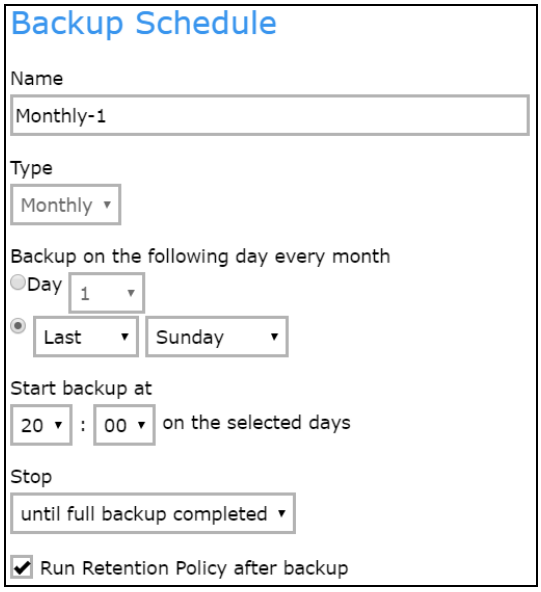
- **Name** – the name of the backup schedule.
- **Type** – the type of the backup schedule. There are four (4) different types of backup schedule: Daily, Weekly, Monthly and Custom.
  - **Daily** – the time of the day when the backup job will run.



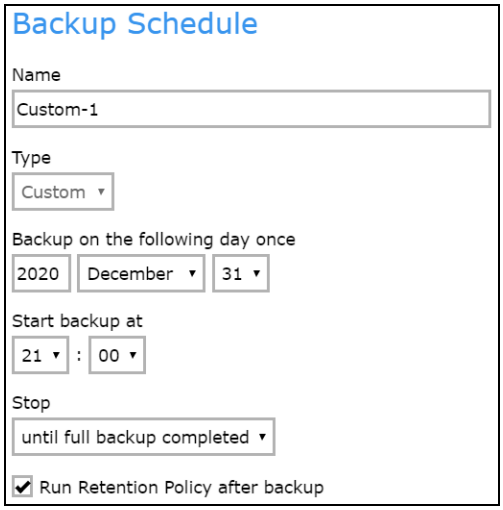
- **Weekly** – the day of the week and the time of the day when the backup job will run.



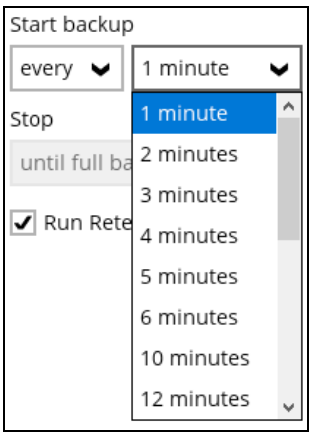
- **Monthly** – the day of the month and the time of the day when the backup job will run.

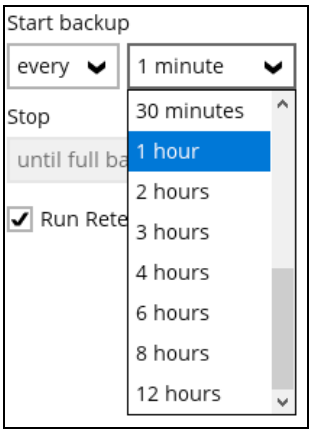


- **Custom** – a specific date and the time when the backup job will run.

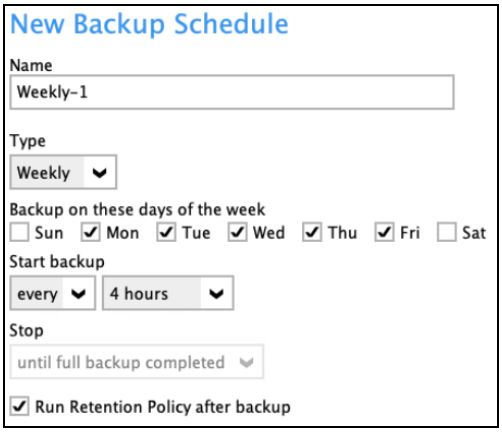


- **Start backup** – the start time of the backup job.
  - **at** – this option will start a backup job at a specific time.
  - **every** – this option will start a backup job in intervals of minutes or hours.





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



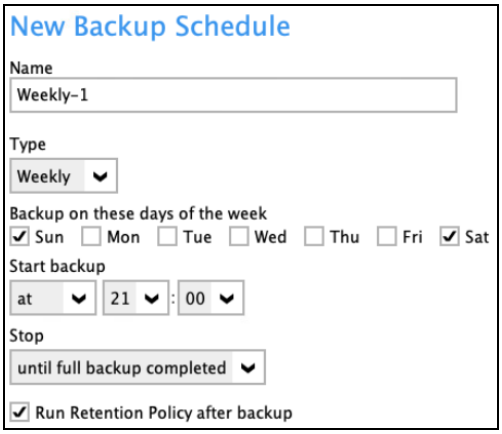


Figure 1.1 ***Figure 1.2***

Figure 1.1 – Periodic scheduled every 4 hours Monday - Friday for business hours

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

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

The number of hours must be enough to complete a backup of all files in the backup set. For small files in a backup, if the number of hours is not enough

to back up all files, then the outstanding files will be backed up in the next backup job. However, if the backup set contains large files, this may result in partially backed up files.

For example, if a backup set 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.

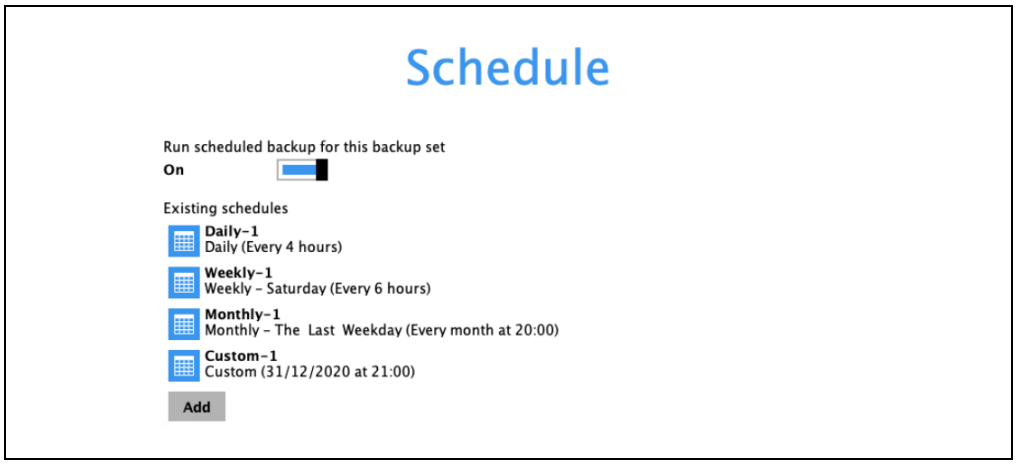
The partially backed up data will have to be removed by running the data integrity check.

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 AhsayACB will run a retention policy job to remove files from the backup destination(s) which have exceeded the retention policy after performing a backup job.

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

Click the [Save] button to save settings and multiple backup schedules can be created.

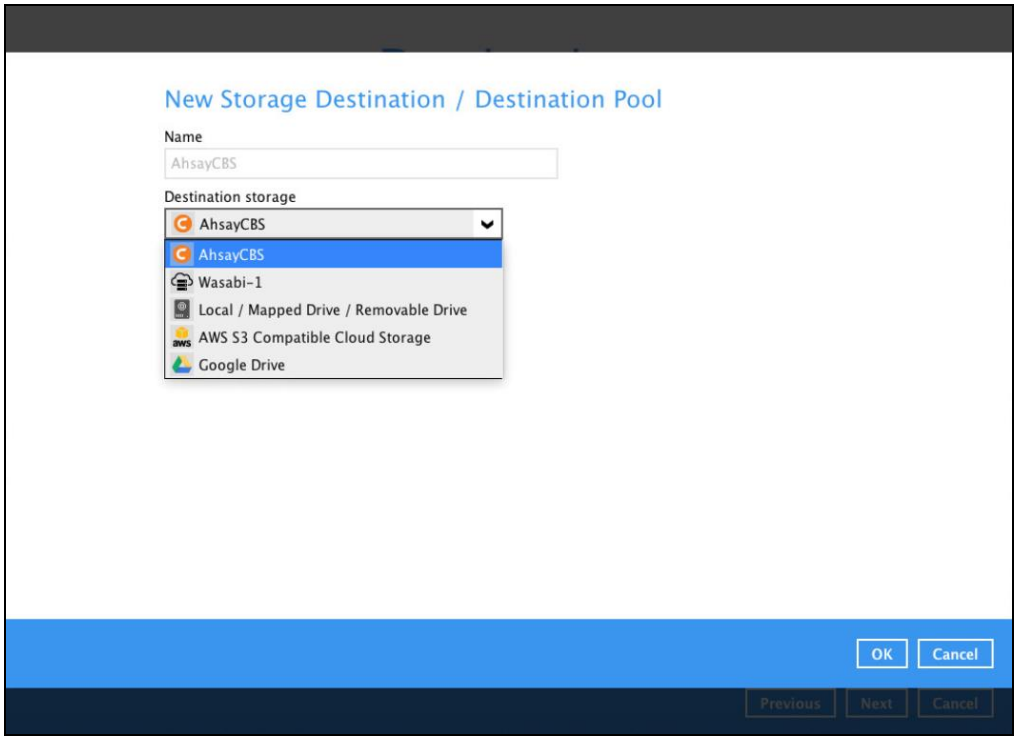


6. In the **Destination** menu, select a backup destination where the backup data will be stored. Click the "**+**" icon next to **Add new storage destination / destination pool**.

NOTE

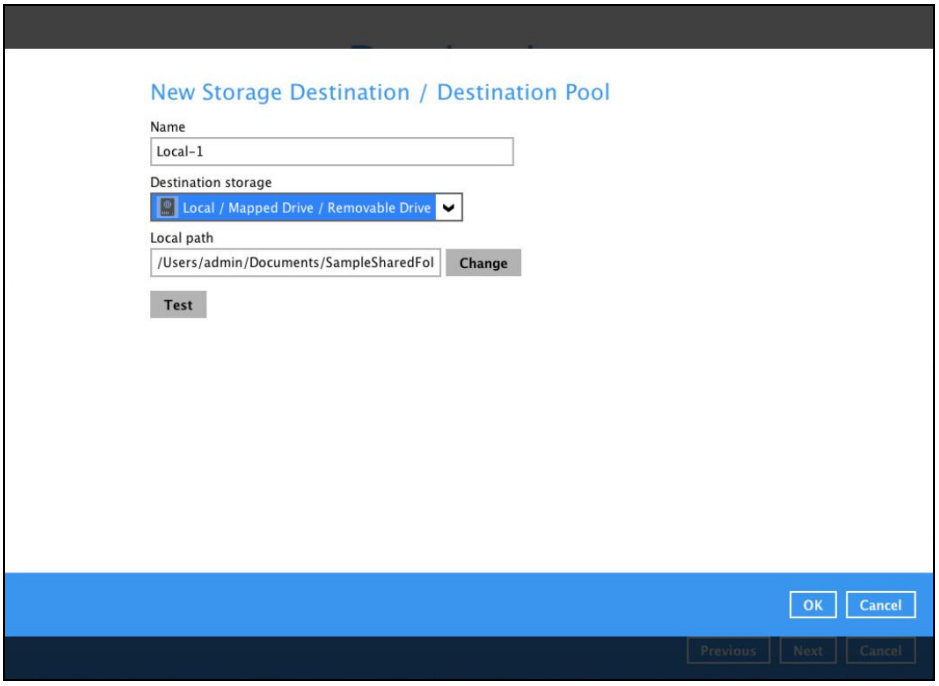
For more details on Backup Destination, refer to the following Wiki article for details:
http://wiki.ahsay.com/doku.php?id=public:8002_faq:faq_on_backup_destination

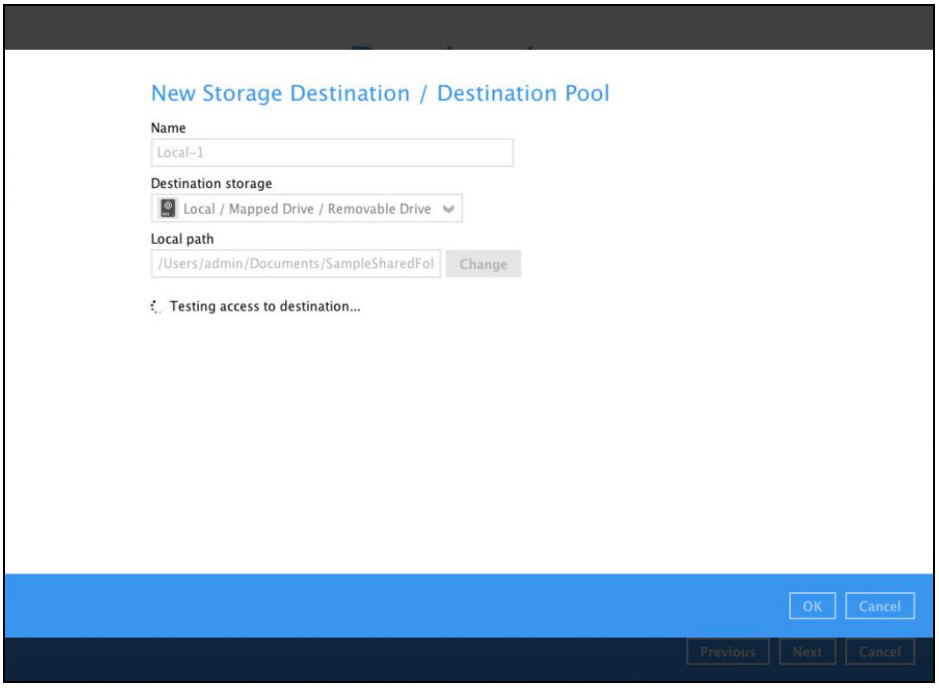
Select storage destinations.

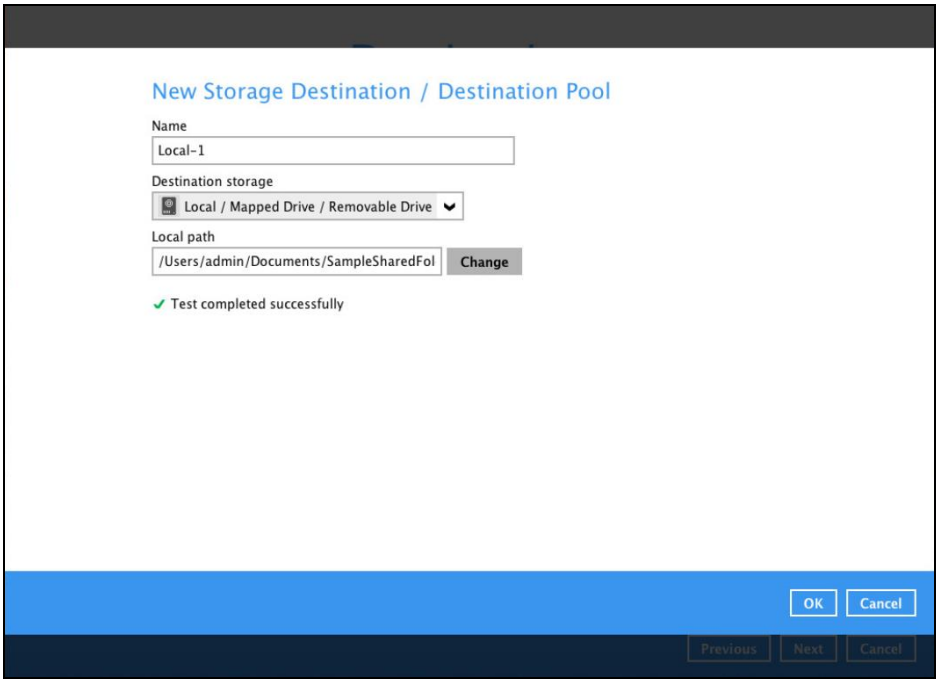


You can choose a storage combination of the Local/Mapped drive/Removable Drive or Cloud storage. Click **OK** to proceed when you are done with the settings.

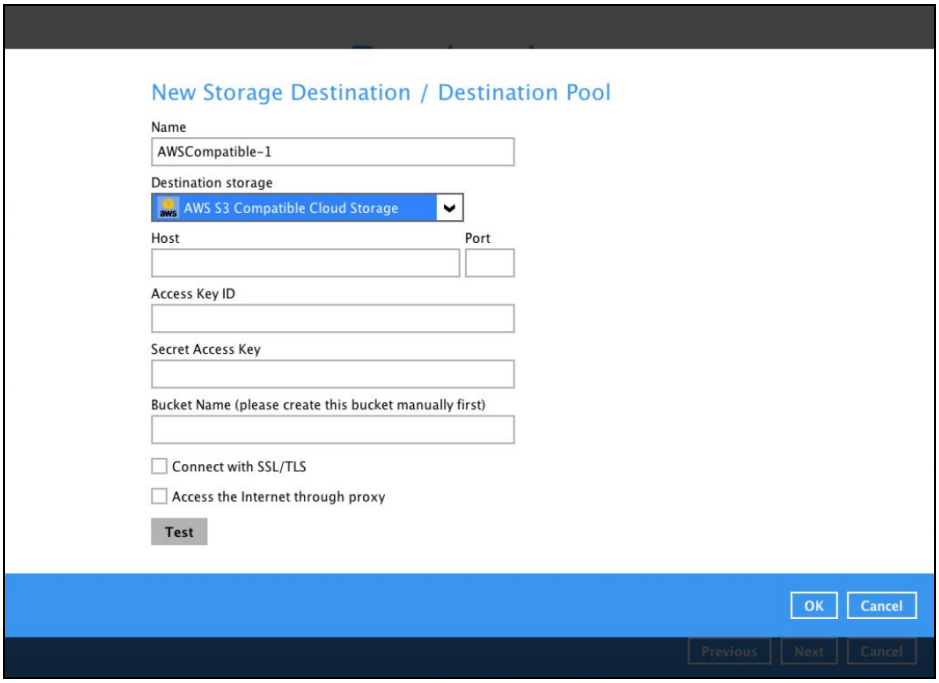
- If you have chosen the **Local / Mapped Drive / Removable Drive** option, click **Change** to browse to a directory path where backup data will be stored, then click **Test** to validate the path. **Test completed successfully** shows when the validation is done.

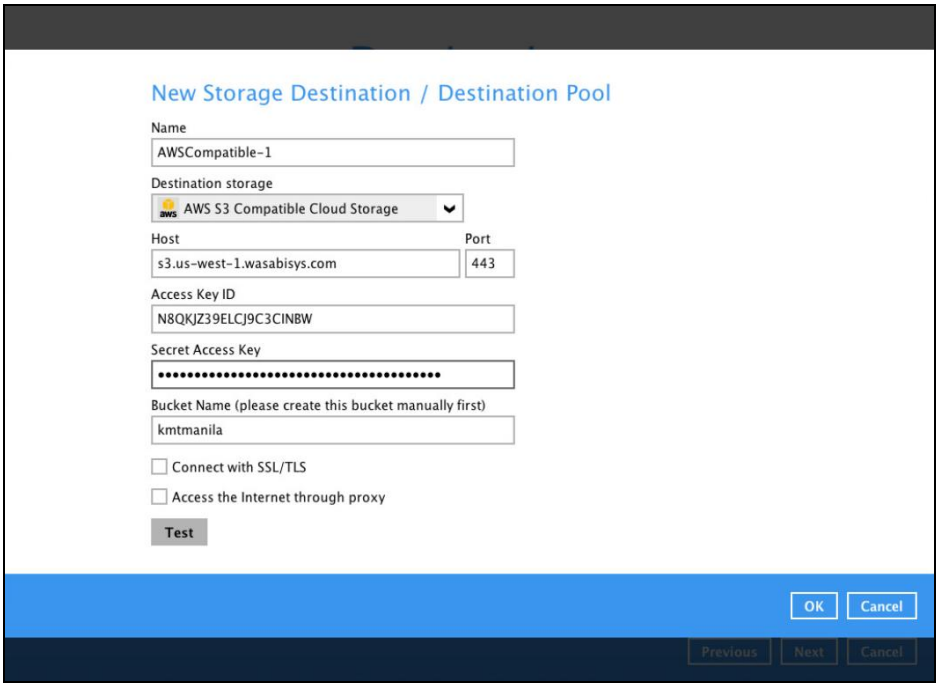


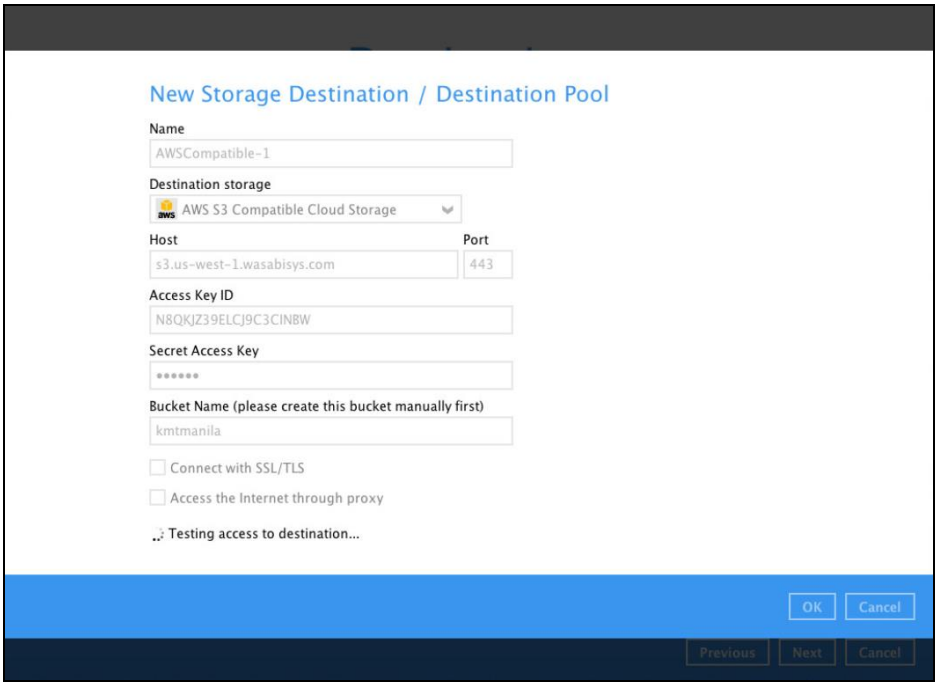


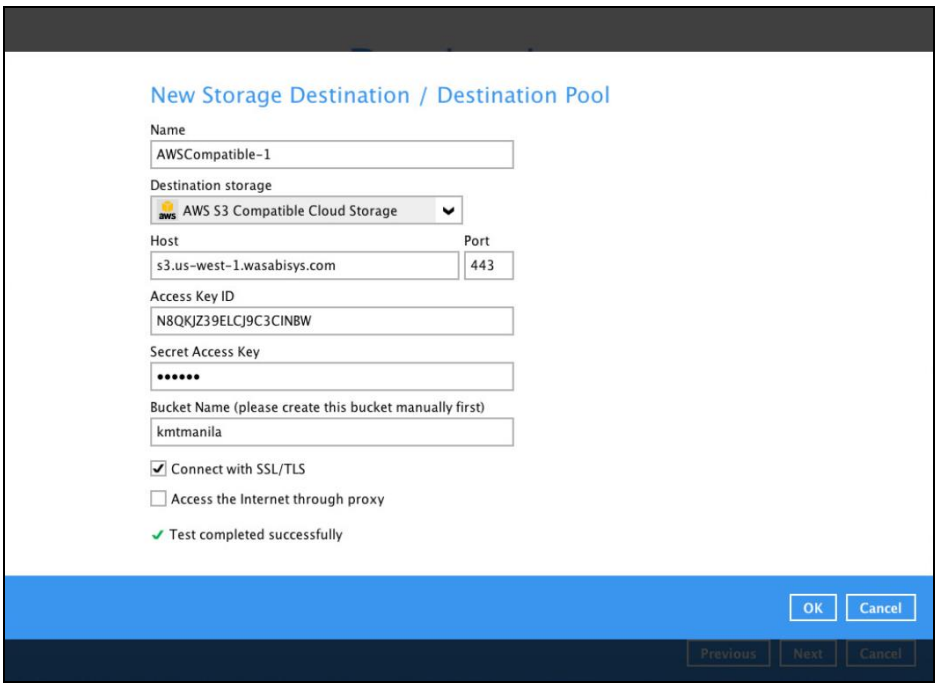


- If you have chosen the **AWS S3 Compatible Cloud Storage**, select from the destination storage then click **OK**. Enter the required details and click **Test** to validate. **Test completed successfully** shows when the validation is done.


New Storage Destination / Destination Pool
Name
AWSCompatible-1
Destination storage
AWS S3 Compatible Cloud Storage
Host
Port
Access Key ID
Secret Access Key
Bucket Name (please create this bucket manually first)
Connect with SSL/TLS
Access the Internet through proxy
Test
OK
Cancel
Previous
Next
Cancel

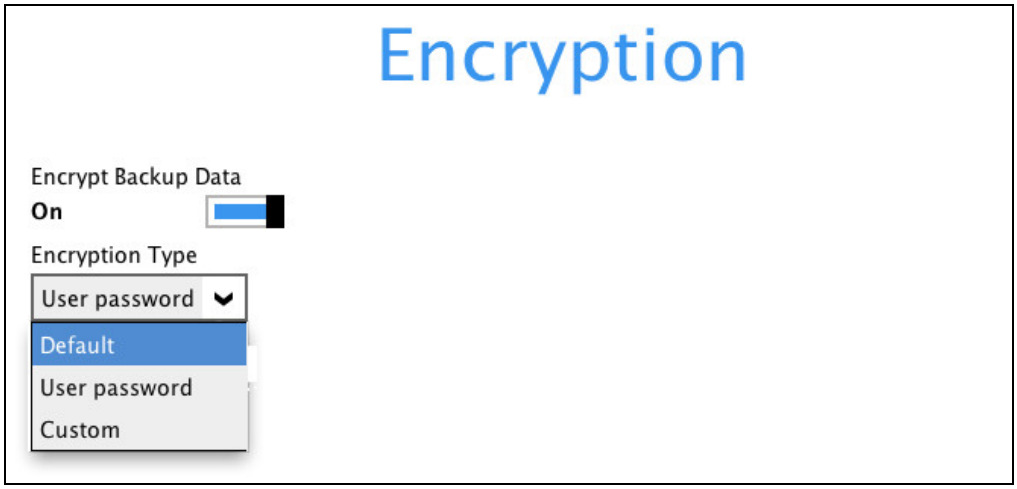

New Storage Destination / Destination Pool
Name
AWSCompatible-1
Destination storage
AWS S3 Compatible Cloud Storage
Host
s3.us-west-1.wasabisys.com
Port
443
Access Key ID
N8QKJZ39ELCJ9C3CINBW
Secret Access Key
Bucket Name (please create this bucket manually first)
kmtmanila
Connect with SSL/TLS
Access the Internet through proxy
Test
OK
Cancel
Previous
Next
Cancel





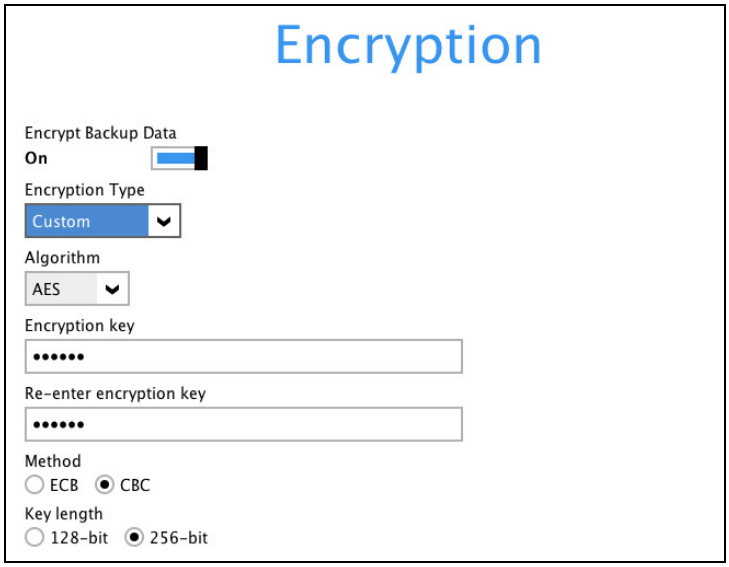
You can add multiple storage destinations. The backup data will be uploaded to all the destinations you have selected in the order you added them. Press the icon to alter the order. Click **Next** to proceed when you are done with the selection.

7. 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:

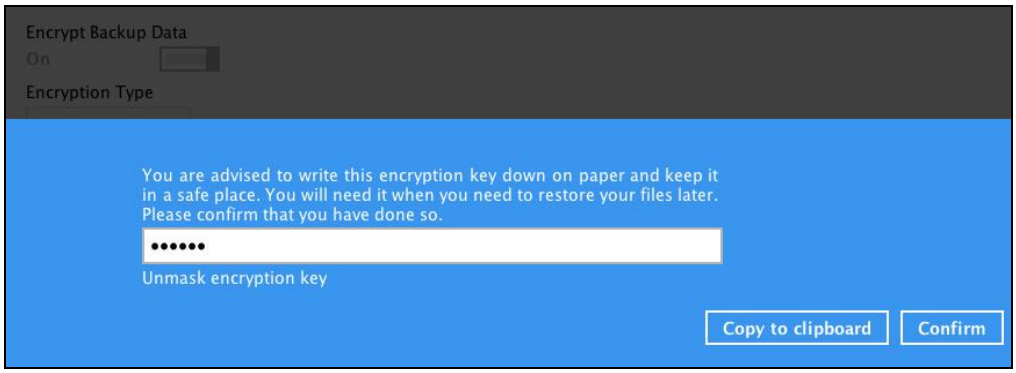
- **Default** – an encryption key with 44 alpha numeric characters will be randomly generated by the system
- **User password** – the encryption key will be the same as the login password of your AhsayACB at the time when this backup set is created. Please be reminded that if you change the AhsayACB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



Note: *For best practice on managing your encryption key, refer to the following Wiki article.*
http://wiki.ahsay.com/doku.php?id=public:5034_best_practices_for_managing_encryption_key

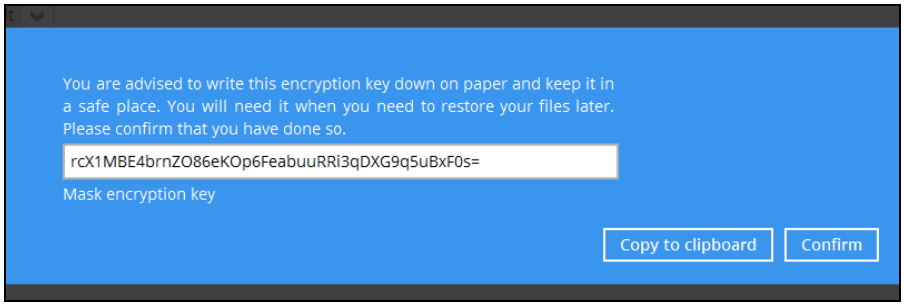
Click **Next** when you are done setting.

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.



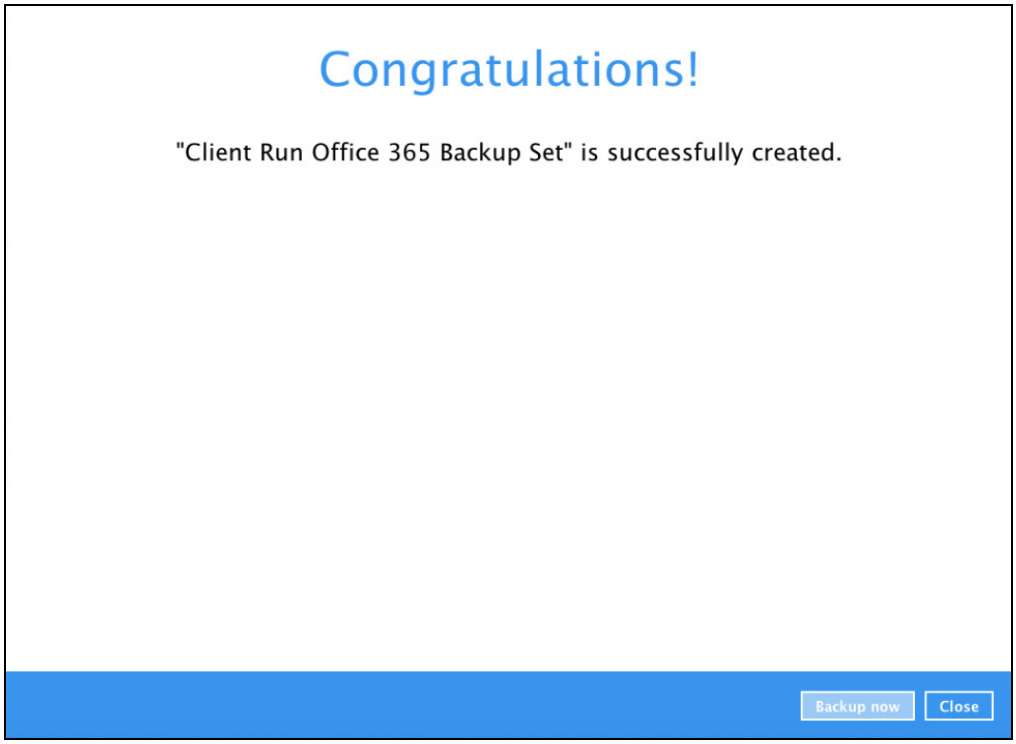
The pop-up window has the following three options to choose from:

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



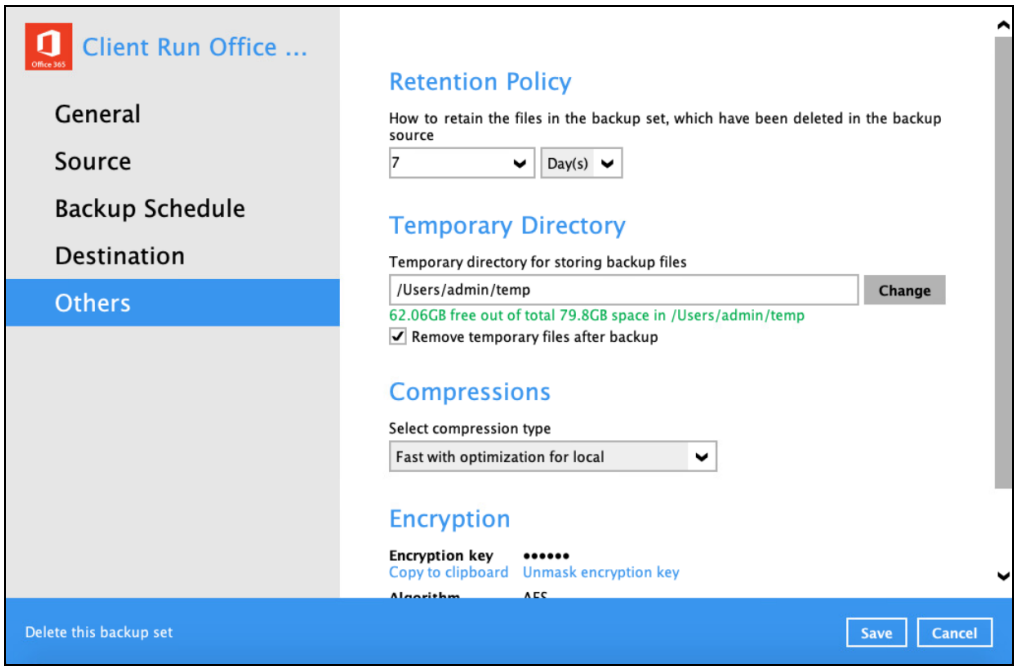
- **Copy to clipboard** – Click to copy the encryption key, then you can paste it in another location of your choice.
- **Confirm** – Click to exit this pop-up window and proceed to the next step.

8. The following screen is displayed when the new Office 365 backup set is created successfully. Click Close to go back to main screen.



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

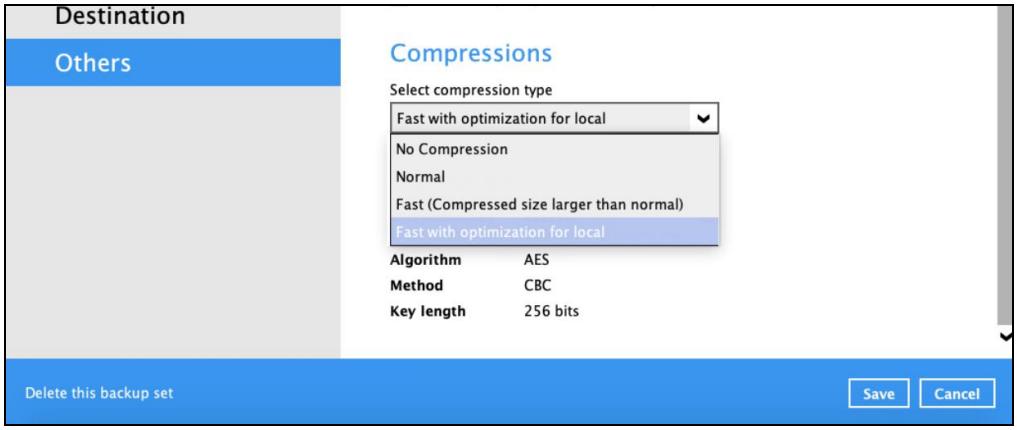
   Go to **Others** > **Temporary Directory**. Click **Change** to browse for another location.



