Ahsay Backup

Ahsay Online Backup Manager v8

Office 365 Backup & Restore Guide for Windows

Ahsay Systems Corporation Limited

7 April 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 K	New
9 October 2020	Updated screenshots in Ch. 7, Appendices B and G	Modifications
25 January 2021	Updated screenshot in Ch. 2.6; Updated login steps in Ch. 3; Updated PDIC diagram in Ch. 5; Reorganized Permission Requirements in Ch. 2.14; Added Ch. 2.18; Modified Limitations in Ch. 2.19	Modifications
29 January 2021	Updated screenshots in Chapters 2, 7 and Appendix I	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

Table of Contents

1 Overview 1

1.1 What is this software? 1

1.2 System Architecture 1

1.3 Why should I use AhsayOBM Run on Client (Agent-based) solution to back up my Office 365 data? 2

1.4 Why should I use AhsayOBM to backup/restore my Office 365 domain? 8

1.5 About This Document 10

2 Preparing for Backup and Restore 11

2.1 Hardware Requirement 11

2.2 Software Requirement 11

2.3 AhsayOBM Installation 11

2.4 Antivirus Exclusion Requirement 11

2.5 Upgrade VMware Tools Requirement 11

2.6 Add-on Module Requirement 12

2.7 Access for AhsayCBS User Web Console 13

2.8 Backup Quota Requirement 13

2.9 Public Folder Backup 13

2.10 SharePoint Site Backup 13

2.11 Java Heap Size 13

2.12 AhsayOBM License Requirements 13

2.13 Office 365 License Requirements 14

2.14 Office 365 Permission Requirements 15

2.14.1 Assigning Global Admin Role to Accounts 16

2.14.2 Granting Term Store Administrator Role 18

2.14.3 Granting Permission Discovery Management Group 20

2.14.4 Granting Permission to Accounts for Creating Backup Set 22

2.14.5 Granting Permission to restore all share link types to alternate location in Office 365 25

2.15 Data Synchronization Check (DSC) Setup 28

2.16 Authentication 30

2.17 Supported Services 33

2.18 Maximum Supported File Size 40

2.19 Limitations 40

2.19.1 Ahsay Limitations 40

2.19.2 Microsoft Limitations 44

2.20 Best Practices and Recommendations 46

3 Login to AhsayOBM 50

3.1 Login to AhsayOBM with no 2FA 50

3.2 Login to AhsayOBM with 2FA using Twilio 52

3.3 Login to AhsayOBM with 2FA using Mobile Authentication 54

4 Creating an Office 365 Backup Set 57

4.1 Modern Authentication 57

4.2 Hybrid Authentication 80

5 Overview of Office 365 Backup Process 106

5.1 Periodic Data Integrity Check (PDIC) Process 107

5.2 Backup Set Index Handling Process 109

5.2.1 Start Backup Job 109

5.2.2 Completed Backup Job 110

5.3 Data Validation Check Process 111

6 Running Backup Job 112

7 Restoring Office 365 Backup Set 118

7.1 Restore Backup with AhsayOBM 120

7.1.1. From Users 121

7.1.2. From Site Collections 147

7.2 Restore Filter with AhsayOBM 170

7.2.1. From Users 171

7.2.2. From Site Collections 183

8 Contacting Ahsay 192

8.1 Technical Assistance 192

8.2 Documentation 192

Appendix 193

Appendix A: Example Scenarios for Office 365 License Requirement and Usage 193

Appendix B: Example for backup of large numbers of Office 365 users 198

Appendix C: Example Scenarios for Restore Filter using AhsayOBM 200

Appendix D: Setting Multi-Factor Authentication (MFA) in Microsoft 365 Admin Center 215

Appendix E: Example Scenario for Backup Set Maintenance 228

Appendix F: Example Scenario for Data Synchronization Check (DSC) with sample backup logs 229

Appendix G: Setting the Data Synchronization Check (DSC) 234

Appendix H: Steps on How to Increase the Number of Concurrent Backup Threads 235

Appendix I: Steps on How to view Item count and Storage used in Microsoft 365 Admin Center 236

Appendix J: Migrating Authentication of Office 365 Backup Set 241

Appendix K: Steps on How to Change the Office 365 Authentication 252

1 Overview

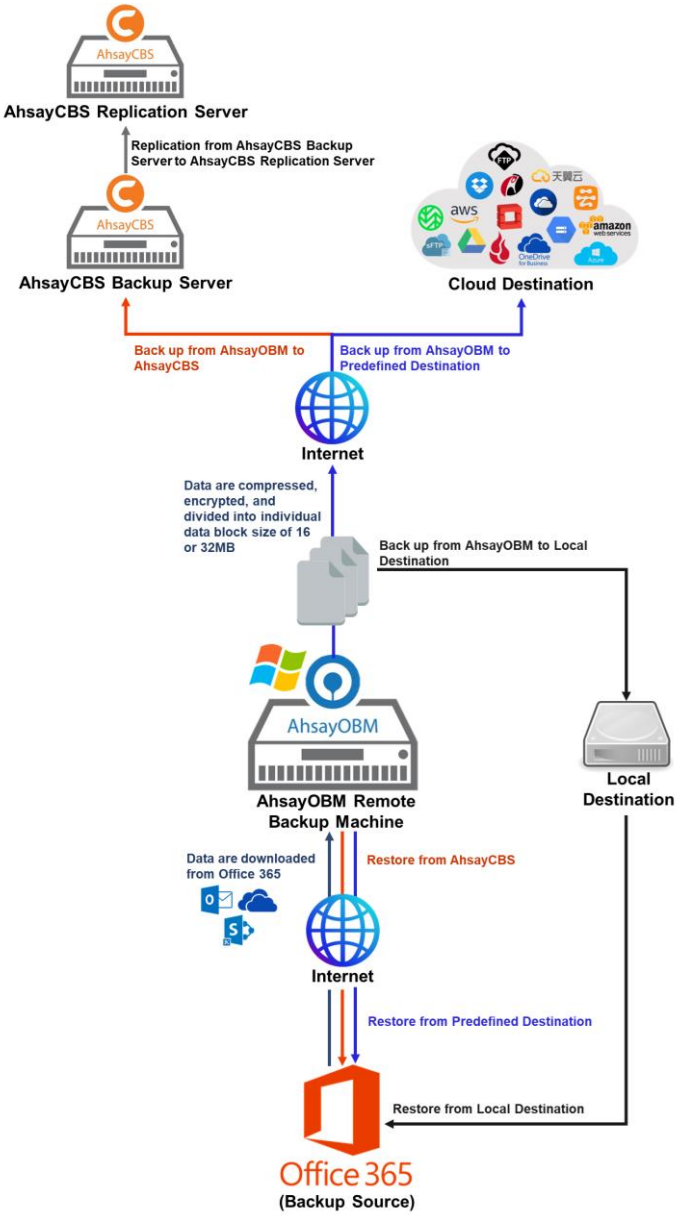
1.1 What is this software?

Ahsay brings you specialized client backup software, namely AhsayOBM, 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

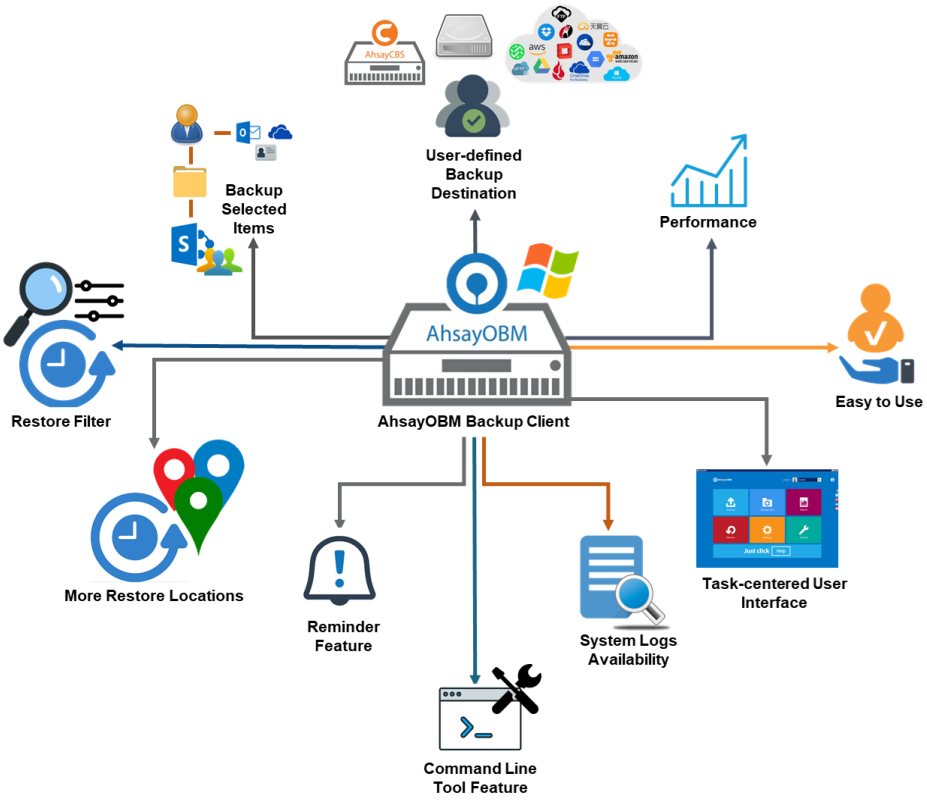
Below is the system architecture diagram illustrating the major elements involved in the backup process among the Office 365 service, AhsayOBM and AhsayCBS.

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



1.3 Why should I use AhsayOBM Run on Client (Agent-based) solution to back up my Office 365 data?

We are committed to bringing you a comprehensive Office 365 backup solution with AhsayOBM. Below are some key areas that we can help to make 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 has 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 backup sets with large number of Office 365 accounts 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.

Command Line Tool

Agent-based backup solution has a feature that allows user to configure a pre and/or post-backup command which can be an operating system level command, script or batch file, or third-party utilities that will run before and/or after a backup job.

Reminder Feature

With the agent-based backup, a reminder feature is provided which will display a backup confirmation dialog box that will prompt user to run a backup job during machine log off, restart or shut down when enabled.

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).

Restore Filter

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

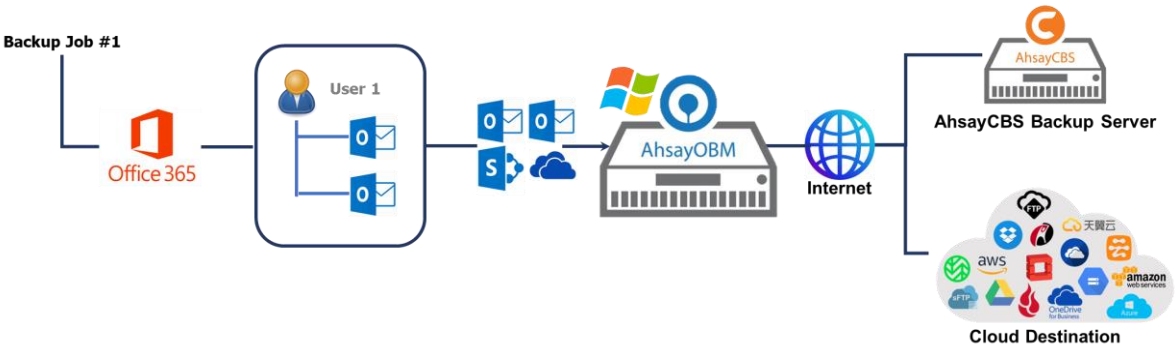
Fast and Efficient

We understand that backup could be a time and resources consuming process, which is why AhsayOBM 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.

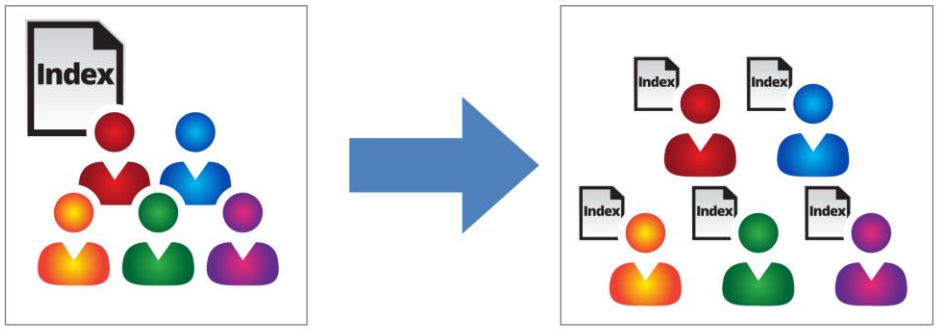
Backup job uses a maximum of 4 concurrent threads.



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 resources can be user level, site collection level and even item level.

- Flexible backup options:
  - Only select the required users, specific site collection or items for backup.
- Flexible restore options:
  - Restore all the users or just one user or restore the whole site collection or just one site or restore the whole user contents or just one item.
  - Restore items to the original location or an alternate location.

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 Client Office 365 Backup Set	Run on Server 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 Why should I use AhsayOBM to backup/restore my Office 365 domain?

You may be wondering why you need to use AhsayOBM to backup/restore your Office 365. Well, people assume that Microsoft is responsible for backing up everything from your calendars and your emails to your files in SharePoint and OneDrive. As the backups performed by Microsoft are to provide a system wide recovery rather than to facilitate the recovery of individual items for the end user.

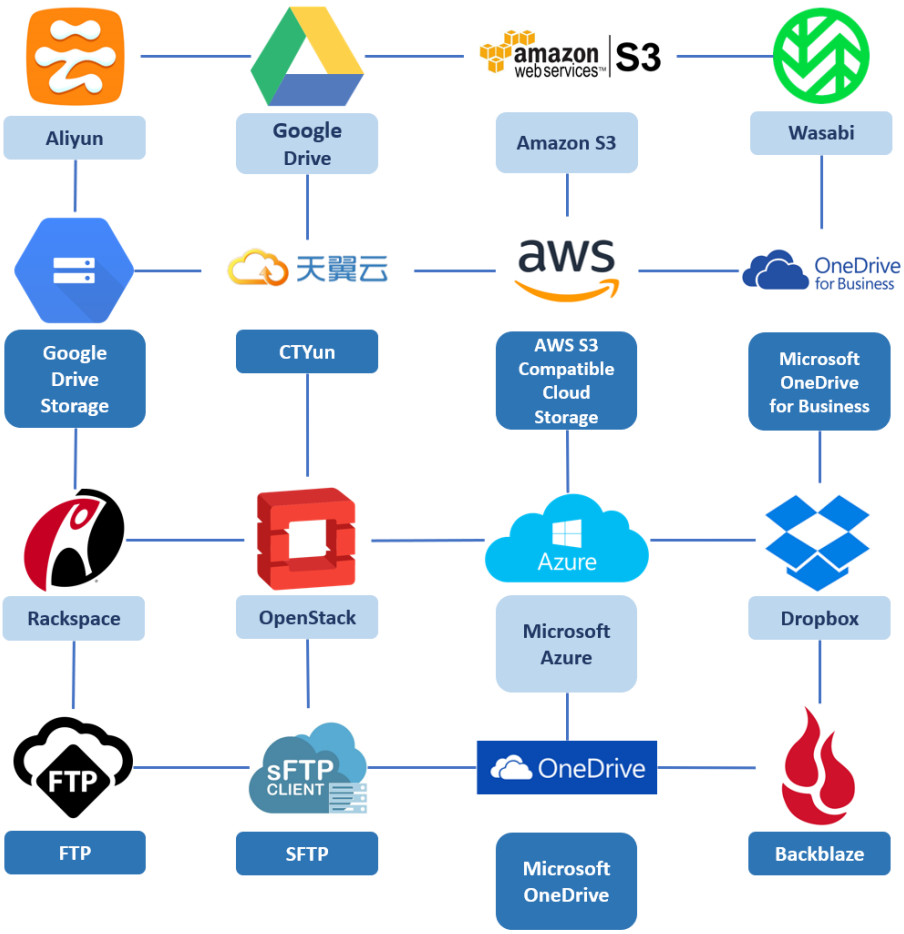
Let's take a look at some of the Microsoft's Office 365 backup capabilities and limitations

- Microsoft is only responsible for the Office 365 infrastructure and uptime of the cloud and apps with Office 365. So, if you are relying on Microsoft to protect your organization from data loss, your data and organization are at high risk if you do not implement additional data protection. These are some of the scenarios that Microsoft is responsible for on their cloud platform:
    - Hardware Failure
    - Software Failure
    - Natural Disaster
    - Power Outage
- On the other hand, Microsoft is not responsible in any of these scenarios and you have to face the harsh reality that there's no guarantee a complete and speedy restore incase these happens:
    - Accidental Data Deletion (Human error)
    - Malicious Attacks
    - Viruses/Malware
- Microsoft has a retention policy for mailbox and public folder that are only up to 14 days to 30 days. To support this, please refer to this article for more information: Microsoft: Overview of retention policy.
- Microsoft has set the same limitations for SharePoint Online and OneDrive. It only stores deleted items for a period of 93 days, once you exceed the retention period, the data is gone indefinitely.
- End users do not have control over what were backed up and what can be restored.
- End users have no direct access to their backup data of their Office 365 domains/accounts.

Now, let's check the capabilities of AhsayOBM for Office 365

- AhsayOBM ensures protection from data loss, ensuring the all information in your Office 365 environment are protected to avoid disruptions to day-to-day operations.
- We offer fully flexible retention policy that can be configured by days, weekly, monthly, quarterly, years compare to Microsoft's limited retention period which is 14 to 30 days only.
- Using AhsayOBM, end user has access or control over items that will be backed up or restore, whether it is individual item, calendar entries, notes or even corrupted mailbox and more.

- AhsayOBM also provides multiple backup destinations from your Office 365 to your local machine, to any of our supported cloud destinations, and to our AhsayCBS Server.



- Flexible restore is also a key feature of AhsayOBM that is designed to have multiple restore options.

Local Machine	Restore your data to your local computer where the AhsayOBM is running. Note: This option only applies to restore of items such as files, images, video, music and more from OneDrive and not items from Outlook mailbox.
Original Location	Restore your data to the original Office 365 account.
Alternate Location	Restore your data to an alternate location of another Office 365 account on the same domain.
Alternate Office 365 Account	Restore your data to an alternative Office 365 that has a different domain.

- Ahsay has automated backups and manual (on demand) backups You are also able to check the restore and backup status with corresponding backup and restore reports.

1.5 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 AhsayOBM.

The document can be divided into three (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 AhsayOBM

Creating a Backup Set
Create a backup set using AhsayOBM

Running a Backup Set
Run a backup set using the AhsayOBM

Configuring an Automated Backup
Configure backup schedule for automated backup

Part 3: Restoring Office 365 Backup

Restoring a Backup Set using AhsayOBM
Restore a backup using the AhsayOBM

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 AhsayOBM, 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 AhsayOBM 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 AhsayOBM. 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 AhsayOBM Installation

For agent-based backup and restore, make sure that the latest version of AhsayOBM 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 AhsayOBM is released. To get our latest product and company news through email, please subscribe to our mailing list. https://www.ahsay.com/jsp/en/home/subscribe_mail_list.jsp

2.4 Antivirus Exclusion Requirement

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

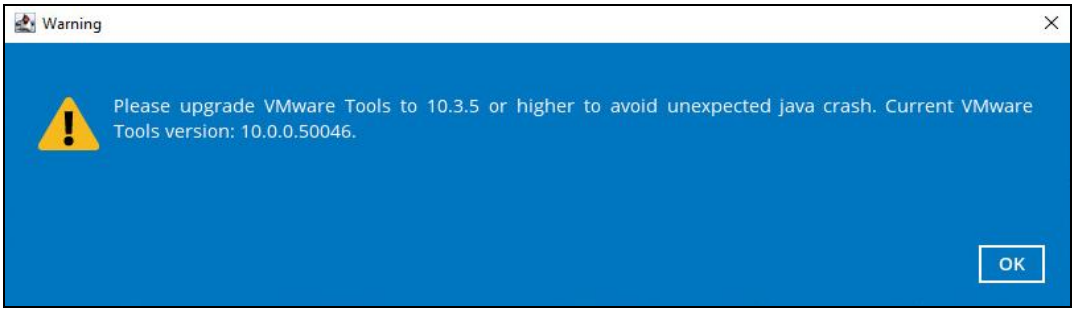
NOTE

The bJW.exe process is automatically added to Windows Defender exclusion list for Windows 10 and 2016, and 2019 during installation / upgrade via installer or upgrade via AUA.

2.5 Upgrade VMware Tools Requirement

To avoid unexpected java crash, if the Windows machine is a guest VM hosted on a VMware Host then it is highly recommended that the VMware tools version installed on the guest VM must be 10.0.5 or above.

Below is the warning message that will be displayed if the version of the VMware Tools is less than 10.0.5.