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

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

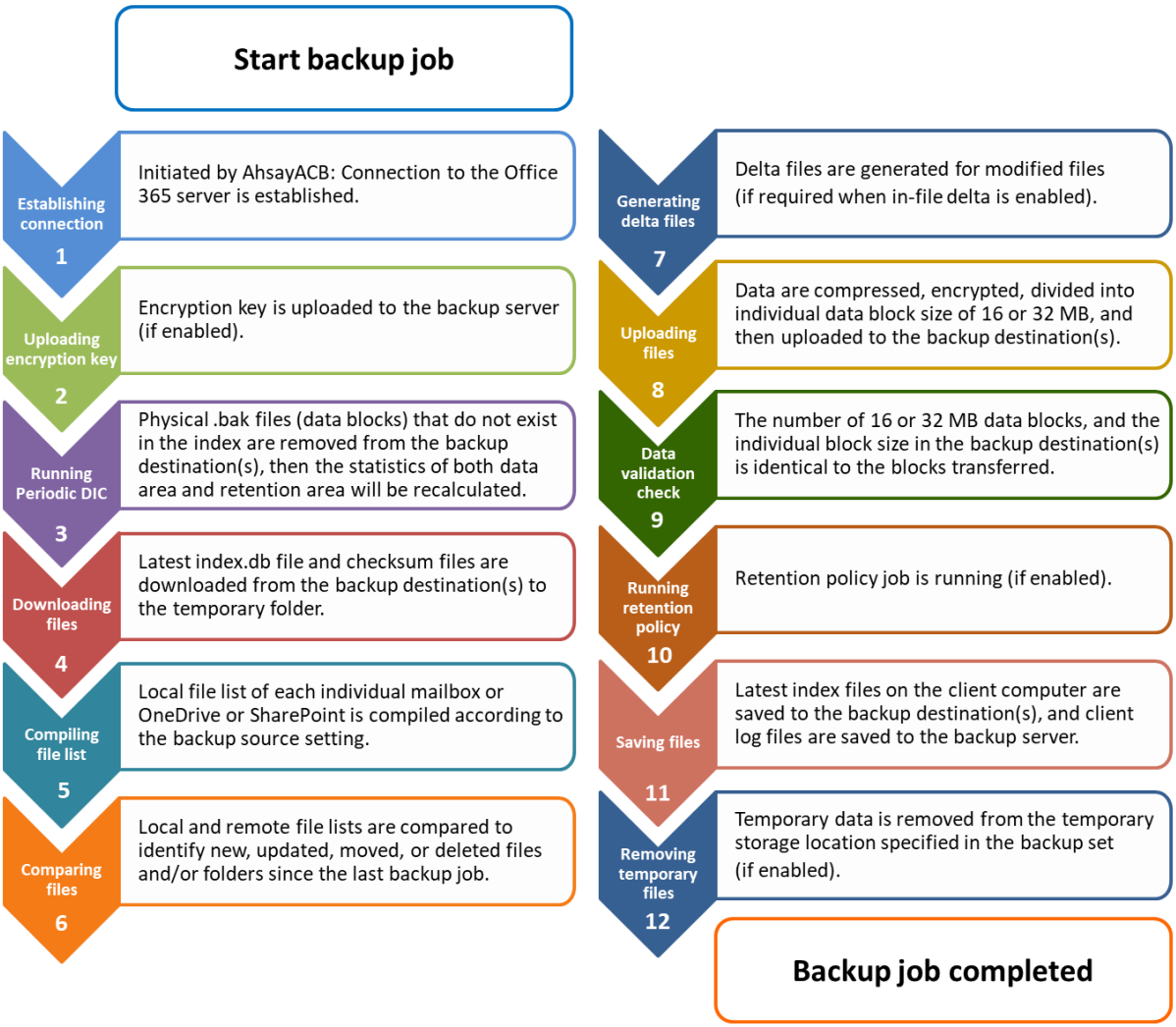
    - No Compression
    - Normal
    - Fast
    - Optimal for Local (Low CPU Usage)



5 Overview of Office 365 Backup Process

The following steps are performed during an Office 365 backup job. For an overview of the detailed process for Steps **3**, **4**, **9**, and **11**, please refer to the following chapters.

- Periodic Data Integrity Check (PDIC) Process **(Step 3)**
- Backup Set Index Handling Process
  - Start Backup Job **(Step 4)**
  - Completed Backup Job **(Step 11)**
- Data Validation Check Process **(Step 9)**



5.1 Periodic Data Integrity Check (PDIC) Process

For AhsayACB 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:

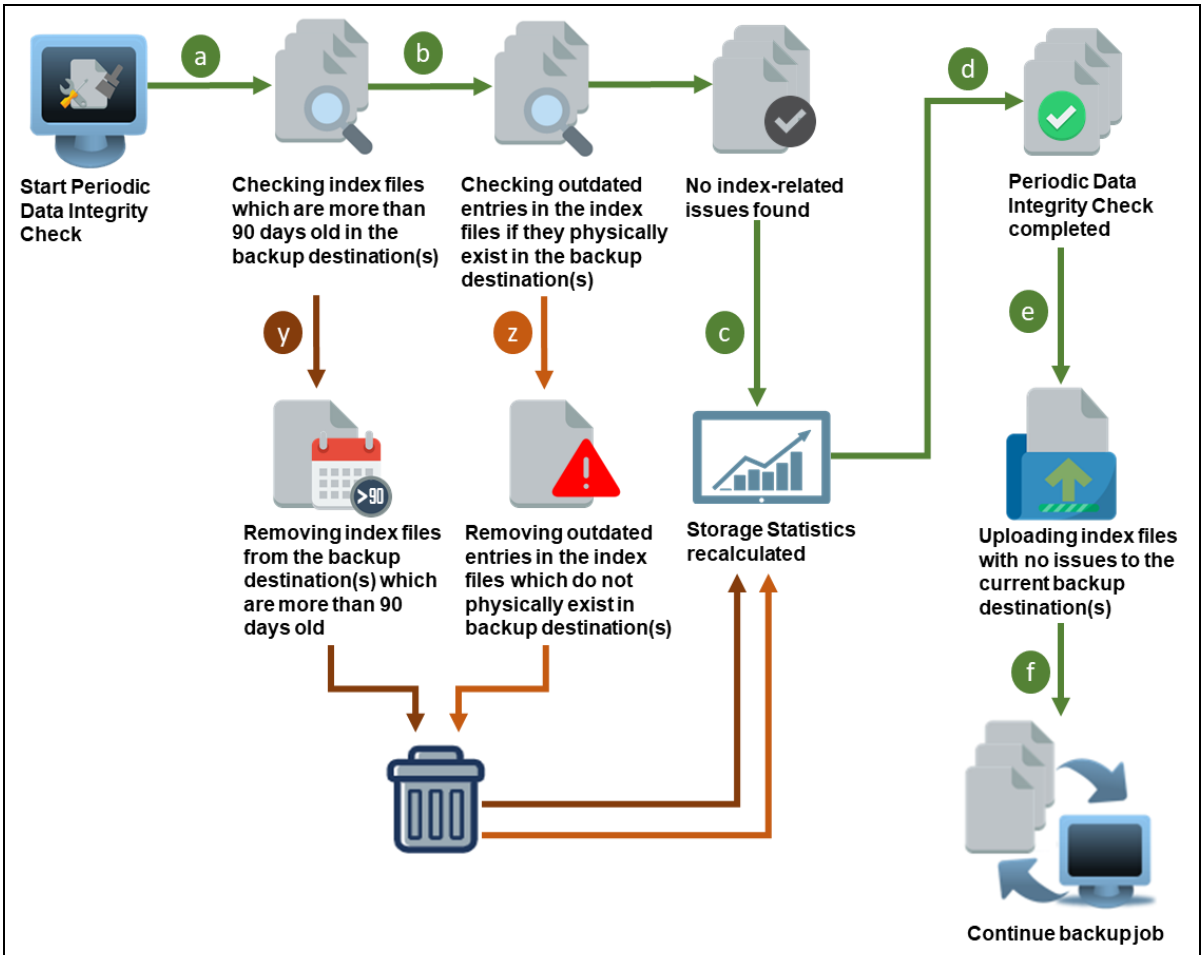
- the PDIC will run on the first backup job that falls on Wednesday; or
- if there is no active backup job(s) running from Monday to Friday, then the PDIC will run on the next available backup job.

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 AhsayACB 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.

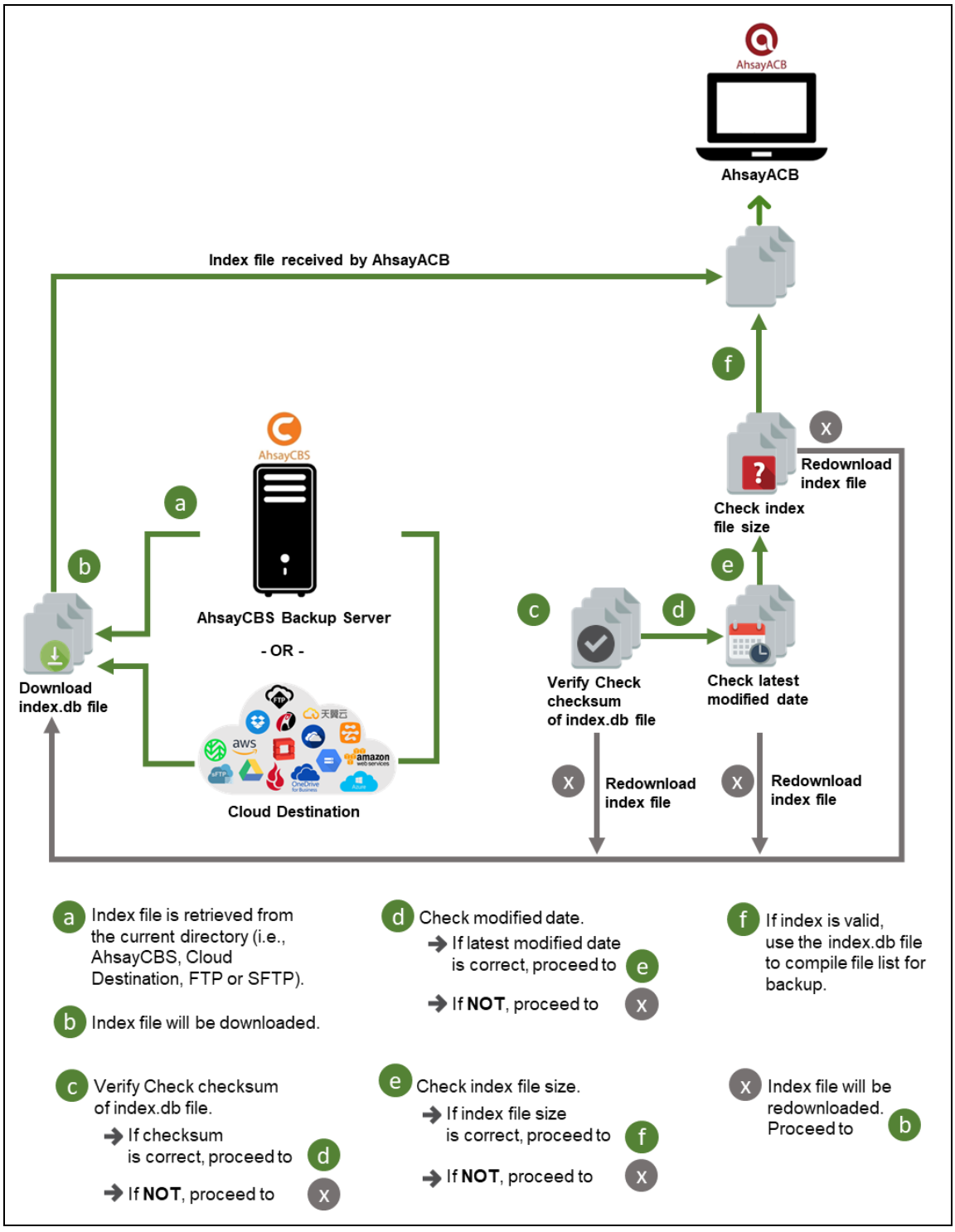
y Index files which are more than 90 days old will be removed from the backup destination(s).

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

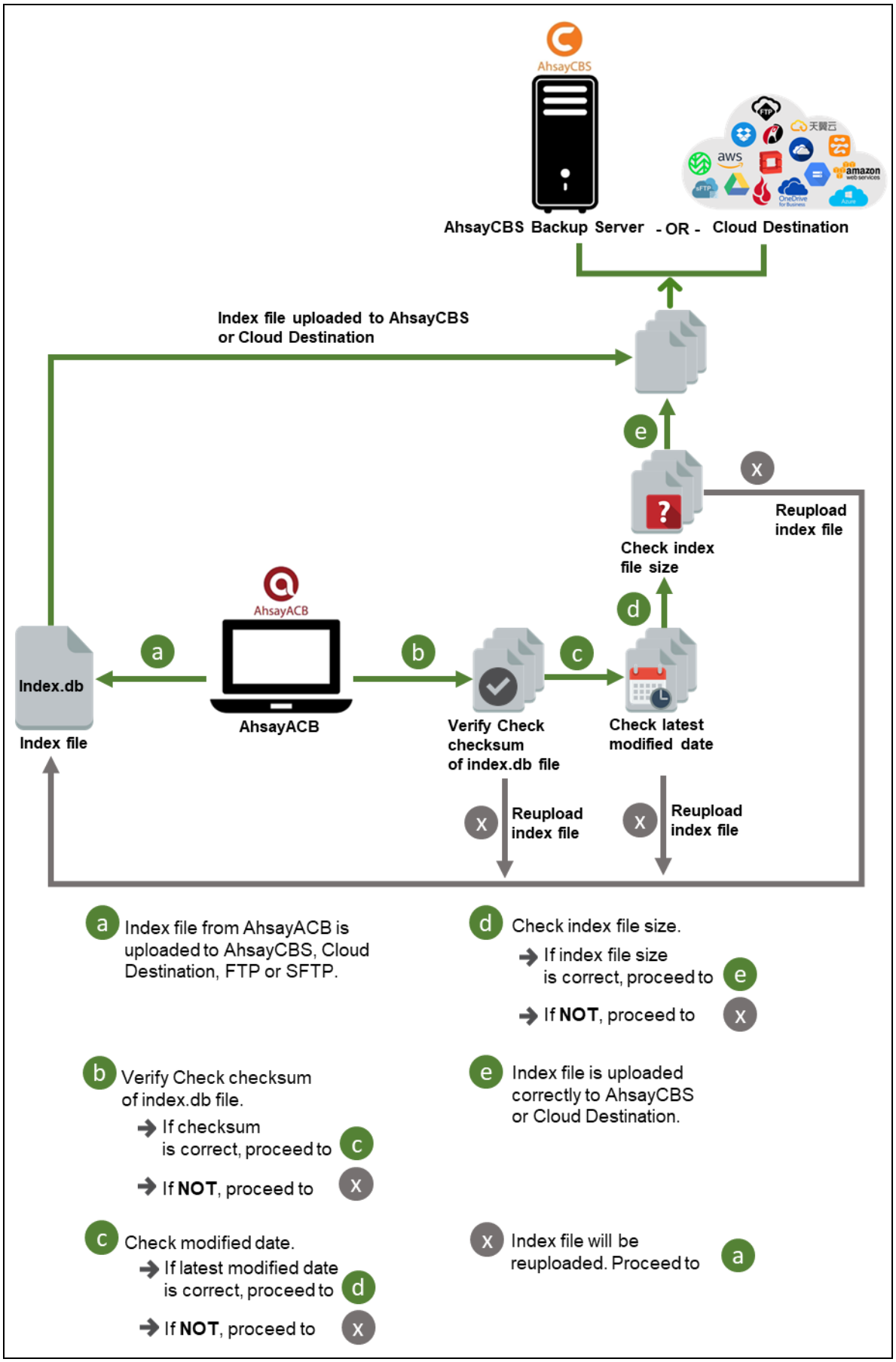
5.2 Backup Set Index Handling Process

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

5.2.1 Start Backup Job

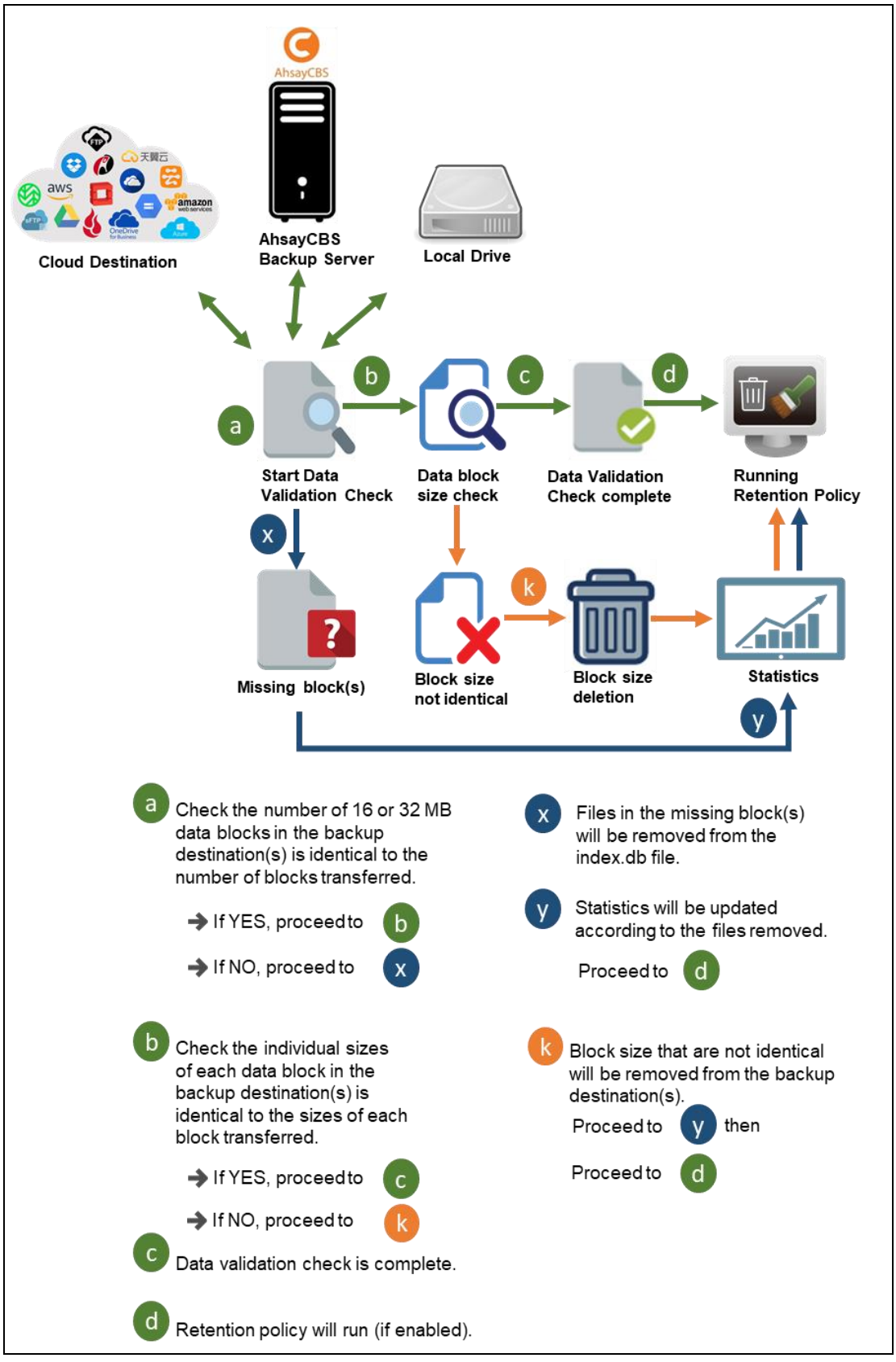


5.2.2 Completed Backup Job



5.3 Data Validation Check Process

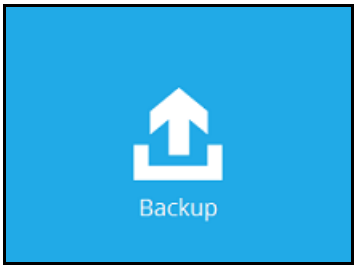
As an additional measure to ensure that all files transferred to the backup destination(s) are received and saved correctly, both the number of 16 or 32 MB data block files and the size of each block file are checked again after the files are transferred.



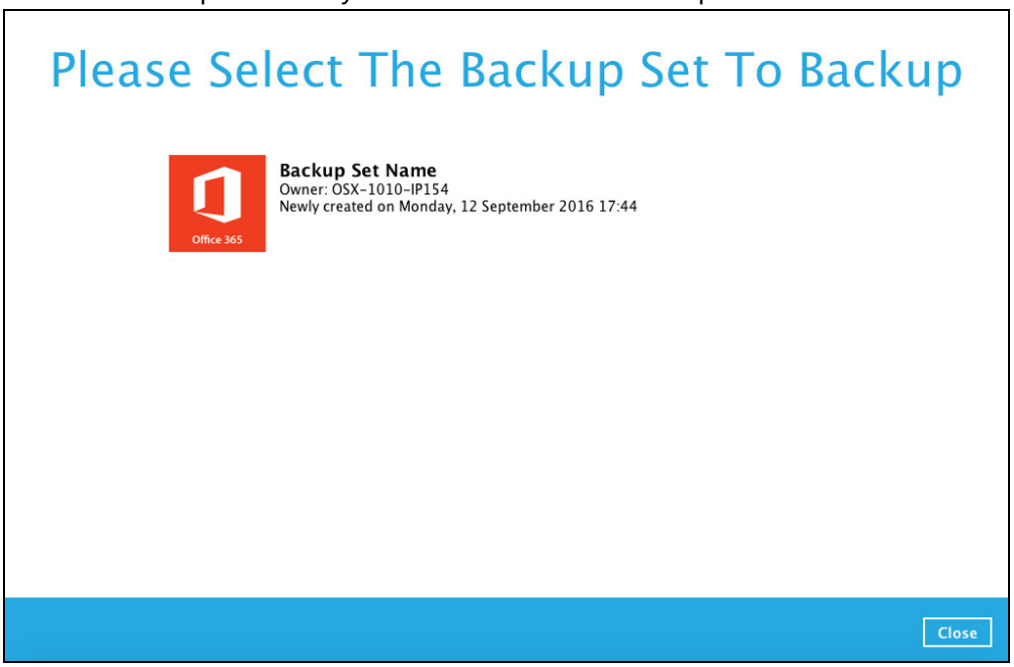
6 Running Backup Job

1. Login to AhsayACB according to the instructions in Login to AhsayACB.

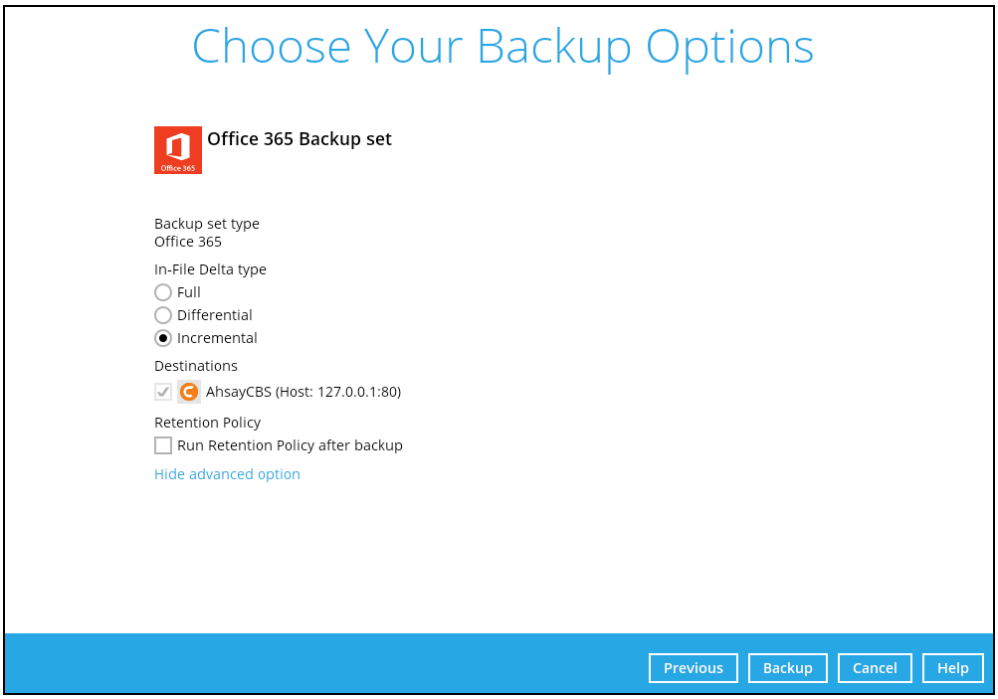
2. Click the **Backup** icon on the main interface of AhsayACB.



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**.



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

7 Restoring Office 365 Backup Set

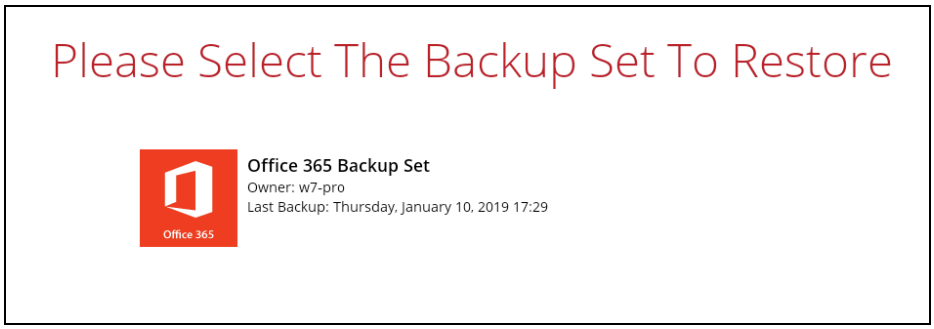
Follow the instructions below to restore the Office 365 backup to the original and alternate Office 365 account.

7.1 Restore Backup with AhsayACB

5. Login to AhsayACB according to the instructions in Login to AhsayACB.

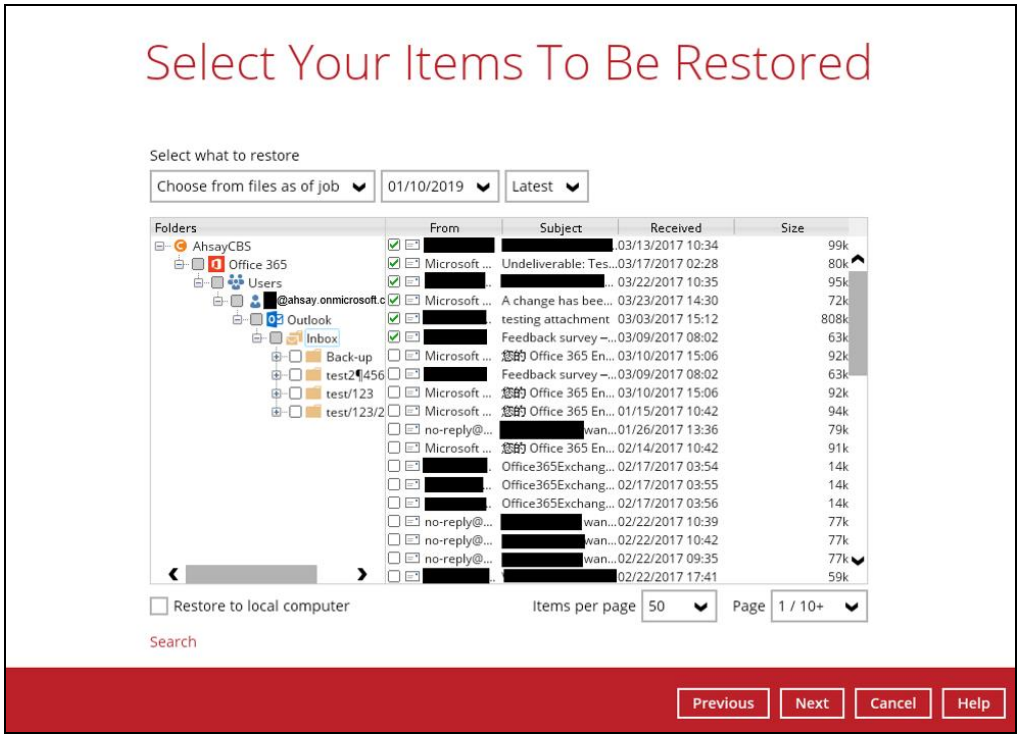
6. Click the **Restore** icon on the main interface of AhsayACB.

7. Select the backup set that you would like to restore.



8. Select the backup destination that you would like to restore mail items to.

9. Select the item(s) you would like to restore. You can also choose to restore backed up file from a specific backup job of your choice using the **Select what to restore** drop-down menu at the top. Click **Next** to proceed when you are done with the selection.



10. The backed-up items can be restored to the Original location and Alternate Office 365 account. Click **Next** when you see this screen to proceed.

7.1.1 Local machine

Tick the **Restore to local computer** checkbox and click **Next** to proceed.

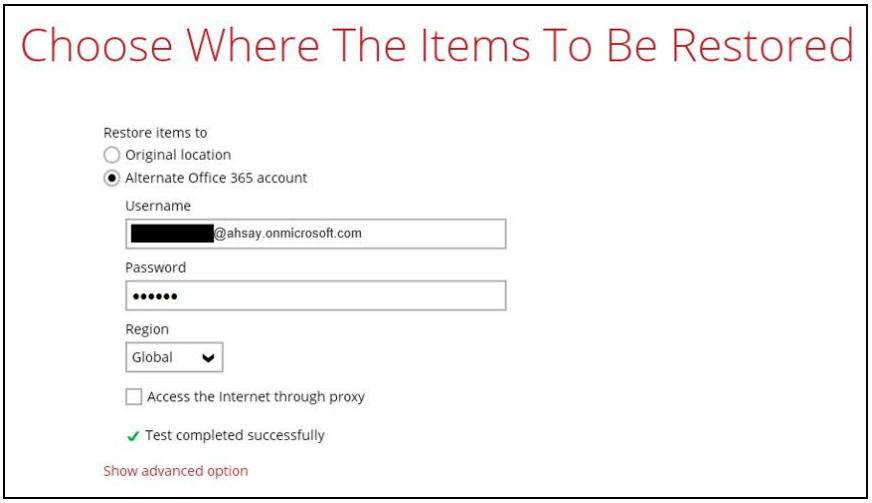
Click the **Browse** button to select a path on where you want the items to be restored on your local computer. Make sure it has enough space to accommodate your restoration.

7.1.2 Original Location

Restore items to the original location where you backed them up.

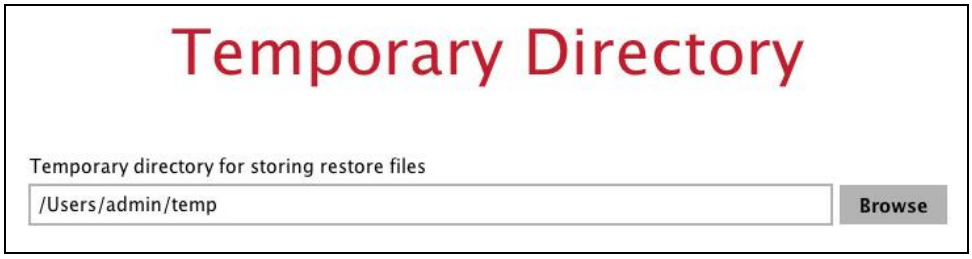
7.1.3 Alternate Office 365 Account

Restore items to another Office 365 account. Input the Username and Password and choose the region for the other Office 365 account and press **Test** to validate the account.



Test completed successfully shows when the validation is successful, then click **Next** to continue.

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



7.2 Restore Filter with AhsayACB

This search feature allows you to search files, folders, and mails. For Office 365, these items can be search from **Users** and **Public Folders.**

For Users, you can search from Outlook, OneDrive, and Personal Site.

To make it more flexible, the search feature offers filtering. You can add additional pattern upon searching. Pattern includes the following criteria:

Contains
These are Directories, Files, Folders, and Mails with the name **containing** the specific letter or word.

Exact
These are Directories, Files, Folders, and Mails with the **exact** or **accurate** name.

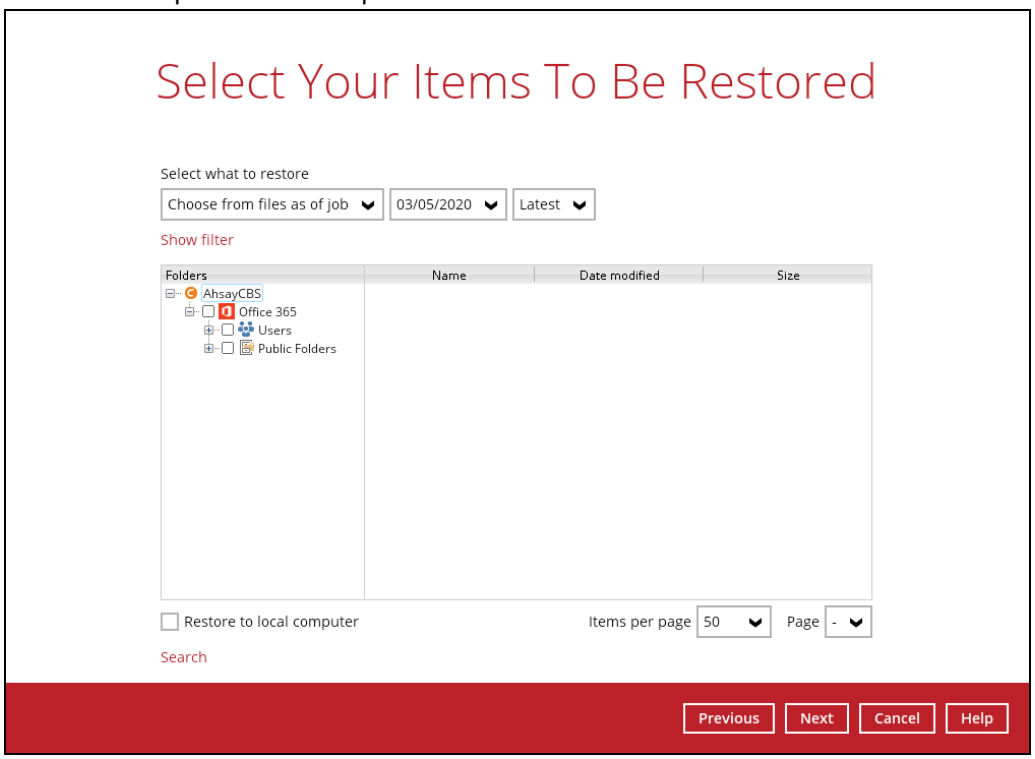
Start With
These are Directories, Files, Folders, and Mails with the name **starting** with a specific letter or word.

Ends With
These are Directories, Files, Folders, and Mails with the name **ending** with a specific letter or word.

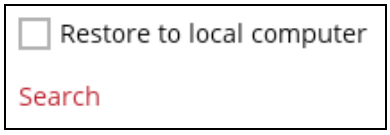
It also has the **Match Case** function, which serves as an additional accuracy when searching for any specific directories, files, folders, and mails.

For more detailed examples using the restore filter on AhsayACB, refer to Appendix B: Example Scenarios for Restore Filter using AhsayACB.

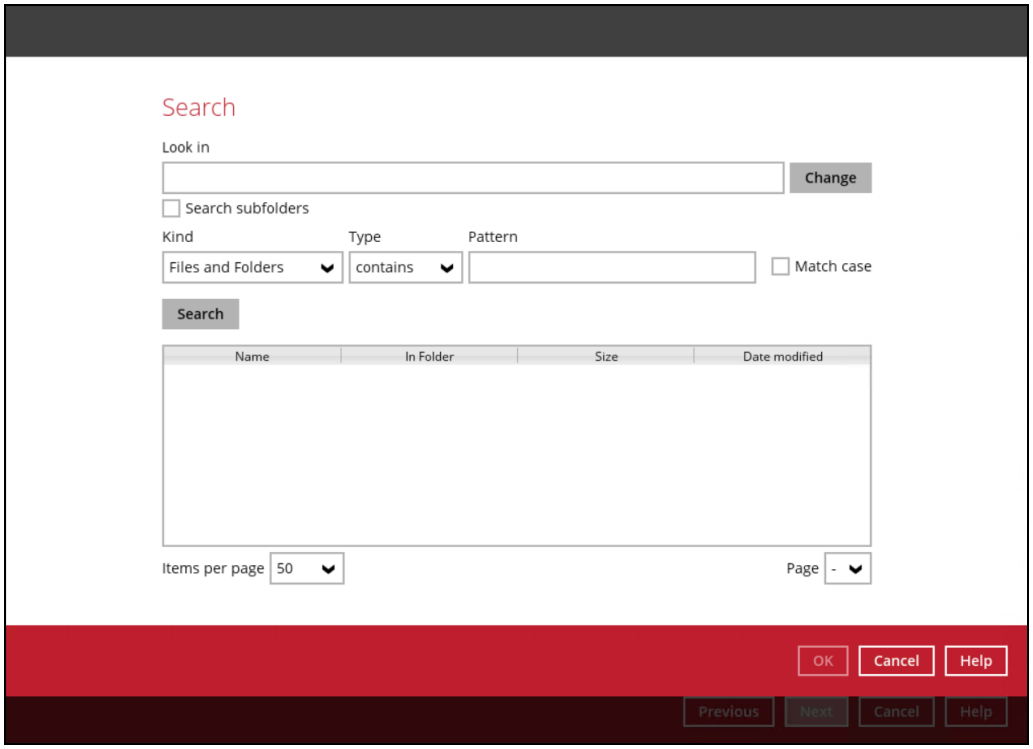
1. Login to AhsayACB according to the instructions in Login to AhsayACB.
2. Click the Restore icon on the main interface of AhsayACB.
3. Select the backup set that you would like to restore.
4. Select the backup destination that you would like to restore backed-up items to.
5. Select the item(s) you would like to restore. You can also choose to restore backed-up file from a specific backup job of your choice using the Select what to restore drop-down menu at the top. Click Next to proceed.

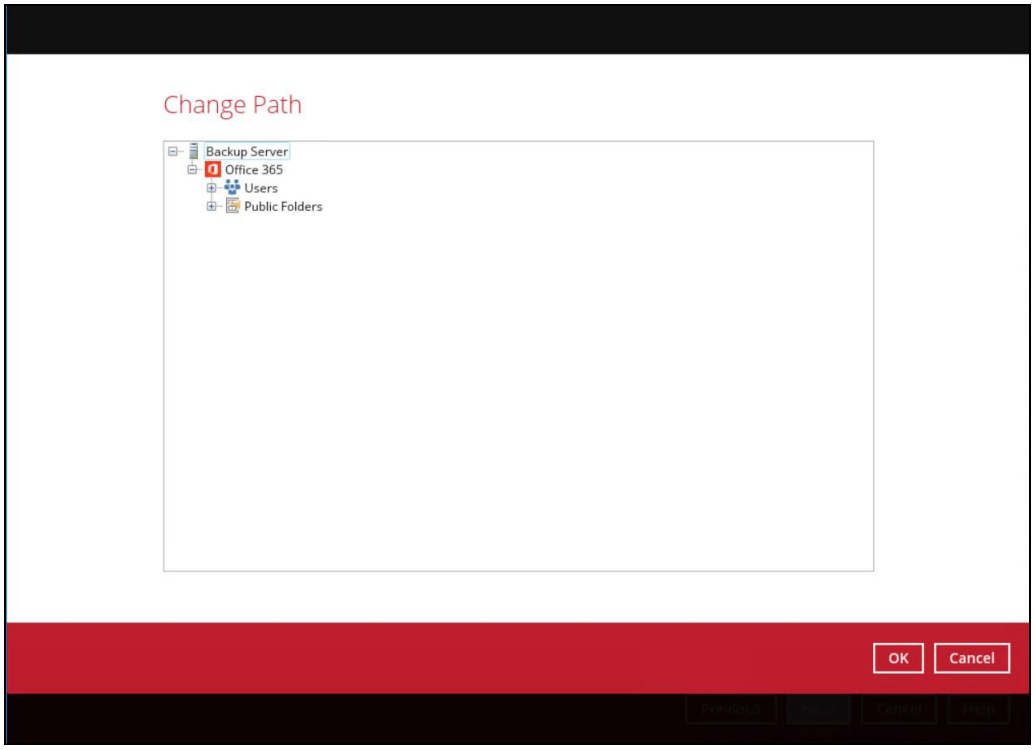


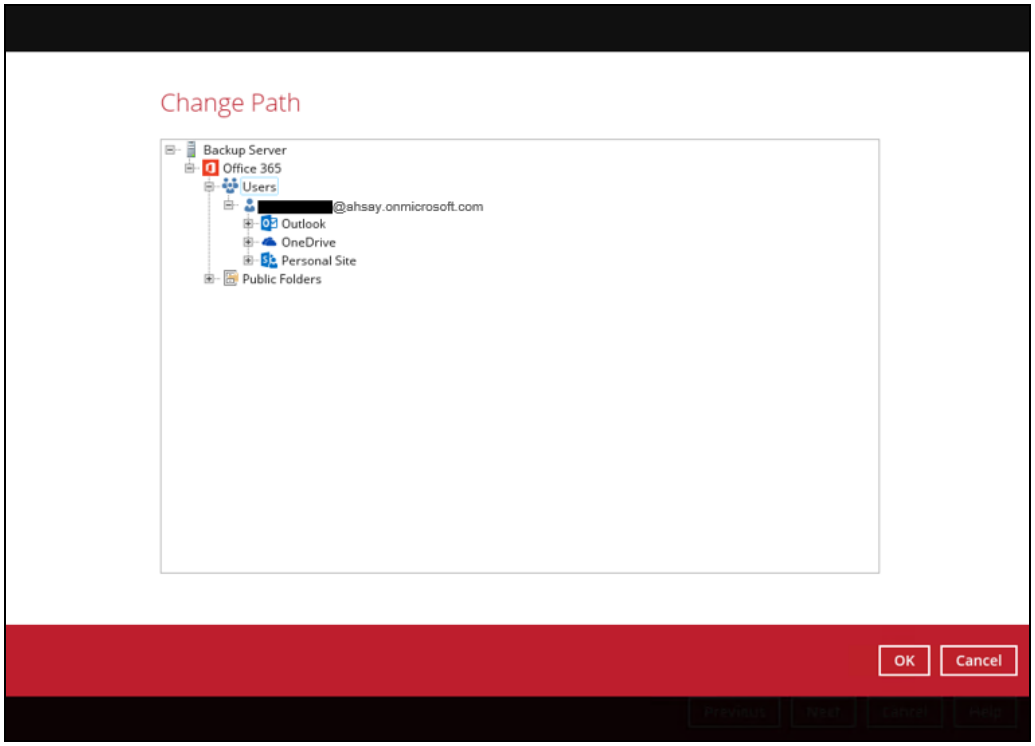
Click the Search located below the Restore to local computer checkbox.



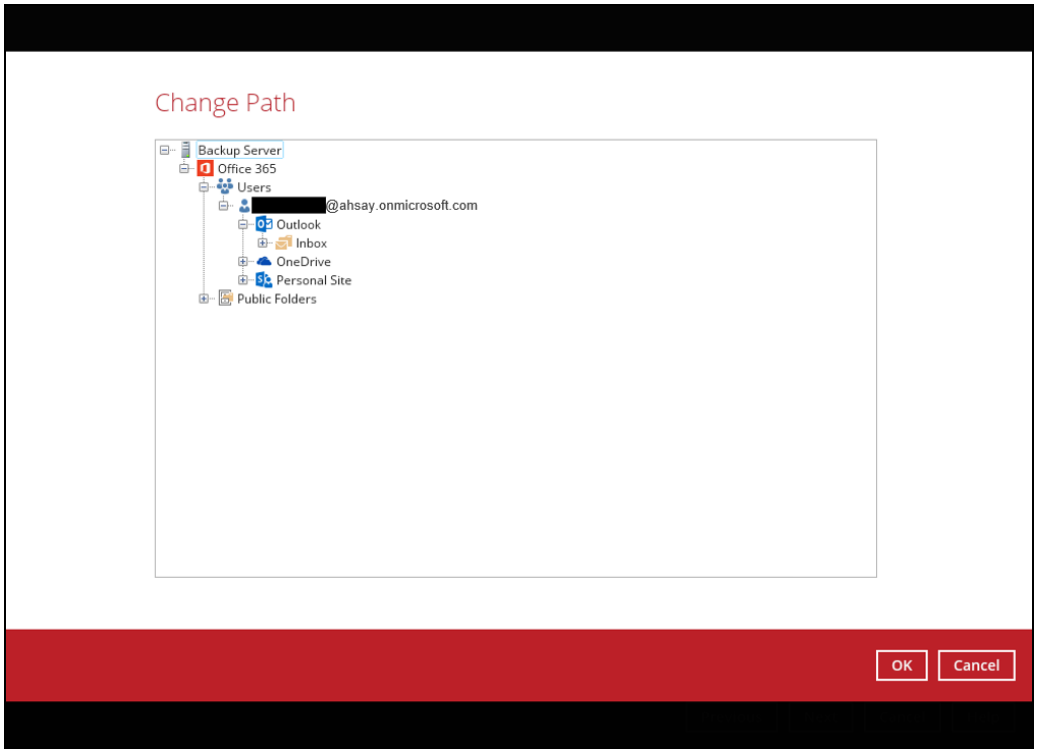
Change the path if you want to restore items from other location. Click the Change button then click OK to proceed.

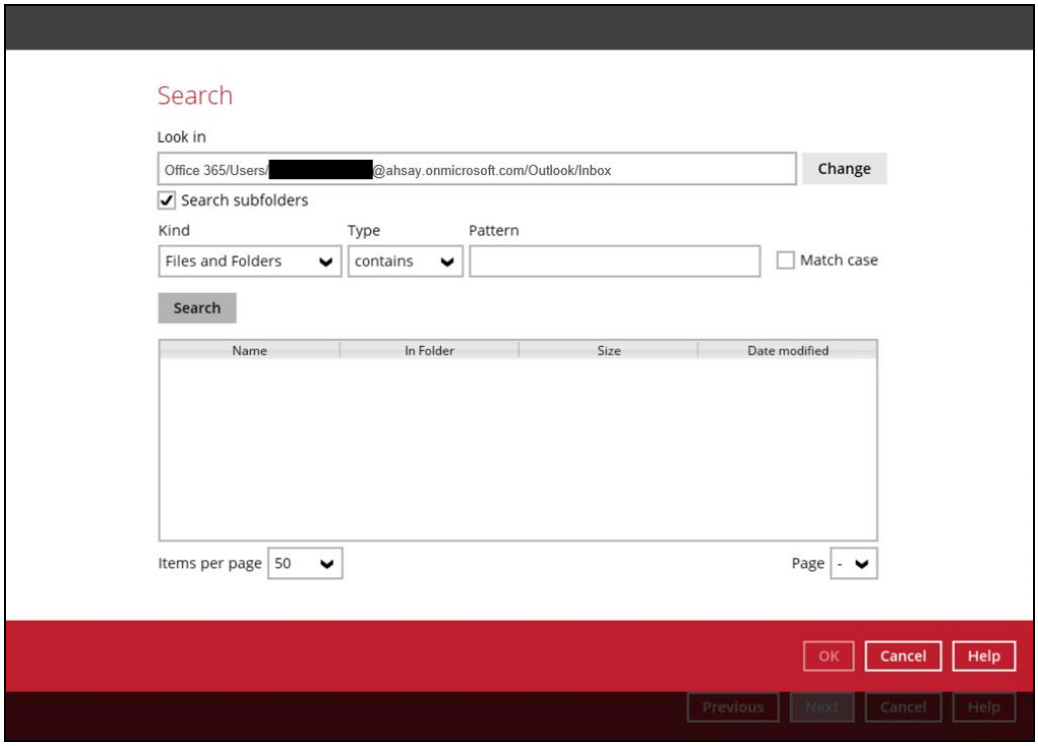

Search
Look in
Change
Search subfolders
Kind
Type
Pattern
Files and Folders
contains
Match case
Search
Name
In Folder
Size
Date modified
Items per page
50
Page
-
OK
Cancel
Help
Previous
Next
Cancel
Help


Change Path
Backup Server
Office 365
Users
Public Folders
OK
Cancel



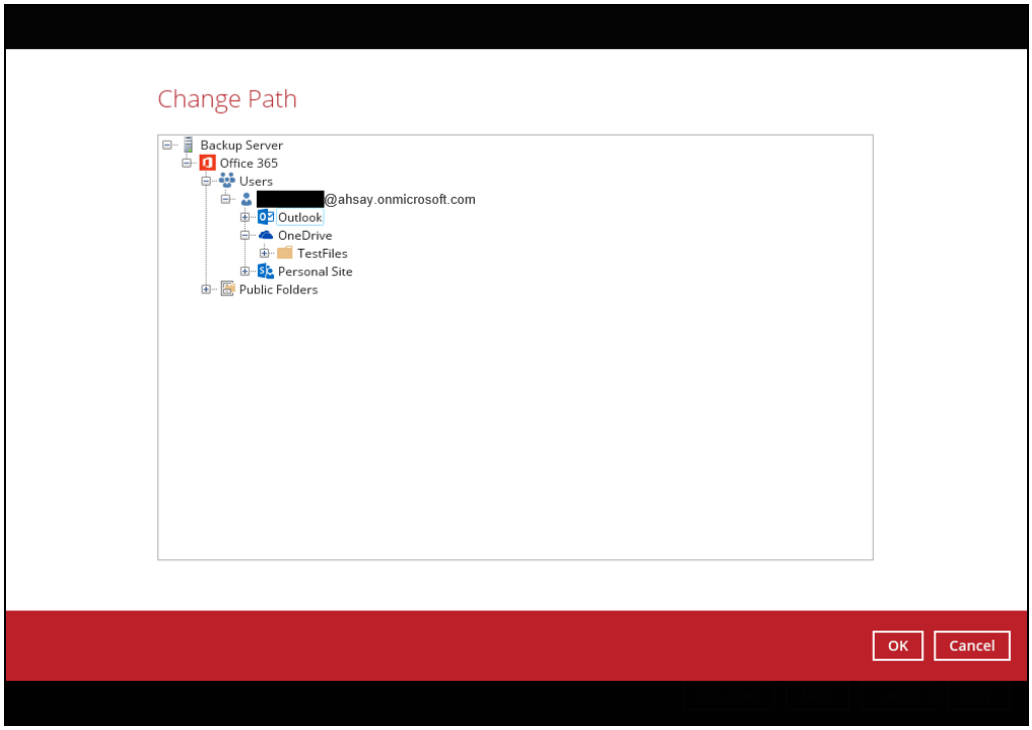
If you are going to search for specific mails, then click the Outlook to expand for more selection. In our example below, **Inbox** of **abc@ahsay.onmicrosoft.com** is selected.

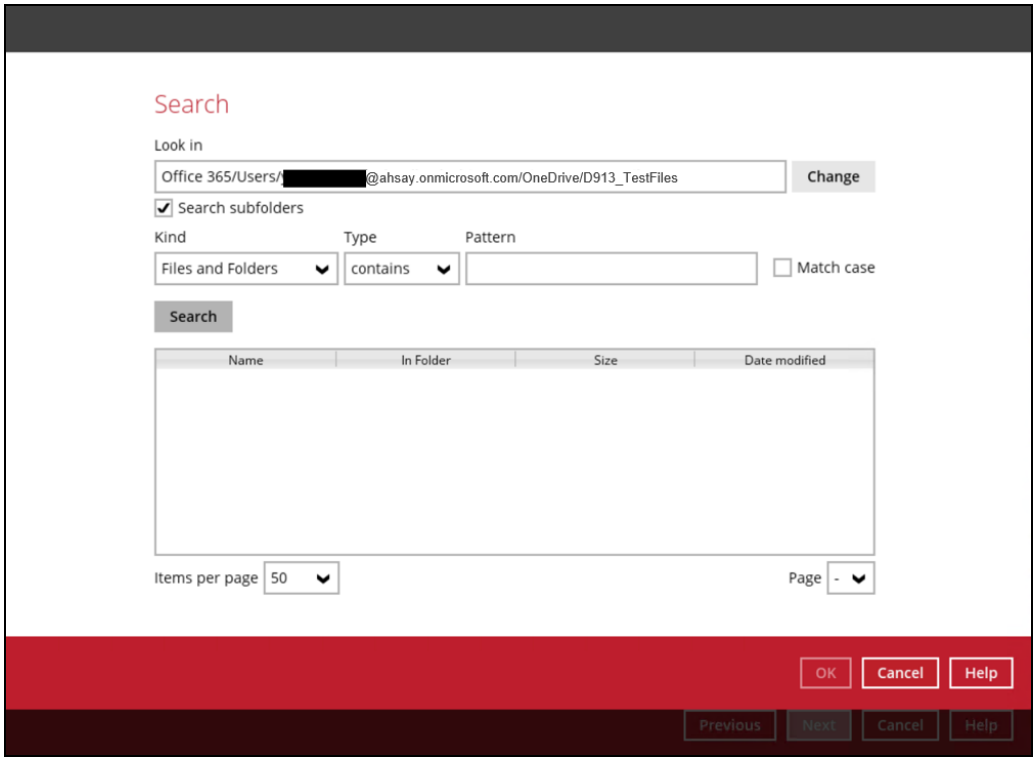




OR

If you are going to search for specific files and/or folders, then click the OneDrive to expand for more selection. In our example below, **TestFiles** folder in **OneDrive** is selected.

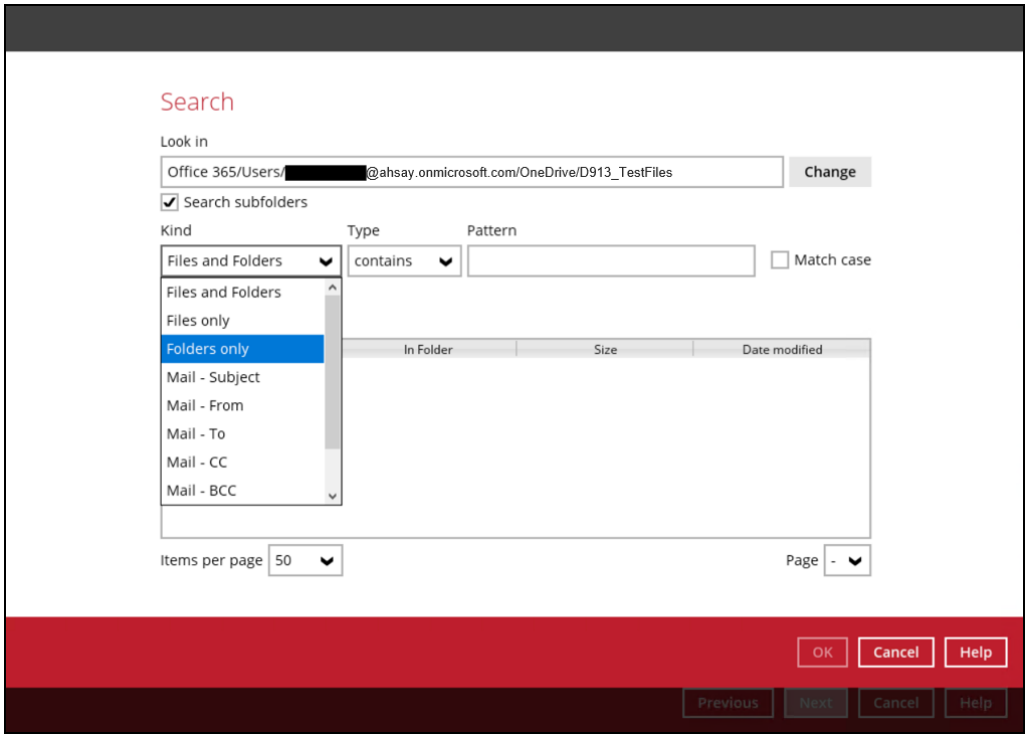




Tick the Search subfolders checkbox if you want to include available subfolders upon searching.

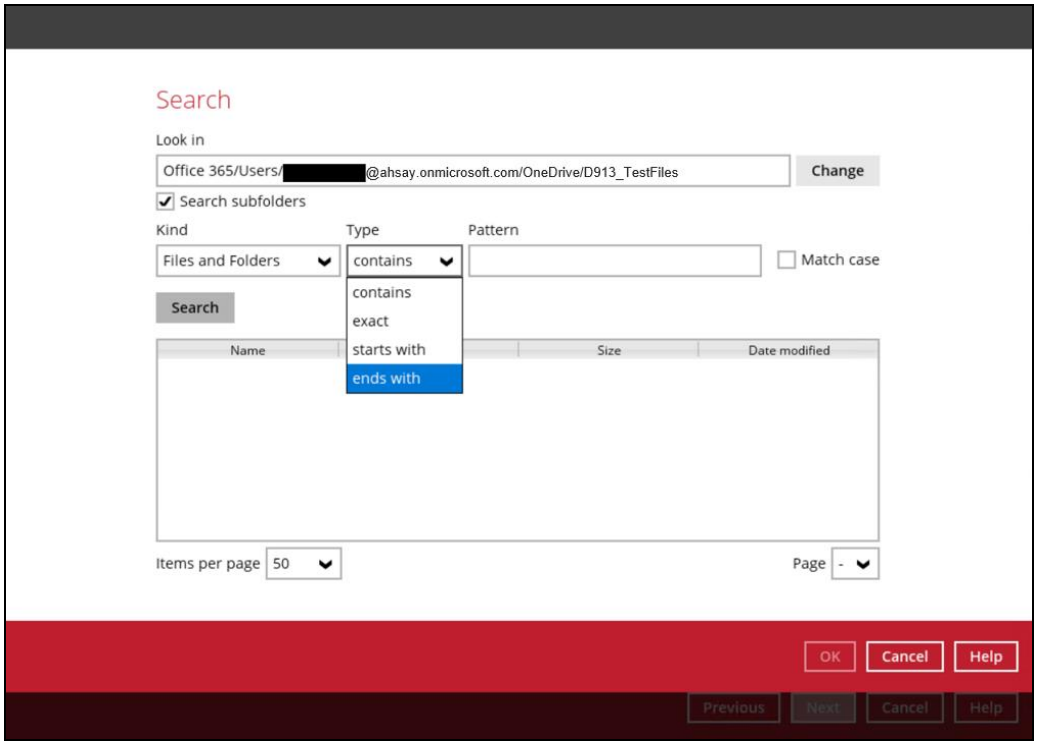
Select from the following kind of files you want to search.

- Files and Folders
- Files only
- Folders only
- Mail – Subject
- Mail – From
- Mail – To
- Mail – CC
- Mail – BCC
- Mail – Received Date
- Mail – Sent Date

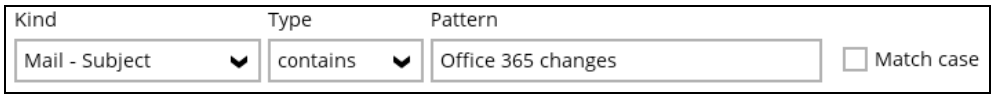


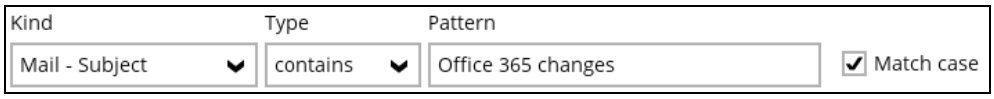
Select from the following type of filtering you want to search.

- Contains
- Exact
- Starts With
- Ends With

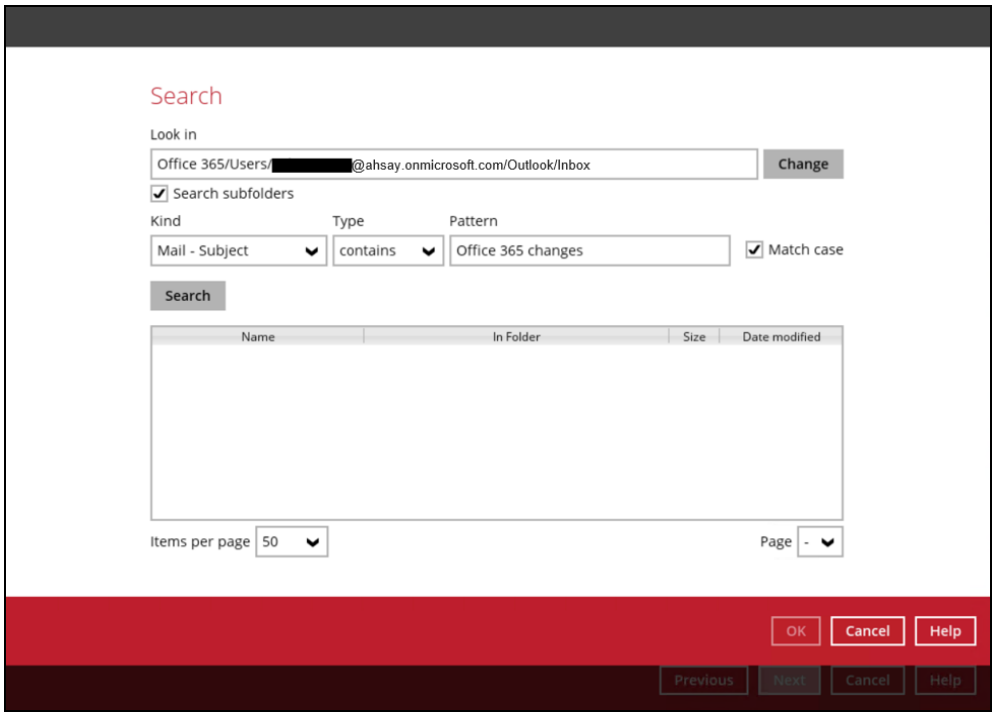


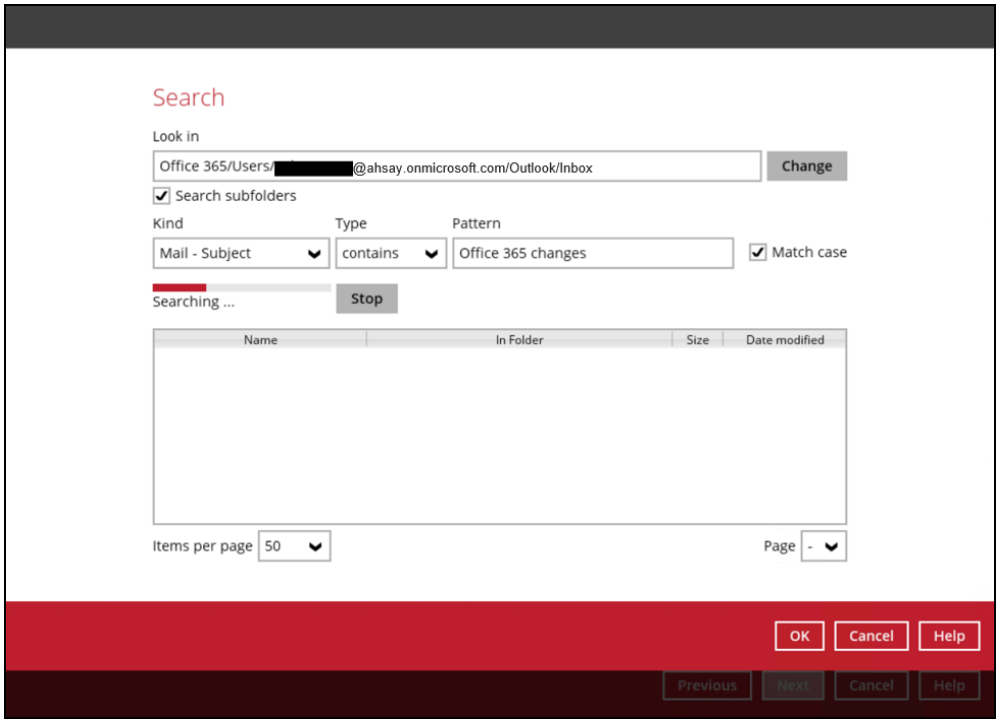
Enter a pattern you want and Tick the Match Case checkbox if you want to accurately search for a specific file.



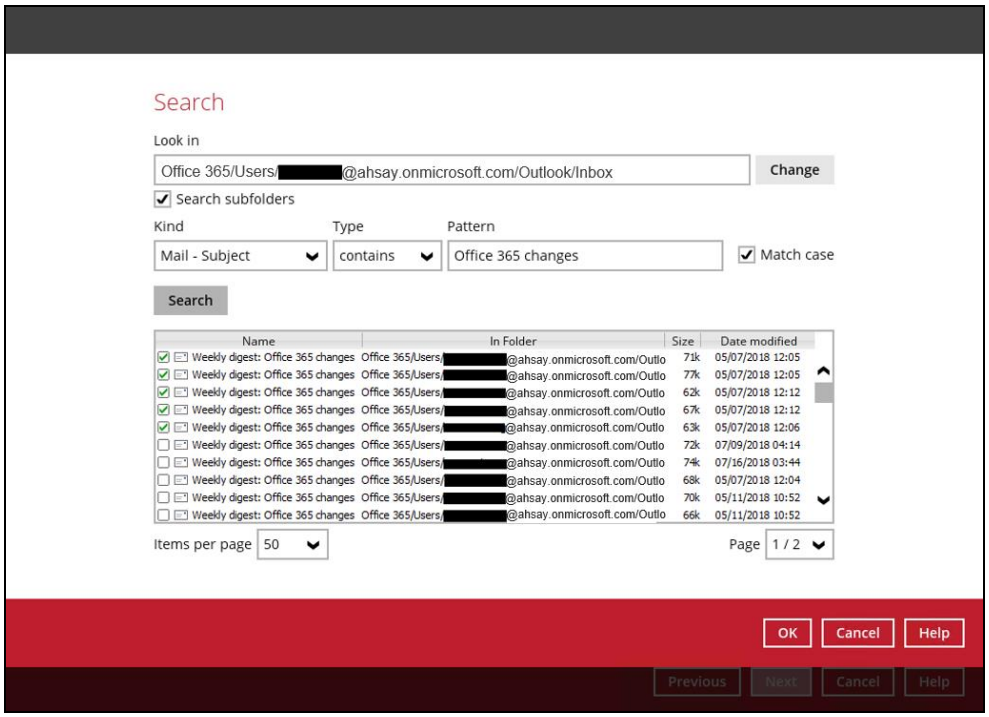


Click the Search button and the result will be displayed.

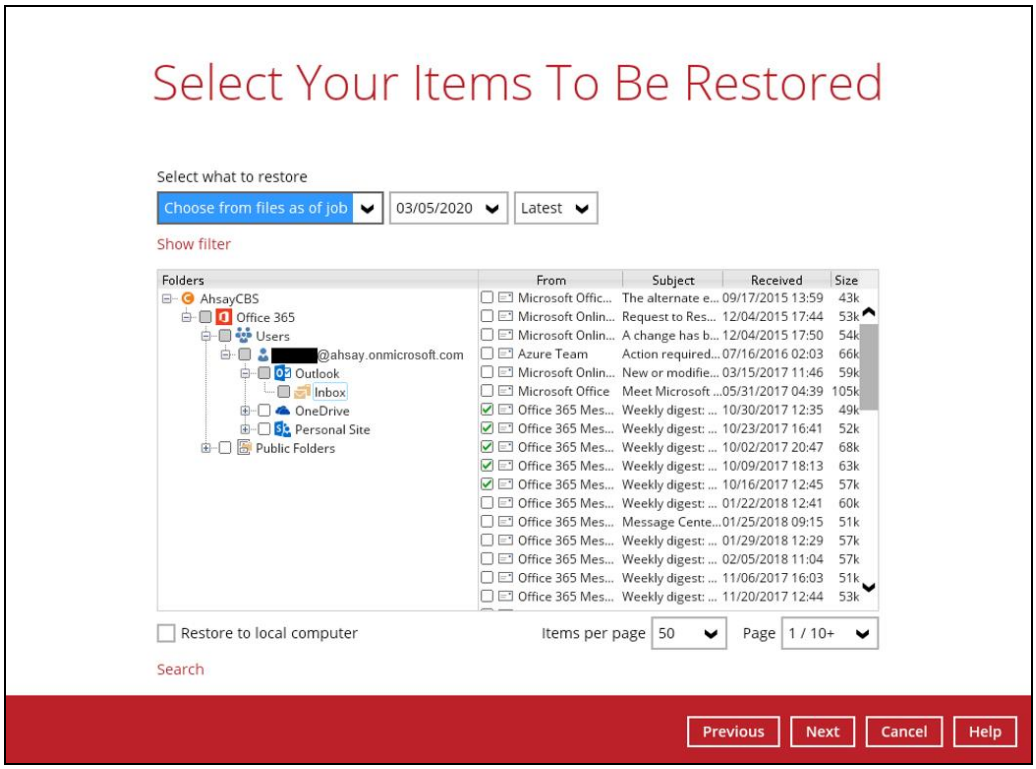




Choose files by ticking each checkbox that you wanted to restore and click the OK button.



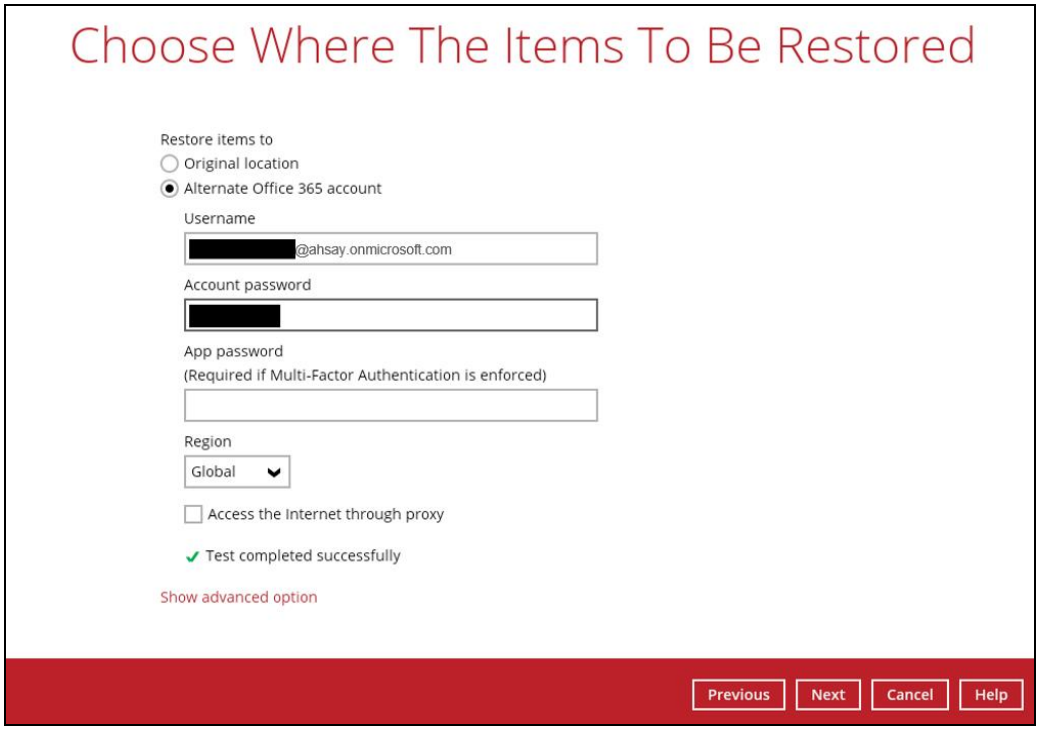
The selected files will reflect on the Restore main screen. Click the Next button to proceed.



Select which location the items will be restored. Choose from the following options:

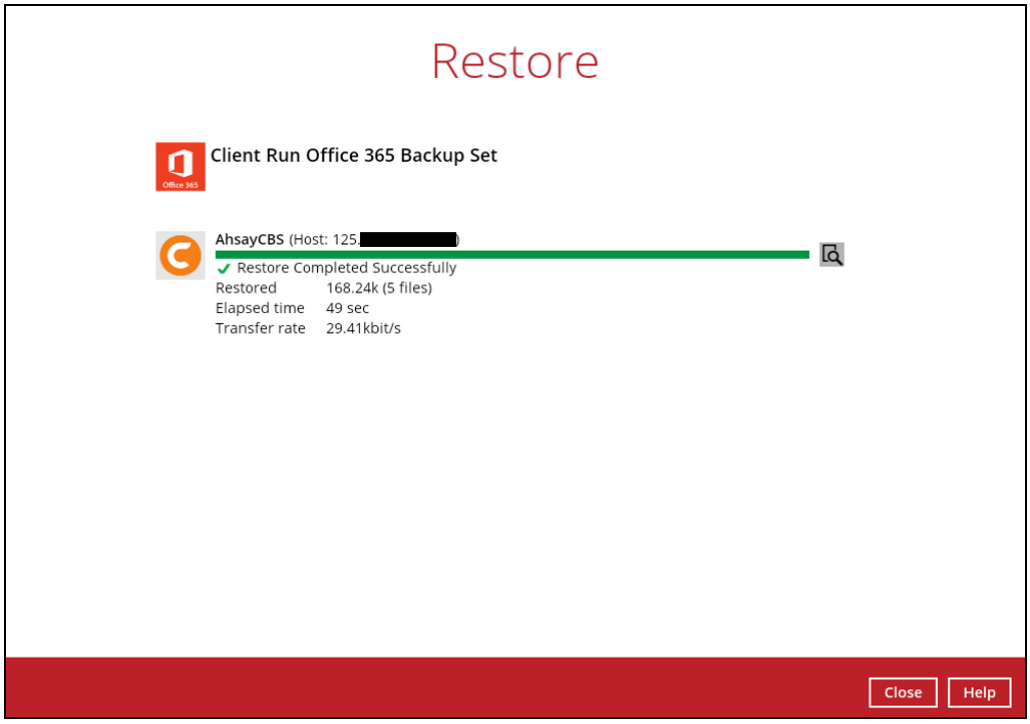
- Local machine – this option is located on the Restore main screen, lower left part.
- Original location
- Alternate Office 365 account

Click the Next button to proceed.