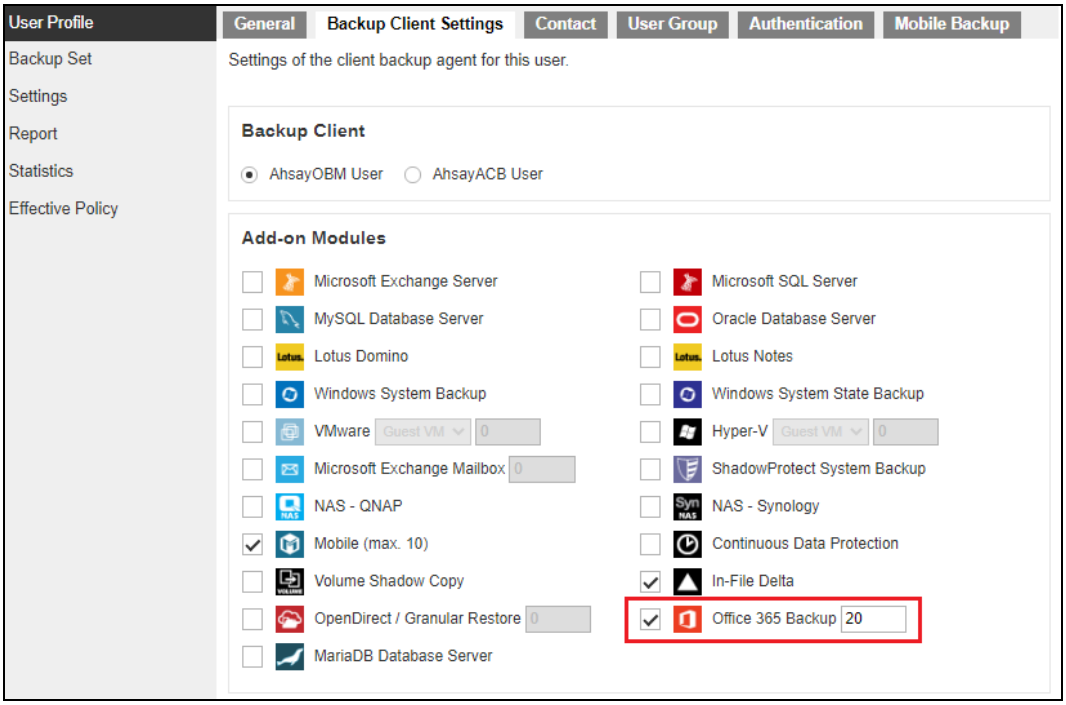
NOTE

For more information about the upgrade of VMware Tools, refer to this article, https://wiki.ahsay.com/doku.php?id=public:5288_ahsayobc_crash_on_vm_with_vmware_tools_pre-10.0.5.

2.6 Add-on Module Requirement

Make sure that the Office 365 Backup feature has been enabled as an add-on module in your AhsayOBM 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 AhsayOBM User with an add-on module of Office 365 with 20 licenses.



The Ahsay licenses for the Office 365 module are calculated by the number of unique licensed or unlicensed Office 365 user accounts. If same Office 365 account is backed up on multiple backup sets with an AhsayOBM user account would be counted a one Office 365 license.

- Each licensed or unlicensed Office 365 user account selected for backup requires one Office 365 license.
- Each Equipment Mailbox, Room Mailbox, or Shared Mailbox selected for backup requires one Office 365 license.
- If just only SharePoint Sites under the Site Collections and/or files of folders under Public Folder are selected for backup, this requires only one Office 365 license.

However, if any items from either Outlook, Items from OneDrive, or Personal Sites under Users are selected for backup, the Office 365 license count will be calculated based on the number of the user account selected.

For more detailed examples about the Office 365 license requirement and usage, refer to Appendix A: Example Scenarios for Office 365 License Requirement and Usage.

2.7 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 AhsayOBM 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.

Please contact your backup service provider for more details.

2.8 Backup Quota Requirement

Make sure that your AhsayOBM 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 I: Steps on How to view Item count and Storage used in Microsoft 365 Admin Center

2.9 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.

2.10 SharePoint Site Backup

To be able to backup Personal Sites and/or SharePoint 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 and/or SharePoint Sites selected. As backup and restore of SharePoint metadata are not fully supported.

2.11 Java Heap Size

The default Java setting heap 2048M, is sufficient for Office 365 backups based on the default 4 concurrent backup threads.

The Java heap size should only be increased if the number of current backup threads is increased as more backup threads is expected to consume more memory. But this does not guarantee that the overall backup speed will be faster since there will be an increased chance of throttling.

As the value of 4 concurrent backup threads is found to be the optimal setting for Office 365 backups, to ensure best backup performance, minimal resource usage, and lowest probability of throttling of Ahsay backup requests by Microsoft Office 365.

For more detailed information on how to increase the backup thread, please refer to this link: Appendix H: Steps on How to Increase the Number of Concurrent Backup Threads.

2.12 AhsayOBM License Requirements

AhsayOBM licenses are calculated on a per device basis:

To backup users with one (1) backup client computer

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

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

Example: If there are ten (10) backup sets to backed-up across three (3) backup client computers, then 3 AhsayOBM licenses are required.

2.13 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 AhsayOBM or AhsayCBS User Web Console.

Office 365 Business	Office 365 Business Essentials
Office 365 Business Premium	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

- **Restore Requirement**

  When restoring data of Office 365 user, the account which the data will be restored to requires valid license(s):

  - Requires Exchange License

    Example: Exchange Online Plan and Office 365 E3 are required when restoring Outlook's / Public Folder's items.

  - Requires SharePoint License

    Example: SharePoint Online Plan and Office 365 E3 are required when restoring OneDrive's / Personal Site's items.

2.14 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 AhsayOBM 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. 2.14.1.

- **Term Store Administrator Role**

  The Term Store Administrator Role may be required for backup and restore of SharePoint items. To assign the role, please refer to Ch. 2.14.2.

- 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. 2.14.3.

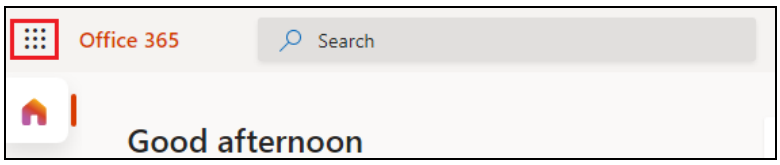
  - ApplicationImpersonation
  - Legal Hold
  - Mailbox Import Export
  - Mailbox Search
  - Public Folders

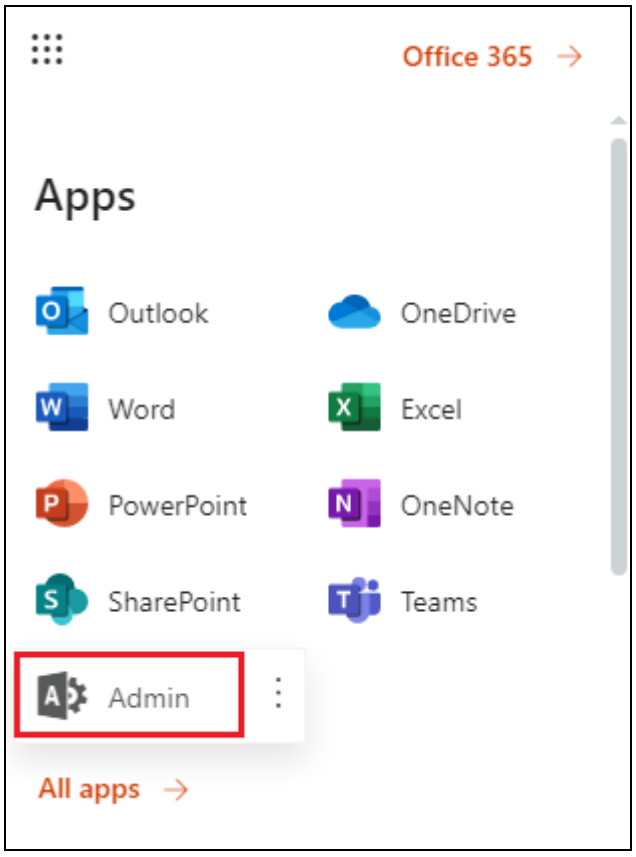
Otherwise, proceed to grant all necessary permissions to the Office user account as shown in the following chapters 2.14.1, 2.14.2, 2.14.3, 2.14.4, and 2.14.5.

2.14.1 Assigning Global Admin Role to Accounts

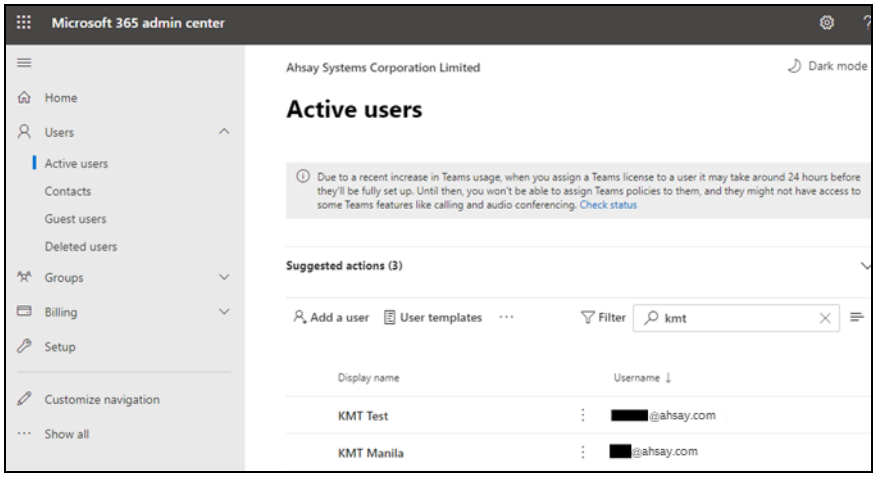
To assign the Global Admin role to accounts, follow the steps below:

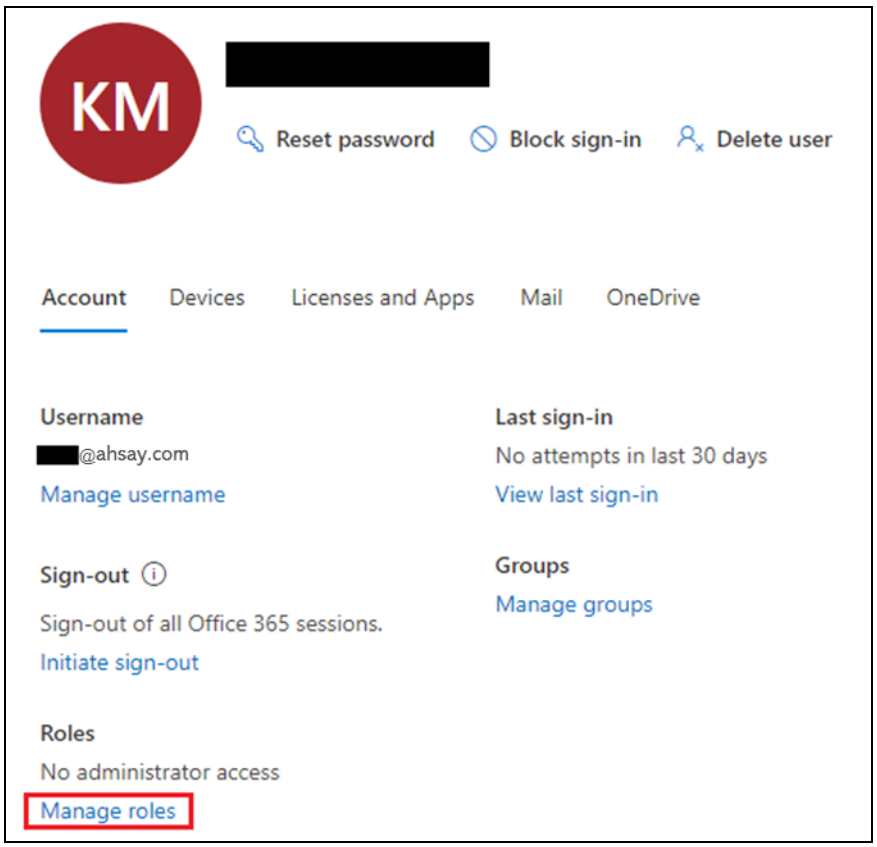
i. Click the App launcher in the upper left side then click **Admin** to go to the Microsoft 365 admin center.



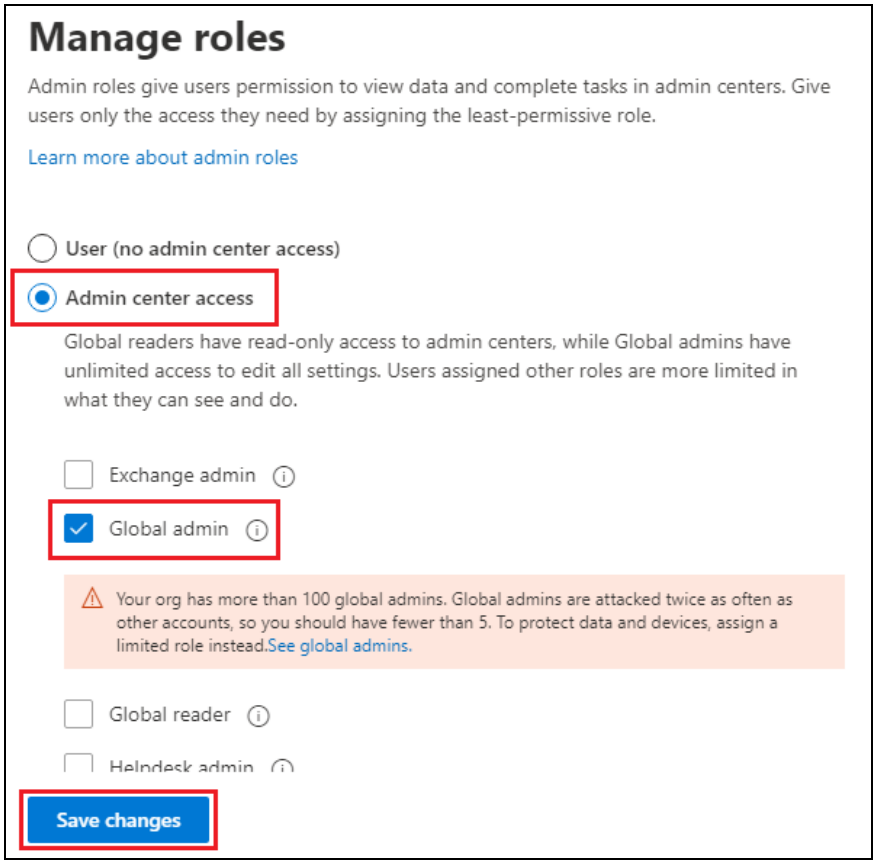


ii. In the Microsoft 365 admin center, on the left panel click **Users**. Find the user you want to assign the Global Admin role and select **Manage roles**.





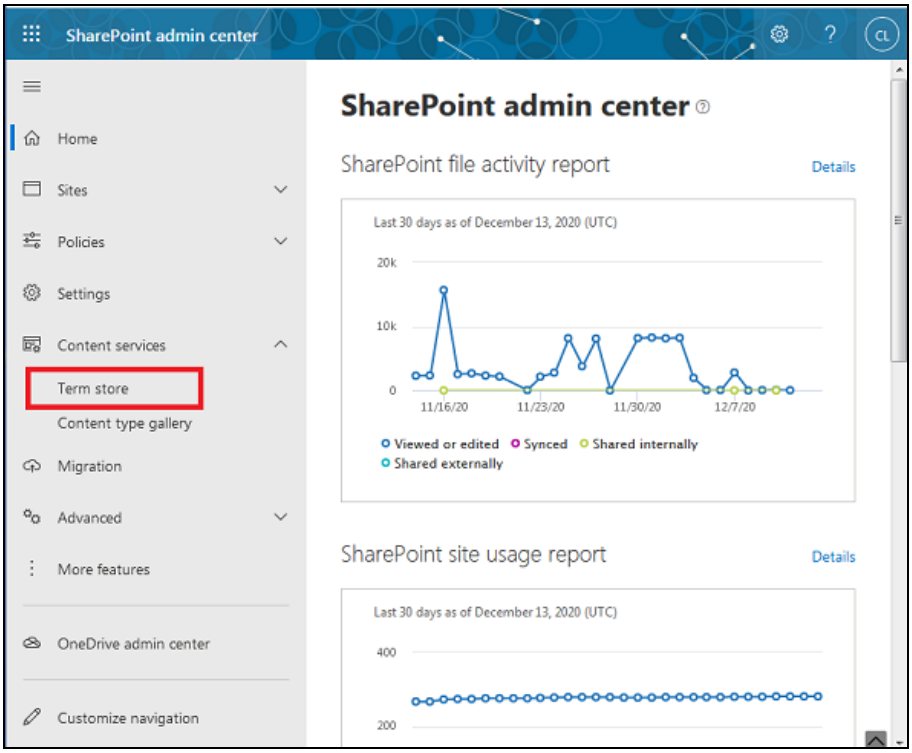
iii. In the Manage roles window, select **Admin center access** then check the box beside **Global admin**. Click **Save Changes** to save the role you assigned.



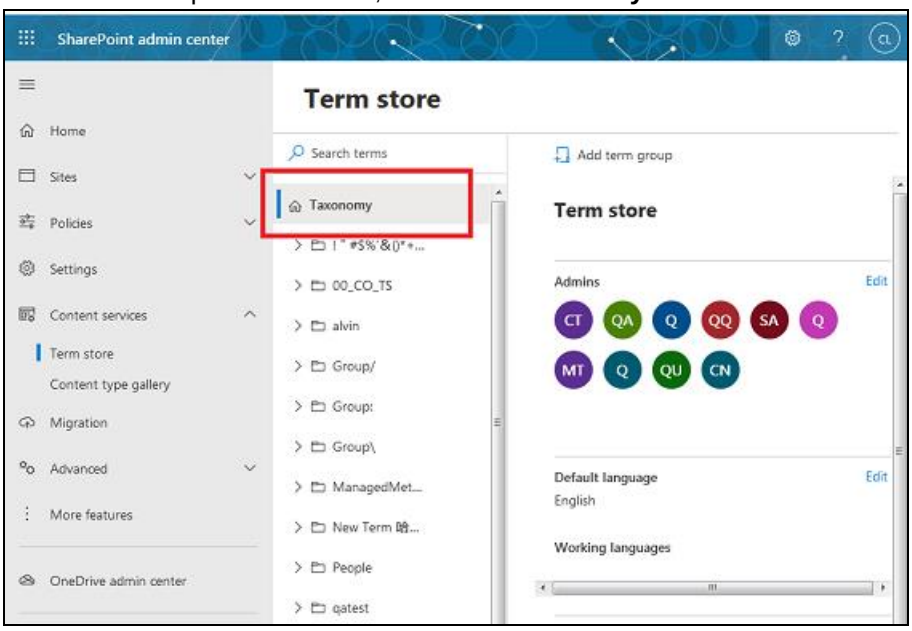
2.14.2 Granting Term Store Administrator Role

To add Term Store Administrator role to the Office 365 user account used to authenticate the Office 365 backup set.

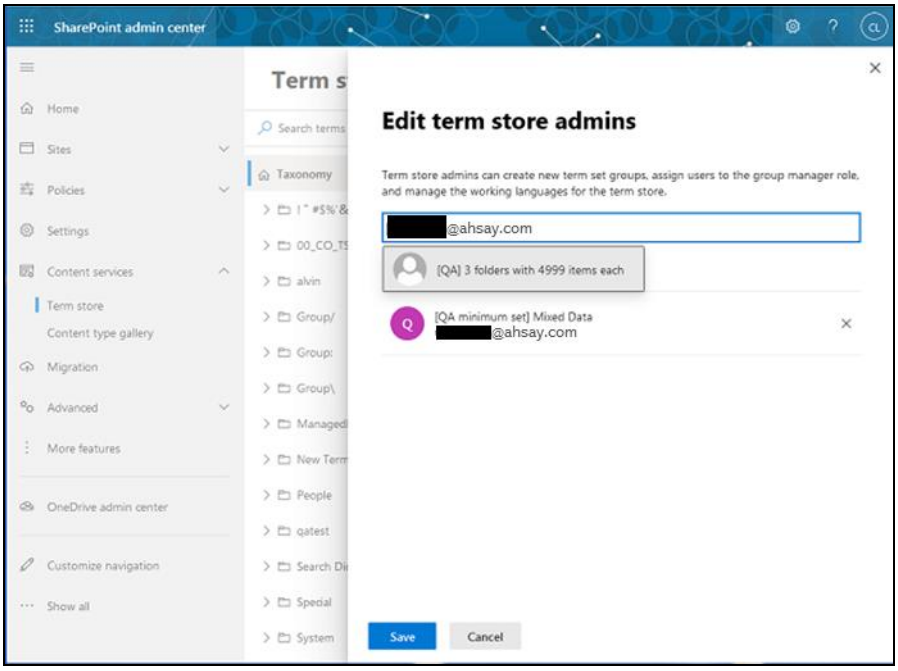
i. In the SharePoint admin center, under **Content services**, click **Term store**.



ii. In the tree view pane on the left, select the **Taxonomy**.



iii. In the Term store page, for Admins, select Edit. The **Edit term store admins** panel appears.



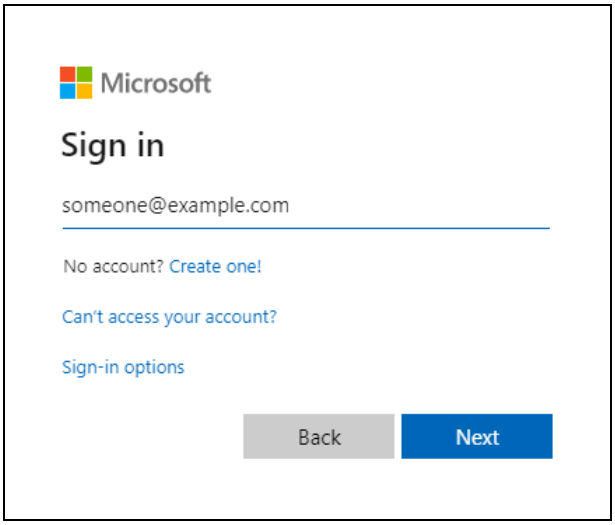
iv. Enter the names or email addresses of the Office 365 user who you want to add as term store admins. Select **Save**.