Input the temporary directory or click the Browse button to browse for the path. Click the Restore button to start.

If restore is completed, the status of the activity should be, Restore Completed Successfully.



8 Contacting Ahsay

8.1 Technical Assistance

To contact Ahsay support representatives for technical assistance, visit the following website:
https://www.ahsay.com/jsp/en/contact/kbQuestion.jsp

Also use the Ahsay Wiki for resource such as Hardware Compatibility List, Software Compatibility List, and other product information:
http://wiki.ahsay.com/doku.php?id=public:home

8.2 Documentation

Documentations for all Ahsay products are available at:
https://www.ahsay.com/jsp/en/home/index.jsp?pageContentKey=ahsay_downloads_documentation_guides

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

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

Appendix

Appendix A Example Scenarios for Office 365 License Requirement and Usage

Note that maximum of two (2) Office 365 accounts are only allowed for Office 365 Backup on AhsayACB. Each AhsayACB Office 365 backup set is limited to one Office 365 user account. Therefore, when you backup two Office 365 user accounts it will require two separate backup sets.

Scenario No. 1: Backing up Office 365 user accounts in multiple backup sets

The required Office 365 licenses are calculated by the number of Office 365 user accounts that you want to backup.

Example No. 1: To back up one (1) Office 365 user account on multiple backup sets, only one Office 365 license is needed.

Backup Set Name	Office 365 User Account
Backup Set A	user01@company-office365.com
Backup Set B	user01@company-office365.com
Backup Set C	user01@company-office365.com

Example No. 2: To back up two (2) Office 365 user accounts on multiple backup sets, two Office 365 licenses are needed.

Backup Set Name	Office 365 User Account
Backup Set A	user01@company-office365.com
Backup Set B	user02@company-office365.com

Scenario No. 2: Backing up files and/or folders under Public Folder in multiple backup sets.

The required Office 365 license is only one.

Example No. 1: To back up files and/or folders under Public Folder, only one (1) Office 365 license is needed.

Backup Set Name	Files and/or Folders
Backup Set A	Folder01 ○ microsoftword01.docx ○ powerpointpresentation01.pptx ○ spreadsheet01.xls ○ notepad01.txt ○ picture01.jpg ○ picture02.jpg
Backup Set B	Folder01 ○ microsoftword01.docx ○ powerpointpresentation01.pptx ○ spreadsheet01.xls ○ notepad01.txt ○ picture01.jpg ○ picture02.jpg
	Folder02
	Folder03
Backup Set C	Folder01 ○ microsoftword01.docx ○ powerpointpresentation01.pptx ○ spreadsheet01.xls ○ notepad01.txt ○ picture01.jpg ○ picture02.jpg
	Folder02
	Folder03 ○ microsoftword02.docx ○ powerpointpresentation02.pptx ○ spreadsheet02.xls ○ notepad02txt ○ picture05.jpg ○ picture06.jpg

Scenario No. 3: Backing up Office 365 User Accounts and files and/or folders under Public Folder in multiple backup sets.

The required Office 365 license will depend on the number of unique Office 365 accounts.

Example No. 1: To back up two (2) Office 365 user accounts and files and/or folders under Public Folder on multiple backup sets, two (2) Office 365 licenses are needed.

Backup Set Name	Office 365 User Account, SharePoint Site, and Files and/or Folders
Backup Set A	user01@company-office365.com
Backup Set B	Folder01 ○ microsoftword01.docx ○ powerpointpresentation01.pptx ○ spreadsheet01.xls ○ notepad01.txt ○ picture01.jpg ○ picture02.jpg
Backup Set C	Folder01 ○ microsoftword01.docx ○ powerpointpresentation01.pptx ○ spreadsheet01.xls ○ notepad01.txt ○ picture01.jpg ○ picture02.jpg

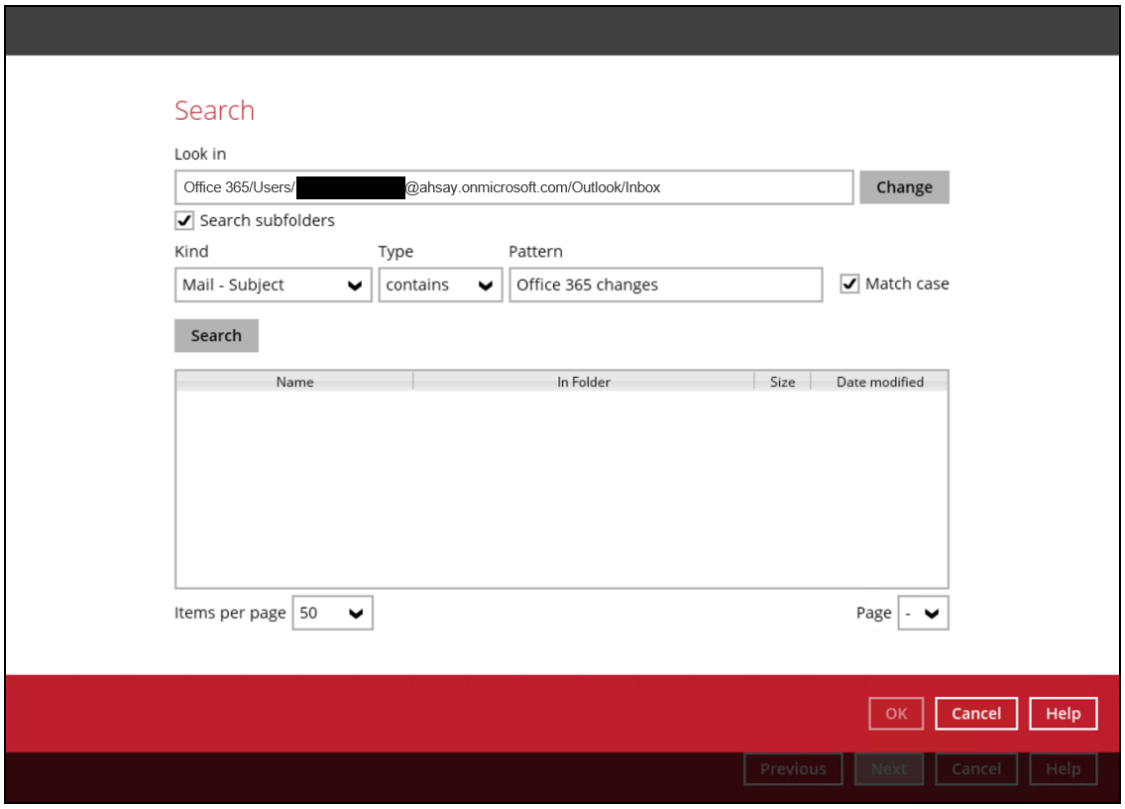
Appendix B Example Scenarios for Restore Filter using AhsayACB

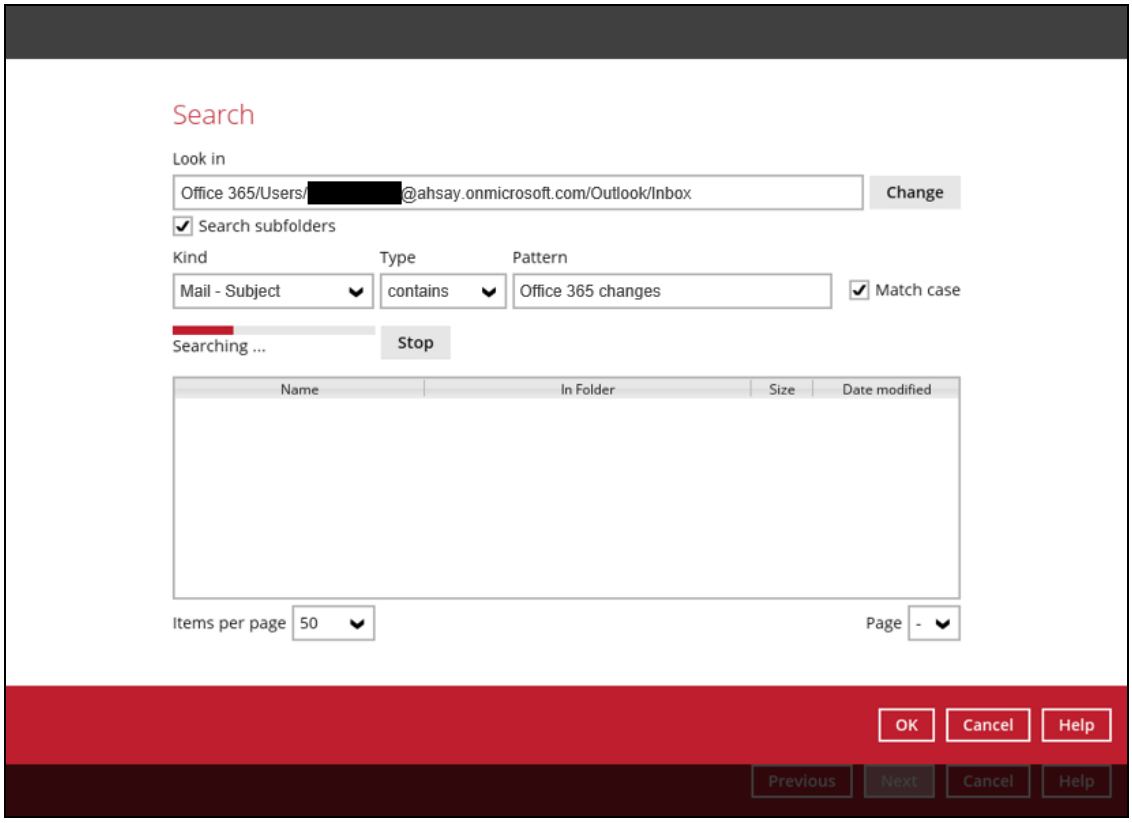
Scenarios No. 1: Items from Users

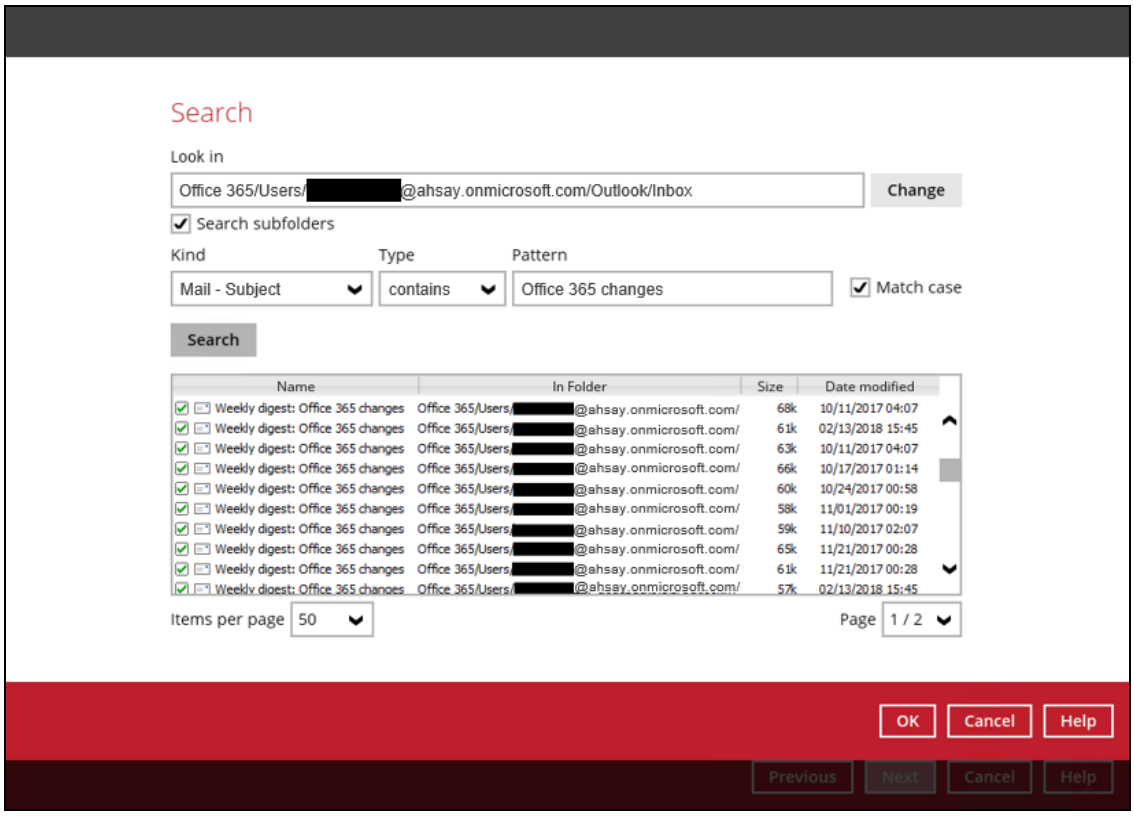
Example No. 1: Restore filter setting from an Office 365 user account's outlook inbox

Location:	Office 365/Users/abc@ahsay.onmicrosoft.com/Outlook/Inbox
Search subfolders:	True
Kind:	Mail – Subject
Type:	Contains
Pattern:	Office 365 changes
Match Case:	True

Follow the step-by-step procedure indicated on Restore Filter with AhsayACB.




Search
Look in
Office 365/Users/[redacted]@ahsay.onmicrosoft.com/Outlook/Inbox
Change
Search subfolders
Kind
Type
Pattern
Mail - Subject
contains
Office 365 changes
Match case
Searching ...
Stop
Name
In Folder
Size
Date modified
Items per page
50
Page
-
OK
Cancel
Help
Previous
Next
Cancel
Help


Search
Look in
Office 365/Users/[redacted]@ahsay.onmicrosoft.com/Outlook/Inbox
Change
Search subfolders
Kind
Type
Pattern
Mail - Subject
contains
Office 365 changes
Match case
Search
Name
In Folder
Size
Date modified
Weekly digest: Office 365 changes
Office 365/Users/[redacted]@ahsay.onmicrosoft.com/
68k
10/11/2017 04:07
61k
02/13/2018 15:45
63k
10/11/2017 04:07
66k
10/17/2017 01:14
60k
10/24/2017 00:58
58k
11/01/2017 00:19
59k
11/10/2017 02:07
65k
11/21/2017 00:28
61k
11/21/2017 00:28
57k
02/13/2018 15:45
Items per page
50
Page
1 / 2
OK
Cancel
Help
Previous
Next
Cancel
Help

Explanation:

All mails under Office 365/Users/abc@ahsay.onmicrosoft.com/Outlook/Inbox that has a subject and contains 'Office 365 changes' with match case set to true will be included upon performing search.

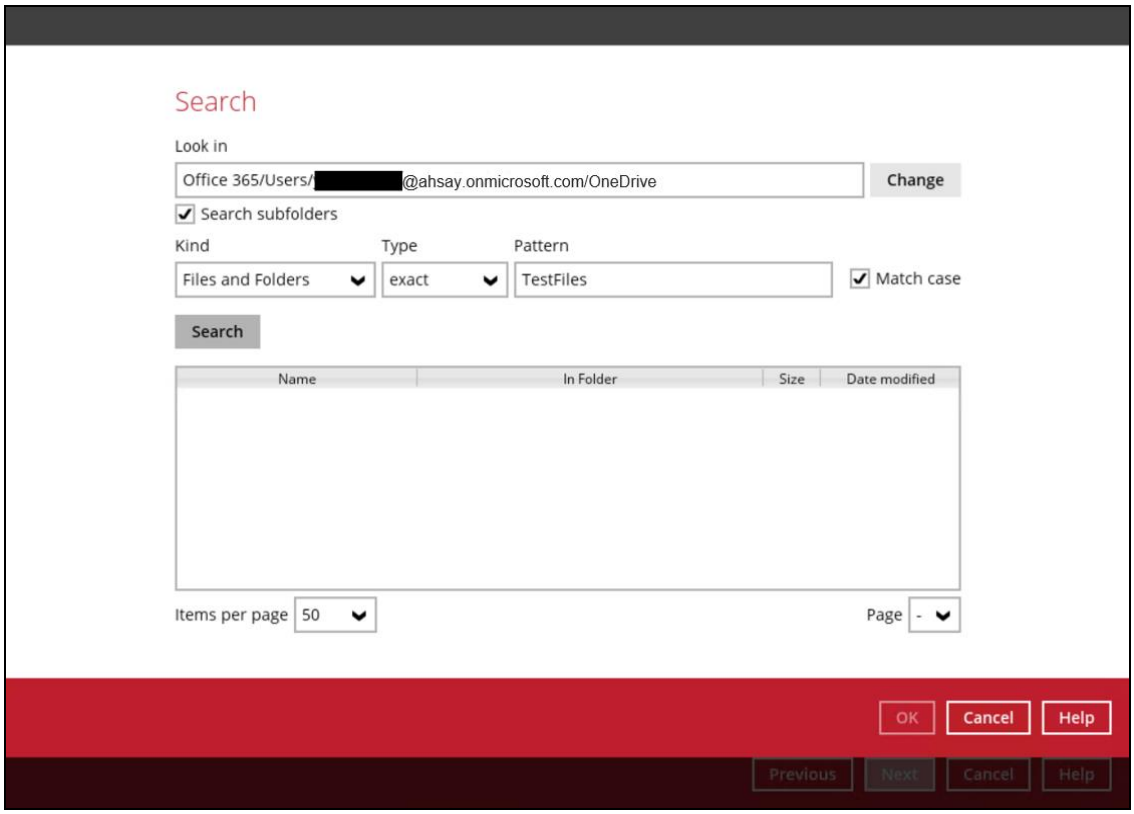
As you can see on the screen shot above, the result panel contains the Name of the mail, Directory of the mails which are indicated In-Folder column, Size of each mails, and Date Modified.

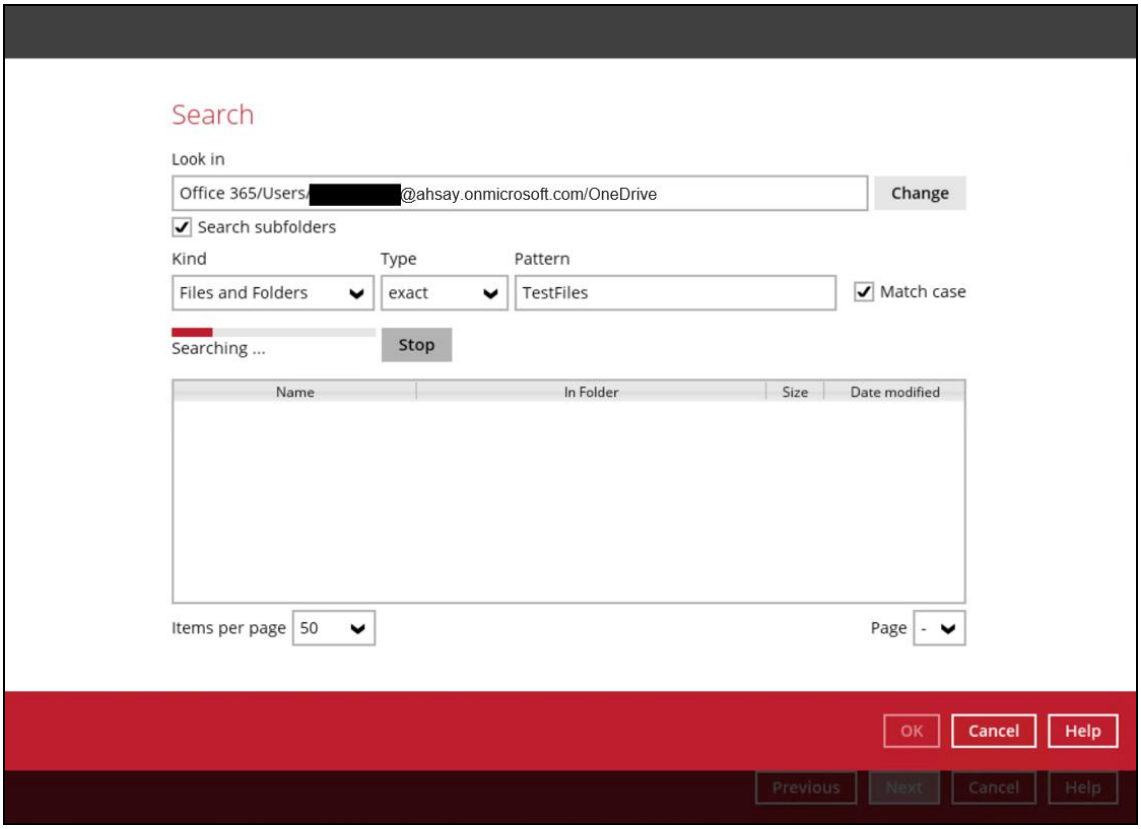
The restore filter setting includes the Search subfolder and Match case set to true. This means that the filter will include all available subfolders in the Outlook Inbox upon searching. And it will strictly search only the specified pattern and case which is the 'Office 365 changes'.

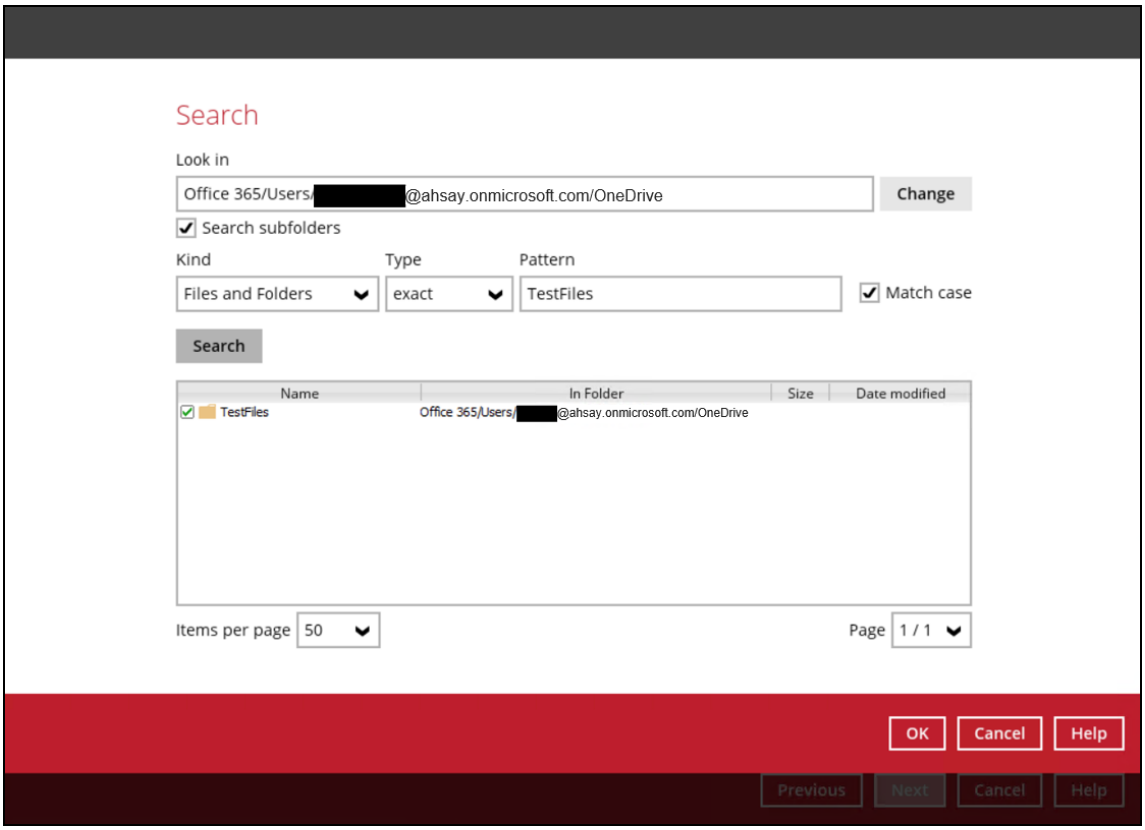
Example No. 2: Restore filter setting from an Office 365 user account's OneDrive

Location:	Office 365/Users/abc@ahsay.onmicrosoft.com/OneDrive
Search subfolders:	True
Kind:	Files and Folders
Type:	Exact
Pattern:	TestFiles
Match Case:	True

Follow the step-by-step procedure indicated on Restore Filter with AhsayACB.




Search
Look in
Office 365/Users/[redacted]@ahsay.onmicrosoft.com/OneDrive
Change
Search subfolders
Kind
Type
Pattern
Files and Folders
exact
TestFiles
Match case
Searching ...
Stop
Name
In Folder
Size
Date modified
Items per page
50
Page
-
OK
Cancel
Help
Previous
Next
Cancel
Help


Search
Look in
Office 365/Users/[redacted]@ahsay.onmicrosoft.com/OneDrive
Change
Search subfolders
Kind
Type
Pattern
Files and Folders
exact
TestFiles
Match case
Search
Name
In Folder
Size
Date modified
TestFiles
Office 365/Users/[redacted]@ahsay.onmicrosoft.com/OneDrive
Items per page
50
Page
1 / 1
OK
Cancel
Help
Previous
Next
Cancel
Help

Explanation:

All files and folders under Office 365/Users/abc@ahsay.onmicrosoft.com/OneDrive that has the exact pattern of 'TestFiles' with match case set to true will be included upon performing search.

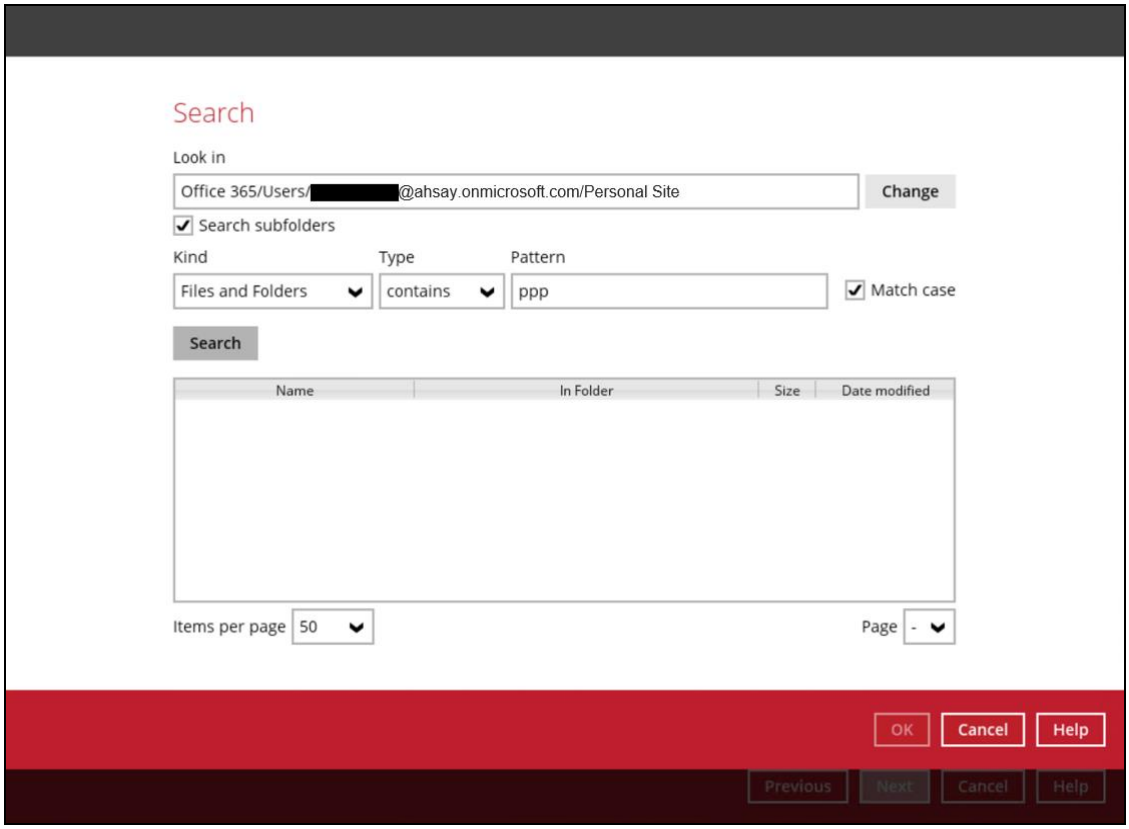
As you can see on the screen shot above, the result panel contains the Name of the mail, Directory of the mails which are indicated In-Folder column, Size of each mails, and Date Modified.

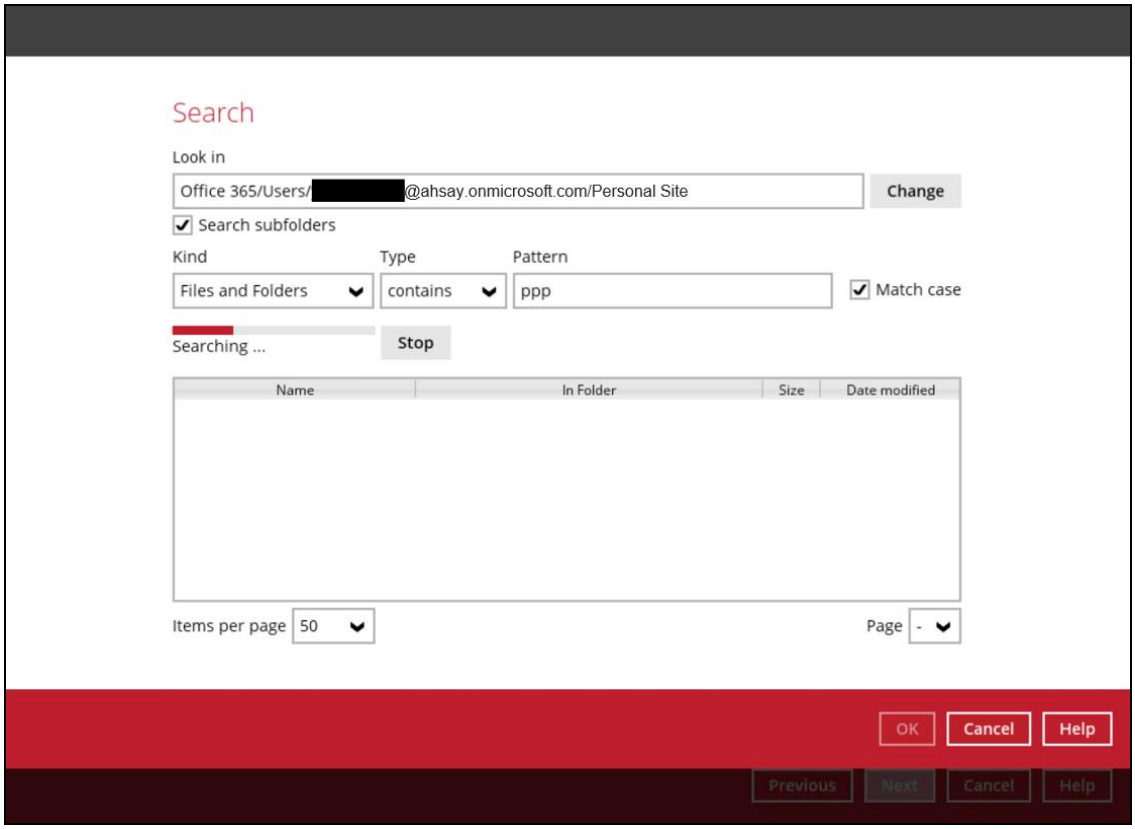
The restore filter setting includes the Search subfolder and Match case set to true. This means that the filter will include all available subfolders in OneDrive upon searching. And it will strictly search only the specified pattern and case which is the 'TestFiles'.

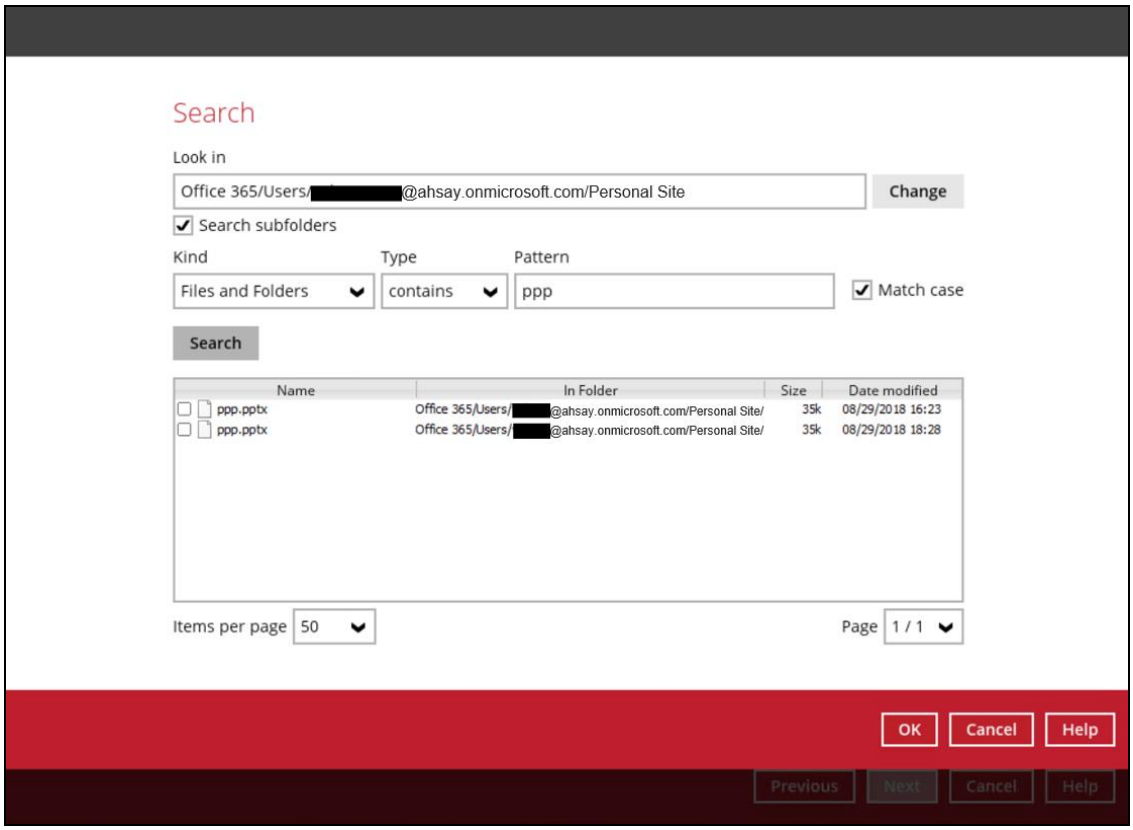
Example No. 3: Restore filter setting from an Office 365 user account's personal site

Location:	Office 365/abc@ahsay.onmicrosoft.com/Personal Site
Search subfolders:	True
Kind:	Files and Folders
Type:	contains
Pattern:	ppp
Match Case:	True

Follow the step-by-step procedure indicated on Restore Filter with AhsayACB.




Search
Look in
Office 365/Users/[redacted]@ahsay.onmicrosoft.com/Personal Site
Change
Search subfolders
Kind
Type
Pattern
Files and Folders
contains
ppp
Match case
Searching ...
Stop
Name
In Folder
Size
Date modified
Items per page
50
Page
-
OK
Cancel
Help
Previous
Next
Cancel
Help


Search
Look in
Office 365/Users/[redacted]@ahsay.onmicrosoft.com/Personal Site
Change
Search subfolders
Kind
Type
Pattern
Files and Folders
contains
ppp
Match case
Search
Name
In Folder
Size
Date modified
ppp.pptx
Office 365/Users/[redacted]@ahsay.onmicrosoft.com/Personal Site/
35k
08/29/2018 16:23
ppp.pptx
Office 365/Users/[redacted]@ahsay.onmicrosoft.com/Personal Site/
35k
08/29/2018 18:28
Items per page
50
Page
1 / 1
OK
Cancel
Help
Previous
Next
Cancel
Help

Explanation:

All personal site under Office 365/Users/abc@ahsay.onmicrosoft.com/Personal Site that has the pattern that contains with ‘ppp’ with match case set to true will be included upon performing search.

As you can see on the screen shot above, the result panel contains the Name of the mail, Directory of the mails which are indicated In-Folder column, Size of each mails, and Date Modified.