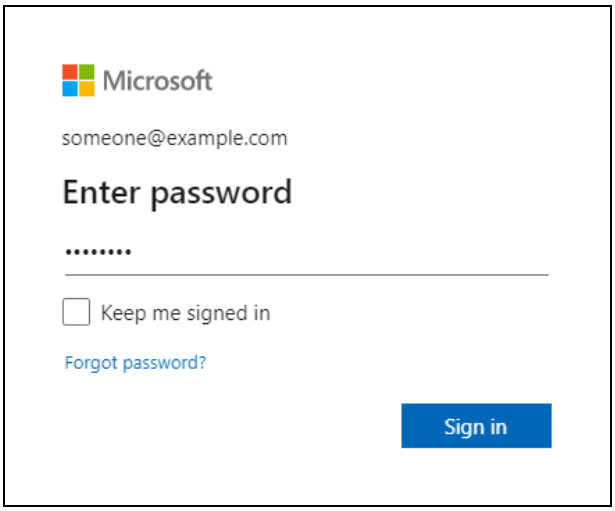
2.14.3 Granting Permission Discovery Management Group

This permission allows users added under the **Members** section of the **Discovery Management** group (refer to Ch. 2.14.4 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.

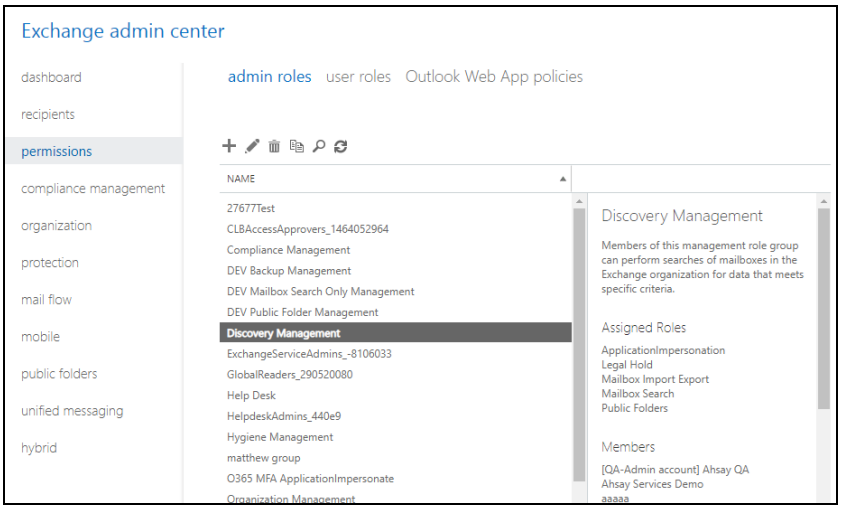
i. Open https://outlook.office365.com/ecp

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



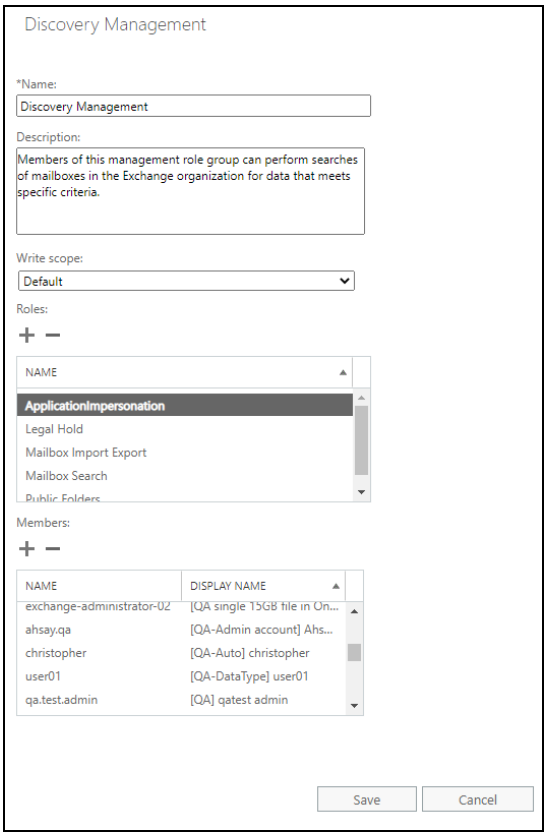


iii. Select the **permissions** menu on the left, then double click on **Discovery Management** on the right.



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

- ApplicationImpersonation
- Legal Hold
- Mailbox Import Export
- Mailbox Search
- Public Folders

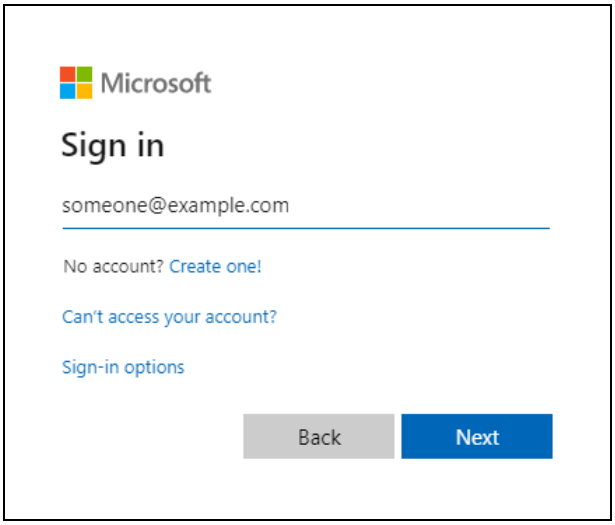


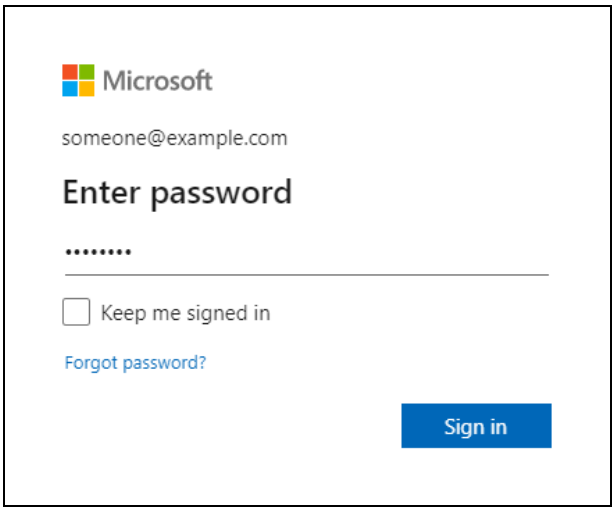
v. Click **Save** to confirm and exit the setting.

2.14.4 Granting Permission to Accounts for Creating Backup Set

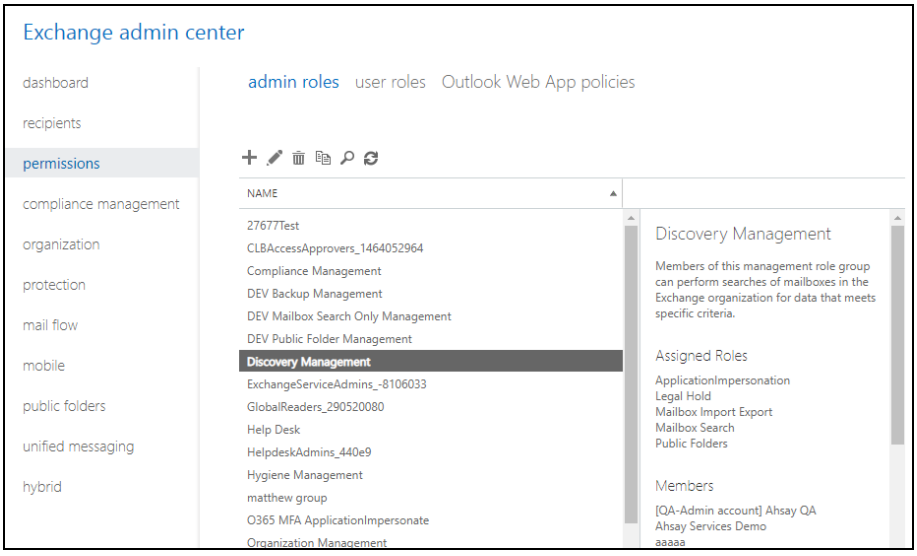
i. Open https://outlook.office365.com/ecp

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

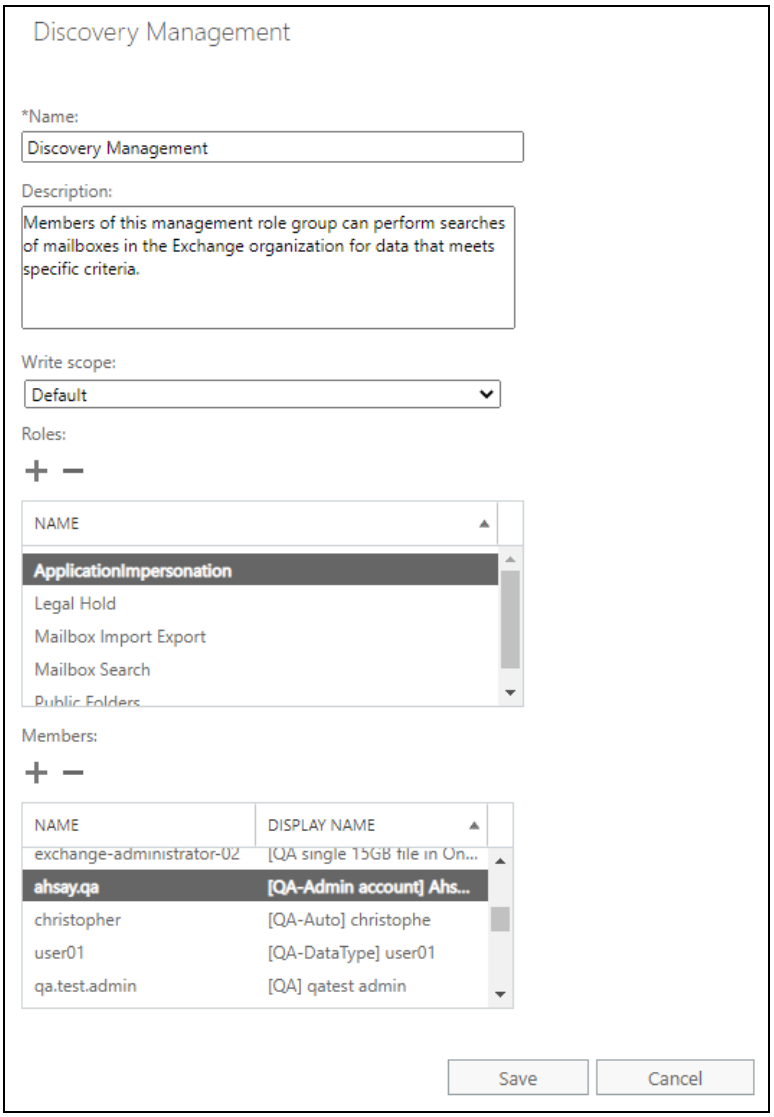




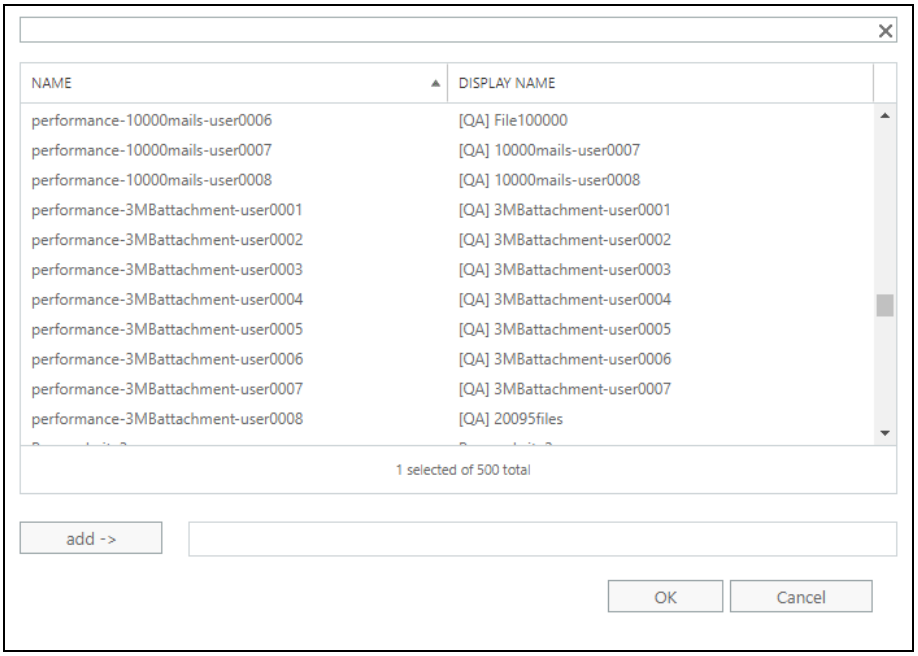
iii. Select the **permissions** menu on the left, then double click on **Discovery Management** on the right.



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.



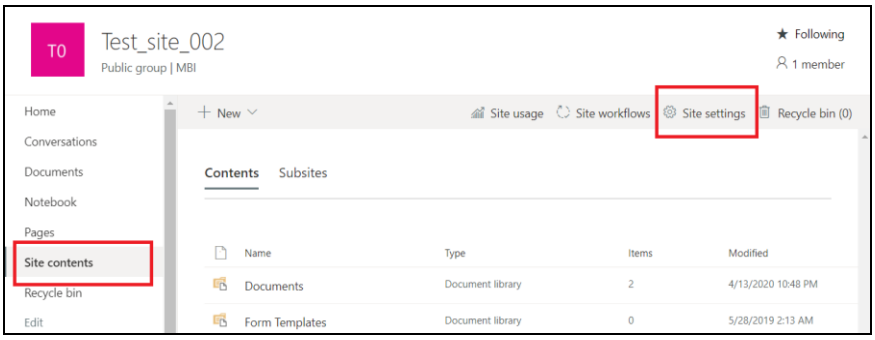
vi. Click **Save** to confirm and exit the setting.

2.14.5 Granting Permission to restore all share link types to alternate location in Office 365

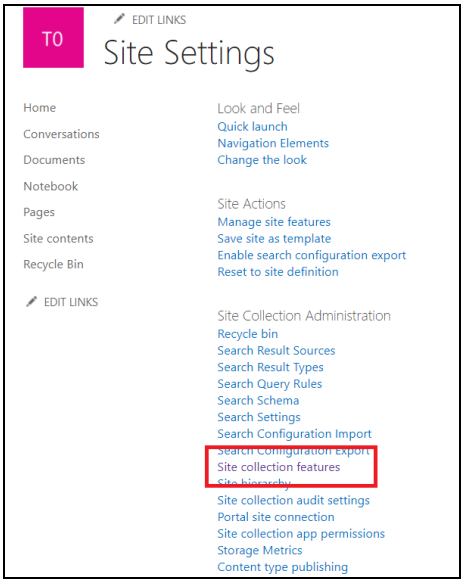
To successfully restore all share link types to alternate location of the same organization in Office 365, follow the settings below:

- Allowing anonymous users to access application pages

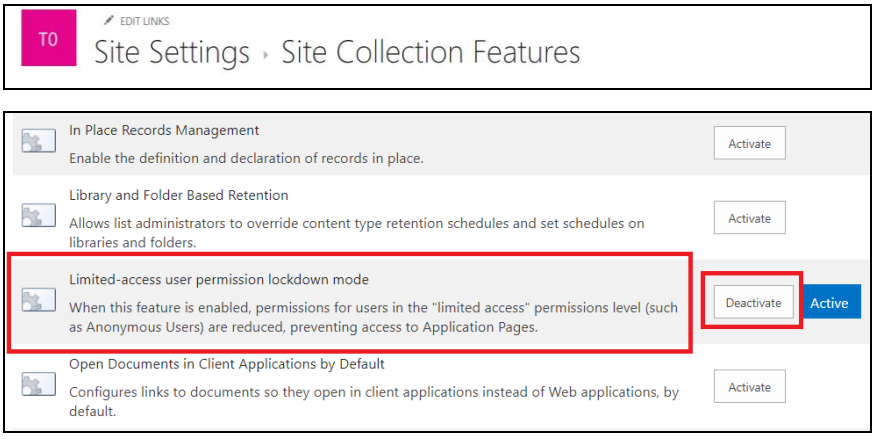
i. Go to the alternate Site > in the left pane, select **Site Contents** > **Site Settings**



ii. Go to **Site Collection features**

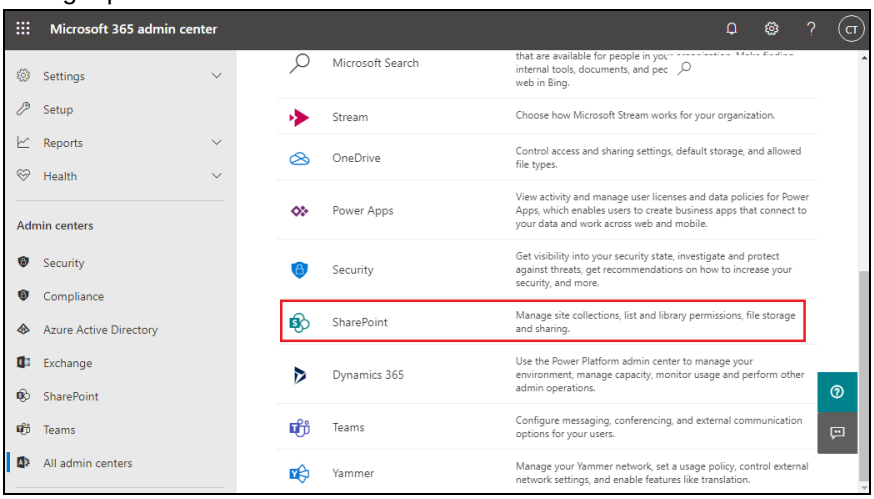


iii. Deactivate "**Limited-Access user permission lockdown mode**" feature

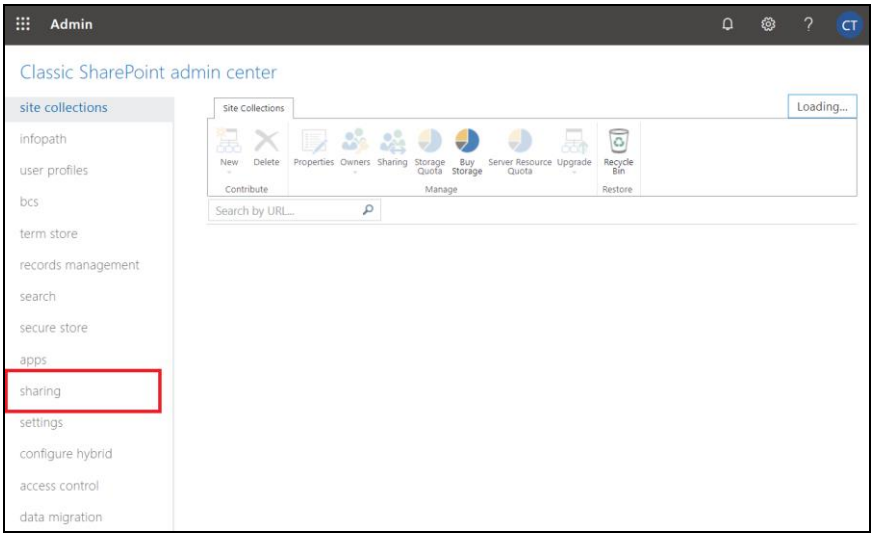


- Allowing sharing to external users

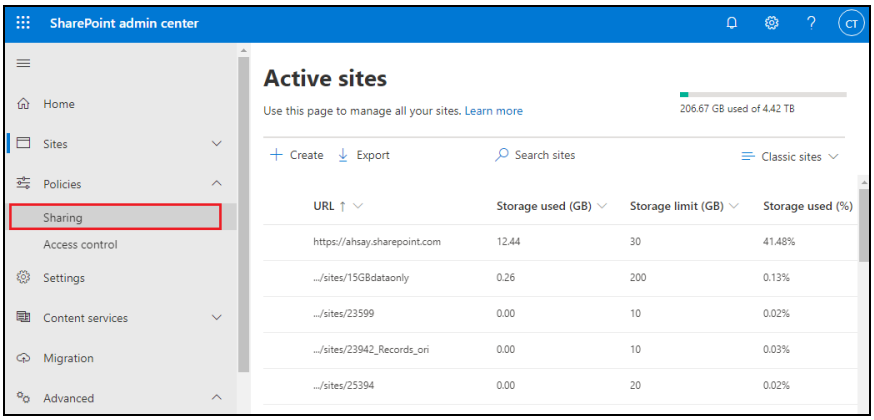
i. Go to your **Microsoft 365 Admin Center** > **All admin centers** > in the right pane select **SharePoint**



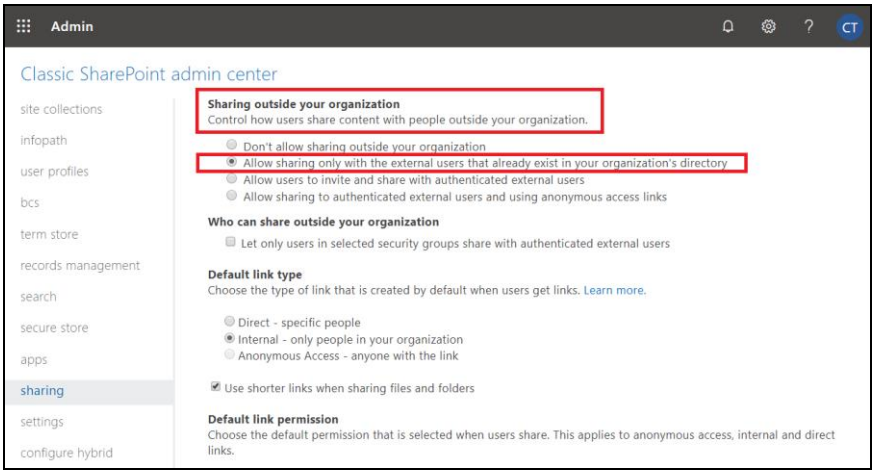
ii. Go to **Sharing**



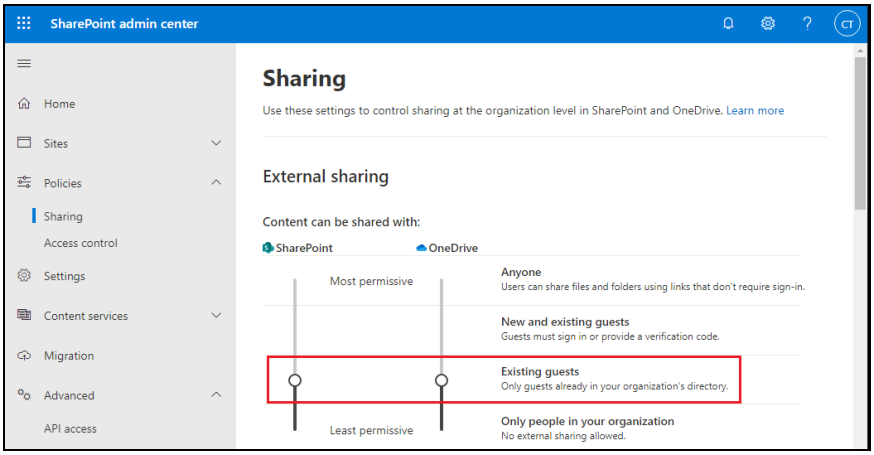
If using **Classic sites view**, go to **Policies > Sharing**.



iii. Under Sharing outside your organization, select "**Allow sharing only with the external users that already exist in your organization's directory**" and click OK.



If using **Classic sites view**, under External sharing the button must be in line with "**Existing guests**" and click **Save**.



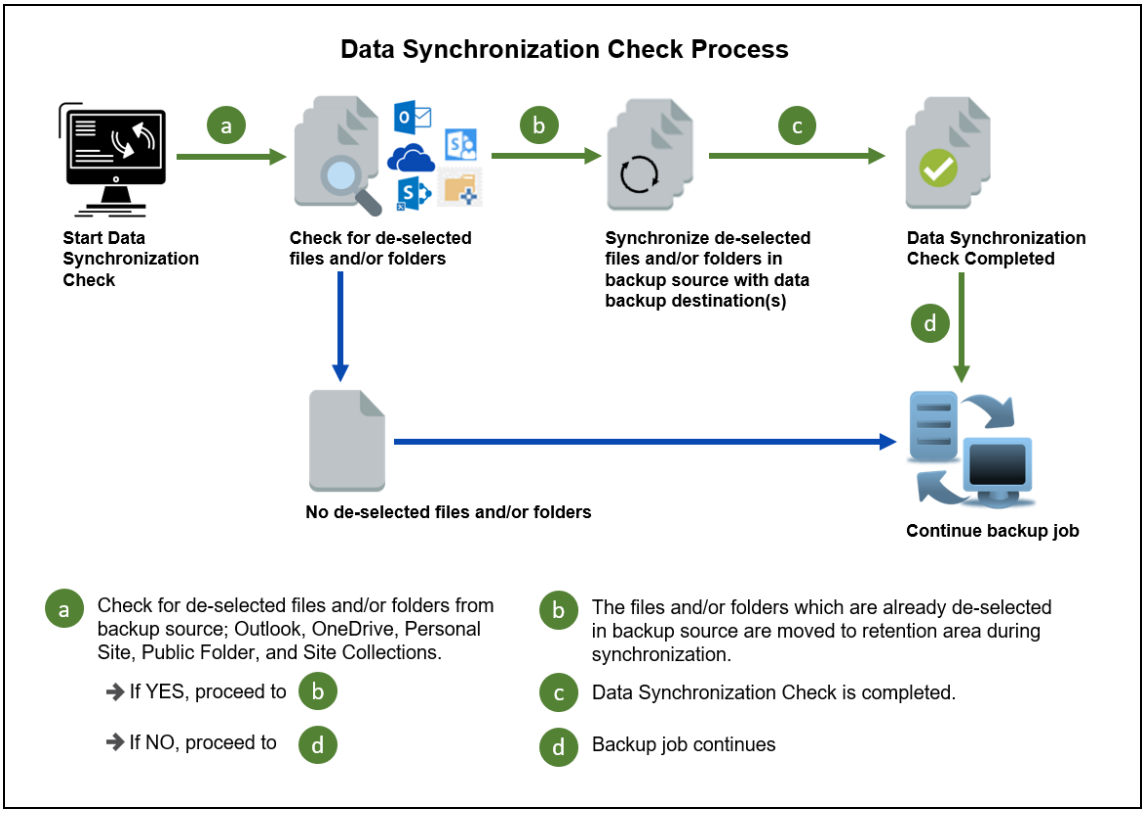
2.15 Data Synchronization Check (DSC) Setup

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 or Site Collections. Un-selected individual Office 365 user accounts or Site Collections 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 be 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 G Setting the Data Synchronization Check (DSC)

2.16 Authentication

To comply with Microsoft's product roadmap for Office 365, from AhsayOBM 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 AhsayOBM 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 J: Migrating Authentication of Office 365 Backup Set. After the upgrade to AhsayOBM 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.

In order to migrate existing backup sets to Hybrid Authentication or Modern Authentication there are two (2) methods:

- The first method is the Office 365 account used for the backup set is assigned the Global Admin role.
- The second method is the Office 365 account used for the backup set is an ordinary account. When changing the settings of the backup set, the user can ask an Office 365 Global Admin account to login their credentials first to authorize the migration of authentication. This is only required in migrating from Basic Authentication to Modern Authentication. **This only needs to be done once per backup set**.

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.

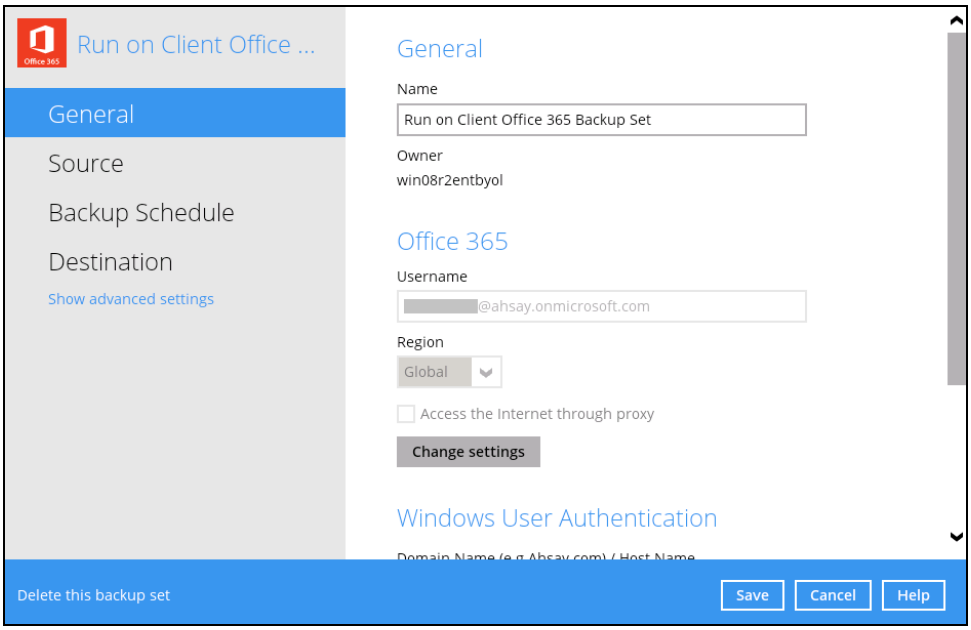
To check the current authentication being used in your Office 365 backup set, see criteria below:

- Basic Authentication

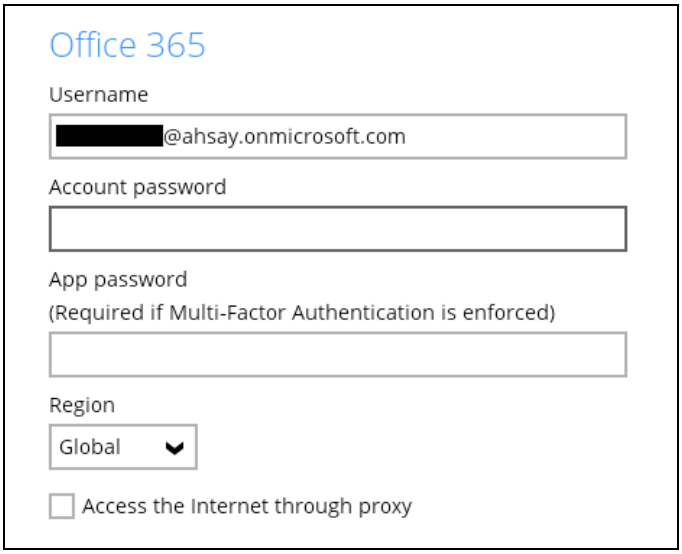
  If you click on the backup set and the following pop up message is displayed, then the backup set is using Basic Authentication.

- Modern Authentication

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



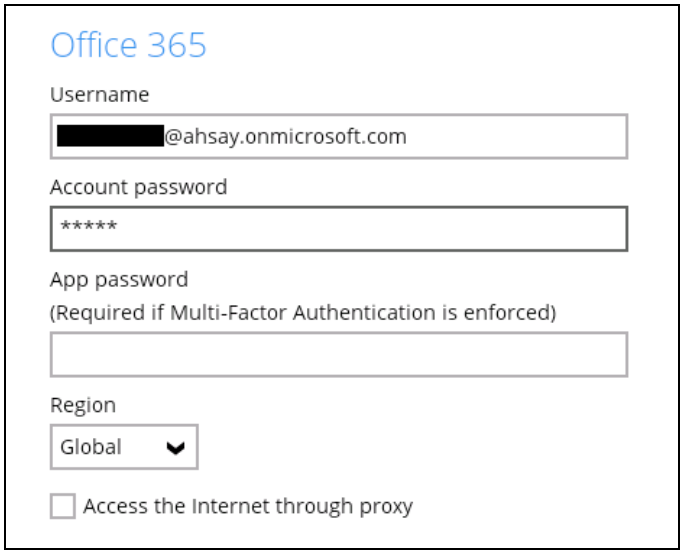
  In the Office 365 credentials page, the region is Global and the Username exists but has no password, then the backup set is using Modern Authentication.



- Hybrid Authentication

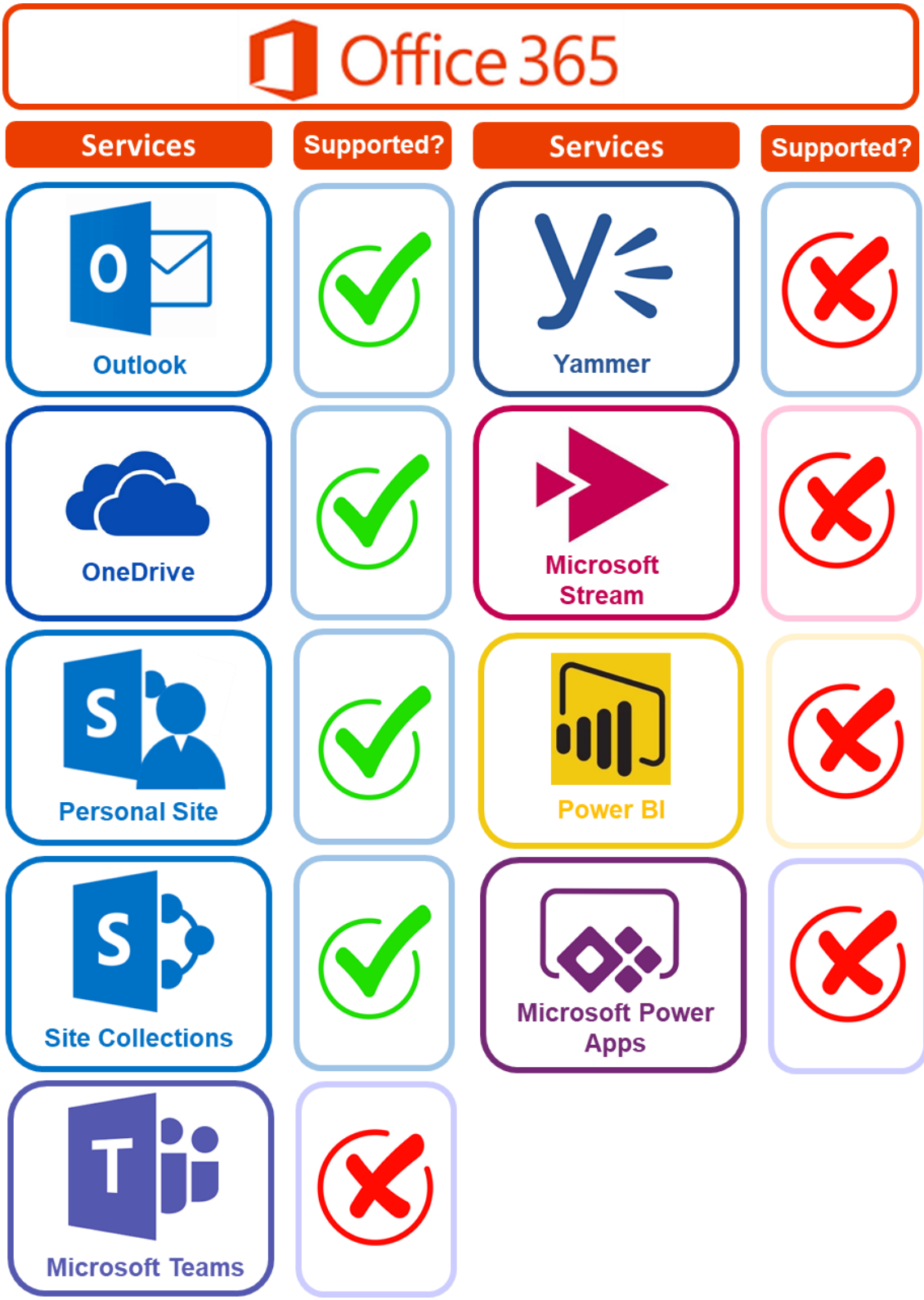
  1. There is no pop up authentication alert.

  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 .

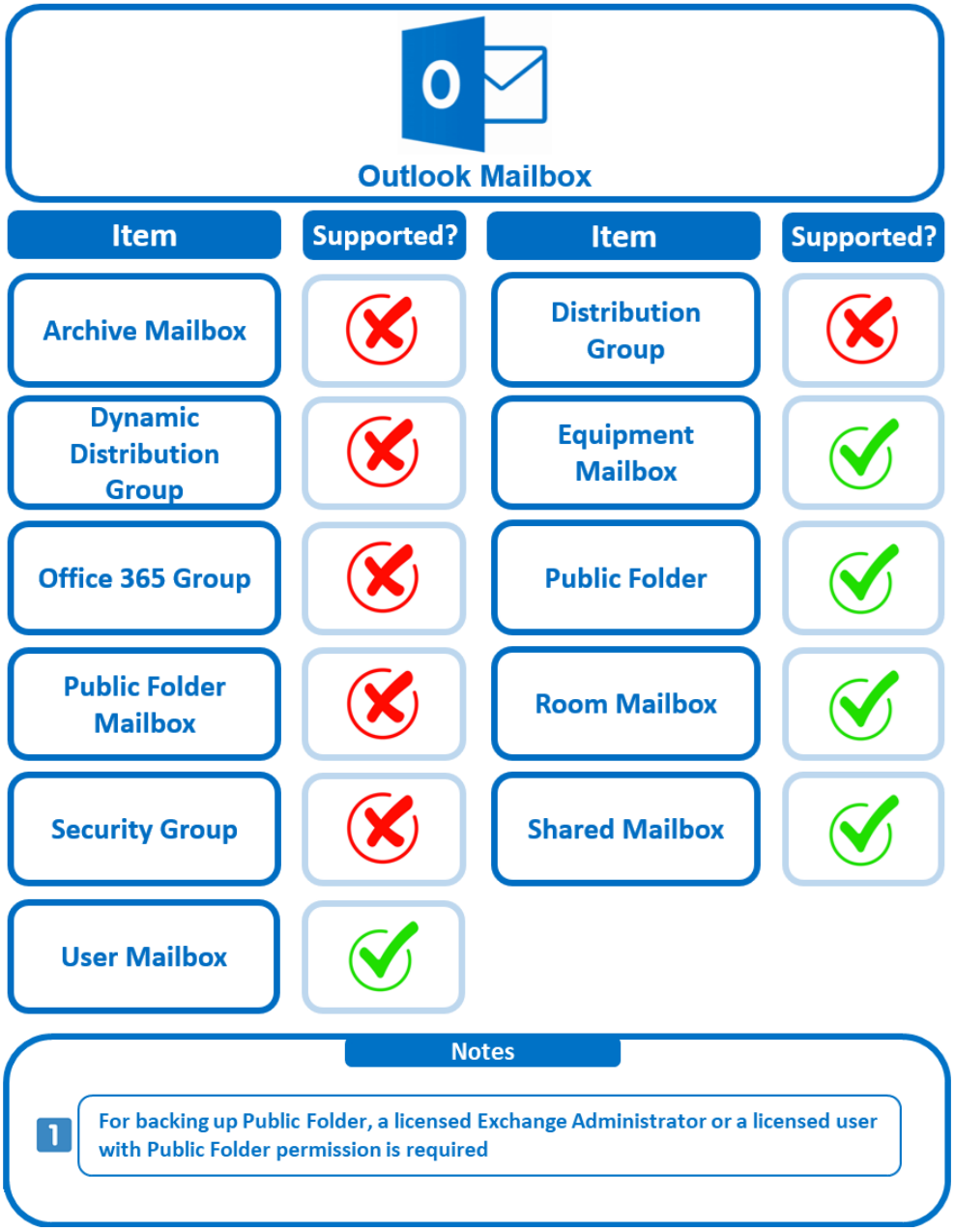


2.17 Supported Services

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.



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



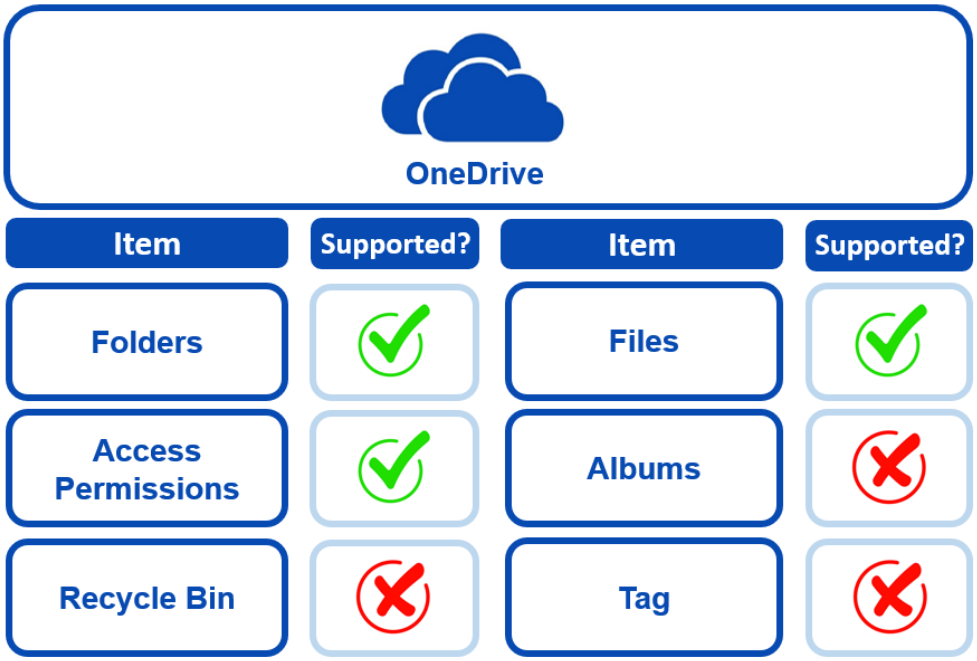
Below are the items that you can back up or restore from an Outlook mailbox.

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	✗	RSS Feeds	✓
Search Folders	✗	Sent Items	✓
Social Activity Notifications	✗	Sync Issues	✗
Tasks	✓	Trash	✓

Note

AhsayOBM supports the folders types which are shown in the Outlook Web Access (OWA), except the Conversation History because it is not related to mail objects.

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



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

Below are the SharePoint Site Collections template that you can back up or restore from an Office 365 backup set.

Below is the Site Column Type that you can back up or restore from an Office 365 backup set.

Item	Supported?	Item	Supported?
CalendarFolderType	✓	CalendarItemType	✓
ContactItemType	✓	ContactsFolderType	✓
DistributionListType	✓	FolderType	✓
MeetingCancellationMessageType	✓	MeetingMessageType	✓
MeetingRequestMessageType	✓	MeetingResponseMessageType	✓
MessageType	✓	PostItemType	✓
SearchFolderType	✓	TasksFolderType	✓
TaskType	✓	UserConfigurationType	✓

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	✓

2.18 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
Site Collections	8 GB

2.19 Limitations

2.19.1 Ahsay Limitations

- **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.
  - Backup and restore of the site features setting for SharePoint Site Collection and/or Personal Site using Modern Authentication is not supported.
  - 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 SharePoint Site and Personal Site.