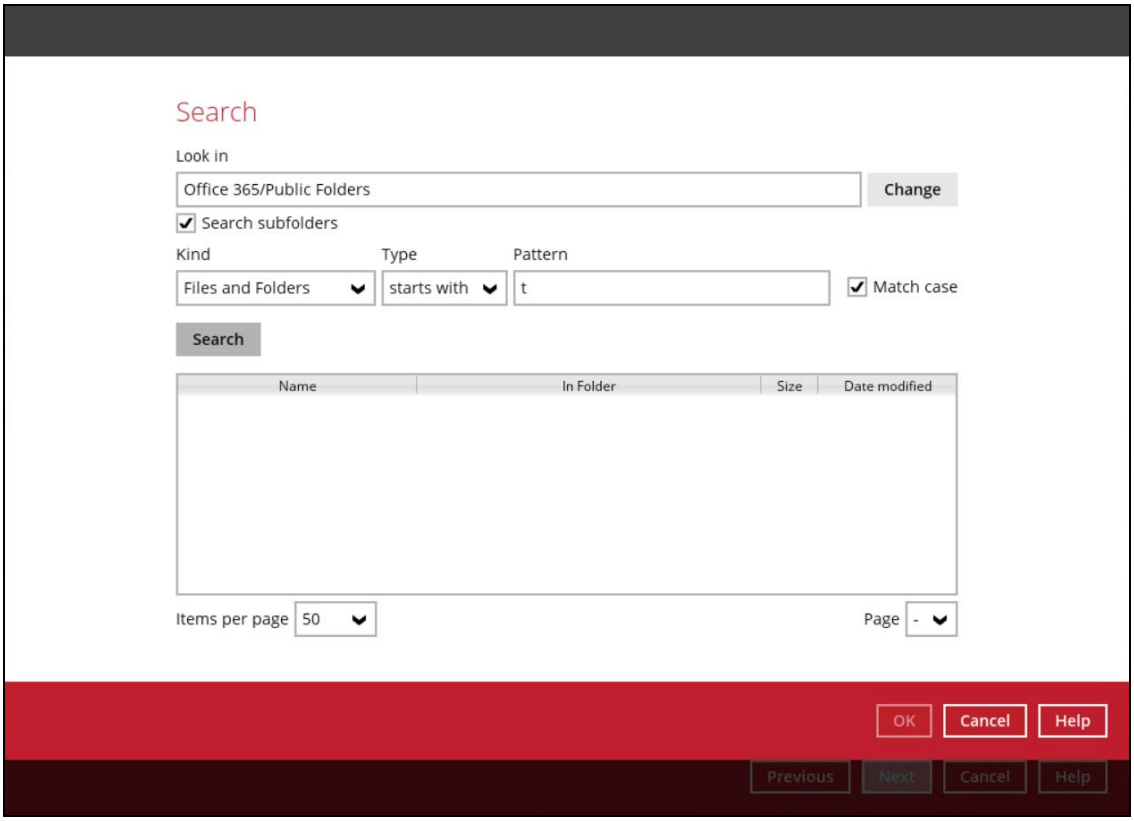
The restore filter setting includes the Search subfolder and Match case set to true. This means that the filter will include all available subfolders in Personal Site upon searching. And it will strictly search only the specified pattern and case which starts with ‘ppp’.

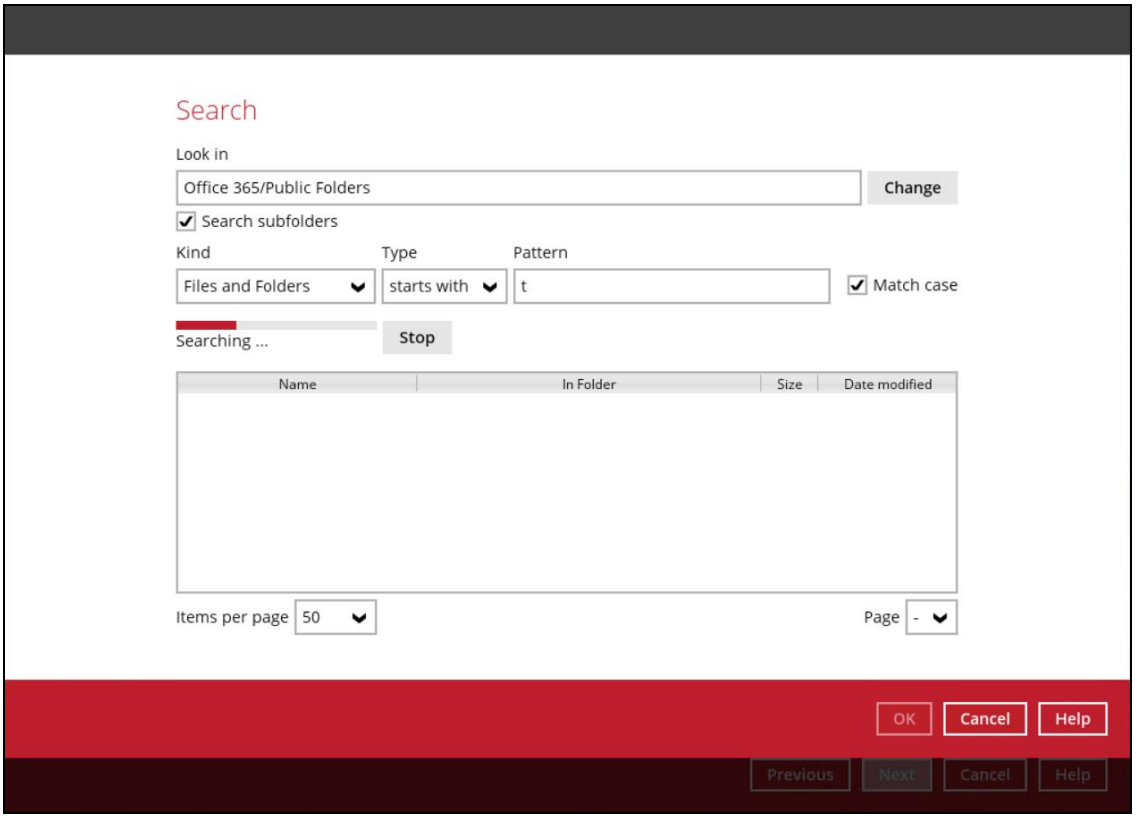
Scenarios No. 2: Items from Public Folders

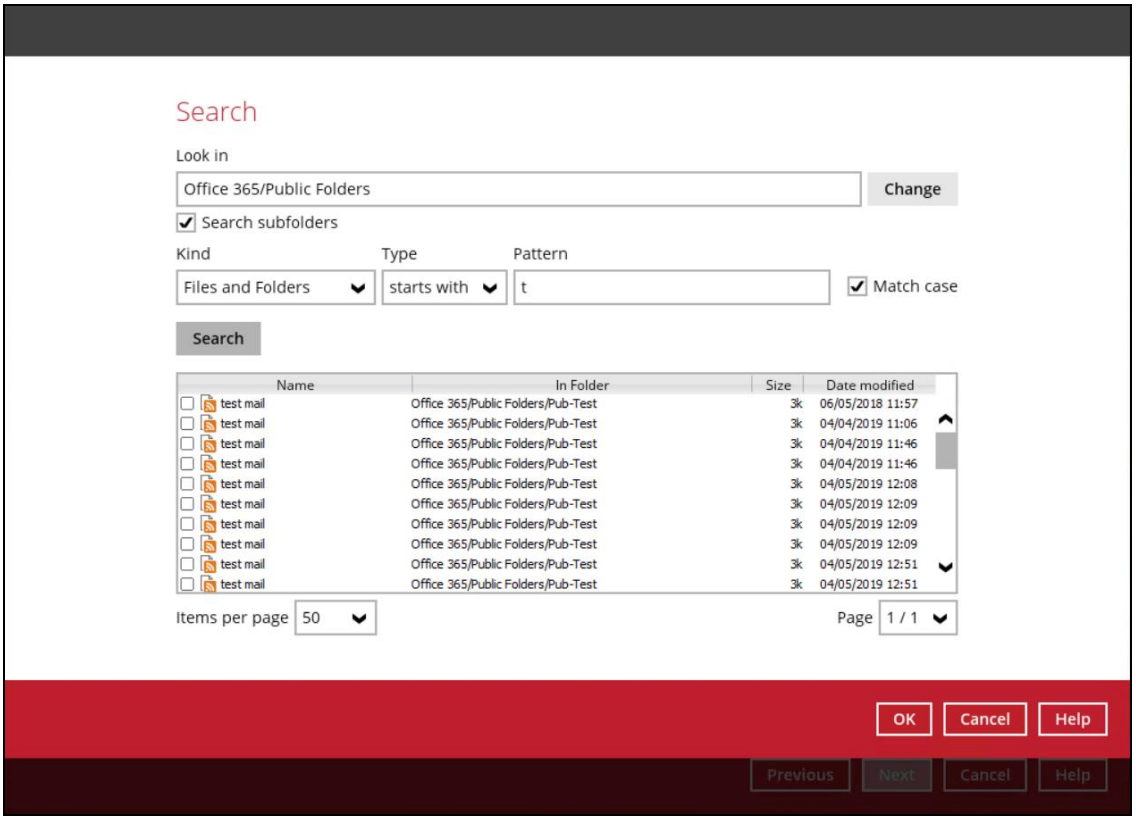
Example No. 1: Restore filter setting from Public Folders

Location:	Office 365/Public Folder
Search subfolders:	True
Kind:	Files and Folders
Type:	Starts With
Pattern:	t
Match Case:	True

Follow the step-by-step procedure indicated on Restore Filter with AhsayACB.




Search
Look in
Office 365/Public Folders
Change
Search subfolders
Kind
Type
Pattern
Files and Folders
starts with
t
Match case
Searching ...
Stop
Name
In Folder
Size
Date modified
Items per page
50
Page
-
OK
Cancel
Help
Previous
Next
Cancel
Help


Search
Look in
Office 365/Public Folders
Change
Search subfolders
Kind
Type
Pattern
Files and Folders
starts with
t
Match case
Search
Name
In Folder
Size
Date modified
test mail
Office 365/Public Folders/Pub-Test
3k
06/05/2018 11:57
04/04/2019 11:06
04/04/2019 11:46
04/04/2019 11:46
04/05/2019 12:08
04/05/2019 12:09
04/05/2019 12:09
04/05/2019 12:09
04/05/2019 12:51
Items per page
50
Page
1 / 1
OK
Cancel
Help
Previous
Next
Cancel
Help

Explanation:

All SharePoint Personal Sites under Office 365/Public Folders that has the pattern that starts with ‘A’ with match case set to true will be included upon performing search.

As you can see on the screen shot above, the result panel contains the Name of the mail, Directory of the mails which are indicated In-Folder column, Size of each mails, and Date Modified.

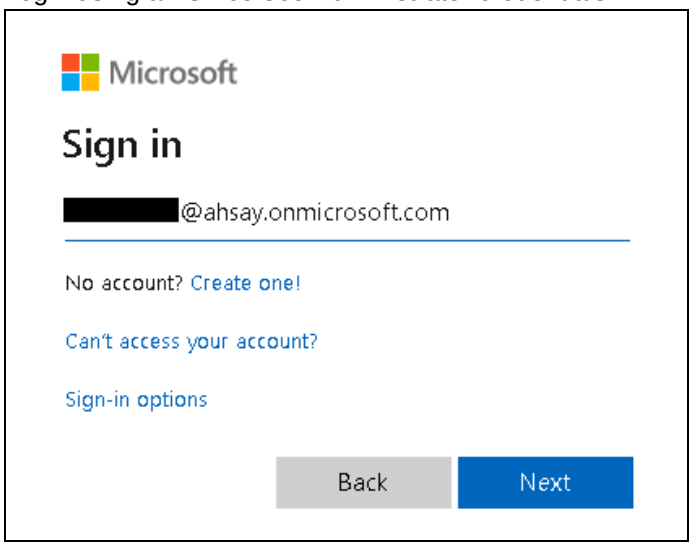
The restore filter setting includes the Search subfolder and Match case set to true. This means the filter will include all available subfolders in Public Folders upon searching. And it will strictly search only the specified pattern and case which starts with ‘t’.

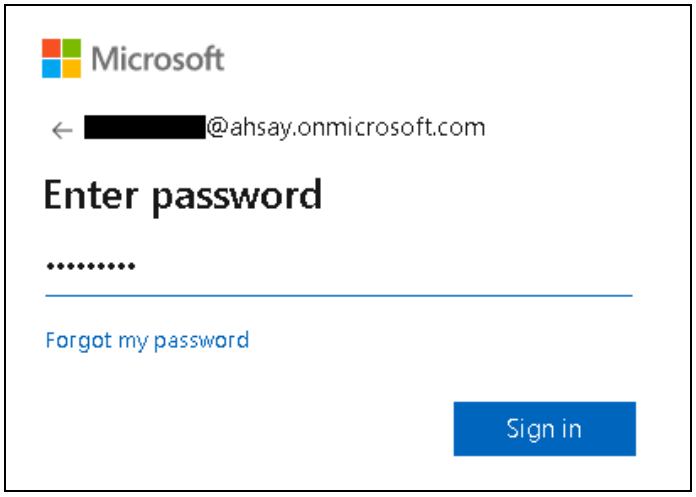
Appendix C Setting Multi-Factor Authentication (MFA) in Microsoft 365 Admin Center

What is a Multi-Factor Authentication (MFA)? It is an authentication method wherein a user will be granted an access only after successfully presenting two or more evidences or proof of personal information or identification. It also adds second layer of security to users upon logging in.

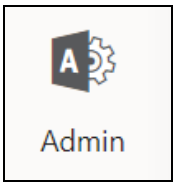
To enable MFA to any Office 365 user accounts, follow the steps below:

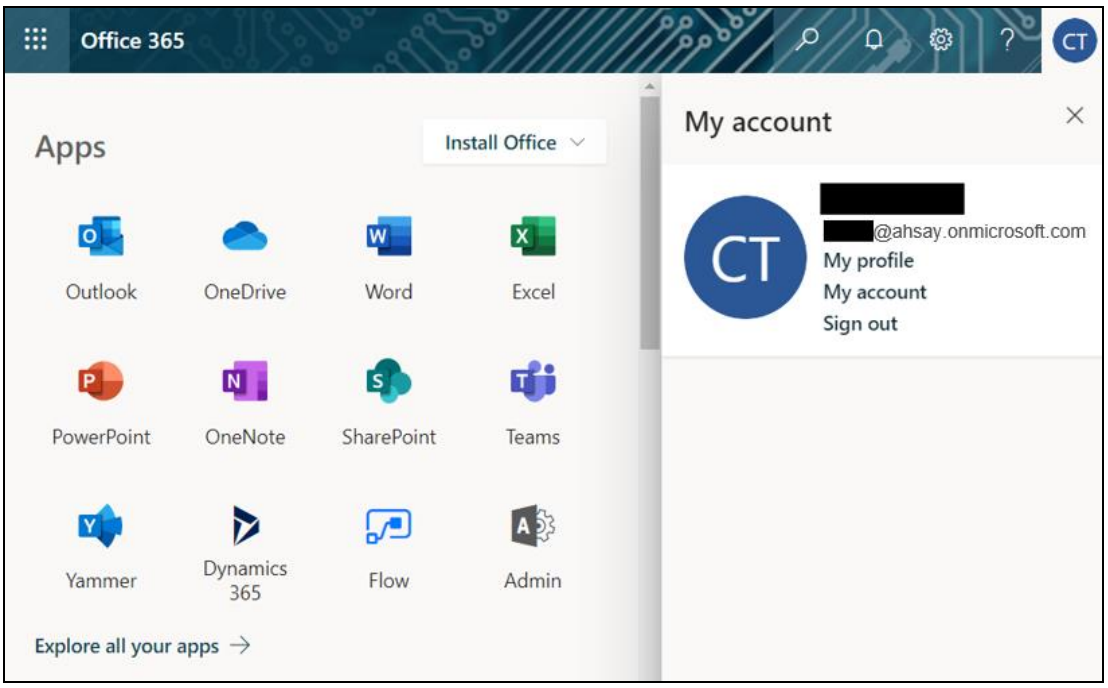
1. Login using an Office 365 Administrator credentials.



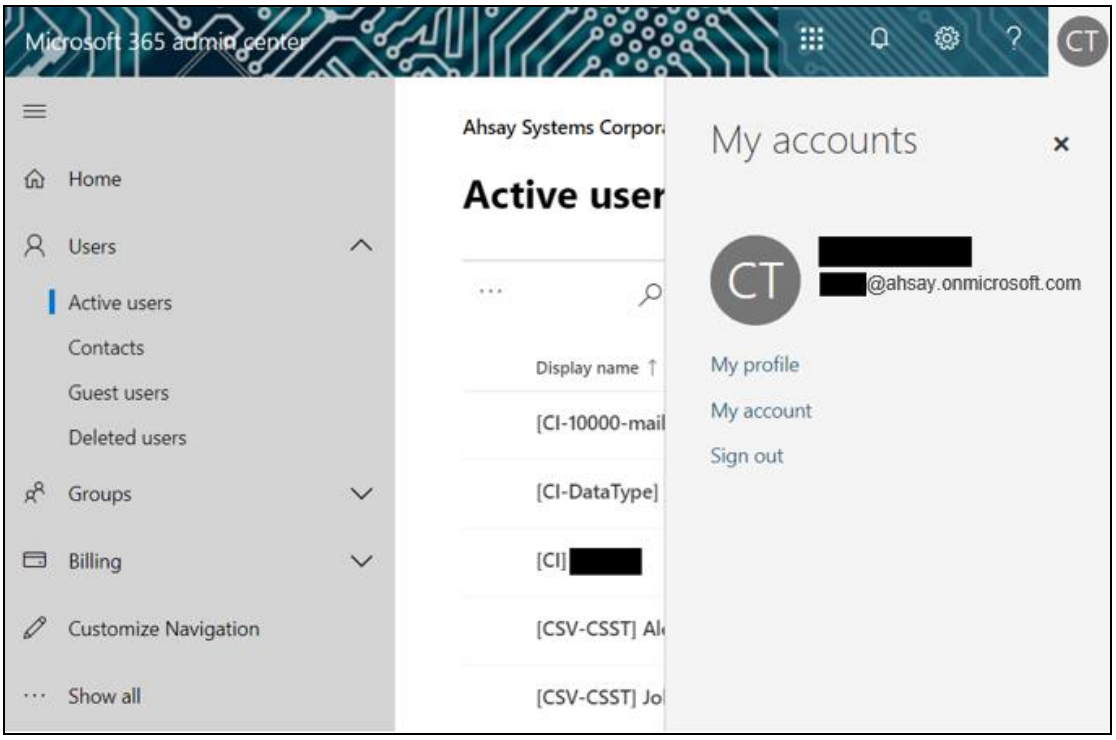


2. Click the **Admin Center** icon.



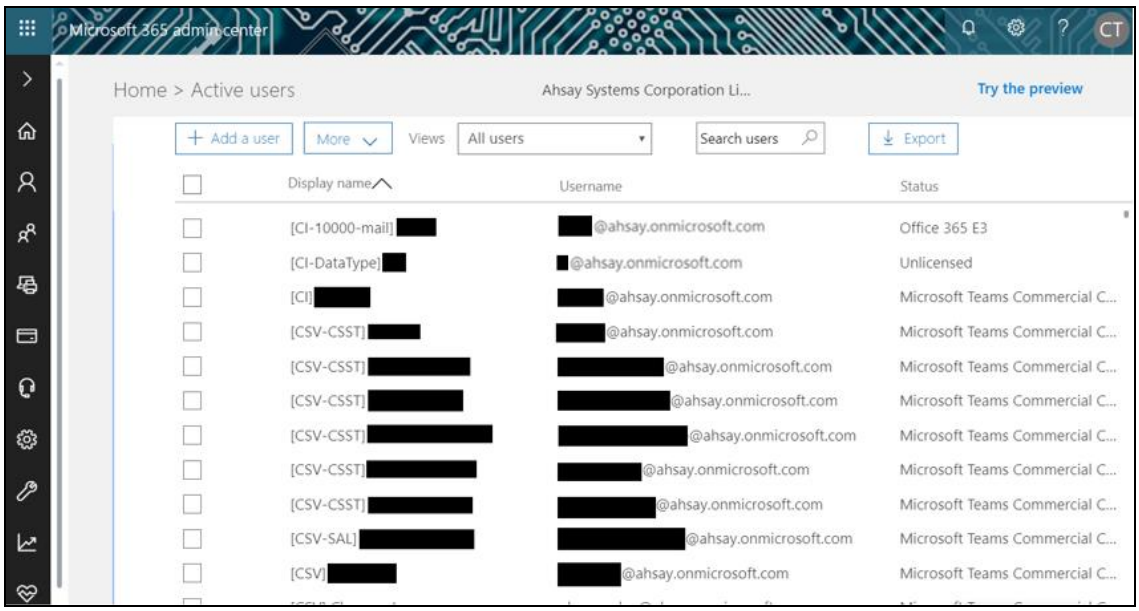


3. Go to **Users** and select the **Active users** from the list.

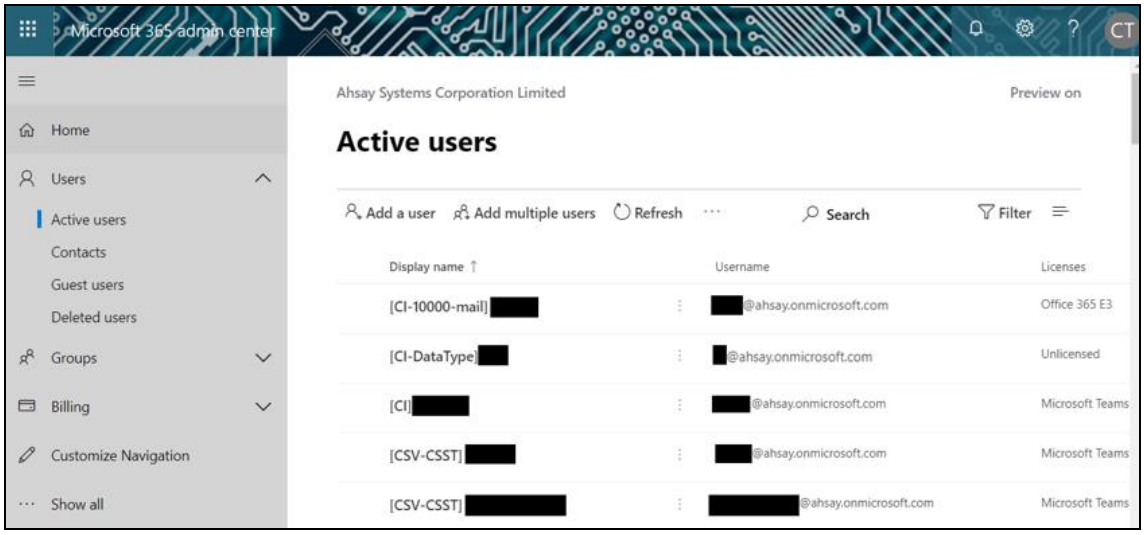


4. There are two (2) modes of viewing the Active users.

   Classic Mode – This is the default mode upon entering the Active users screen.

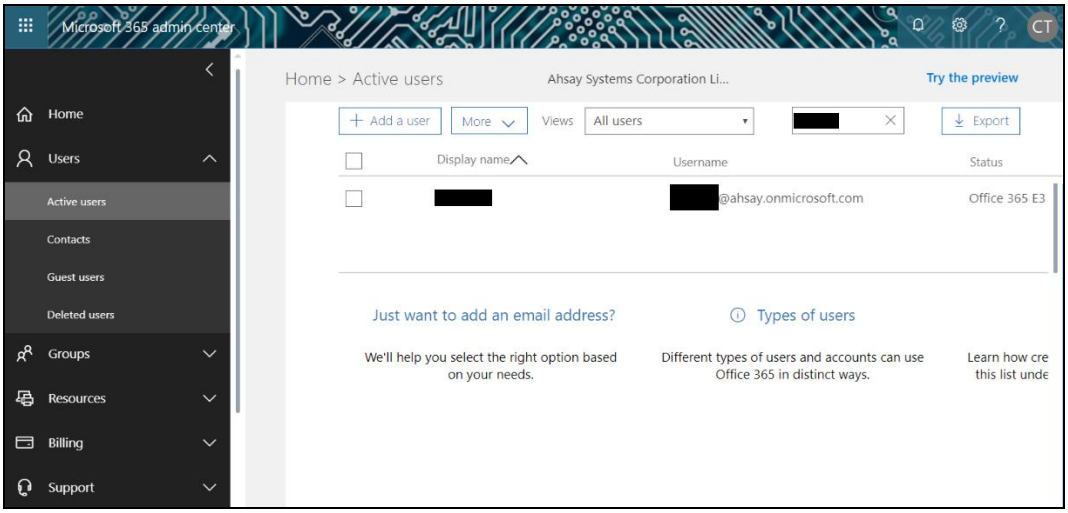


   Preview Mode – This is a new feature in the Office 365 Admin Center that offers simplification to manage your Microsoft 365 and Office 365 services. It also has all the capabilities of the classic mode.

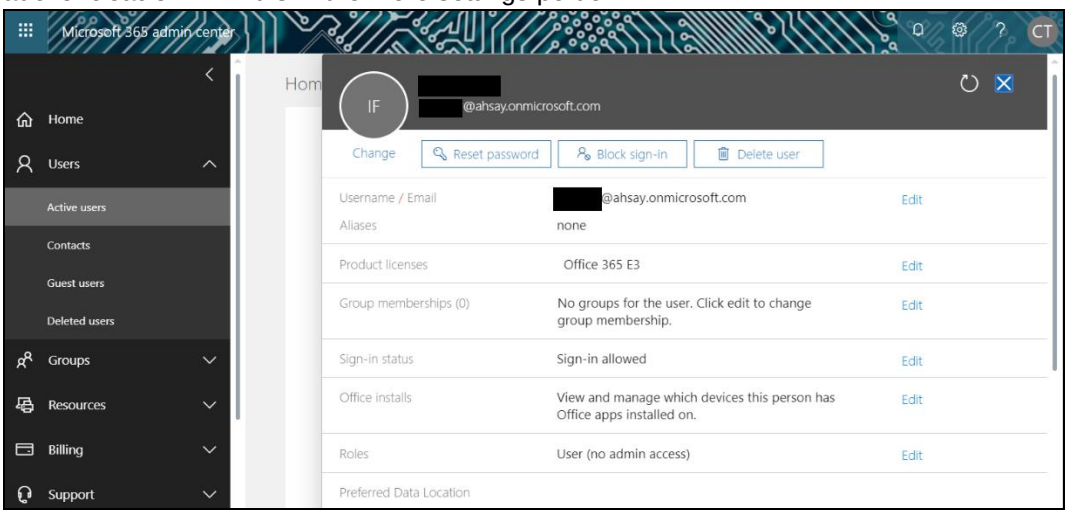


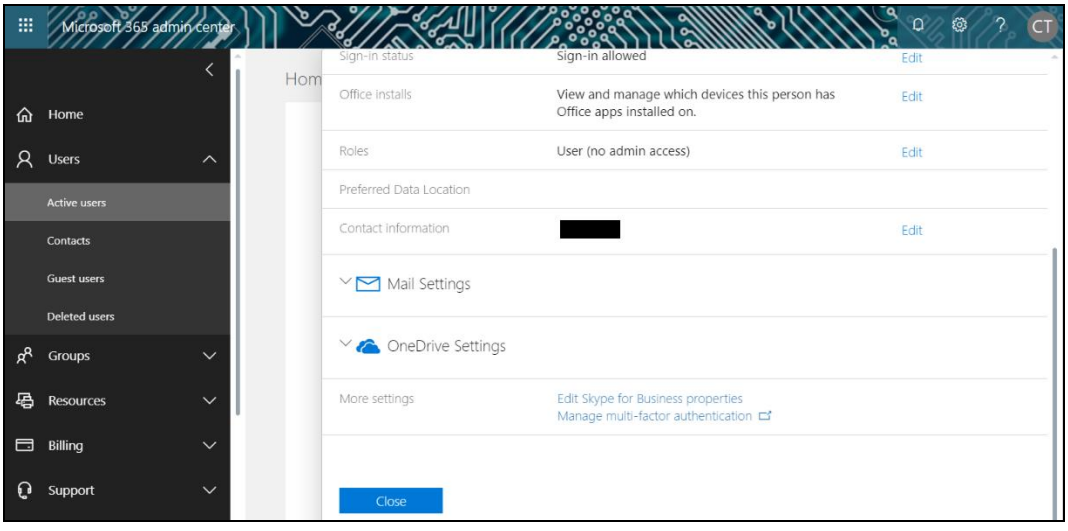
5. To go to the Multifactor Authentication screen, below are the steps for classic and preview mode.
   For the Classic Mode:

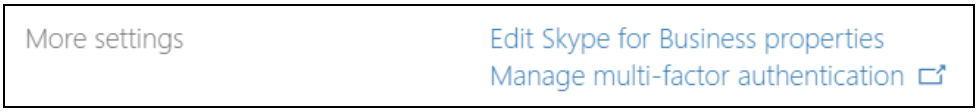
   - Search and select an Office 365 user account. The user's information will be displayed.



- In the lower part of the user's information screen, look for the **Manage multi-factor authentication** link. It is in the More settings portion.



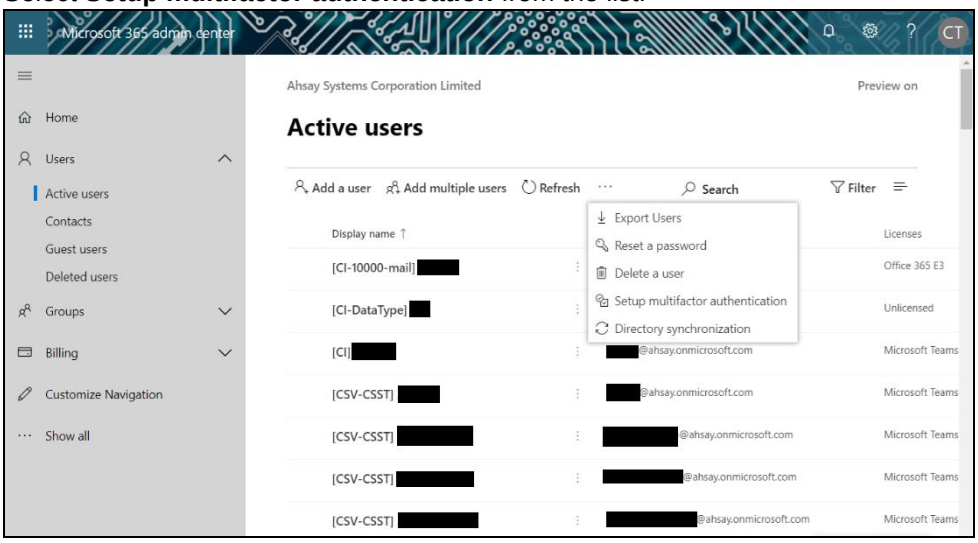




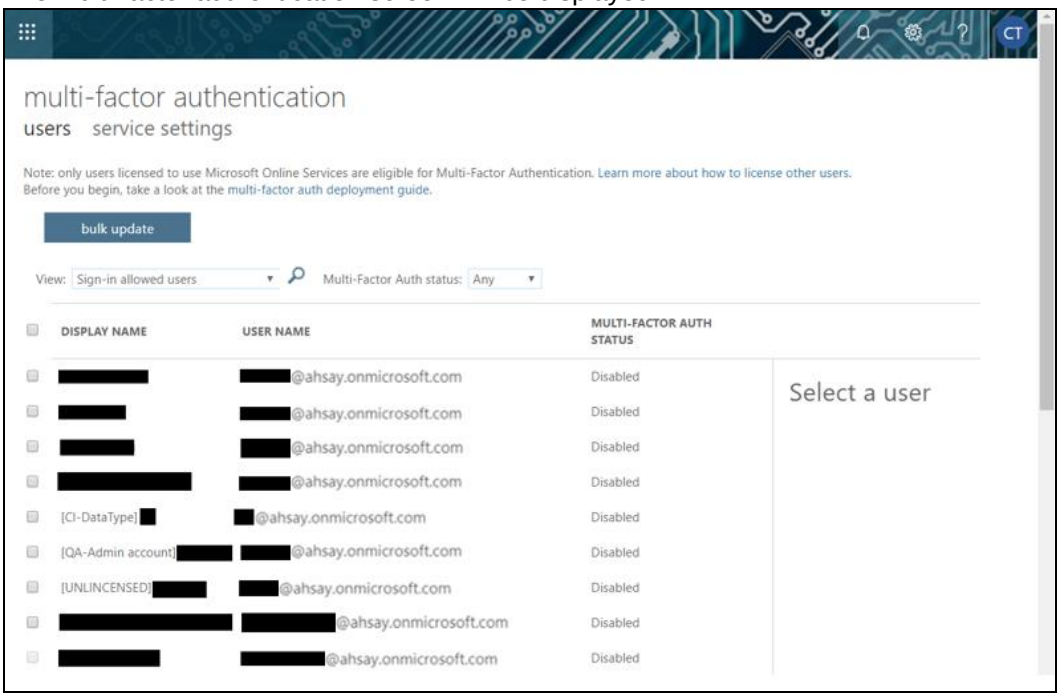
For the Preview Mode:

- In the Active users screen, click the […] ellipses.

- Select **Setup multifactor authentication** from the list.

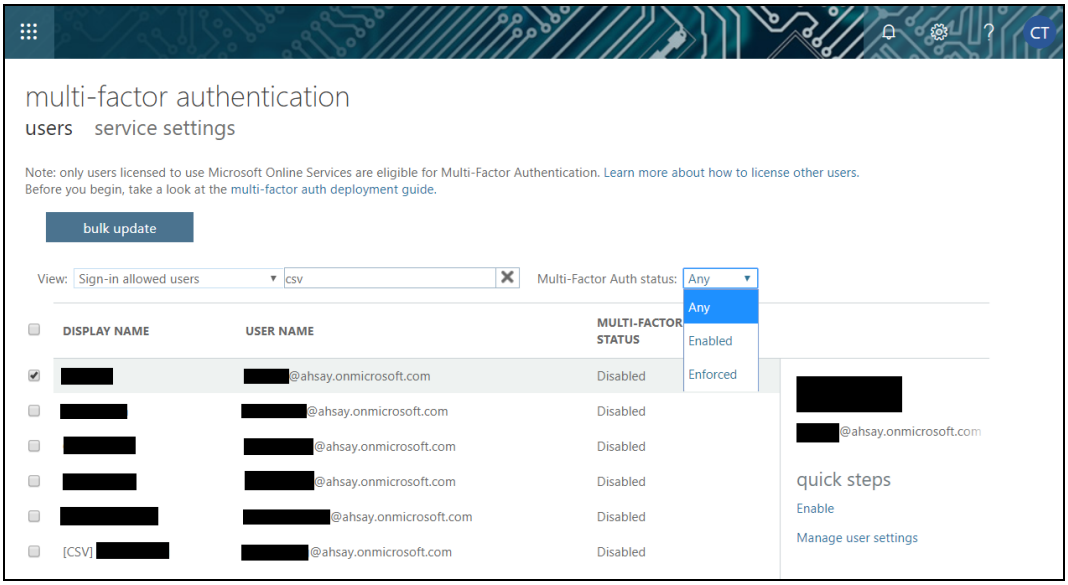


6. The multi-factor authentication screen will be displayed.



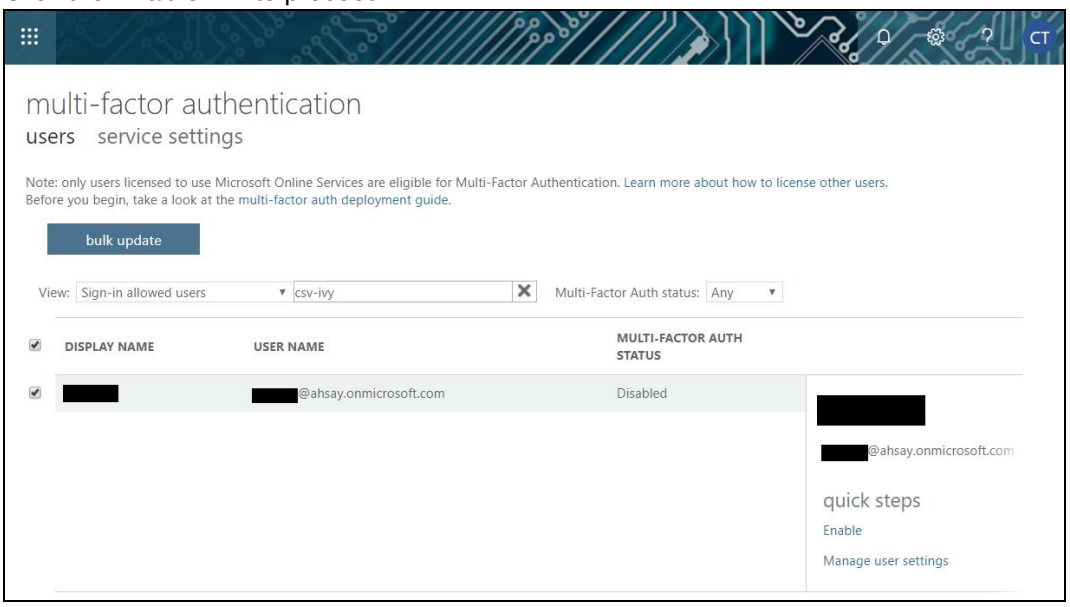
Note: The two (2) modes will go to the same screen.