SharePoint

- Document Libraries, List Items and their default Column Types will be supported, excluding customized Apps and SharePoint App Store applications.
- Most of site lists will be supported, except for certain list types that will be skipped to restore due to API limitation, for example is Microfeed in Classic Team Site.
- Site logos will NOT be restored, it is suggested revisiting the site setting page and manually add the missing images if necessary.
- User-defined workflow templates will NOT be supported for backup and restore.
- Recycle Bin will NOT be supported for backup and restore.
- Most of Site level settings will NOT be restored, except for those essential to support the successful restore of the backup items e.g. Manage Site Feature / Site Collection Feature.
- Most of List level settings (including List view) will NOT be restored, except for those essential to support the successful restore of backup items, e.g. item checkout settings. Following restore, it is suggested revisiting the relevant settings if necessary. This may affect list column ordering and visibility after restoring.
- Restoring External Data column is NOT supported if external content type has been deleted via SharePoint Designer.
- Restoring of multiple Value of managed metadata column when the key name (column name) contains space is NOT supported.
- Restoring of list with local managed metadata column to alternate location is NOT supported.
- The restore of SharePoint documents or folders with the following characters: **/ \ | * : " < >** in item name to a Windows local computer is not supported. As Windows does not support these characters for either a file or folder name.
- Restoring Newsfeed items in **Modern Team Site** will not publish the items to Homepage automatically, user will need to navigate to **Site Content > Page Library**> click on each individual news item and "Post" the news one by one manually.
    - Backup User (except for Global Admin) may not have permission to back up the site collection even if he/she can view it in the backup source tree. FOR EACH site collection, the user can backup it only if he/she is assigned as a site admin of that site collection.
        - If the user is assigned as site admin of the root level site collection only, he/she is not automatically added as site admin of other site collection under that root level site collection (i.e. If user is to backup specific site collection under the root, he/she has to be added as site admin of that specific site collection under the root also).

- For site collection that can be viewed by user in the source tree which he/she is not yet assigned as a site administrator:
    - when user expand the node of that site collection, access denied error pop up will be given.
    - when user tick such site collection to backup, access denied error will be given in the backup log.

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

- **Online Archive Mailbox** will NOT be supported for backup and restore.
- 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 use 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

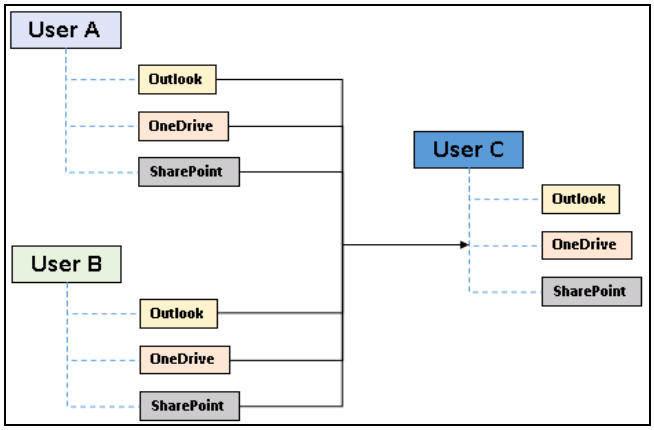
Restore to Alternate location

- Only administrator account or user account with administrative authority can restore backup items to an alternate location.
- If you are trying to restore item(s) from one user to an alternate location user, AhsayOBM will restore the item(s) to their respective destination folder(s) with the same name as the original folder(s).

  Example: Item from Outlook of User-A will be restored to the Outlook of the alternate location User-B; Item from SharePoint of User-A will be restored to the SharePoint of the alternate location User-B.
- Restore of item(s) in public folder to an alternate location public folder is not supported.

  Example: Restore of item(s) in public folder from User-A to alternate location User-B is not supported.
- When restoring to alternate location, data type "Person or Group" will not be restored. Following restore, it is suggested revisiting the relevant settings if necessary. This also affects "Assigned To" column values of some list templates (e.g. Tasks list), and "Target Audience" column values of some list templates (e.g. Content and Structure Reports).

- If you are trying to restore item(s) from several users to an alternate location user, AhsayOBM will restore the item(s) to their respective destination folder(s) in alternate location user with the same name as the original folder(s).



Example: Item from Outlook of User-A and User-B will be restored to the Outlook of the alternate location User-C.

Restore to Alternate Office 365 account

If you are trying to restore item(s) from multiple Office 365 user account to an alternate Office 365 user account, AhsayOBM can only restore one Office 365 user account at a time.

Restore to Alternate Organization

- Restoring of document library (including OneDrive) items '**Share Link** to alternate organization will trigger a warning message.
- Skip to restore **People and groups** and **Site permissions** to alternate origination.

Restore data to a destination user which has a different language

If you are trying to restore the item to a destination user which has a different language setting than the original user, AhsayOBM will restore item(s) to their respective destination folder based on the translation listed below.

For folders such as 'Calendar' or 'Notes', a new folder 'Calendar' or 'Notes' will be created.

For folders in OneDrive and SharePoint, a new folder will be created.

Restore existing documents in checked-out status

Restoring of existing documents in **checked out** status is supported only when the user who has **checked out** the file is the same user who is performing the restore.

Backup source (English)	Action	Destination User with Chinese as default language settings
Inbox	Merge	收件箱
Outbox	Merge	寄件匣
Sent Items	Merge	寄件備份
Deleted Items	Merge	刪除的郵件
Drafts	Merge	草稿
Junk E-Mail	Merge	垃圾電郵
Calendar	Create new folder	Calendar
Notes	Create new folder	Notes
OneDrive Folder	Create new folder	OneDrive Folder
SharePoint Folder	Create new folder	SharePoint Folder

2.19.2 Microsoft Limitations

- **Exchange Online**

  For more detailed information on the limitations of Exchange Online, please refer to this Microsoft article, Exchange Online Limits. These are some of the limitations that will be discussed in the Exchange Online Limits article:

  - Address book
  - Mailbox storage
  - Capacity alerts
  - Mailbox folder
  - Message
  - Receiving and sending
  - Retention
  - Distribution group
  - Journal, Transport, and Inbox rule
  - Moderation
  - Exchange ActiveSync

- **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 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

SharePoint

For more detailed information on the limitations of SharePoint Online, please refer to this Microsoft article, SharePoint Online Limits. These are some of the limitations that will be discussed in the SharePoint Online article:

- Limits by plan

Feature	Office 365 Business Essentials or Business Premium	Office 365 Enterprise E1, E3, or E5, or SharePoint Online Plan 1 or 2	Office 365 Enterprise F1
Total storage per organization[1, 2]	1 TB plus 10 GB per license purchased	1 TB plus 10 GB per license purchased[3]	1 TB[3]
Max storage per site collection[4]	25 TB	25 TB	25 TB[5]
Site collections per organization	1 million[6]	1 million[6]	1 million
Number of users	Up to 300	1- 500,000[7]	1- 500,000[7]

- Service limits for all plans, such as: items in lists and libraries, file size and file path length, moving and copying across site collections, sync, versions, SharePoint groups, managed metadata, subsites, etc.

2.20 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 AhsayOBM only)**

  Temporary directory folder is used by AhsayOBM 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 is important that you do not try to make the test easier, as the objective of a successful test is not to demonstrate that everything is flawless. 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 AhsayOBM 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 AhsayOBM**

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

- **Periodic Backup Schedule**

  The periodic backup schedule should be reviewed regularly to ensure that the interval is sufficient to handle the data volume on the machine. Over time, data usage pattern may change on a production server, i.e. the number of new files created, the number of files which are updated/deleted, and new users may be added etc.

  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.

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 AhsayOBM 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 AhsayOBM 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 and/or SharePoint Sites selected. As a temporary workaround for Office 365 backup sets which require backup of Personal Sites and/or SharePoint Sites selected should be migrated to Hybrid Authentication until the issue has been resolved by Microsoft.

Large number of Office 365 users to Backup

In general, we recommend that each Office 365 backup set does not contain more than 2000 Office 365 users, to ensure a daily incremental backup job completes within 24 hours assuming that only small incremental daily changes will be made on the backup set.

However, the actual number of Office 365 users in a backup set may vary depending on the total number of Outlook, OneDrive, and SharePoint items, as well as the total size of these items. The actual number of Office 365 users in a backup set could be considerably less or could be more than 2000.

For details on the actual item count and size of Office 365 user, it is recommended to check in the Microsoft 365 Admin Centre, please refer to Appendix I: Steps on How to view Item count and Storage used in Microsoft 365 Admin Center.

Also, by splitting up all the users into separate backup sets, the more backup sets, the faster the backup process can achieve.

It is also a requirement that for every split backup sets should have its own unique user account for authentication to minimize the probability of throttling from Microsoft.

Example: If there are 10 split backup sets, then there should be 10 unique user accounts for authentication.

For more detailed example, refer to Appendix B: Example for backup of large numbers of Office 365 users.

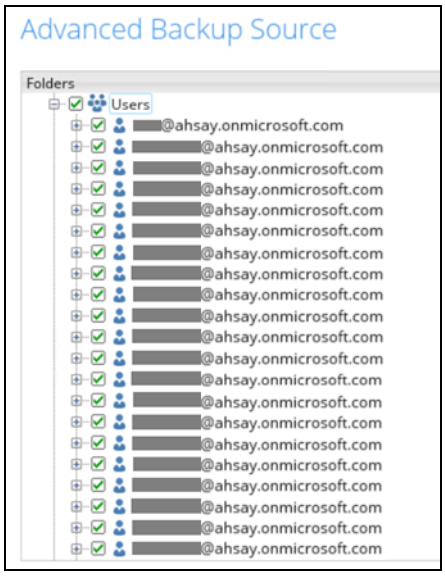
- **Concurrent Backup Thread**

  The value of 4 concurrent backup threads is found to be the optimal setting for Office 365 backups, to ensure best backup performance, minimal resource usage, and lowest probability of throttling of Ahsay backup requests by Microsoft Office 365.

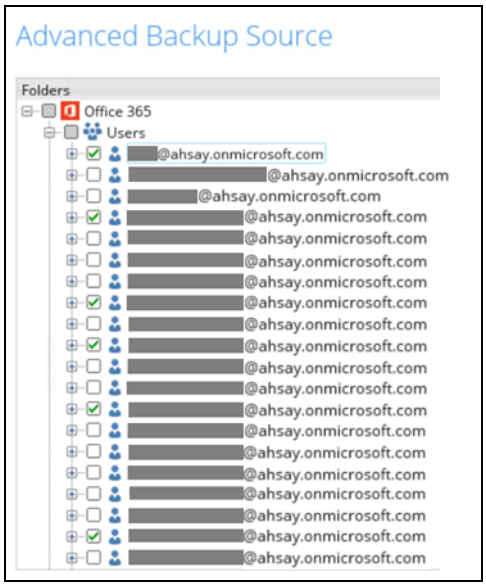
- **Backup Source**

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

  All Office 365 users

  Selective Office 365 user

  - **All Office 365 users**

    If you tick the “Users” checkbox, all of the sub Office 365 user accounts will automatically be selected.

  - **Selective Office 365 user**

    If you tick selective Office 365 user accounts, 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 Office 365 users and selective Office 365 user.

	All Office 365 users	Selective Office 365 user
Backup Set Maintenance	The Admin does not need to manage the backup set, i.e. to select or unselect use when an Office 365 user account was added or removed, the changes are automatically updated in the backup source.	The Admin will have to select or unselect users manually when an Office 365 user account was added or removed, as the changes are not automatically updated in the backup source this can be very time consuming. If an Office 365 user account is removed from the domain and

		the admin forgets to unselect the Office 365 user account from the backup source, then this will cause a warning that the user does not exist. For more details on the backup set maintenance, please see, Appendix E: Example Scenario for Backup Set Maintenance
Office 365 License	The backup user account must have additional Office 365 license modules assigned to cover any increases Office 365 users. Otherwise, if additional users are added without sufficient modules, then this will cause backup quota exceeded warning and additional users will not be backed up. For more details on the computation on the required license, please see, Appendix A: Example Scenarios for Office 365 License Requirement and Usage	This will allow the admin to easily control or manage the number of license modules used for the backup set.
Backup Time	All Office 365 user accounts will be backed up. This means the initial of full backup job will take longer, any subsequent incremental backup will take longer.	Only selective Office 365 user accounts 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 Office 365 user accounts 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.

3 Login to AhsayOBM

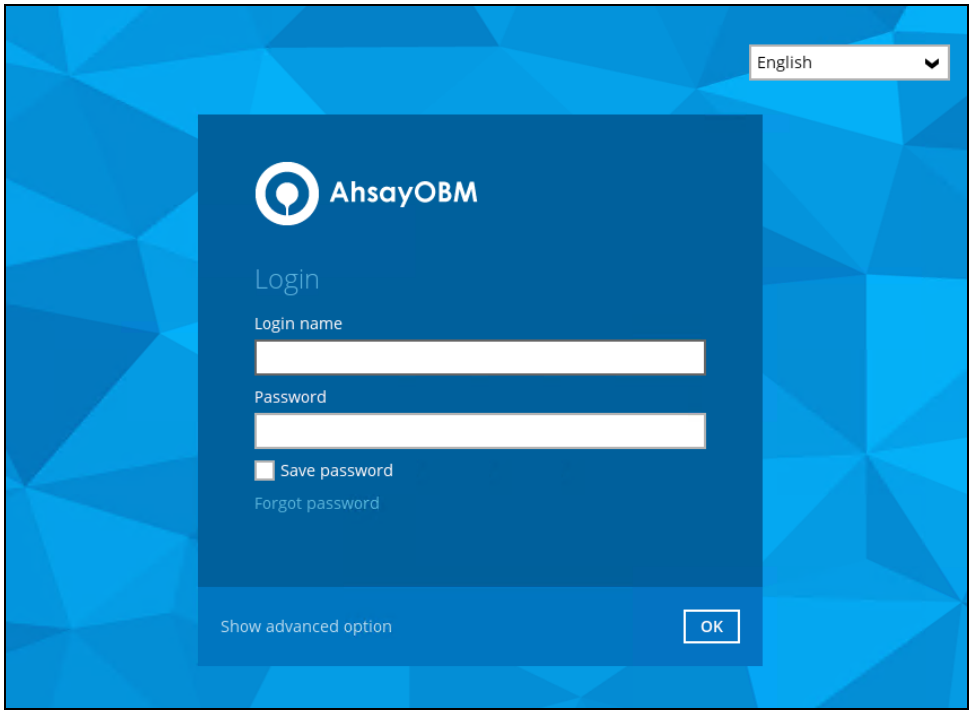
Starting with AhsayOBM v8.5.0.0 there are several login scenarios depending on the setting of the account you are using. The different scenarios will be discussed below:

- Login with no 2FA
- Login with 2FA using Twilio
- Login with 2FA using Mobile Authentication

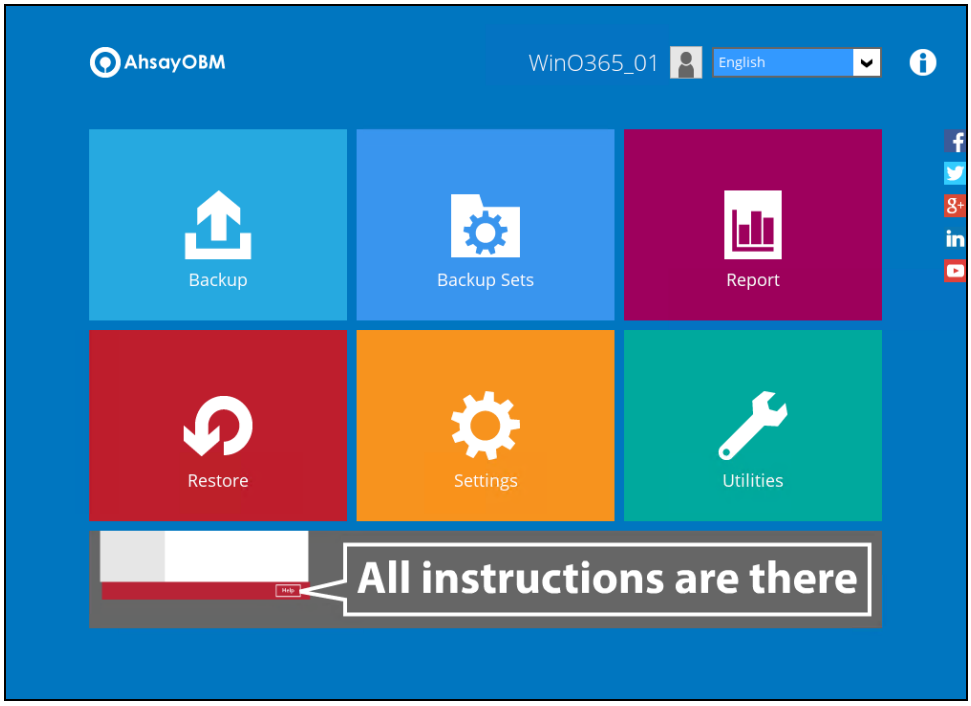
3.1 Login to AhsayOBM with no 2FA

1. Login to the AhsayOBM application user interface. Double click the AhsayOBM desktop icon to launch the application.

2. Enter the **Login name** and **Password** of your AhsayOBM account then click **OK** to login.



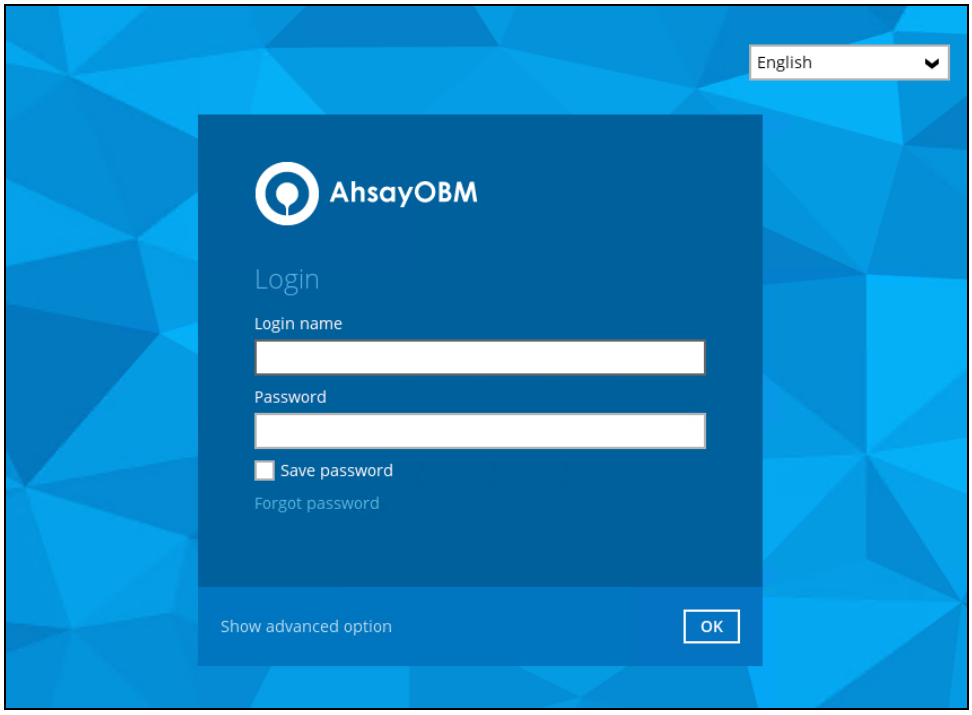
3. After successful login, the following screen will appear.



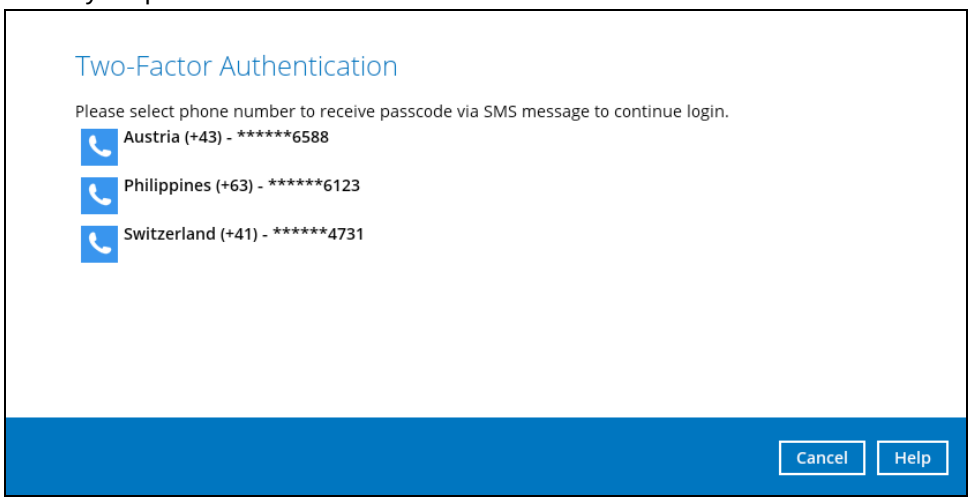
3.2 Login to AhsayOBM with 2FA using Twilio

1. Login to the AhsayOBM application user interface. Double click the AhsayOBM desktop icon to launch the application.

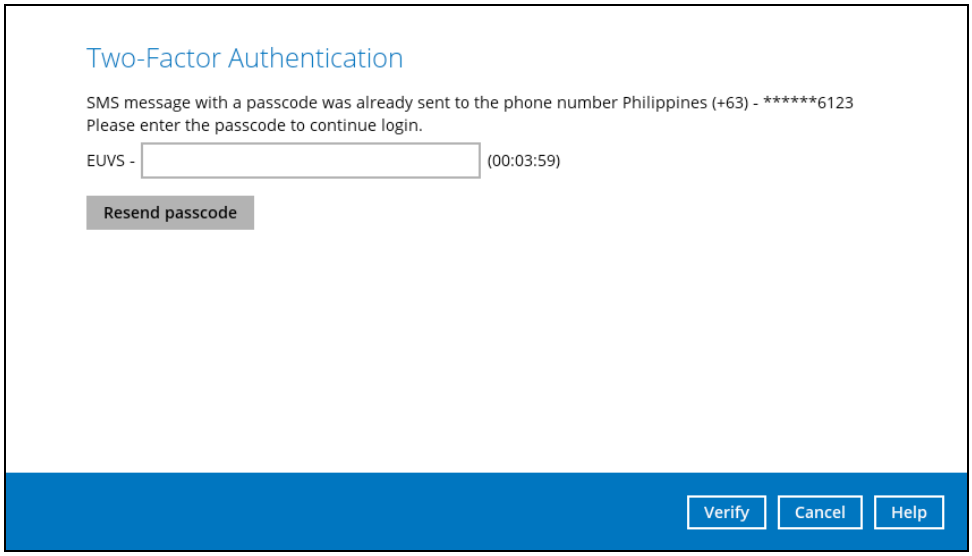
2. Enter the **Login name** and **Password** of your AhsayOBM account then click **OK** to login.