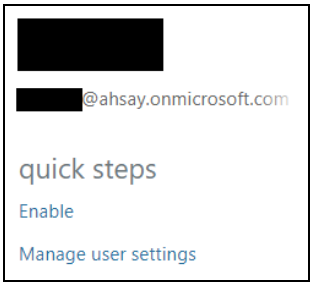
7. You can search and select one or more Office 365 user accounts. There is also a drop-down list available for multi-factor authentication status namely, **Disabled, Enabled**, and **Enforced**.



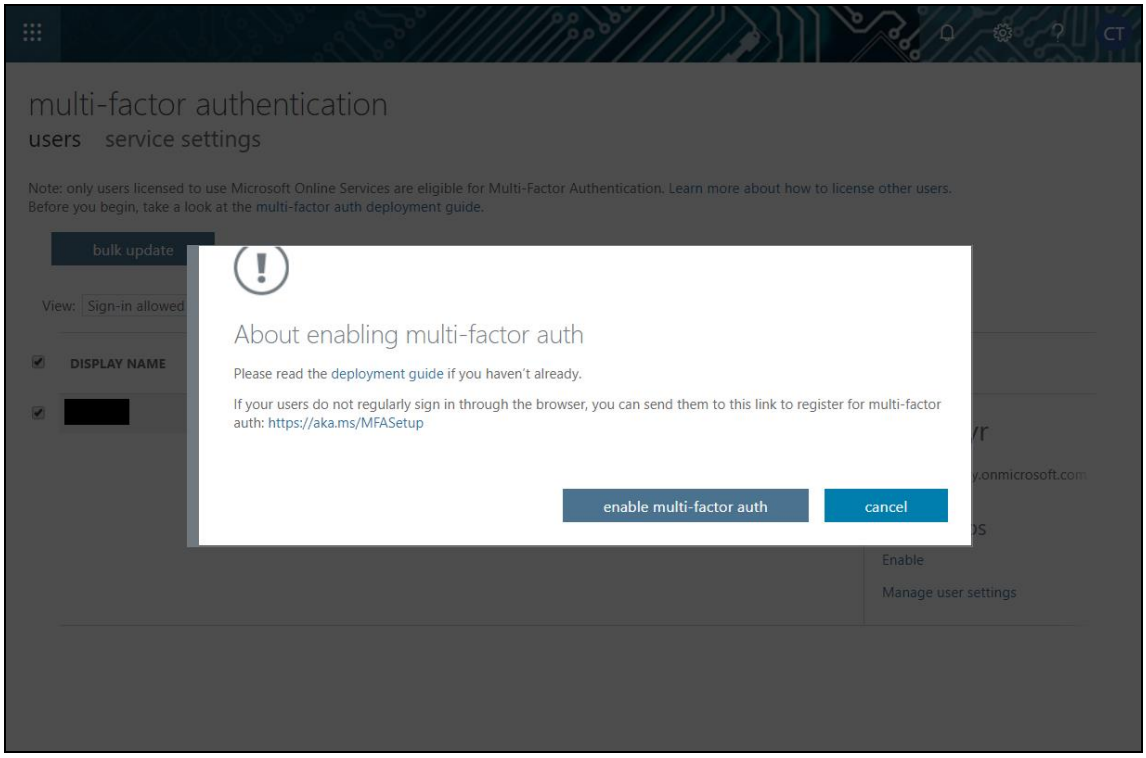
- Disabled – This status refers to the users who are not yet enrolled in the MFA. This is the default status.
- Enabled – This status refers to the users who are enrolled in the MFA, but changes have not yet taken effect.
- Enforced – This status refers to the users who are enrolled in the MFA has completed the registration process.

8. Upon selecting a user, on the right side of the screen it will show you a link to enable the MFA. Click the **Enable** link to proceed.

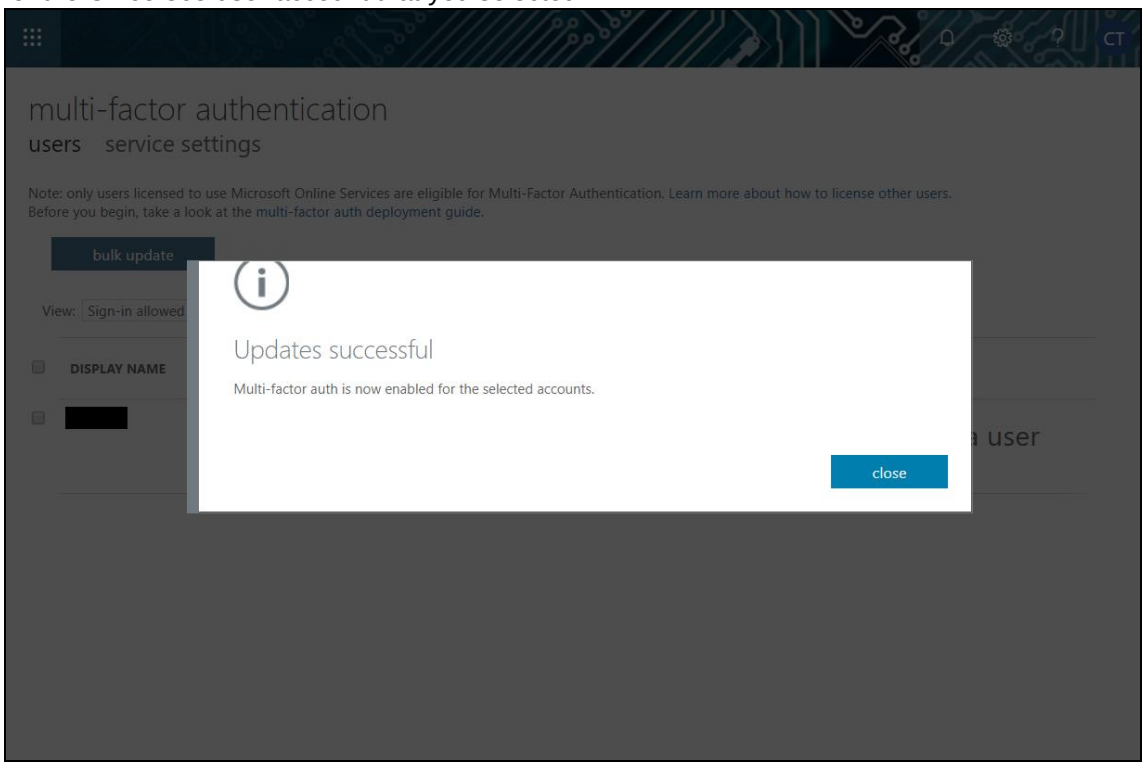




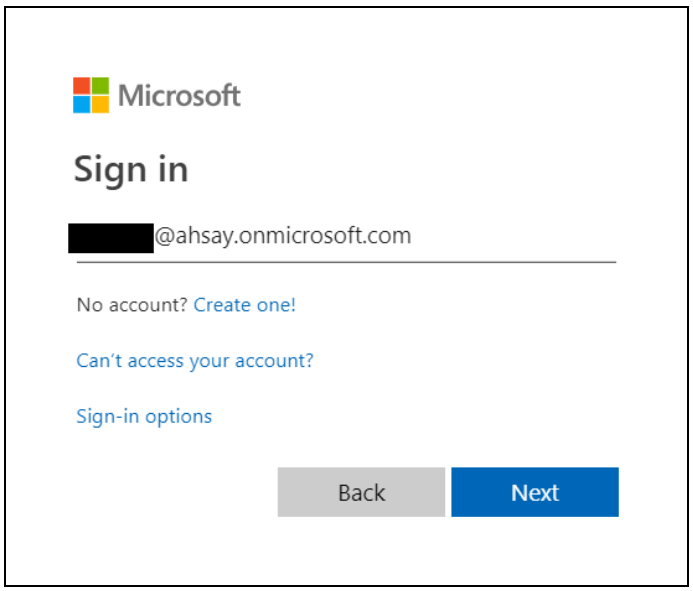
9. A warning message will be displayed. Click the **enable multi-factor auth** button to proceed. Otherwise, click the **cancel** button to abort.

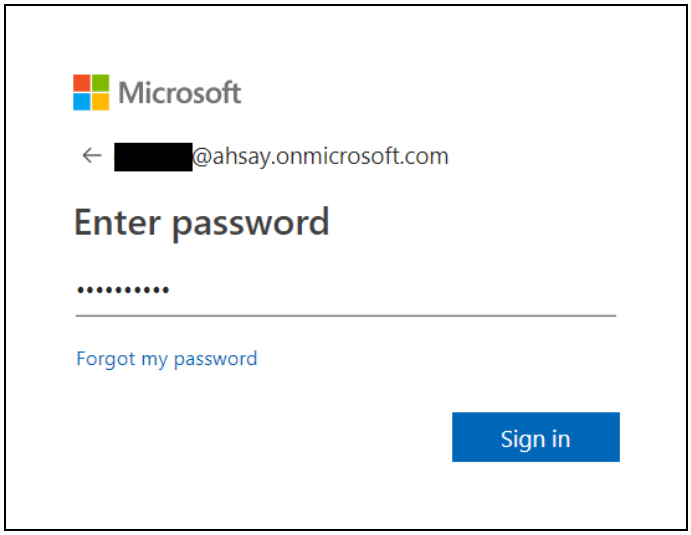


10. If you select enable multi-factor auth, the screen below shows the successful enabling of MFA for the Office 365 user account that you selected.

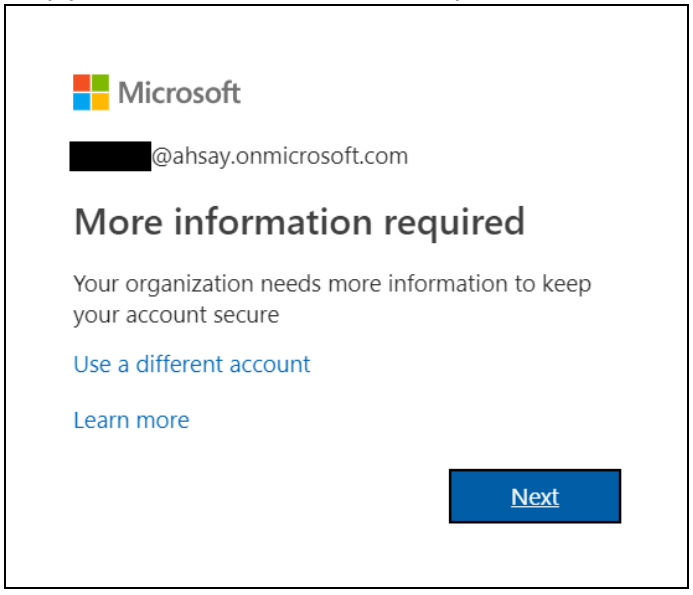


11. To finish the setup for the MFA, login using the MFA enabled Office 365 user account.

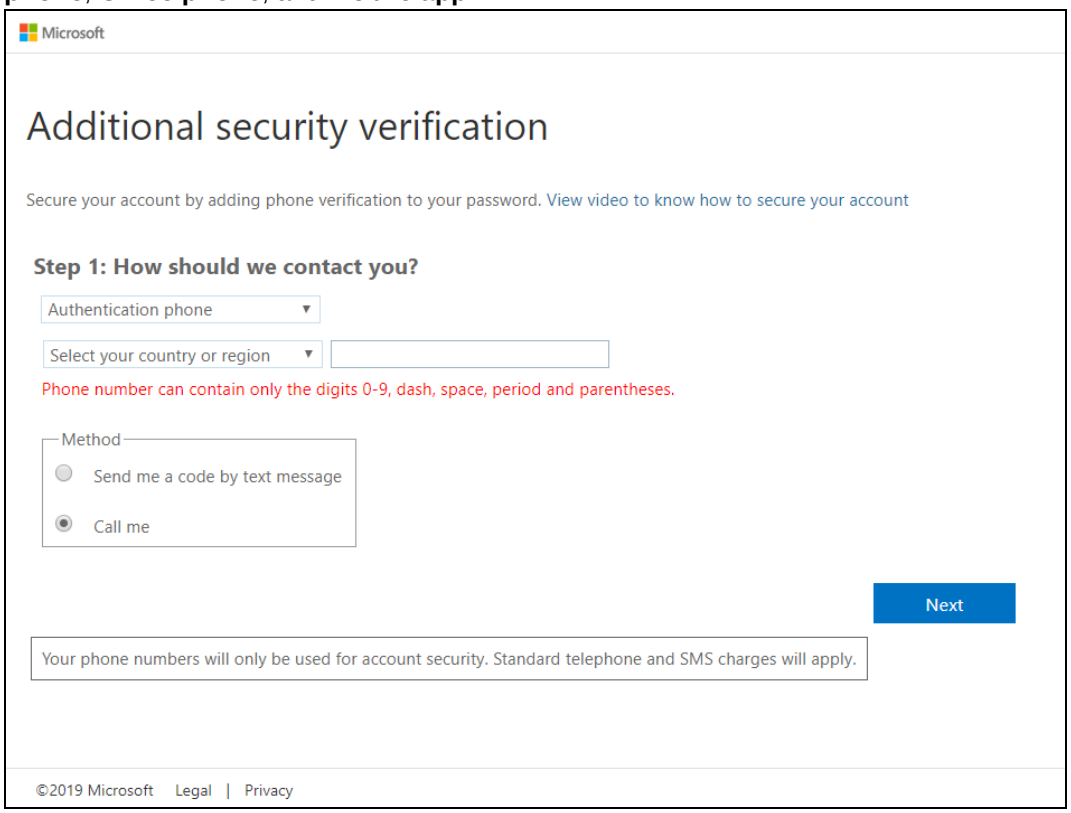




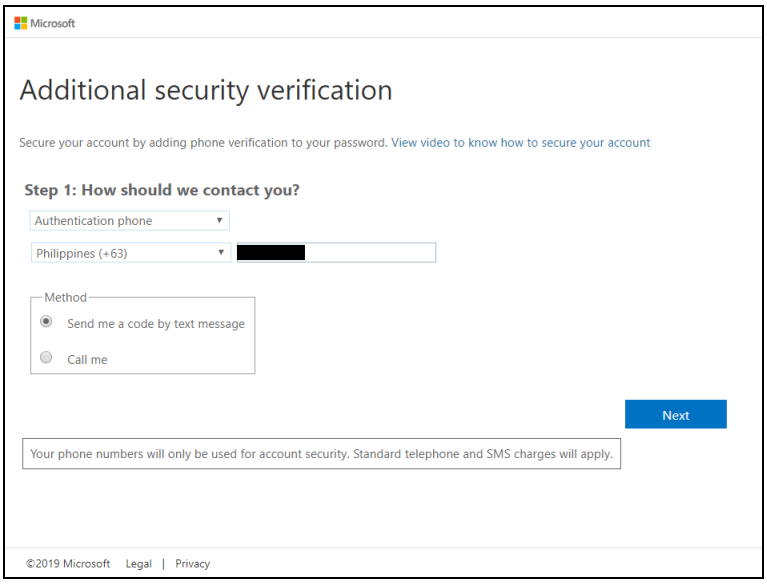
12. Upon logging in, there will be a message that will require you to provide more information to keep your account safe. Click **Next** to proceed.



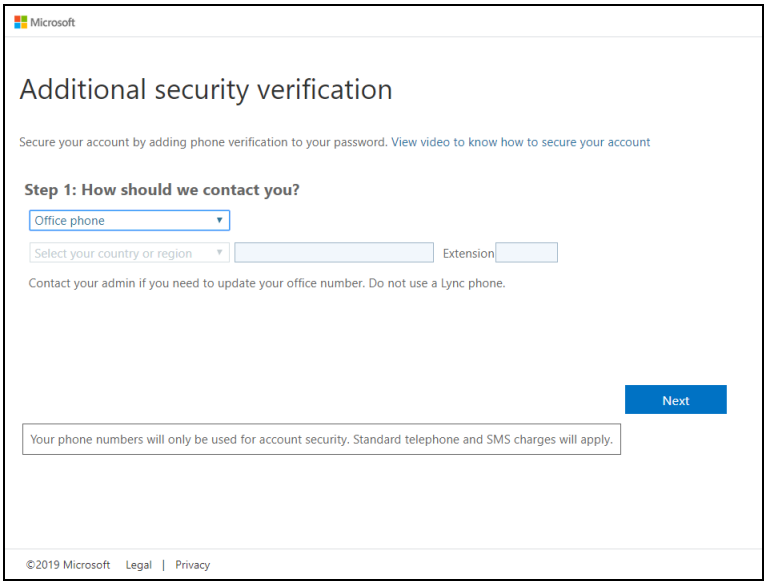
13. The **Additional security verification** screen will be displayed. Select one (1) option you want for the security of your account. You can choose from the three (3) options, **Authentication phone**, **Office phone**, and **Mobile app**.



- Authentication phone
  - Enter valid mobile number.
  - Select a method
    - Send me a code by text message
    - Call me

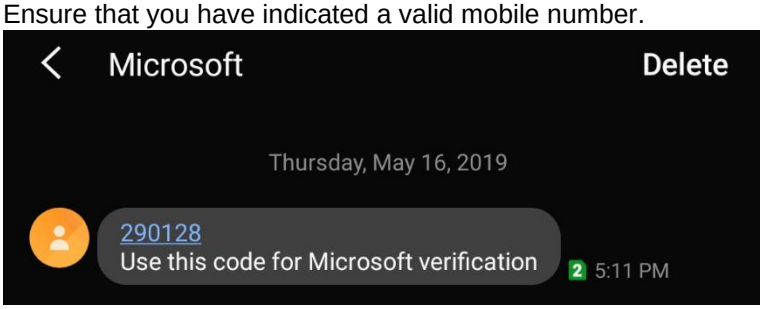


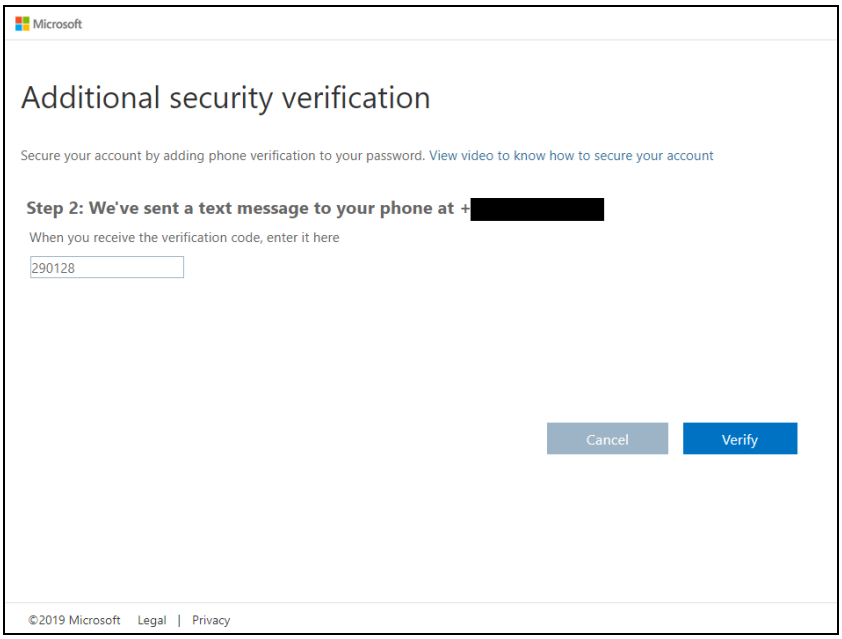
- Office phone – This option is disabled. Please ask your administrator if you need to update your office phone number.

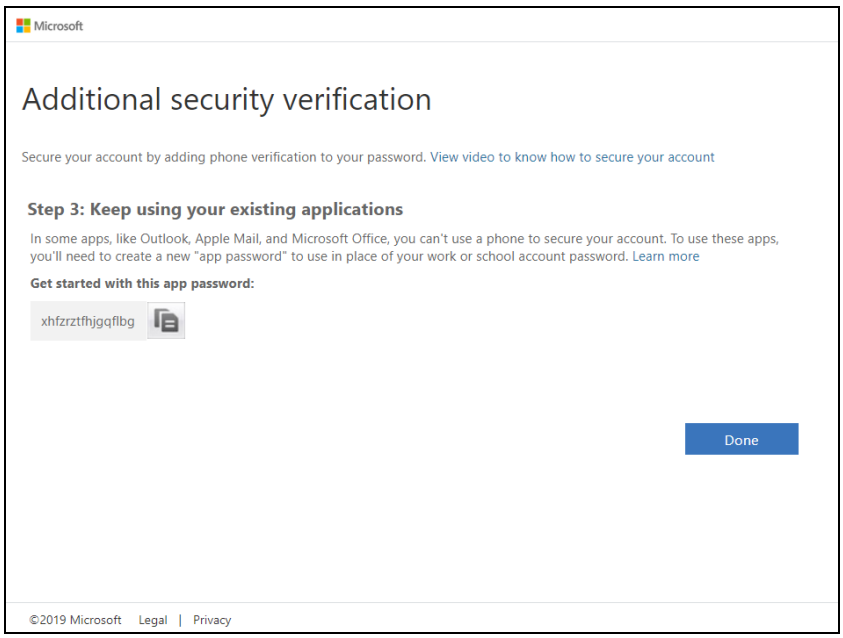


- Mobile app
  - Select which option you like upon using the mobile app
    - Receive notifications for verification
    - Use verification code

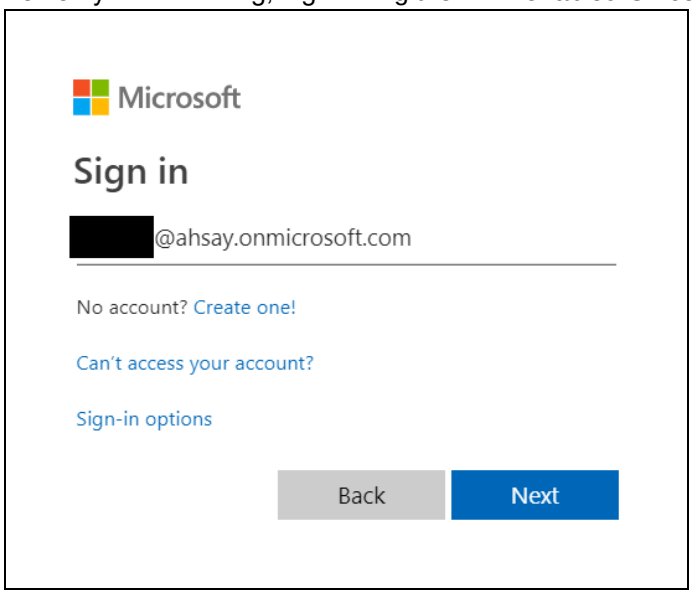
14. If you have selected the first option which is the **Authentication phone** with a method of **Send me a code by text,** you will receive a text message containing the verification code. Ensure that you have indicated a valid mobile number.



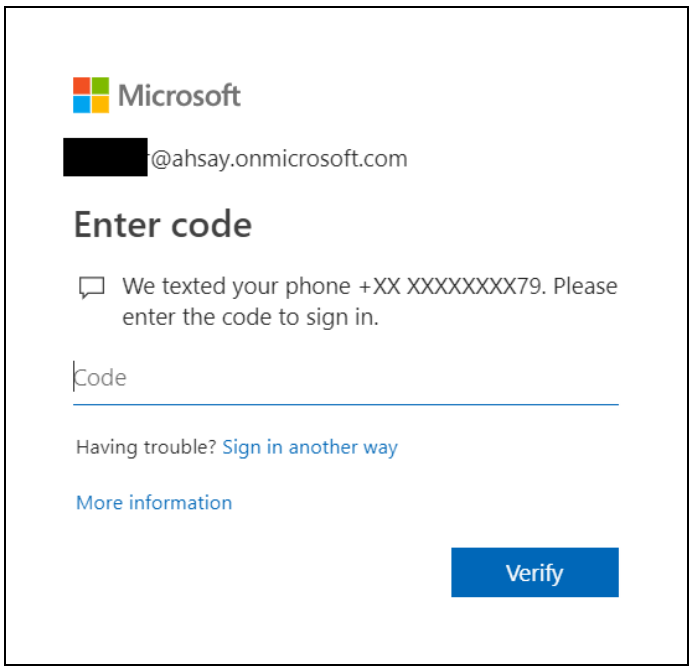


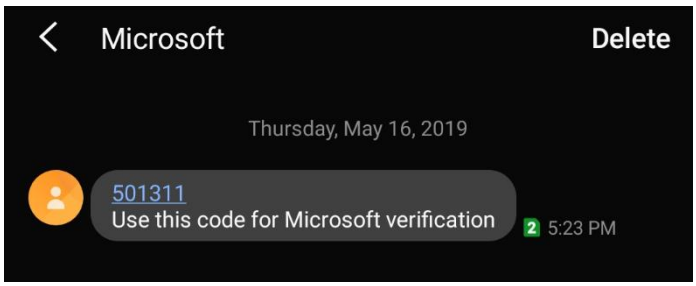


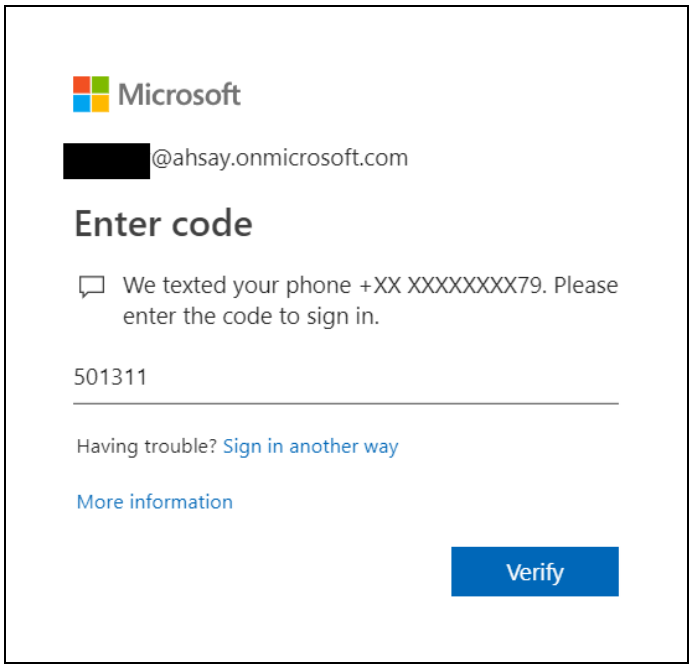
15. To verify if it's working, login using the MFA enabled Office 365 user account.



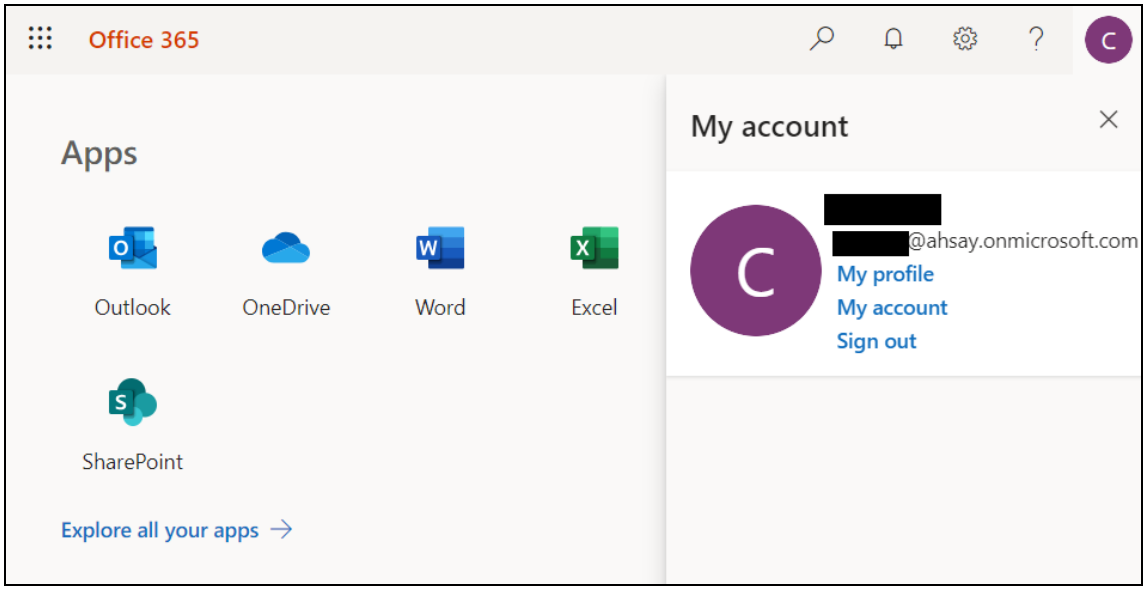
16. Upon logging in, there will be a message that will require you to provide the code that have been sent to your personal mobile number. Click **Verify** to proceed.


Microsoft
[redacted]@ahsay.onmicrosoft.com
Enter code
We texted your phone +XX XXXXXXXX79. Please enter the code to sign in.
Code
Having trouble? Sign in another way
More information
Verify


Microsoft
Delete
Thursday, May 16, 2019
501311
Use this code for Microsoft verification
5:23 PM

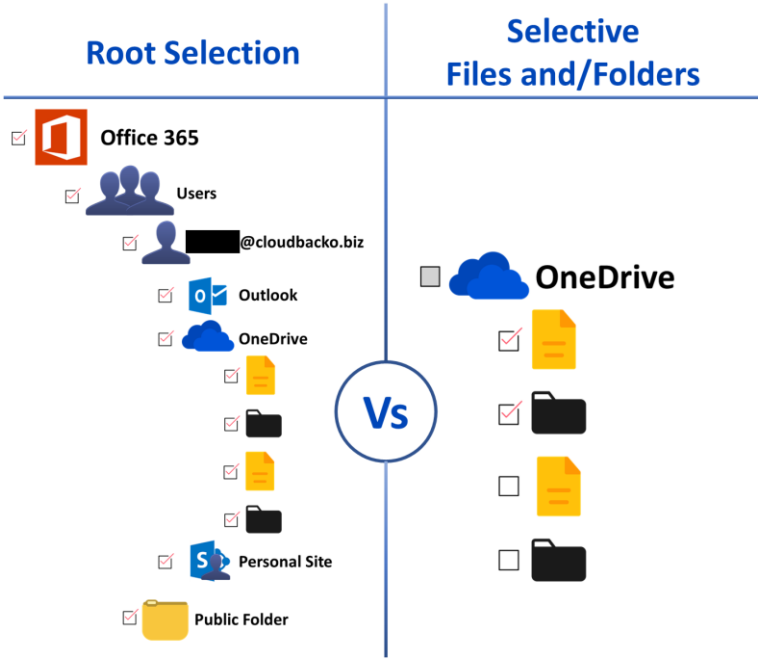

Microsoft
[redacted]@ahsay.onmicrosoft.com
Enter code
We texted your phone +XX XXXXXXXX79. Please enter the code to sign in.
501311
Having trouble? Sign in another way
More information
Verify

17. After the verification process, the screen will be automatically redirected to the Office 365 Main screen.



Appendix D Example Scenario for Data Synchronization Check (DSC) with backup logs

Selection of root folder vs Selective files and/folders

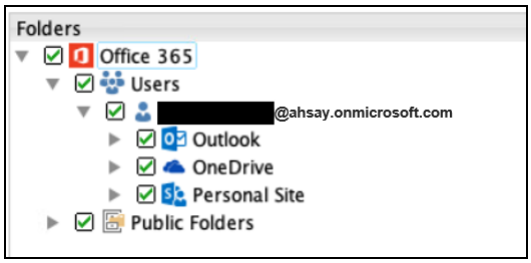


Root Selection

Selecting the root folder automatically selects all the files and/or folders under the Office 365 user account including the Public Folder. On the comparison image above, the checkbox for the root folder "Office 365" is ticked.

Data synchronization check is not required when using root selection backed up. As during a backup job any deleted files in the backup source will be automatically move to retention area.

Below is a sample screenshot of the backup source with root selection.

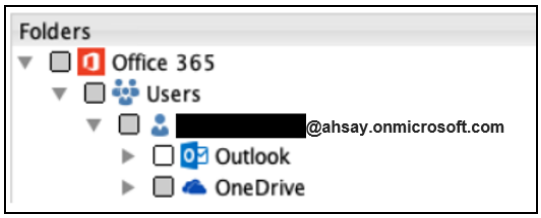


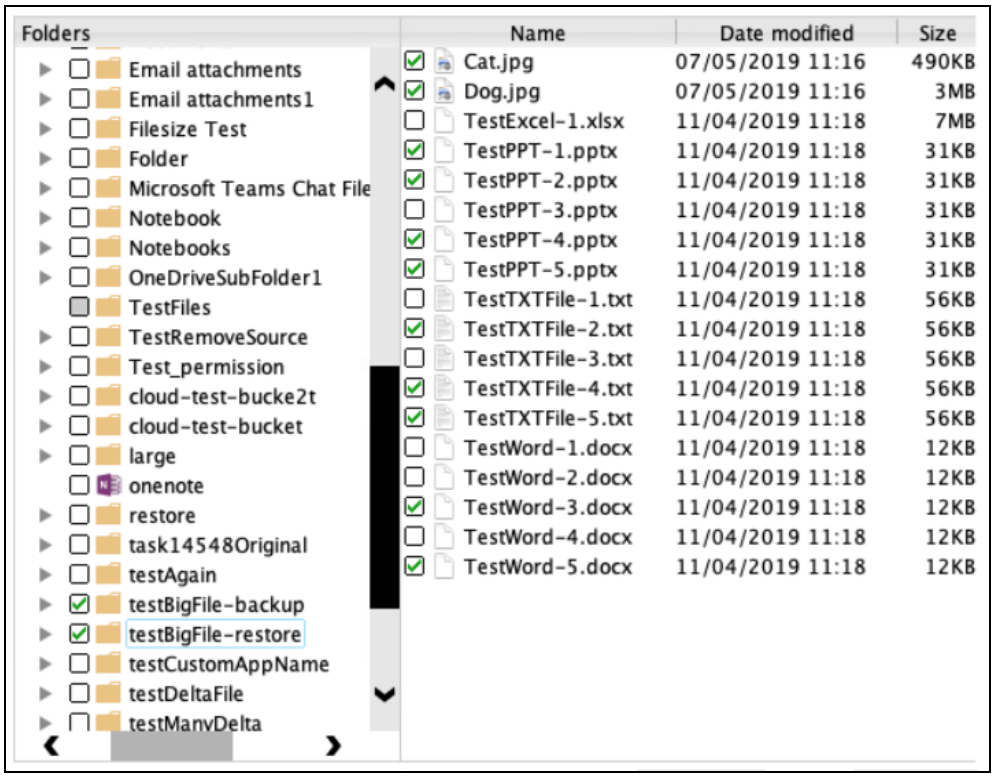
Selective Files and/or Folders

This is when the root folder is not selected and only a few selected files and/or folders are ticked. On the comparison image above, the “OneDrive” checkbox is greyed out because there are only one file and one folder selected.

Data synchronization check is highly recommended to perform to synchronize de-selected files and/folders in the backup source with the backup destination(s). This will ensure that there will be no data build up on the backup destination(s).

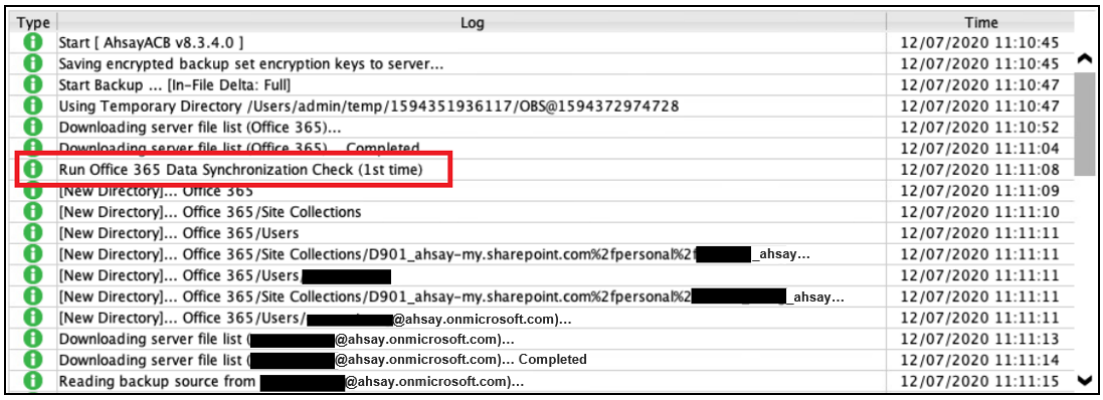
Below is the sample screenshot of the backup source with selective files and/or folders.





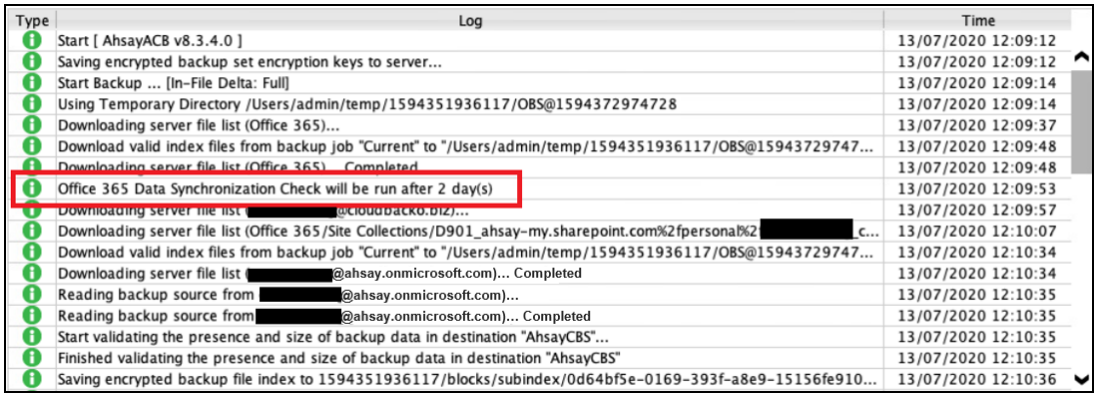
Only selected files and/or folders are selected in OneDrive. Also, the Office 365 user account is greyed out as this indicates that not all items are selected.

On the sample backup log, it shows that data synchronization check is enabled and runs for the first time.



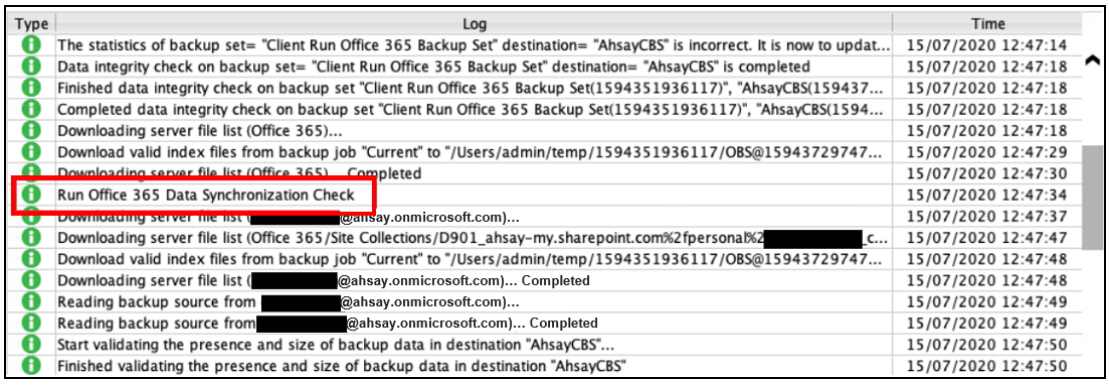
Type	Log	Time
ℹ	Start [AhsayACB v8.3.4.0]	12/07/2020 11:10:45
ℹ	Saving encrypted backup set encryption keys to server...	12/07/2020 11:10:45
ℹ	Start Backup ... [In-File Delta: Full]	12/07/2020 11:10:47
ℹ	Using Temporary Directory /Users/admin/temp/1594351936117/OBS@1594372974728	12/07/2020 11:10:47
ℹ	Downloading server file list (Office 365)...	12/07/2020 11:10:52
ℹ	Downloading server file list (Office 365)... Completed	12/07/2020 11:11:04
ℹ	Run Office 365 Data Synchronization Check (1st time)	12/07/2020 11:11:08
ℹ	[New Directory]... Office 365	12/07/2020 11:11:09
ℹ	[New Directory]... Office 365/Site Collections	12/07/2020 11:11:10
ℹ	[New Directory]... Office 365/Users	12/07/2020 11:11:11
ℹ	[New Directory]... Office 365/Site Collections/D901_ahsay-my.sharepoint.com%2fpersonal%2f[redacted]_ahsay...	12/07/2020 11:11:11
ℹ	[New Directory]... Office 365/Users/[redacted]	12/07/2020 11:11:11
ℹ	[New Directory]... Office 365/Site Collections/D901_ahsay-my.sharepoint.com%2fpersonal%2[redacted]_ahsay...	12/07/2020 11:11:11
ℹ	[New Directory]... Office 365/Users/[redacted]@ahsay.onmicrosoft.com)...	12/07/2020 11:11:11
ℹ	Downloading server file list ([redacted]@ahsay.onmicrosoft.com)...	12/07/2020 11:11:13
ℹ	Downloading server file list ([redacted]@ahsay.onmicrosoft.com)... Completed	12/07/2020 11:11:14
ℹ	Reading backup source from [redacted]@ahsay.onmicrosoft.com)...	12/07/2020 11:11:15

On the sample backup log, it shows the countdown until the next data synchronization check which is in two (2) days. The interval set is three (3) days.



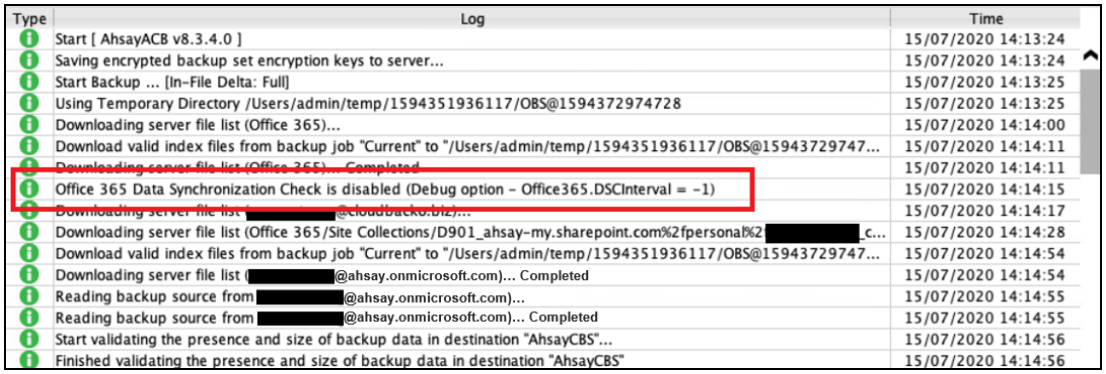
Type	Log	Time
ℹ	Start [AhsayACB v8.3.4.0]	13/07/2020 12:09:12
ℹ	Saving encrypted backup set encryption keys to server...	13/07/2020 12:09:12
ℹ	Start Backup ... [In-File Delta: Full]	13/07/2020 12:09:14
ℹ	Using Temporary Directory /Users/admin/temp/1594351936117/OBS@1594372974728	13/07/2020 12:09:14
ℹ	Downloading server file list (Office 365)...	13/07/2020 12:09:37
ℹ	Download valid index files from backup job "Current" to "/Users/admin/temp/1594351936117/OBS@15943729747...	13/07/2020 12:09:48
ℹ	Downloading server file list (Office 365)... Completed	13/07/2020 12:09:48
ℹ	Office 365 Data Synchronization Check will be run after 2 day(s)	13/07/2020 12:09:53
ℹ	Downloading server file list ([redacted]@cloudbacko.biz)...	13/07/2020 12:09:57
ℹ	Downloading server file list (Office 365/Site Collections/D901_ahsay-my.sharepoint.com%2fpersonal%2[redacted]_c...	13/07/2020 12:10:07
ℹ	Download valid index files from backup job "Current" to "/Users/admin/temp/1594351936117/OBS@15943729747...	13/07/2020 12:10:34
ℹ	Downloading server file list ([redacted]@ahsay.onmicrosoft.com)... Completed	13/07/2020 12:10:34
ℹ	Reading backup source from [redacted]@ahsay.onmicrosoft.com)...	13/07/2020 12:10:35
ℹ	Reading backup source from [redacted]@ahsay.onmicrosoft.com)... Completed	13/07/2020 12:10:35
ℹ	Start validating the presence and size of backup data in destination "AhsayCBS"...	13/07/2020 12:10:35
ℹ	Finished validating the presence and size of backup data in destination "AhsayCBS"	13/07/2020 12:10:35
ℹ	Saving encrypted backup file index to 1594351936117/blocks/subindex/0d64bf5e-0169-393f-a8e9-15156fe910...	13/07/2020 12:10:36

On the sample backup log, it shows the countdown is done and data synchronization check is running.



Type	Log	Time
ℹ	The statistics of backup set= "Client Run Office 365 Backup Set" destination= "AhsayCBS" is incorrect. It is now to updat...	15/07/2020 12:47:14
ℹ	Data integrity check on backup set= "Client Run Office 365 Backup Set" destination= "AhsayCBS" is completed	15/07/2020 12:47:18
ℹ	Finished data integrity check on backup set "Client Run Office 365 Backup Set(1594351936117)", "AhsayCBS(159437...	15/07/2020 12:47:18
ℹ	Completed data integrity check on backup set "Client Run Office 365 Backup Set(1594351936117)", "AhsayCBS(1594...	15/07/2020 12:47:18
ℹ	Downloading server file list (Office 365)...	15/07/2020 12:47:18
ℹ	Download valid index files from backup job "Current" to "/Users/admin/temp/1594351936117/OBS@15943729747...	15/07/2020 12:47:29
ℹ	Downloading server file list (Office 365)... Completed	15/07/2020 12:47:30
ℹ	Run Office 365 Data Synchronization Check	15/07/2020 12:47:34
ℹ	Downloading server file list ([redacted]@ahsay.onmicrosoft.com)...	15/07/2020 12:47:37
ℹ	Downloading server file list (Office 365/Site Collections/D901_ahsay-my.sharepoint.com%2fpersonal%2[redacted]_c...	15/07/2020 12:47:47
ℹ	Download valid index files from backup job "Current" to "/Users/admin/temp/1594351936117/OBS@15943729747...	15/07/2020 12:47:48
ℹ	Downloading server file list ([redacted]@ahsay.onmicrosoft.com)... Completed	15/07/2020 12:47:48
ℹ	Reading backup source from [redacted]@ahsay.onmicrosoft.com)...	15/07/2020 12:47:49
ℹ	Reading backup source from [redacted]@ahsay.onmicrosoft.com)... Completed	15/07/2020 12:47:49
ℹ	Start validating the presence and size of backup data in destination "AhsayCBS"...	15/07/2020 12:47:50
ℹ	Finished validating the presence and size of backup data in destination "AhsayCBS"	15/07/2020 12:47:50

On the sample backup log, it shows that data synchronization check is **disabled**.



Type	Log	Time
ⓘ	Start [AhsayACB v8.3.4.0]	15/07/2020 14:13:24
ⓘ	Saving encrypted backup set encryption keys to server...	15/07/2020 14:13:24
ⓘ	Start Backup ... [In-File Delta: Full]	15/07/2020 14:13:25
ⓘ	Using Temporary Directory /Users/admin/temp/1594351936117/OBS@1594372974728	15/07/2020 14:13:25
ⓘ	Downloading server file list (Office 365)...	15/07/2020 14:14:00
ⓘ	Download valid index files from backup job "Current" to "/Users/admin/temp/1594351936117/OBS@15943729747...	15/07/2020 14:14:11
ⓘ	Downloading server file list (Office 365)... Completed	15/07/2020 14:14:11
ⓘ	Office 365 Data Synchronization Check is disabled (Debug option - Office365.DSCInterval = -1)	15/07/2020 14:14:15
ⓘ	Downloading server file list ([redacted]@cloudbacko.biz)...	15/07/2020 14:14:17
ⓘ	Downloading server file list (Office 365/Site Collections/D901_ahsay-my.sharepoint.com%2fpersonal%2[redacted].c...	15/07/2020 14:14:28
ⓘ	Download valid index files from backup job "Current" to "/Users/admin/temp/1594351936117/OBS@15943729747...	15/07/2020 14:14:54
ⓘ	Downloading server file list ([redacted]@ahsay.onmicrosoft.com)... Completed	15/07/2020 14:14:54
ⓘ	Reading backup source from [redacted]@ahsay.onmicrosoft.com)...	15/07/2020 14:14:55
ⓘ	Reading backup source from [redacted]@ahsay.onmicrosoft.com)... Completed	15/07/2020 14:14:55
ⓘ	Start validating the presence and size of backup data in destination "AhsayCBS"...	15/07/2020 14:14:56
ⓘ	Finished validating the presence and size of backup data in destination "AhsayCBS"	15/07/2020 14:14:56

Appendix E Setting the Data Synchronization Check (DSC)

Data Synchronization Check (DSC) is enabled by default and will run every 60 days.

Assumption: AhsayACB Installation path is **/Users/admin/Applications/AhsayACB.app**

To disable the data synchronization check, follow the instructions below:

1. Make sure there are no active backup or restore job running.
2. Close AhsayACB UI.
3. Stop the Ahsay A-Click Backup Manager services and check if the scheduler service has stopped running using the command highlighted in red.

```
#sudo /Applications/AhsayACB.app/bin/StopScheduler.sh

Password:

#ps -ef|grep java
#501 5721 5705 0 9:02PM ttys000 0:00.00 grep java
```

4. Using the terminal, go to AhsayACB installation path. Use the command highlighted in red.

```
#cd /Applications/AhsayACB.app
```

5. Open the **cb.opt** file using the command highlighted in red. Enter the password for logging in to your Mac when prompted.

```
#sudo vim cb.opt

#Password:
```

6. The following scripts will show.

```
#Print out default values of new backup set to a XML file
# Location: [WORKING_DIR]\DefaultBkupsetProfile.xml
com.ahsay.obc.core.action.GetUserPolicyCmd.debug=

# Print out debug messages for restore/decrypt
# Location: [WORKING_DIR]\DownloadFileSetTree.log
com.ahsay.obc.core.rset.file.DownloadFileSetTree.debug=

# Print out the decrypt list from OBS to restore to a XML file
# Location:
[RESTORE_DESTINATION]\DownloadFileSetTree_[RESTORE_JOB_ID].xml
com.ahsay.obc.core.rset.file.DownloadFileSetTree.SaveXML=
```

7. Press **I** to be able to insert a new line and add this line, *Office365.DSCInterval=-1.*

   A value of **-1** indicates data synchronization check is disabled.

```
Office365.DSCInterval=-1
-- INSERT --
```

   Press **Esc** + **:wq!** to save the changes made.

8. To check if the new line is added, use the commands highlighted in red.

```
#cat cb.opt
```

9. Start the Ahsay A-Click Backup Manager services and check if the scheduler service is running using the command highlighted in red.

```
#sudo /Applications/AhsayACB.app/bin/Scheduler.sh

Password:

#ps -ef|grep java
0 5735 1 0 9:05PM ttys000 0:02.07
/Applications/AhsayACB.app/jvm/bin/ java -Xms128m -Xmx768m -
Djava.library.path=. -cp .:./cbs.jar cbs
/Applications/AhsayACB.app 501 5741 5705 0 9:05PM ttys000
0:00.00 grep java
```

To check if the data synchronization check is enabled, follow the instructions below:

1. Using the terminal, go to AhsayACB installation path. Use the command highlighted in red.

```
#cd /Applications/AhsayACB.app
```

2. Open the **cb.opt** file using the command highlighted in red.

```
#cat cb.opt
```

3. Look for this line, *Office365.DSCInterval=xx*.

   Note:

   If xx is a positive value this indicates the data synchronization check is enabled and represents the interval number of days until the next run of data synchronization check.

   -OR-

   If the interval value is not *-1*.

To adjust the interval number of days, follow the instructions below:

1. Make sure there are no active backup or restore job running.
2. Close AhsayACB UI.
3. Stop the Ahsay A-Click Backup Manager services and check if the scheduler service has stopped running using the command highlighted in red.

```
#sudo /Applications/AhsayACB.app/bin/StopScheduler.sh

Password:

#ps -ef|grep java
#501 5721 5705 0 9:02PM ttys000 0:00.00 grep java
```

4. Using the terminal, go to AhsayACB installation path. Use the command highlighted in red.

```
#cd /Applications/AhsayACB.app
```

5. Open the **cb.opt** file using the command highlighted in red. Enter the password for logging in to your Mac when prompted.

```
#sudo vim cb.opt

#Password:
```

6. The following scripts will show.

```
#Print out default values of new backup set to a XML file
# Location: [WORKING_DIR]\DefaultBkupsetProfile.xml
com.ahsay.obc.core.action.GetUserPolicyCmd.debug=

# Print out debug messages for restore/decrypt
# Location: [WORKING_DIR]\DownloadFileSetTree.log
com.ahsay.obc.core.rset.file.DownloadFileSetTree.debug=

# Print out the decrypt list from OBS to restore to a XML file
# Location:
[RESTORE_DESTINATION]\DownloadFileSetTree_[RESTORE_JOB_ID].xml
com.ahsay.obc.core.rset.file.DownloadFileSetTree.SaveXML=

Office365.DSCInterval=60
```

7. Change the interval number by pressing **I.**

   For example:

   Current interval: *Office365.DSCInterval=60*

   ```
   Office365.DSCInterval=60
   -- INSERT --
   ```

   Updated interval: *Office365.DSCInterval=10*

   ```
   Office365.DSCInterval=-10
   -- INSERT --
   ```

   Explanation:

   On the current interval, the number of days is 60. While, the updated interval, the number of days is reduced to 10.

   WARNING!

   If the interval value is 0, *Office365.DSCInterval=0*, then the Data Synchronization Check (DSC) will run for every backup job.

   Press **Esc** + **:wq!** to save the changes made.

8. To check if the new line is added, use the commands highlighted in red.

   ```
   #cat cb.opt
   ```

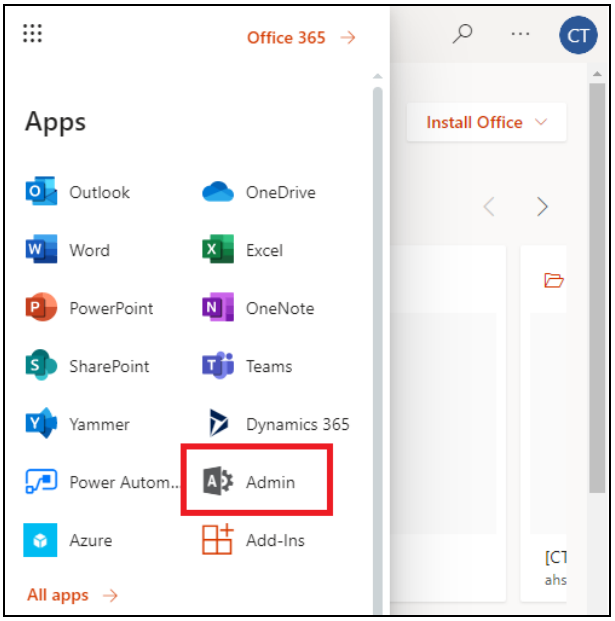
9. Start the Ahsay A-Click Backup Manager services and check if the scheduler service is running using the command highlighted in red.

   ```
   #sudo /Applications/AhsayACB.app/bin/Scheduler.sh

   Password:

   #ps -ef|grep java
   0 5735 1 0 9:05PM ttys000 0:02.07
   /Applications/AhsayACB.app/jvm/bin/ java -Xms128m -Xmx768m -
   Djava.library.path=. -cp .:./cbs.jar cbs
   /Applications/AhsayACB.app 501 5741 5705 0 9:05PM ttys000
   0:00.00 grep java
   ```

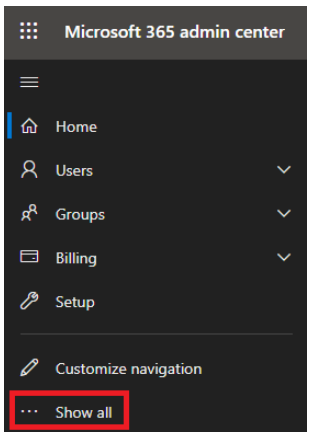
Appendix F Steps on How to view Item count and Storage used in Microsoft 365 Admin Center

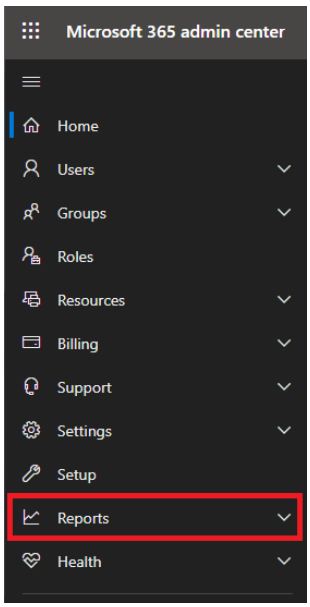
To view the item count and storage size of Office 365 user account based on the usage for Exchange (Outlook) and OneDrive follow the instructions below:

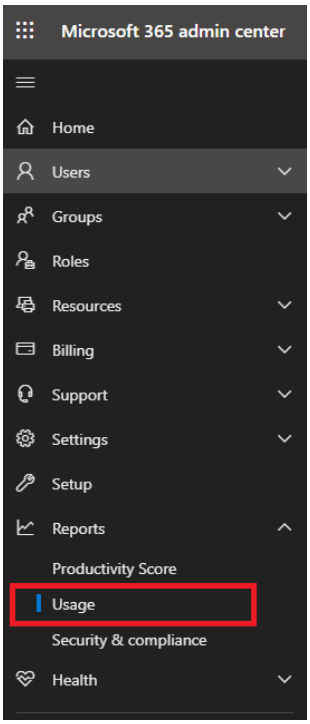
1. Login to the Office 365 (https://login.microsoft.com).
2. Go to Microsoft 365 admin center.



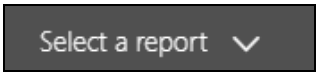
3. On the Microsoft 365 admin center, click **Show all** then click the dropdown arrow for the **Reports** and select **Usage**.

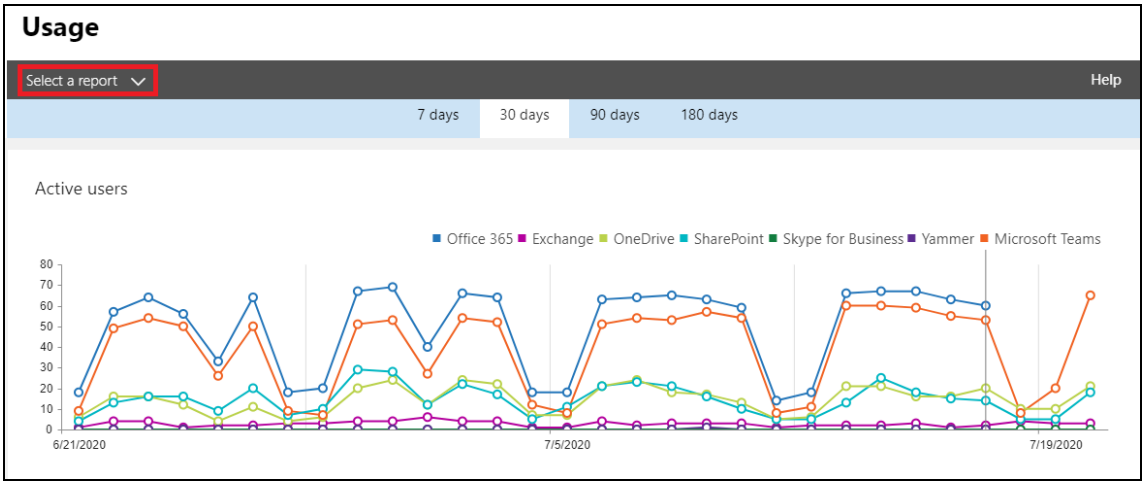


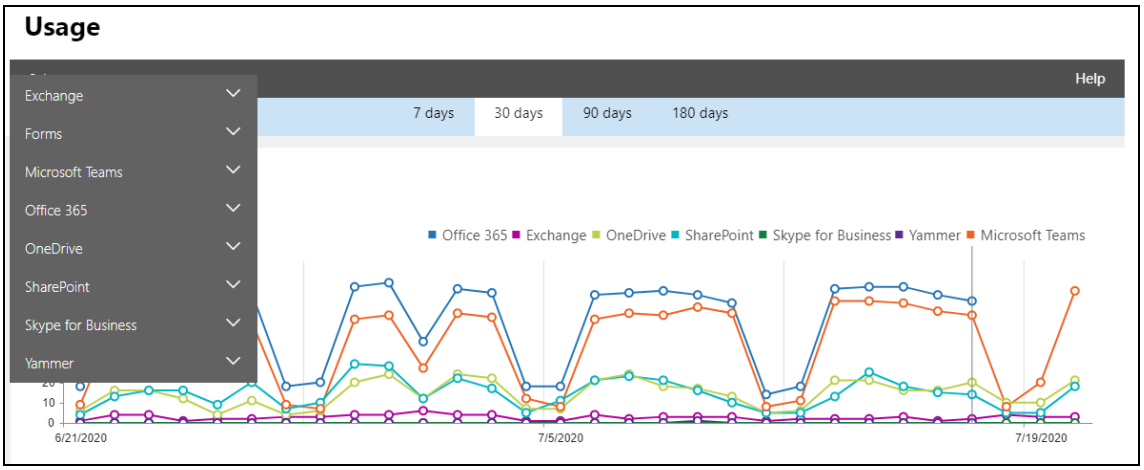




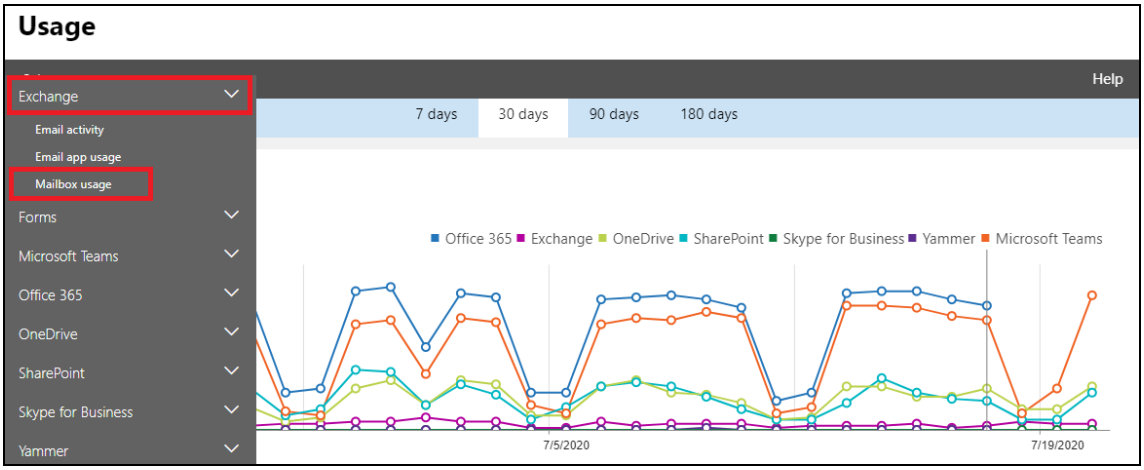
4. On the Usage screen, select a report you want to view.

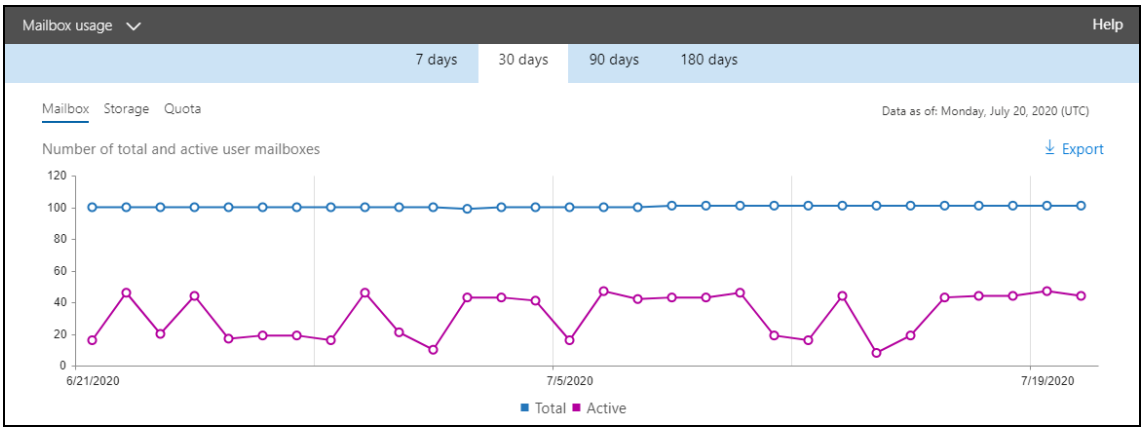






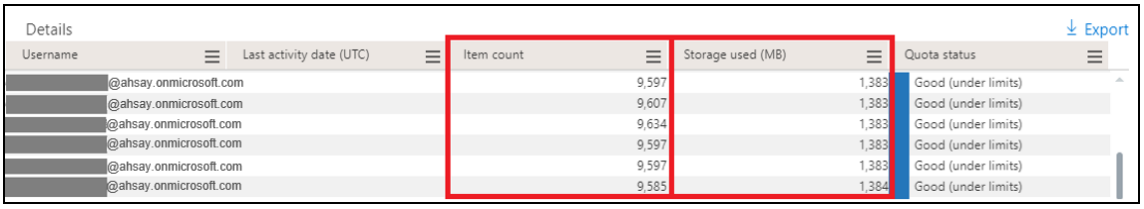
5. For **Exchange**, go to **Mailbox usage**.



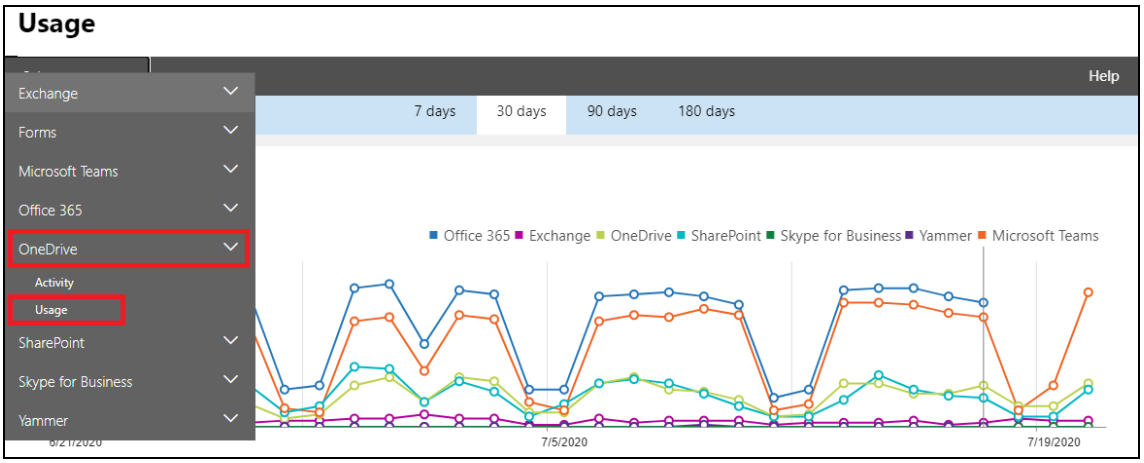


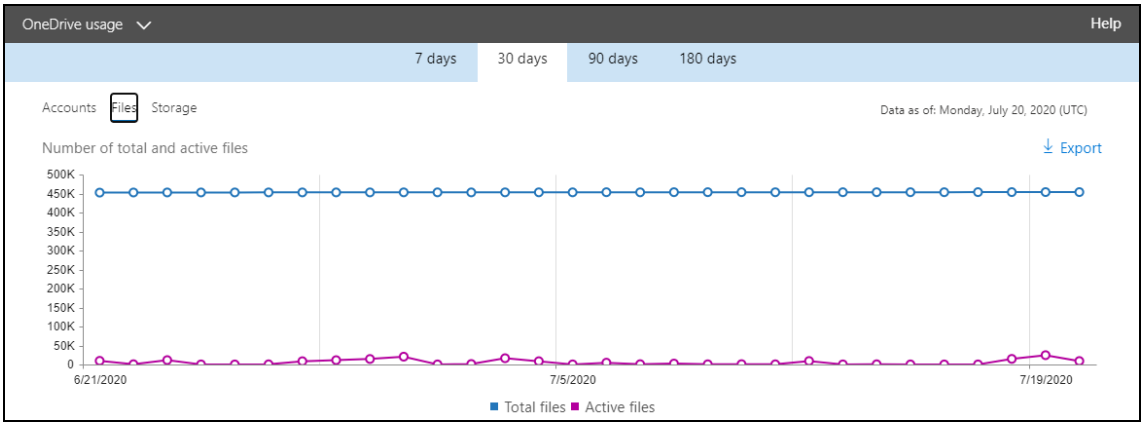
Highlighted columns are, Item count and Storage used (MB).

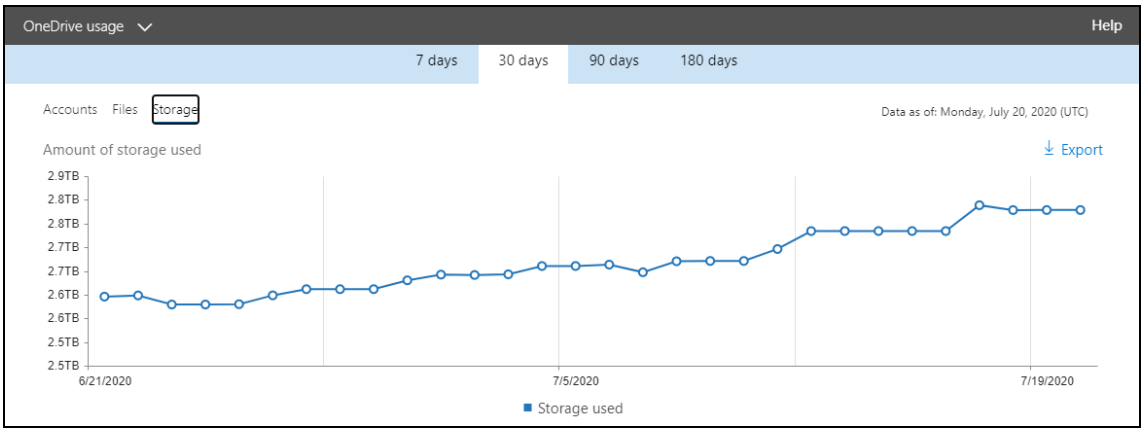
- **Item count** – number of mailbox items in Outlook per Office 365 user account
- **Storage used (MB)** – storage used in MB size per Office 365 user account



6. For **OneDrive**, go to **Usage**







Highlighted columns are, Files and Storage used (MB).

- **Files** – number of files in OneDrive per Office 365 user account
- **Storage used (MB)** – storage used in MB size per Office 365 user account

Appendix G Migrating Authentication of Office 365 Backup Set

Starting with AhsayACB v8.3.6.0 or above, existing backup sets must be migrated to use Modern Authentication. This will ensure that moving forward there will be no backup and restore issues to be encountered once Microsoft implements its product roadmap for Modern Authentication. This only needs to be done once per Office 365 user account.

There are two methods in migrating existing Office 365 backup sets, one is to migrate to Hybrid Authentication, and another is to migrate to Modern Authentication. The following are the required Office 365 account that must be used to authorize the migration of authentication of existing Office 365 backup sets:

- When migrating to Hybrid Authentication, the users Office 365 account may be used to authorize the migration of authentication.
- When migrating to Modern Authentication, an Office 365 account with a Global Admin is required to be used to login their credentials to authorize the migration of authentication.

The following are the two (2) migration scenarios:

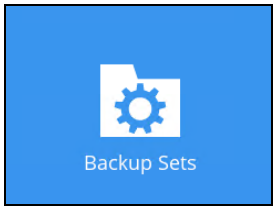
- Basic Authentication to Hybrid Authentication
- Basic Authentication to Modern Authentication

NOTE

Due to the current limitation with Microsoft API, Modern Authentication is currently not suitable for backup sets with Personal Sites selected. As a temporary workaround for Office 365 backup sets which require backup of Personal Sites should migrate to Hybrid Authentication until the issue has been resolved by Microsoft.

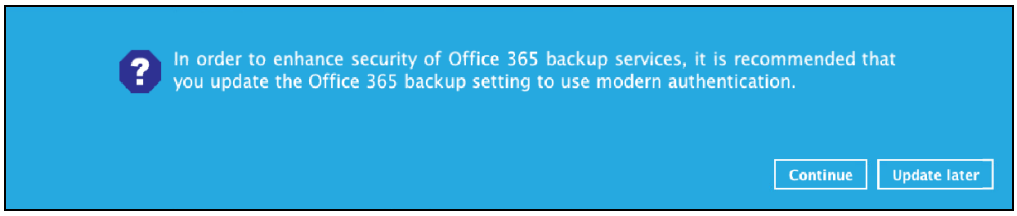
To migrate a backup set from **Basic Authentication to Hybrid Authentication**, follow the instructions below:

1. Logout all Office 365 account on the default browser before starting the migration of backup set.
2. In the AhsayACB main interface, click **Backup Sets**.