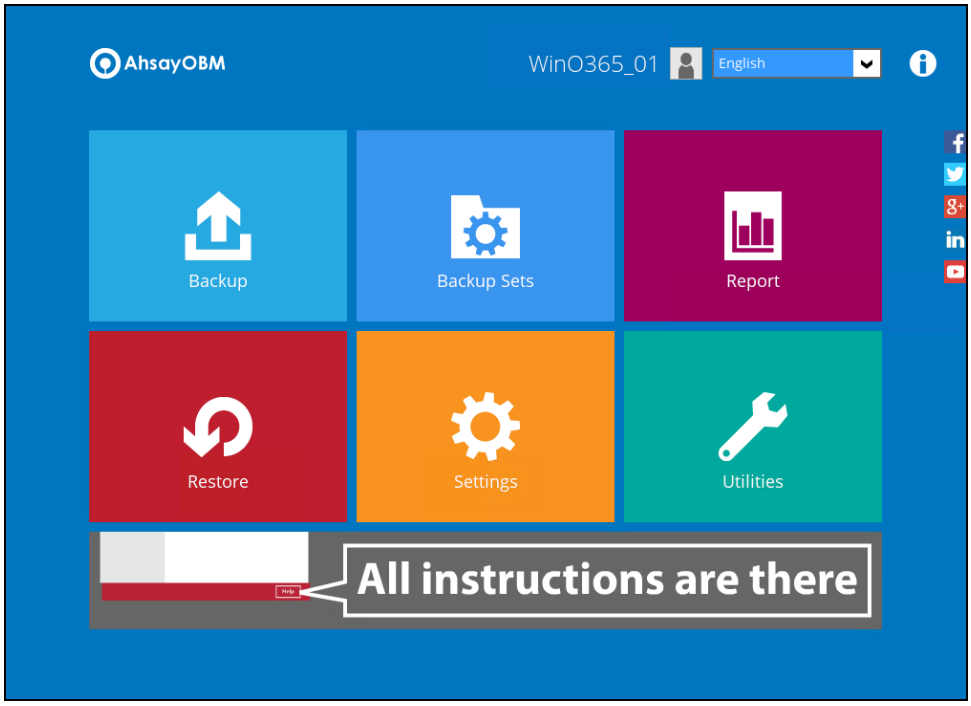
3. Select your phone number.



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



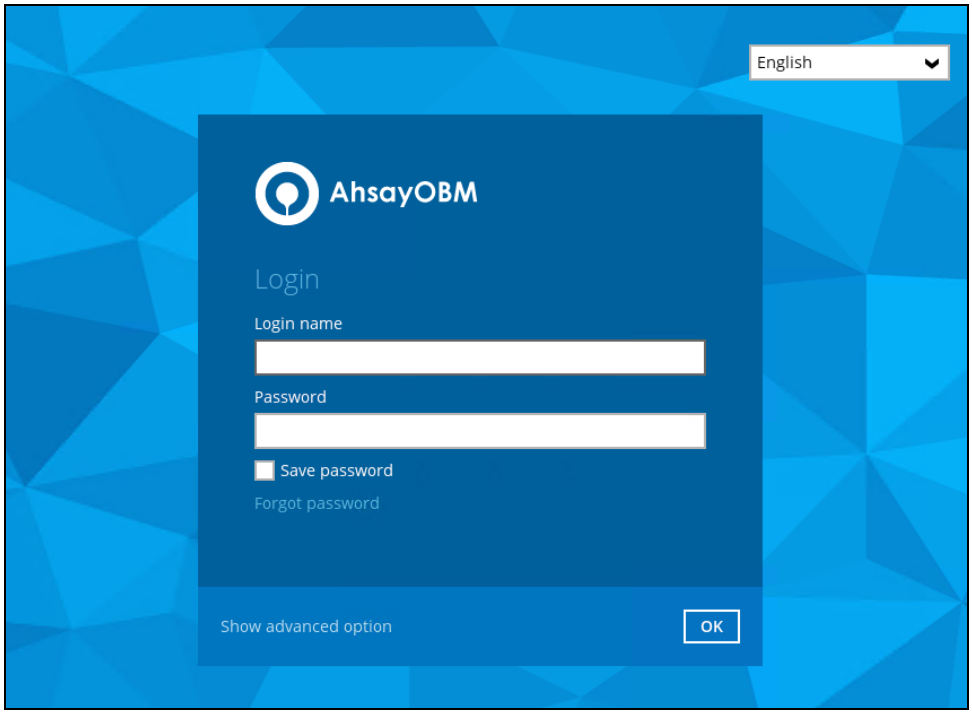
5. After successful login, the following screen will appear.



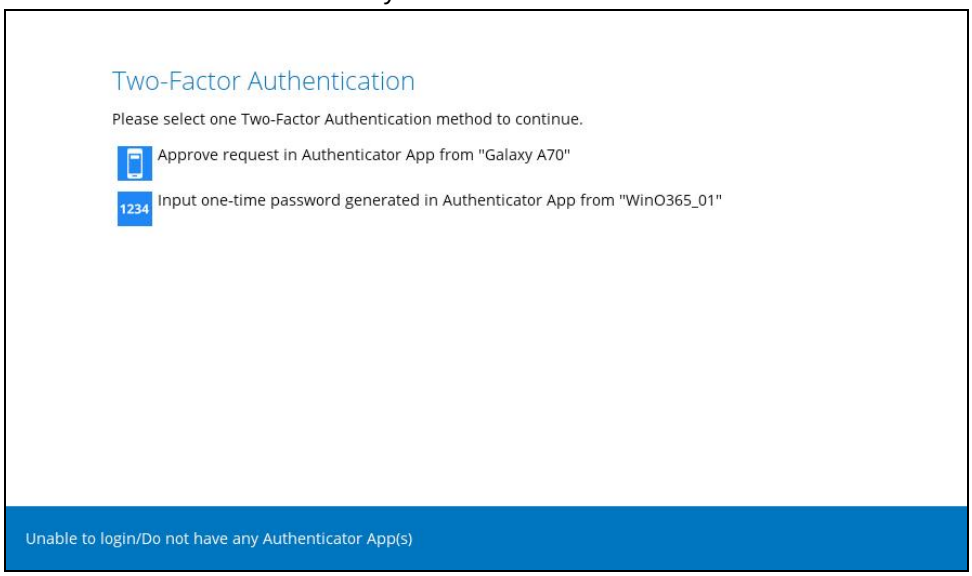
3.3 Login to AhsayOBM with 2FA using Mobile Authentication

1. Login to the AhsayOBM application user interface. Double click the AhsayOBM desktop icon to launch the application.

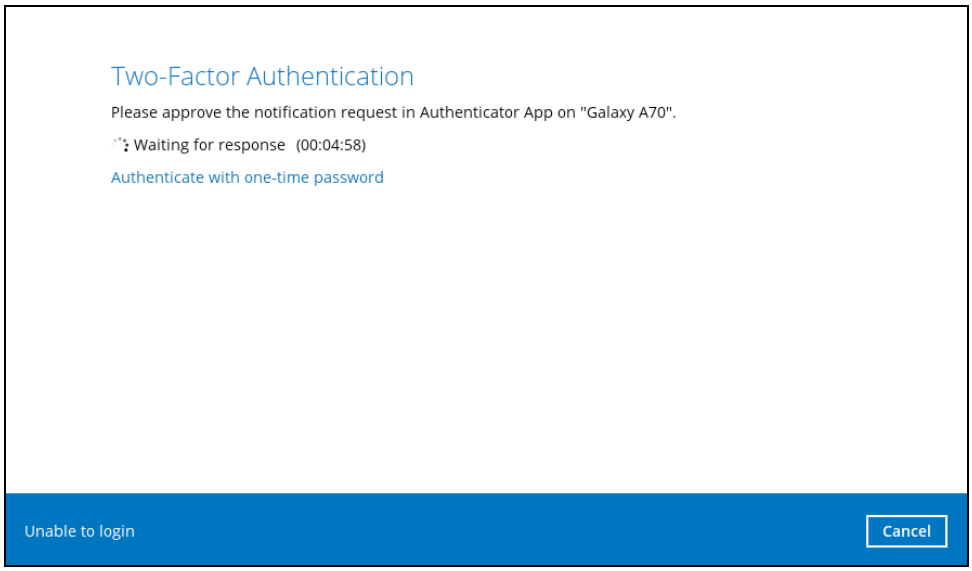
2. Enter the **Login name** and **Password** of your AhsayOBM account then click **OK** to login.



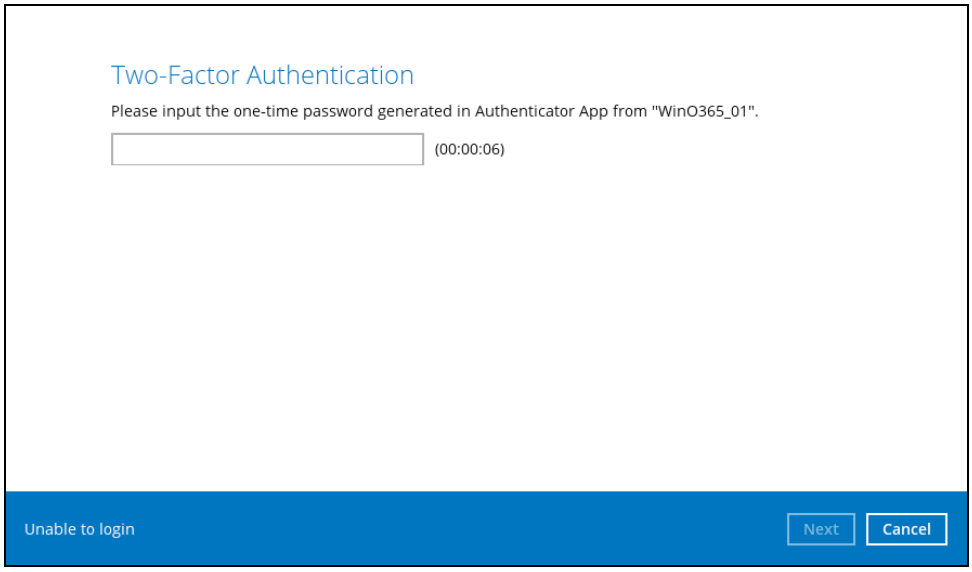
3. Click the authentication method you want to use.



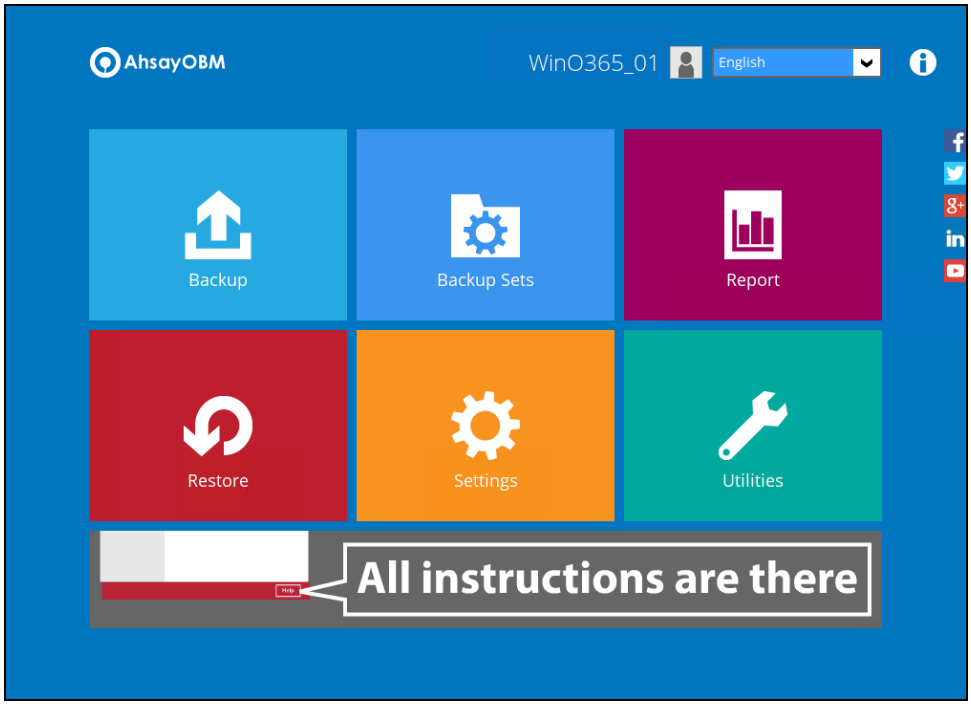
4. If “**Approve request in Authenticator App**” is selected, approve the request in Ahsay Mobile to login.



If “**Input one-time password generated in Authenticator App**” is selected, enter the generated one-time password in the authenticator app and click **Next**.



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

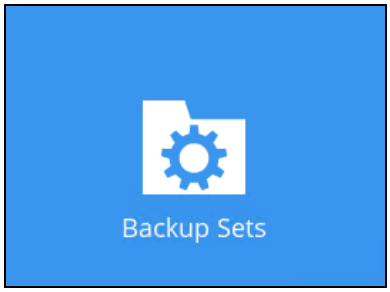


4 Creating an Office 365 Backup Set

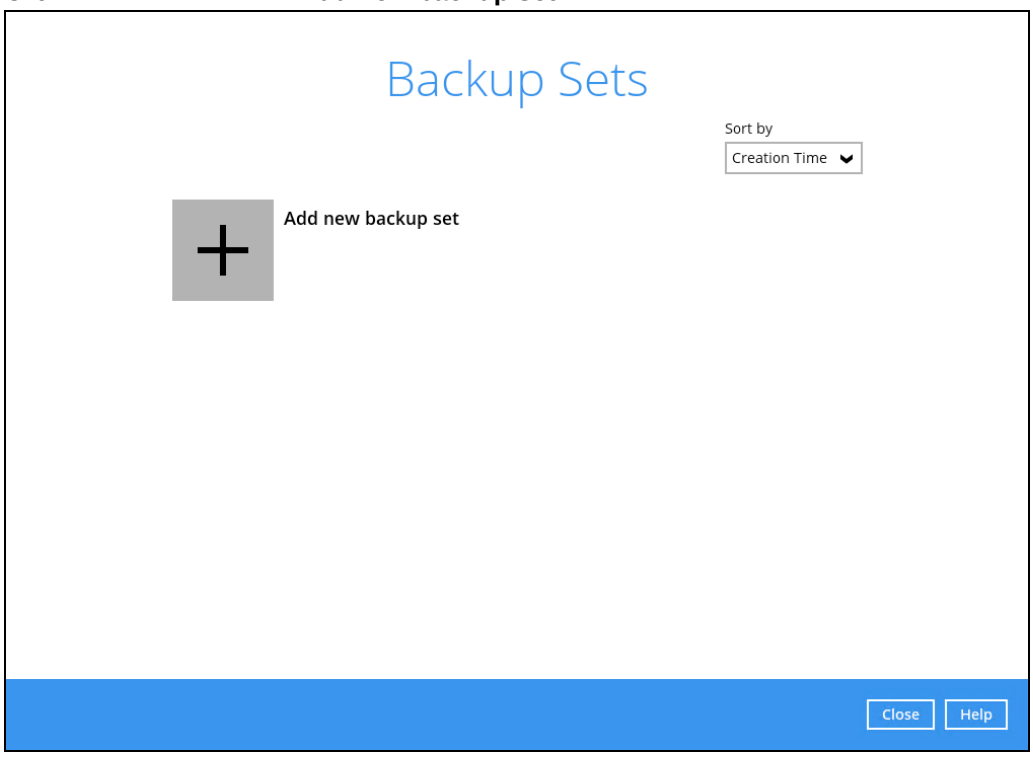
Starting with AhsayOBM v8.3.6.0, Basic Authentication will not be utilized anymore, but instead there are two types of authentication that can be used in creating a backup set namely Modern Authentication or Hybrid Authentication.

4.1 Modern Authentication

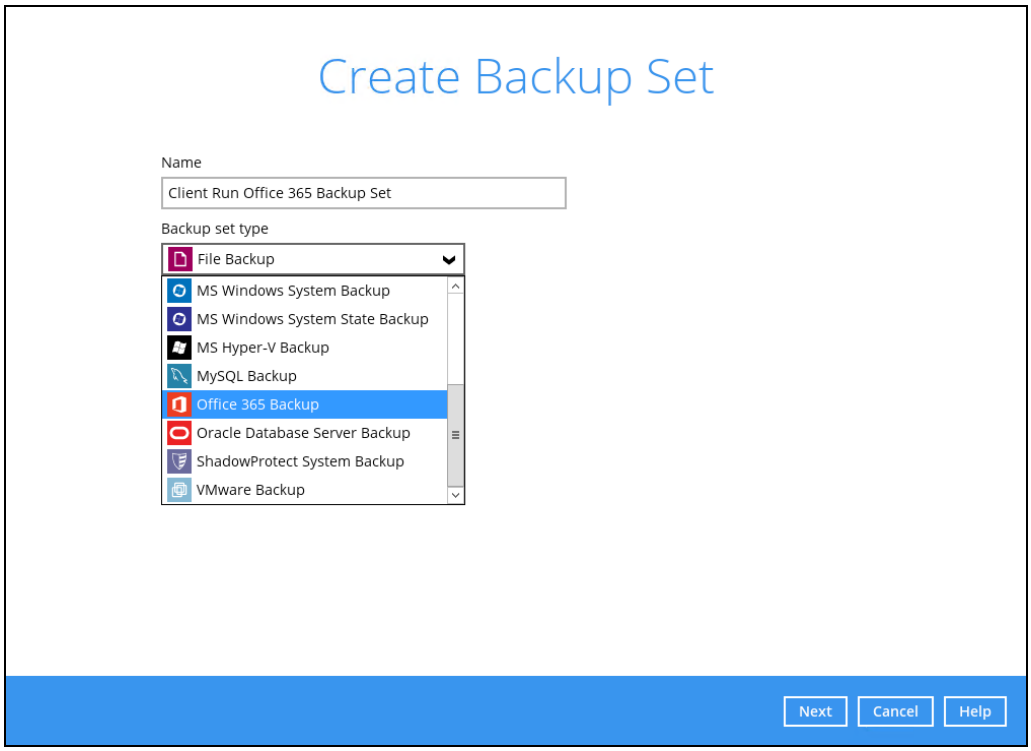
1. In the AhsayOBM main interface, click **Backup Sets**.



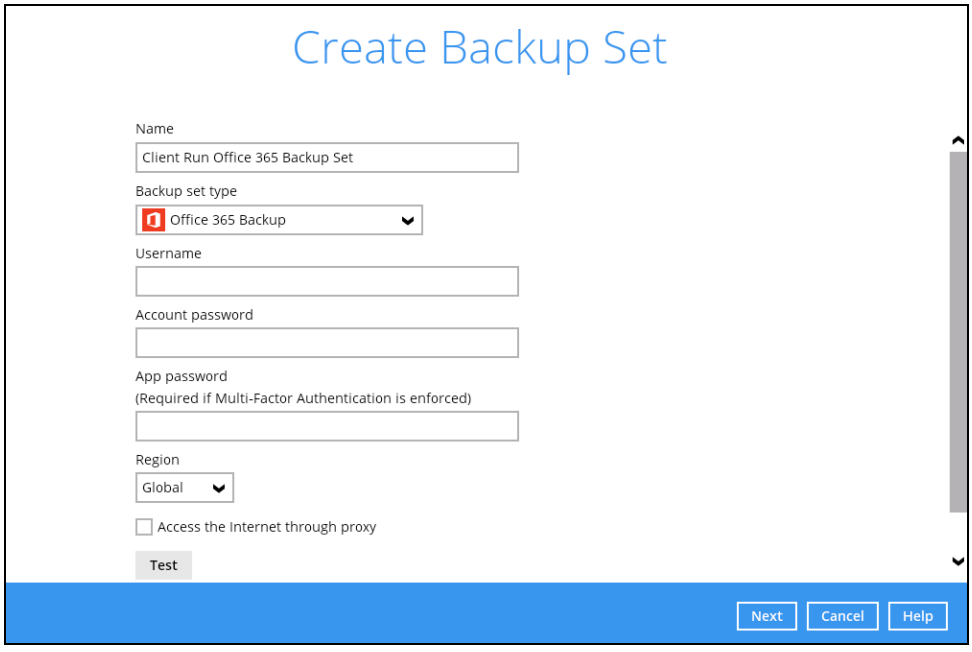
2. Click the "**+**" icon next to **Add new backup set**.



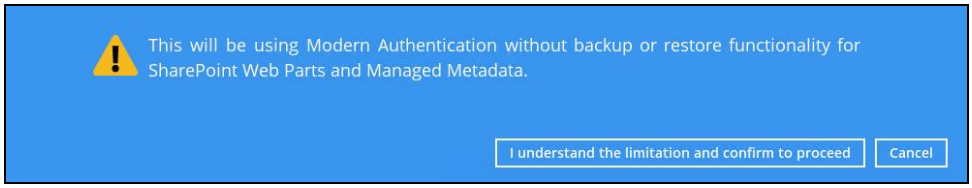
3. Enter a **Name** for your backup set and select **Office 365 Backup** as the **Backup set type**.



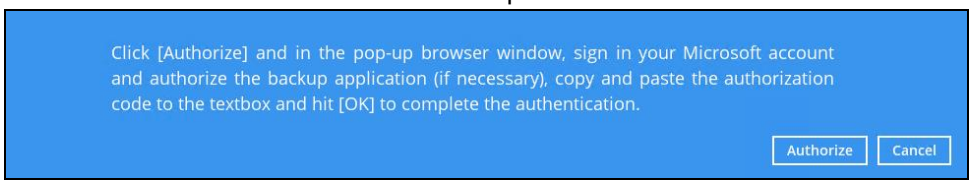
Leave the **Username** and **Account password** blank and click **Test**.



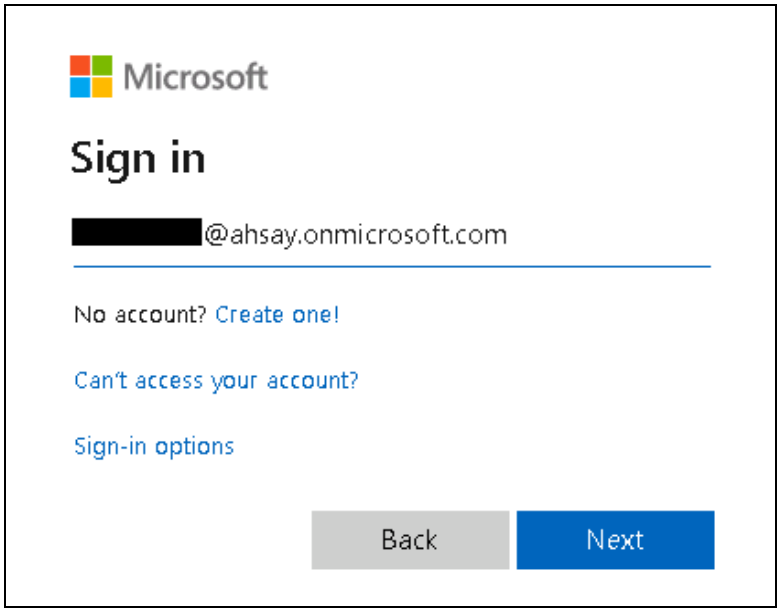
Click **I understand the limitation and confirm to proceed**.

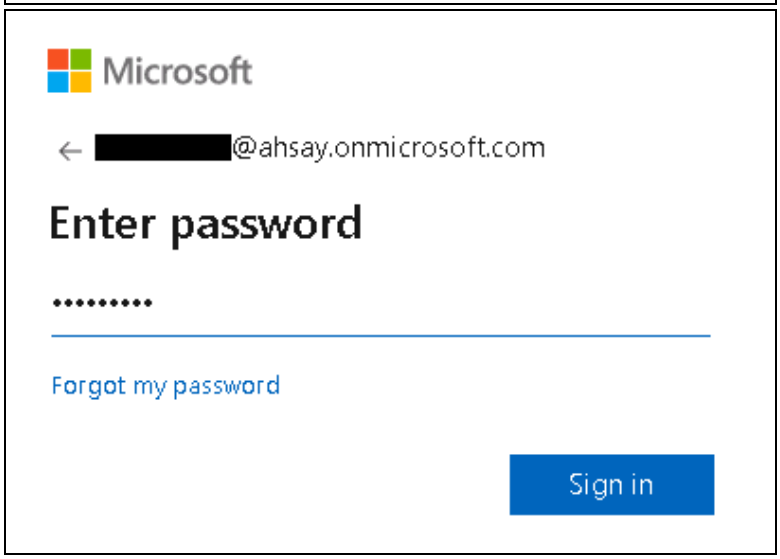


Click **Authorize** to start the authentication process.

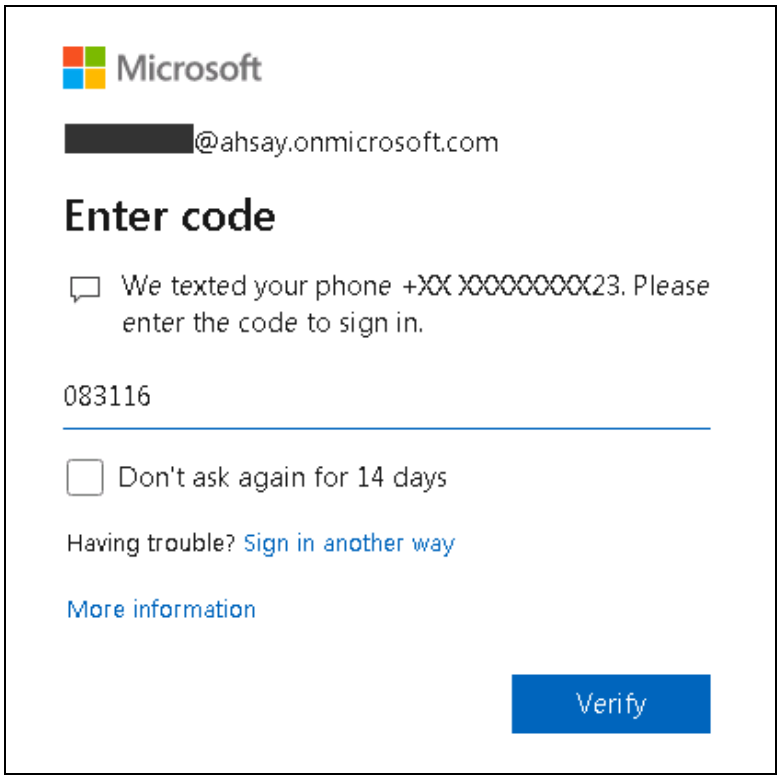


Sign in to your Microsoft account.





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



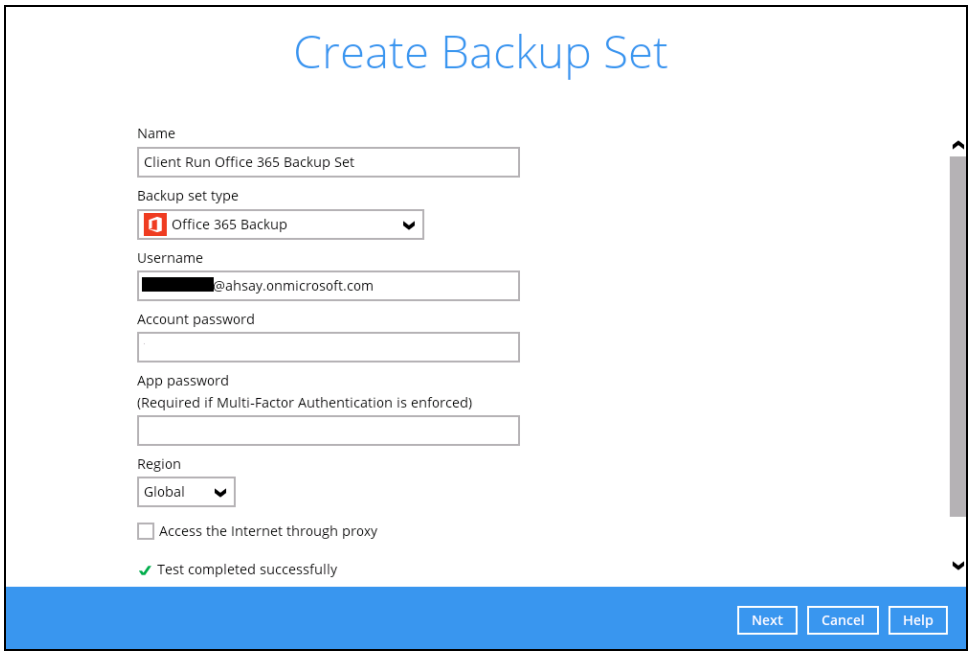
NOTE

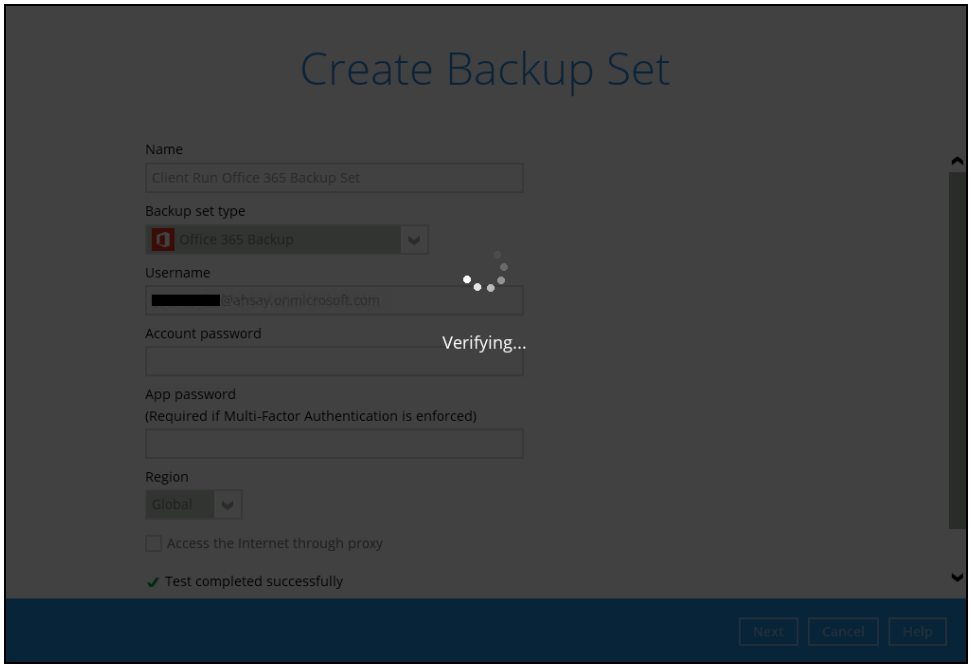
The verification code is only required if the MFA status of an Office 365 account is enforced.

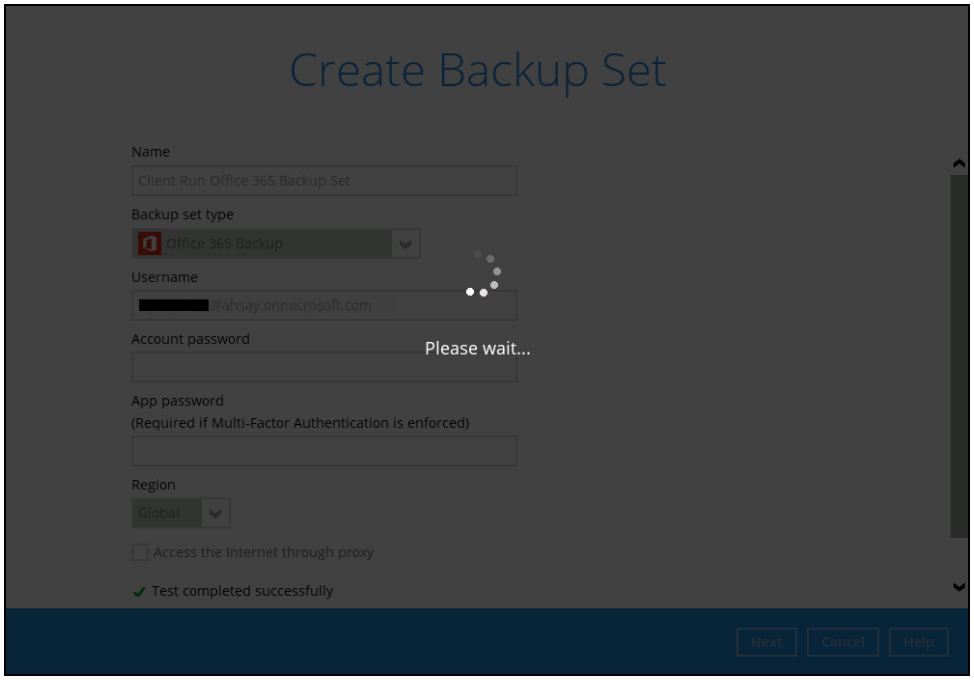
Copy the authorization code.

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

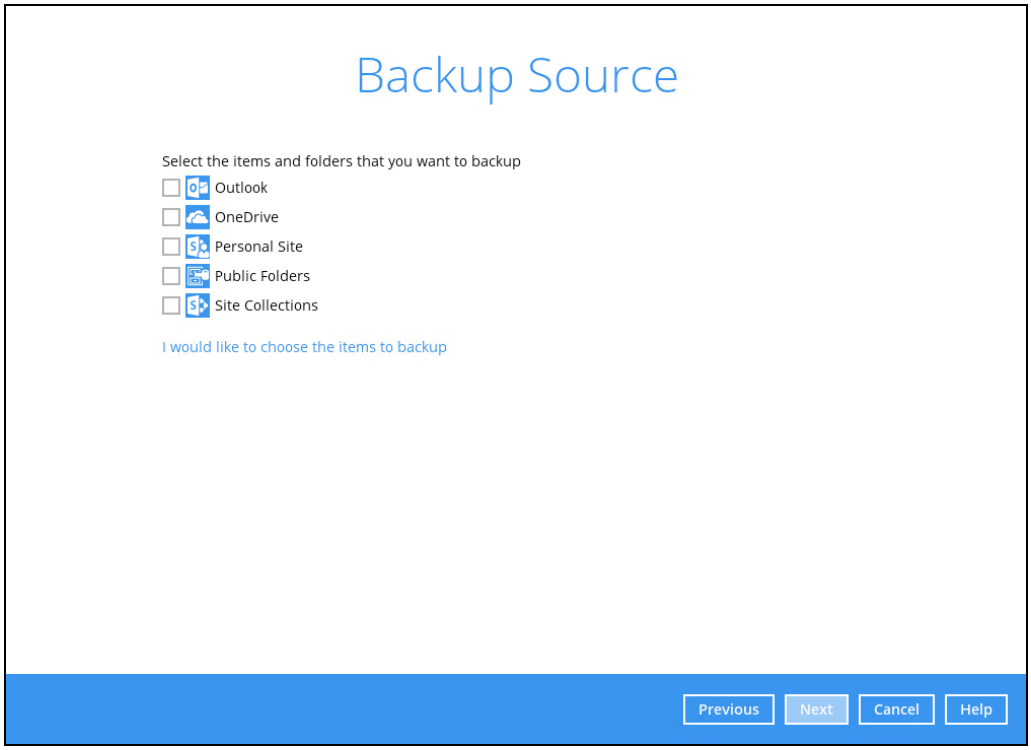
Test completed successfully shows when the validation is successful. Press **Next** to proceed to the next step.



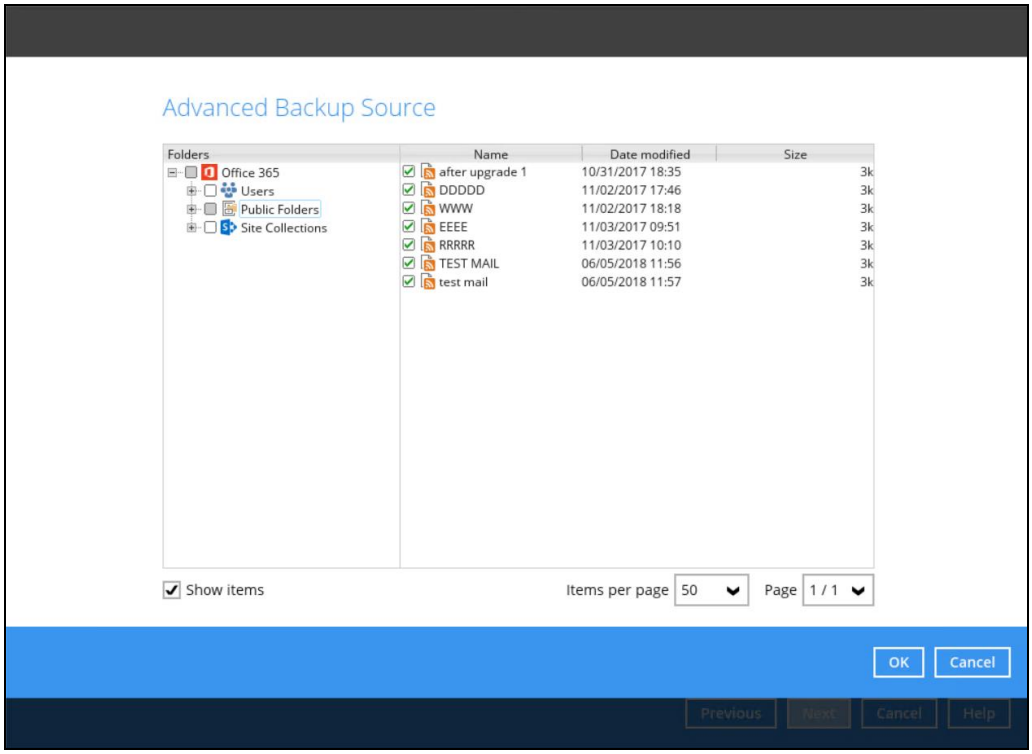




4. In the **Backup Source** menu, select the desired Outlook, OneDrive, Personal Site, Public Folders or Site Collections for backup.

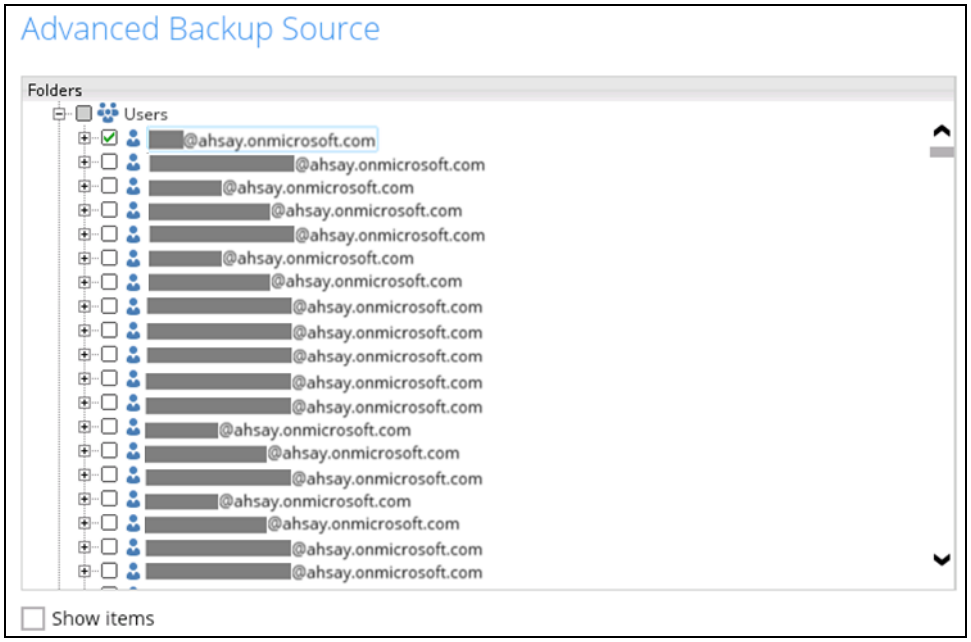


Or click **I would like to choose the items to backup** to choose the detailed items to backup. Enable the **Show items** checkbox at the bottom left corner if you would like to choose individual items for backup.



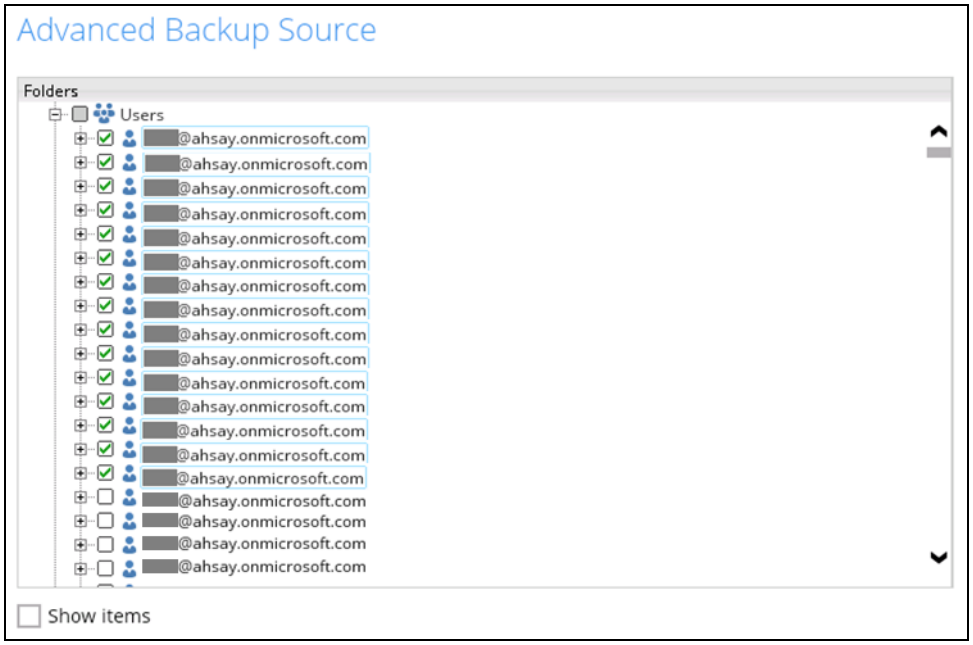
If you will select a large number of items to backup, like 1000 items, you need to click on these 1000 items to select/deselect them individually. Now there is a shortcut that you can use to lessen the burden of selecting/deselecting every 1000 item. You can select/deselect all 100 items at once by using the Shift key. As an example, we will only show how to do this by selecting only 15 users which would fit in our screen. Follow the steps below on how to do this:

i. Select the first user.