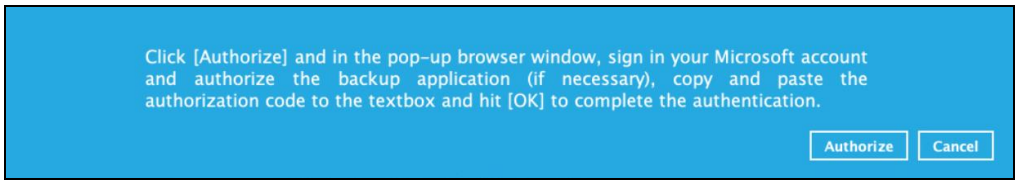


3. Select the backup set that will be migrated.

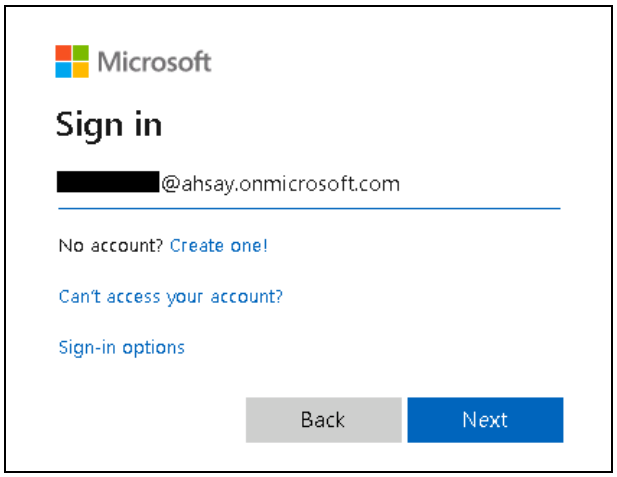
4. Click **Continue**.

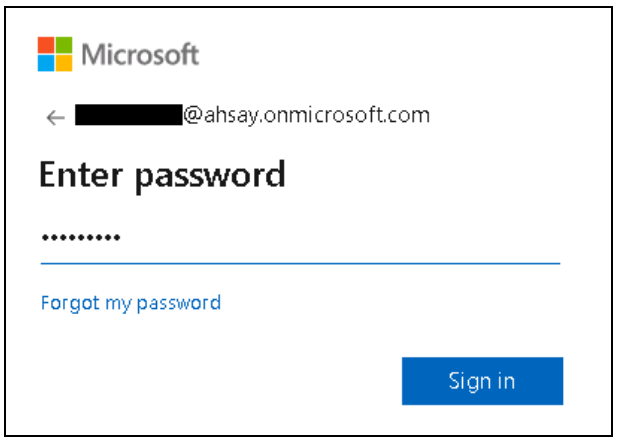


5. Click **Authorize**.

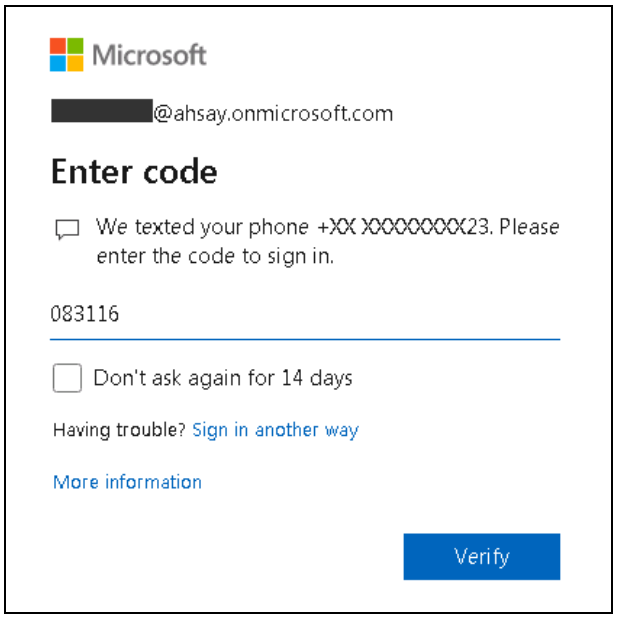


6. Sign in to your account.





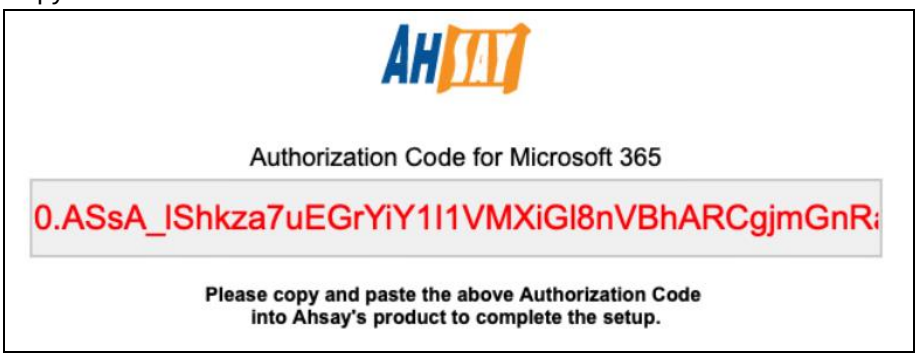
7. If MFA is enforced, enter the verification code sent to your mobile device and click **Verify**. Otherwise proceed to the next step.



NOTE

The verification code will only be required if the MFA status of an Office 365 account is enforced.

8. Copy the authorization code.

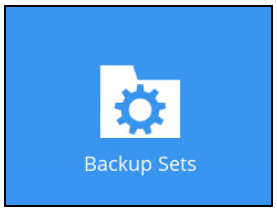


9. Go back to AhsayACB and paste the authorization code. Click **OK** to finish the migration.

To migrate a backup set from **Basic Authentication to Modern Authentication**, follow the instructions below:

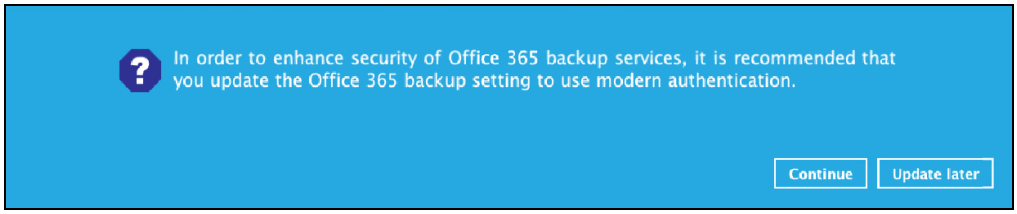
1. Logout all Office 365 account on the default browser before starting the migration of backup set.

2. In the AhsayACB main interface, click **Backup Sets**.

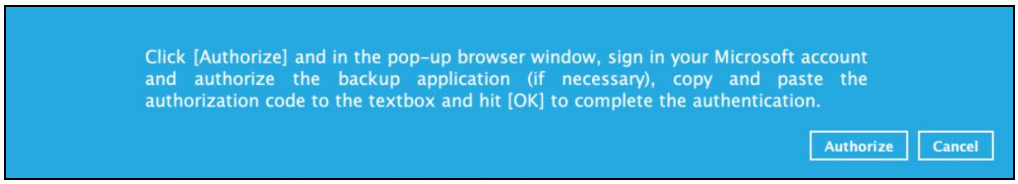


3. Select the backup set that will be migrated.

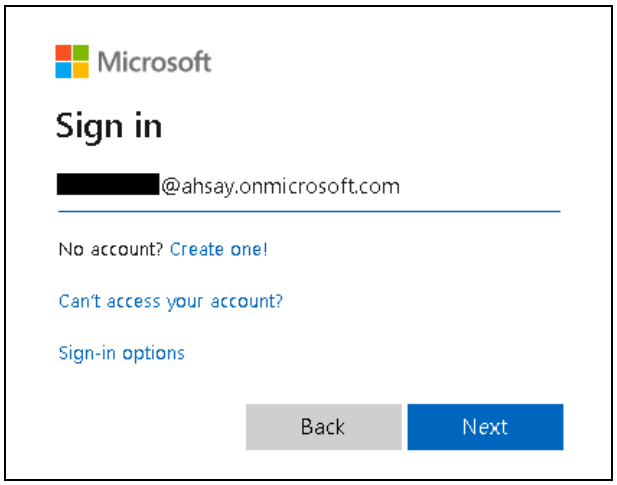
4. Click **Continue**.

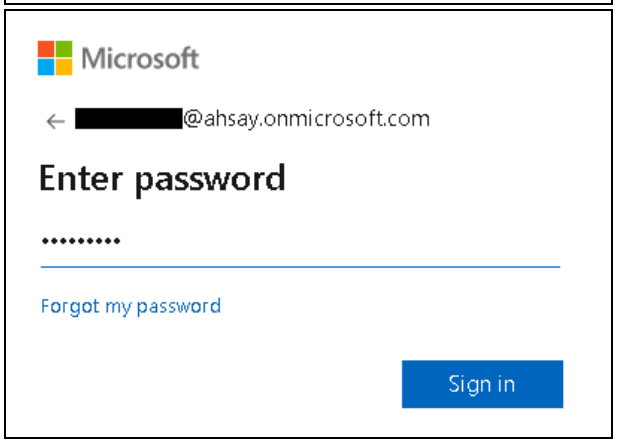


5. Click **Authorize**.

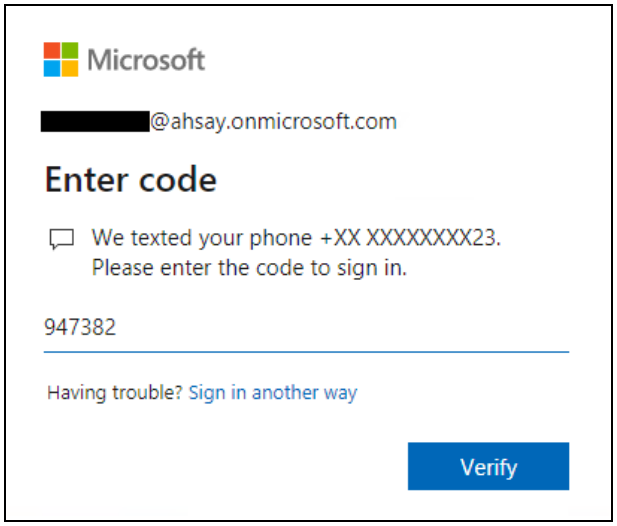


6. Ask your administrator to sign in using an Office 365 account with Global Admin in order to migrate the backup set.





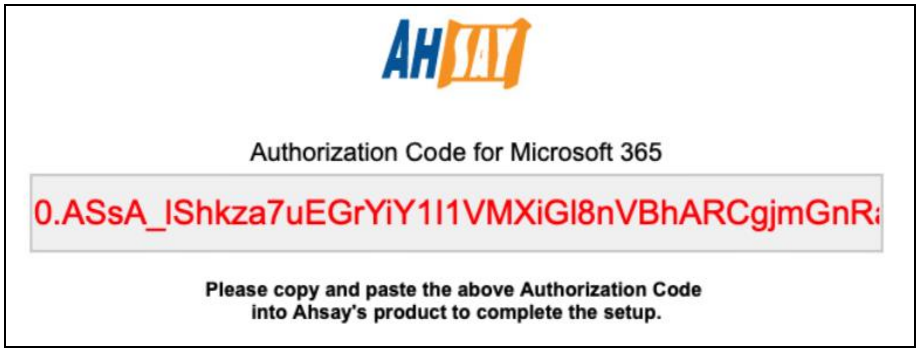
7. If MFA is enforced, enter the verification code sent to your mobile device and click **Verify**. Otherwise proceed to the next step.



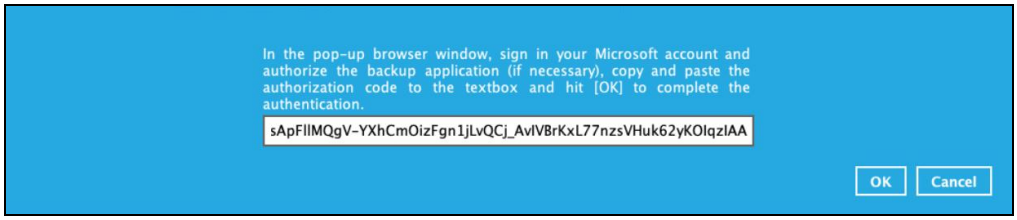
NOTE

The verification code will only be required if the MFA status of an Office 365 account is enforced.

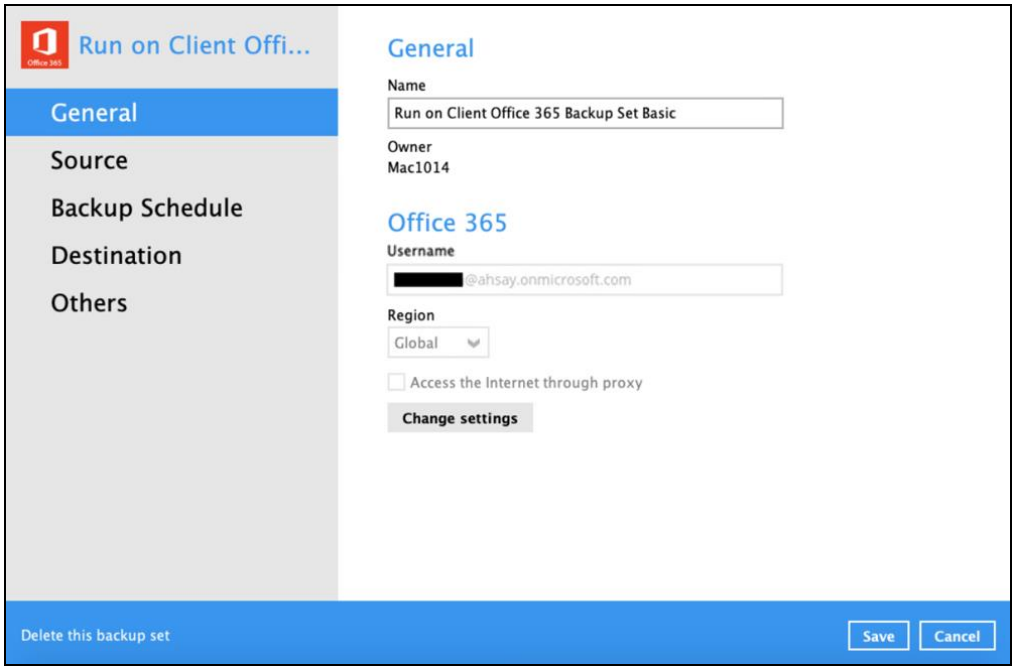
8. Copy the authorization code.



9. Go back to AhsayACB and paste the authorization code. Click **OK** to proceed.



10. Click **Save** to finish the migration.



Appendix H Steps on How to Change the Office 365 Authentication

After upgrading to AhsayACB v8.3.6.0 or above, all newly created Office 365 backup sets will automatically start using Modern Authentication. However, if the user has selected Personal Sites for Office 365 backup, this will not be possible on an Office 365 backup set using Modern Authentication due to limitations with Microsoft API. To resolve this issue, a change from Modern Authentication to Hybrid Authentication is needed. Please refer to Chapters 2.16.1 and 2.16.2 for the complete list of backup and restore limitations using Modern Authentication.

Once the backup and restore of SharePoint Web Parts and Metadata is fully supported using Modern Authentication, Office 365 backup sets using Hybrid Authentication can be changed back to Modern Authentication.

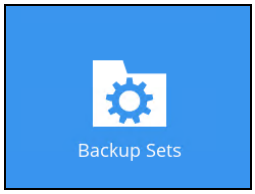
The following are the two (2) types of authentication change:

- Modern Authentication to Hybrid Authentication
- Hybrid Authentication to Modern Authentication

To change the authentication from **Modern Authentication to Hybrid Authentication**, follow the instructions below:

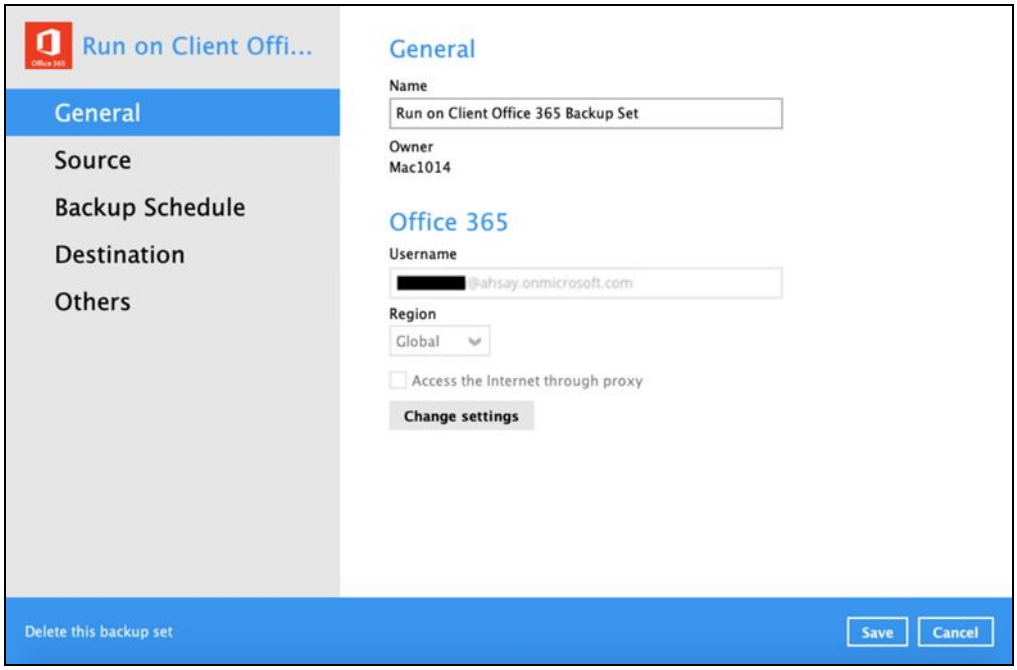
1. Logout all Office 365 account on the default browser before starting the authentication change of the backup set.

2. In the AhsayACB main interface, click **Backup Sets**.

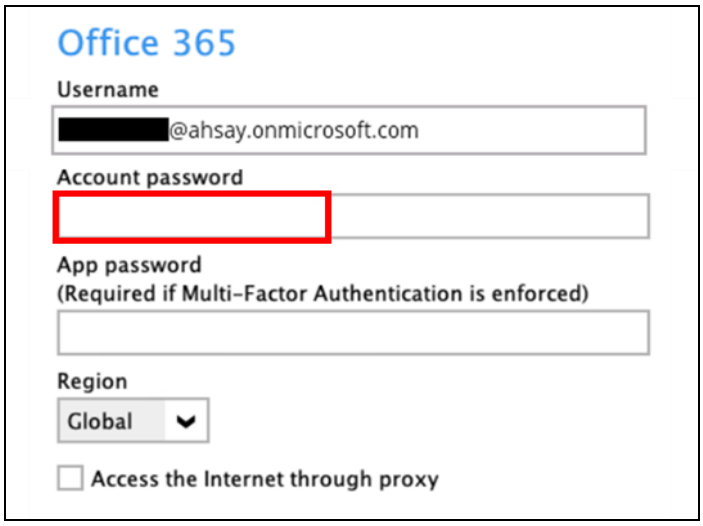


3. Select the backup set that you want to change to Hybrid Authentication.

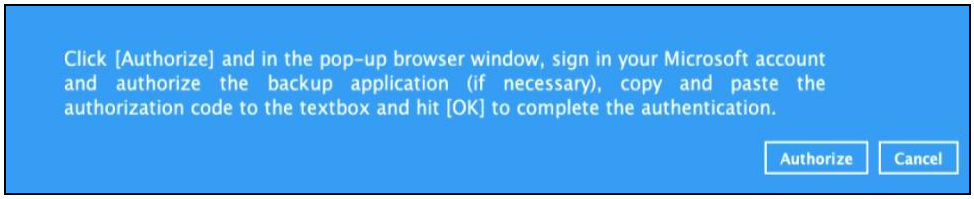
4. In the Backup Set Settings, click **Change settings** under the Office 365 screen.



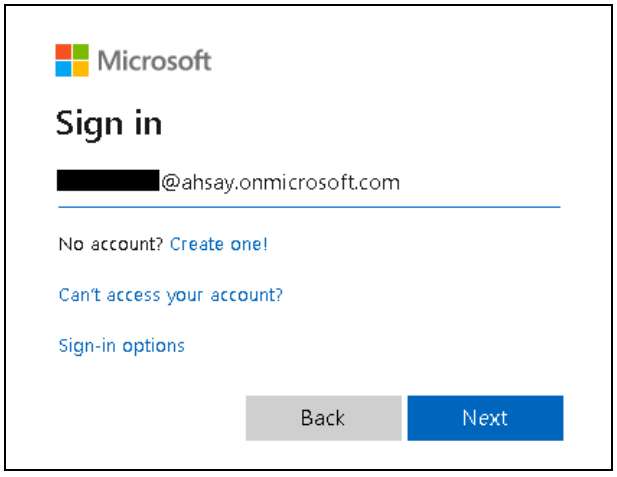
5. In the Office 365 credentials page, **input the Office 365 login account and password** then click **Next**.

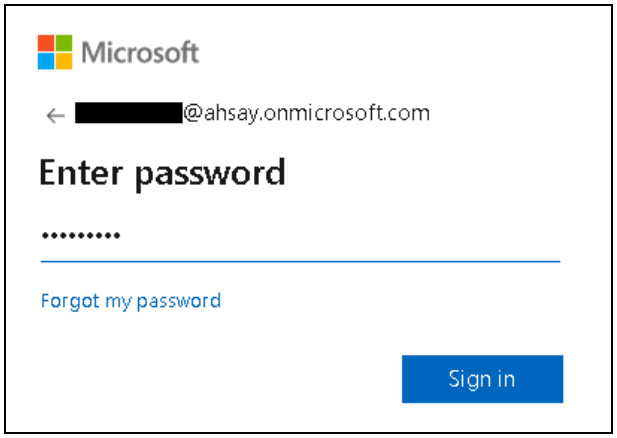


6. Click **Authorize** to start the authentication change process.

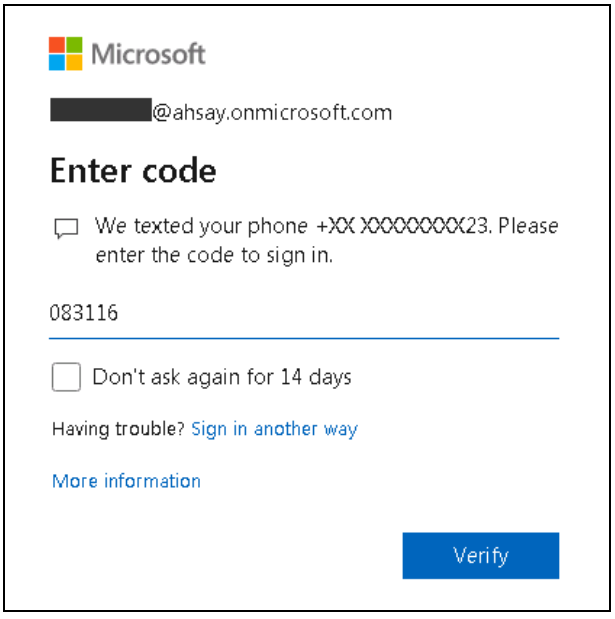


7. Sign in to your account.





8. If MFA is enforced, enter the verification code sent to your mobile device and click **Verify**. Otherwise, proceed to the next step.



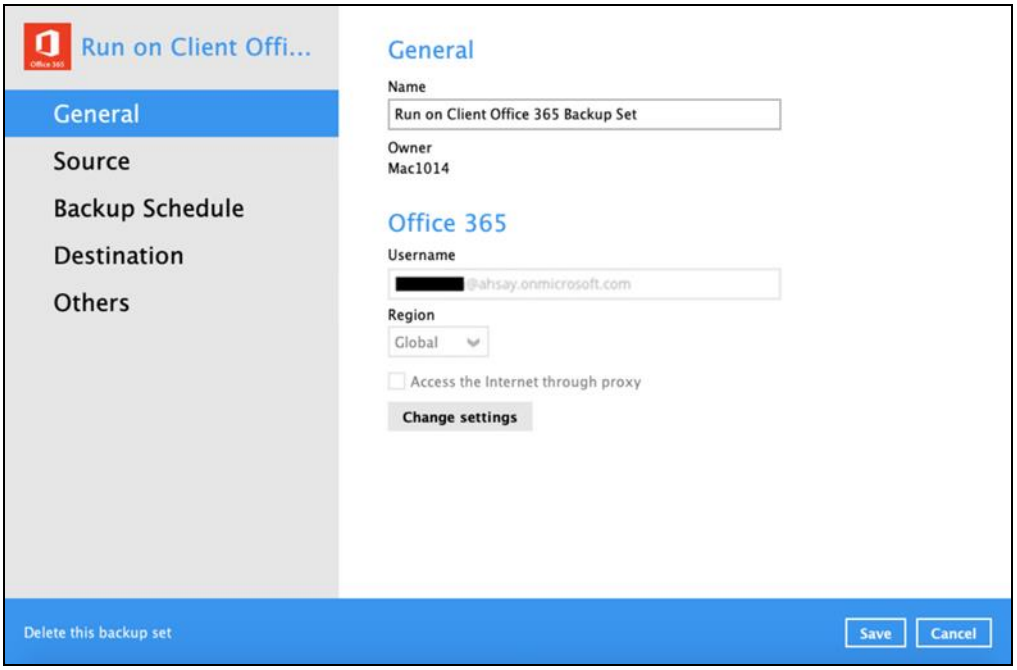
NOTE

The verification code is only required if the MFA status of an Office 365 account is enforced.

9. Copy the authorization code.

10. Go back to AhsayACB and paste the authorization code. Click **OK** to proceed.

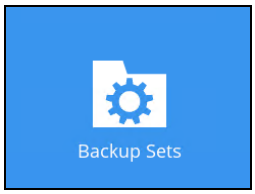
11. Click **Save** to finish the authentication change of the backup set.



To change the authentication from **Hybrid Authentication to Modern Authentication**, follow the instructions below:

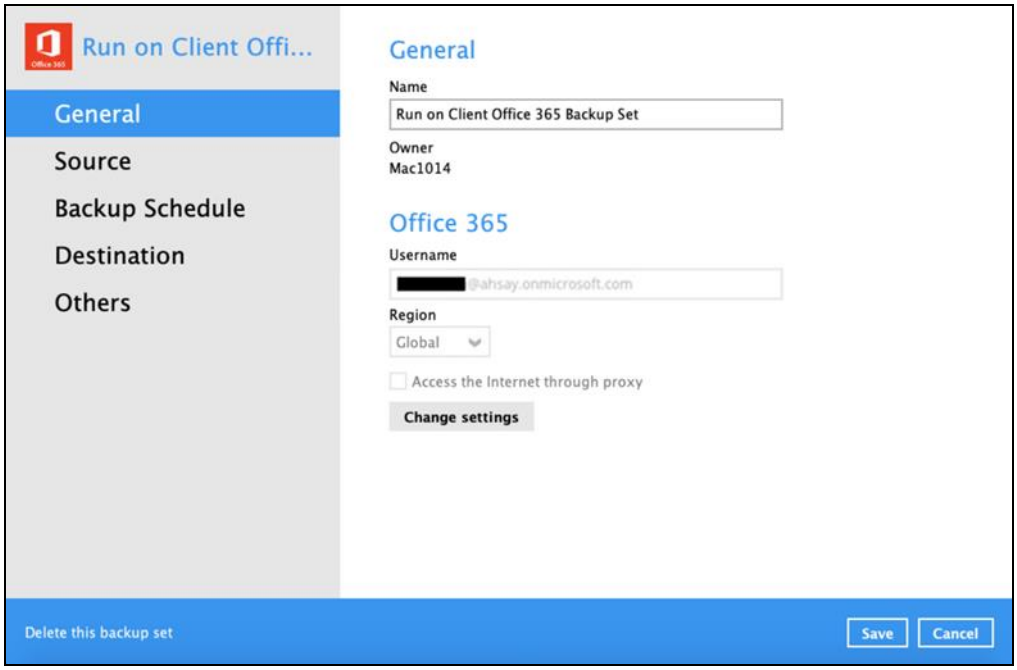
1. Logout all Office 365 account on the default browser before starting the authentication change of the backup set.

2. In the AhsayACB main interface, click **Backup Sets**.

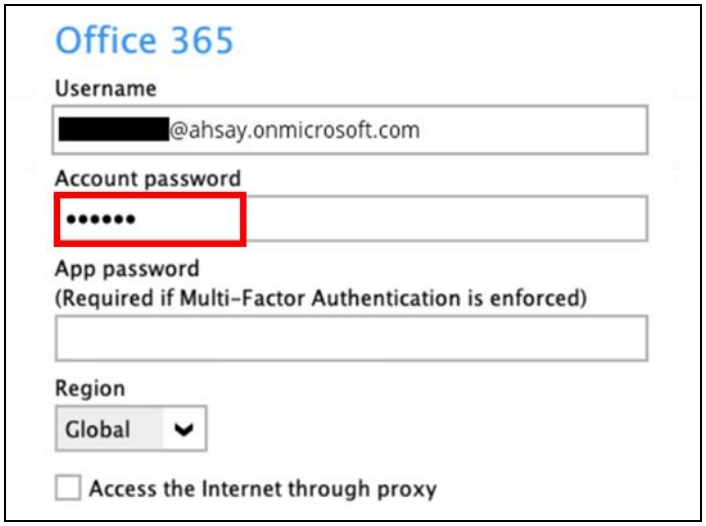


3. Select the backup set that you want to change to Modern Authentication.

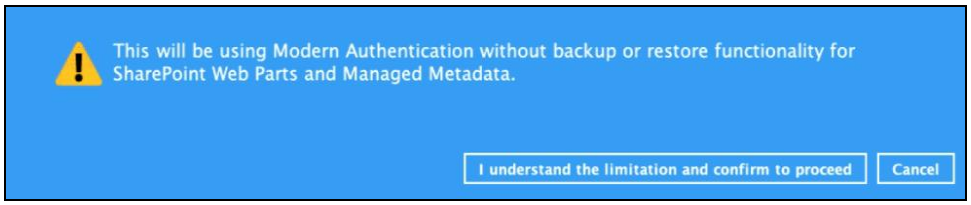
4. In the Backup Set Settings, click **Change settings** under the Office 365 screen.



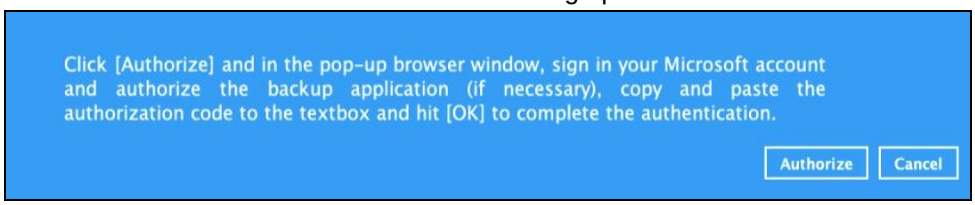
5. In the Office 365 credentials page, **remove the Account password** then click **Next**.



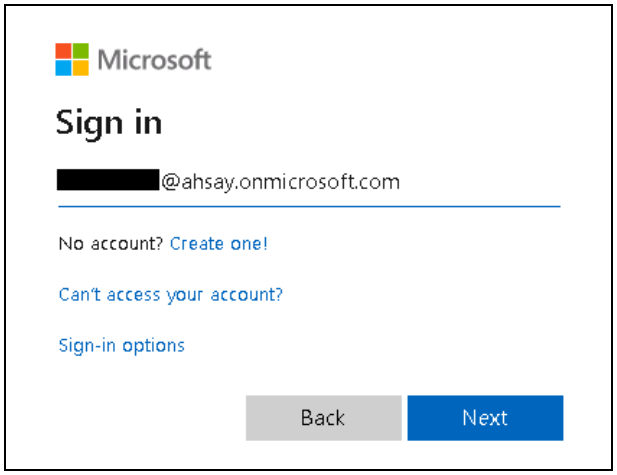
6. Click **I understand the limitation and confirm to proceed**.

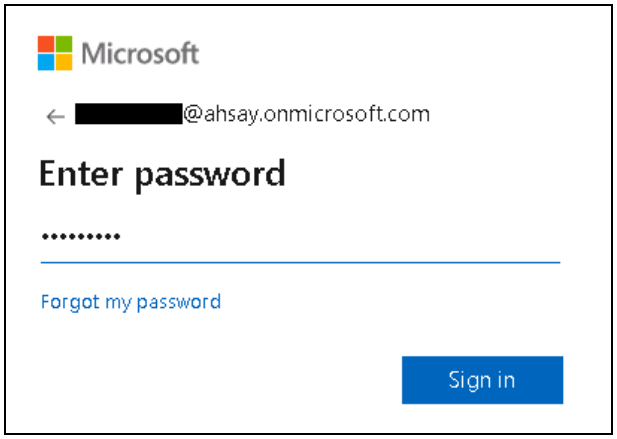


7. Click **Authorize** to start the authentication change process.

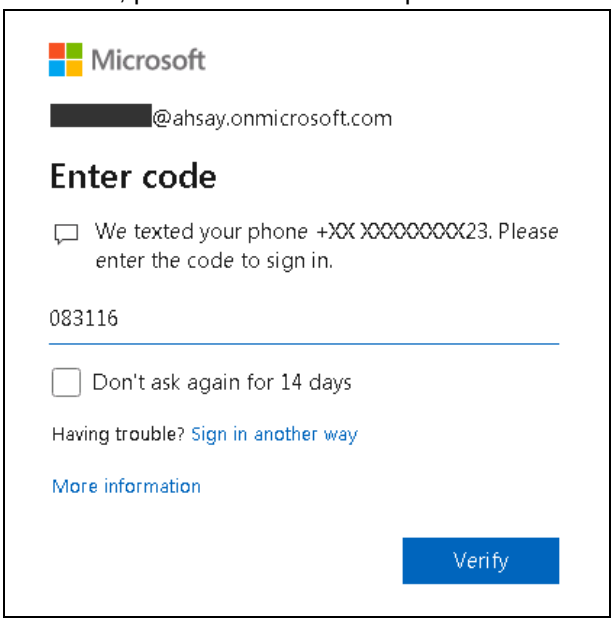


8. Sign in to your account.





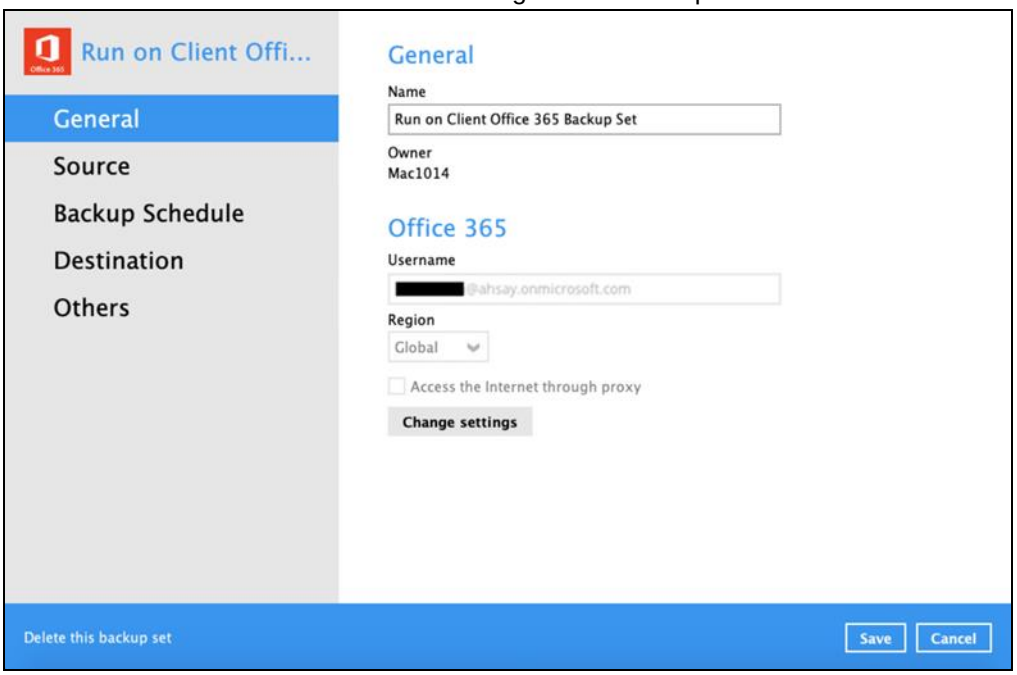
9. If MFA is enforced, enter the verification code sent to your mobile device and click **Verify**. Otherwise, proceed to the next step.



NOTE

The verification code is only required if the MFA status of an Office 365 account is enforced.

10. Copy the authorization code.

11. Go back to AhsayACB and paste the authorization code. Click **OK** to proceed.

12. Click **Save** to finish the authentication change of the backup set.