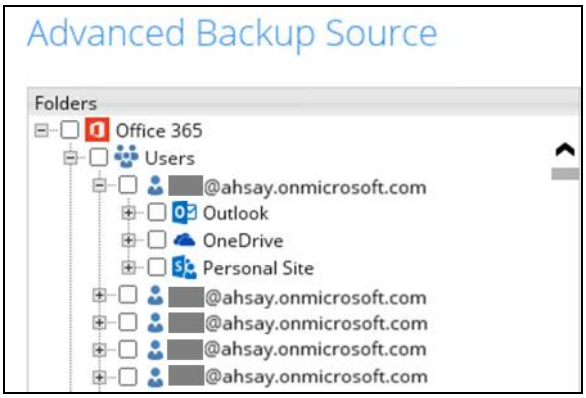
ii. Scroll down to the 15th user.

iii. Hold the **Shift key** then click the 15th user. All the 15 users are now selected.

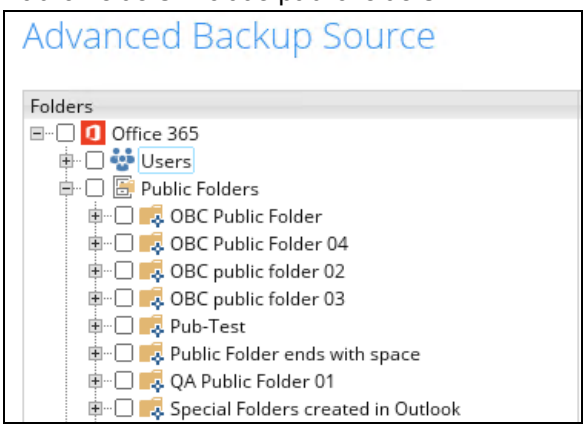


Below are example screenshots for the Users, Public Folders, and Site Collections.

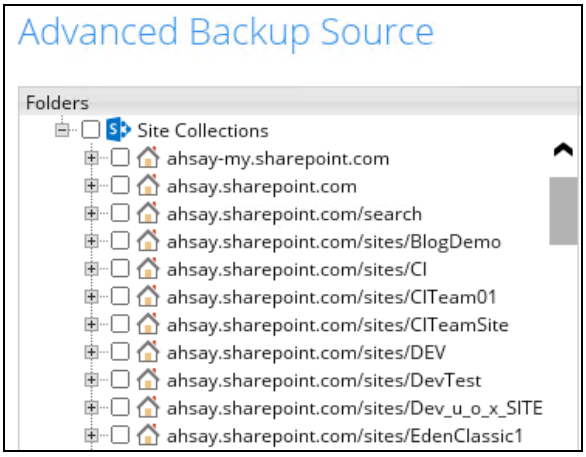
- Users: include Outlook, OneDrive and Personal Sites



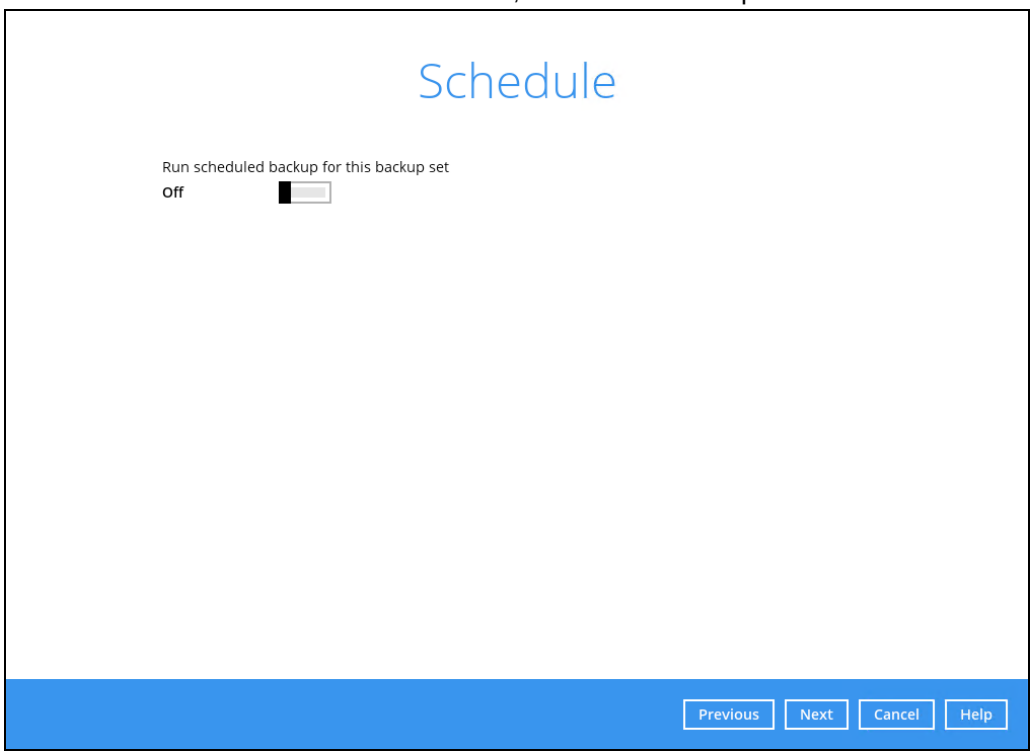
- Public Folders: include public folders

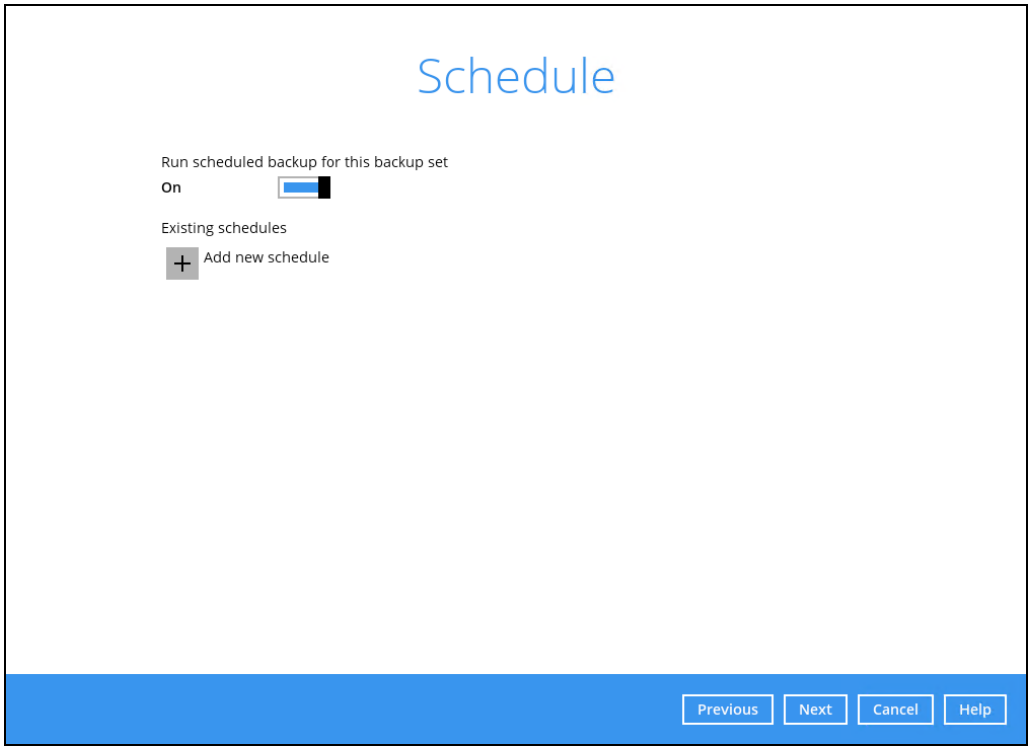


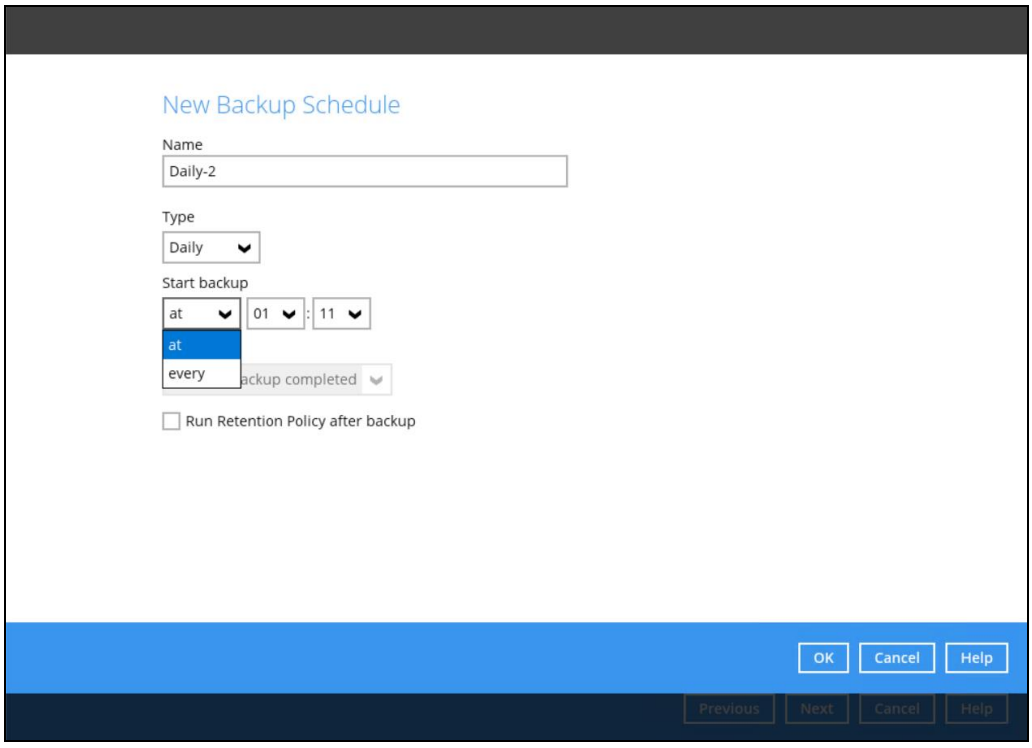
- Site Collections: include Personal Sites and Site Collections



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.



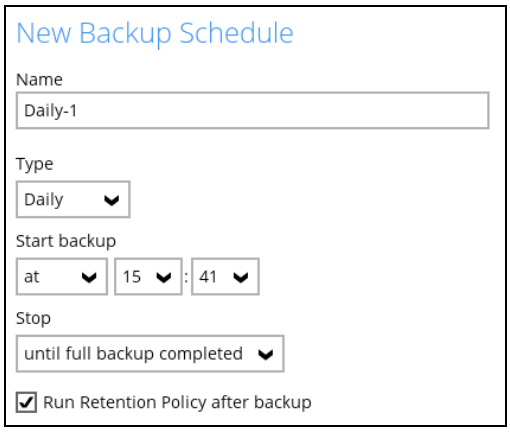




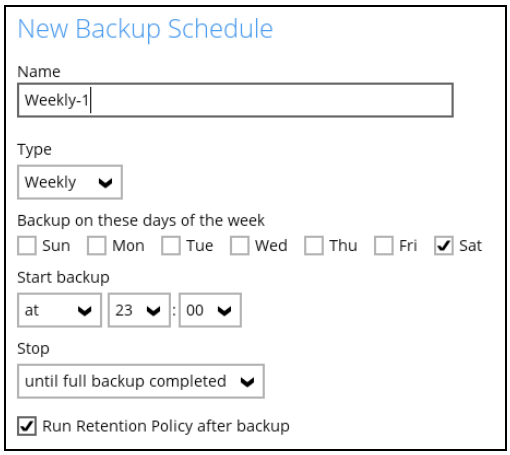
In the New Backup Schedule window, configure the following backup schedule settings.

- **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.

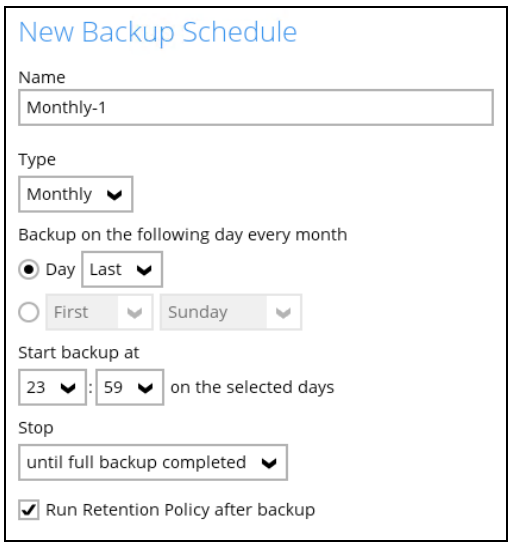
- **Daily** – the time of the day when the backup job will run.



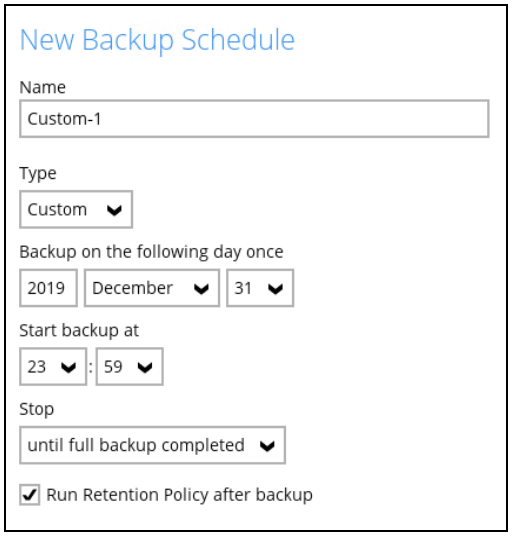
- **Weekly** – the day of the week and the time of the day when the backup job will run.



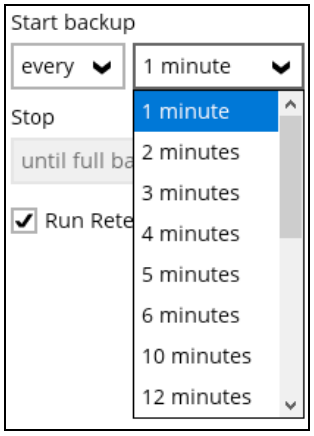
- **Monthly** – the day of the month and the time of the day when the backup job will run.

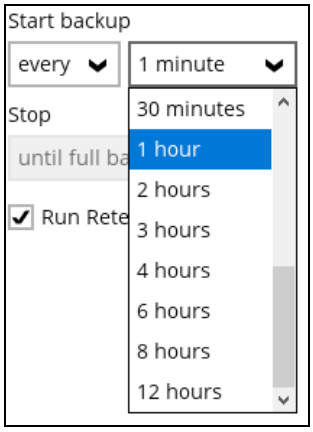


- **Custom** – a specific date and the time when the backup job will run.

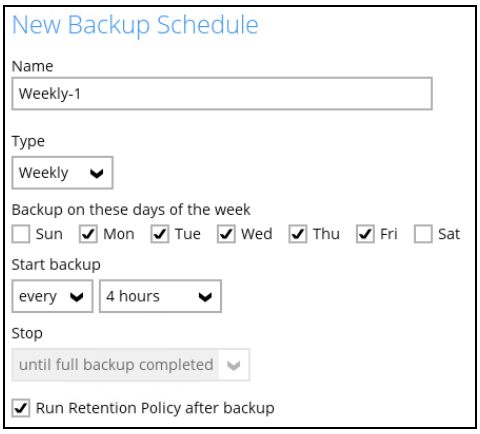


- **Start backup** – the start time of the backup job.
  - **at** – this option will start a backup job at a specific time.
  - **every** – this option will start a backup job in intervals of minutes or hours.





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



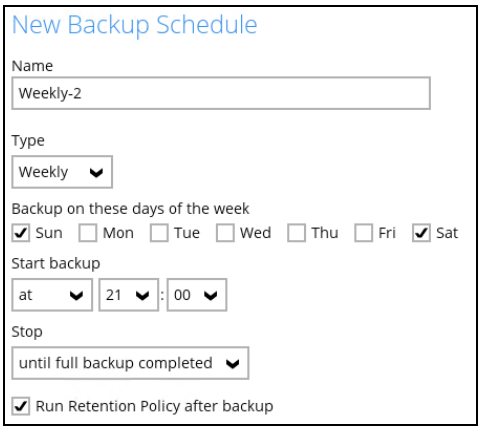


Figure 1.1 ***Figure 1.2***

Figure 1.1 – Periodic schedule every 4 hours Monday - Friday during business hours
Figure 1.2 – Normal schedule run at 21:00 or 9:00 PM on Saturday & Sunday on weekend during 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.

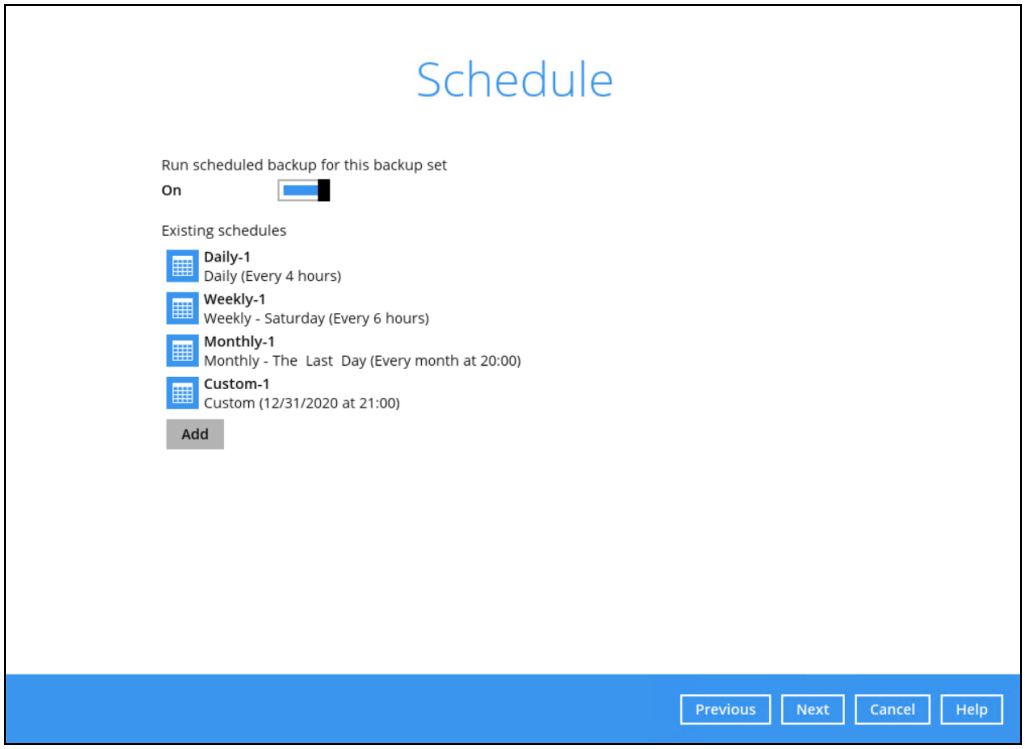
    The partially backed up data will have to be removed by running the data integrity check.

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

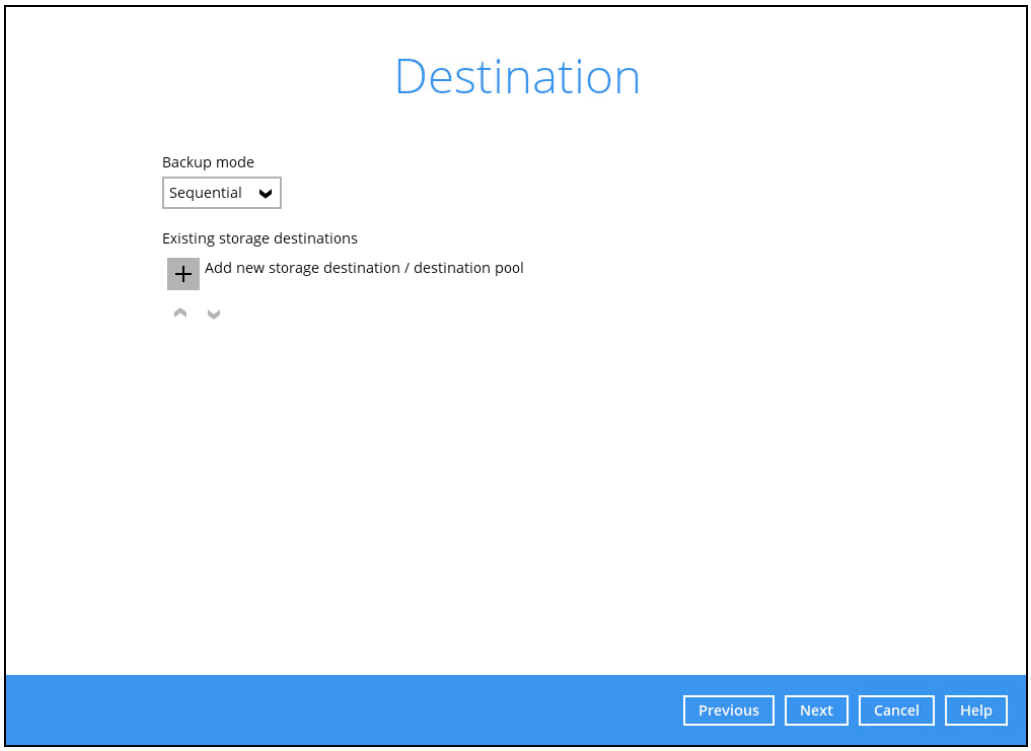
- **Run Retention Policy after backup** – if enabled, the AhsayOBM will run a retention policy job to remove files from the backup destination(s) which have exceeded the retention policy after performing a backup job.

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

Click the **[Next]** button to proceed. Multiple backup schedules can be created.



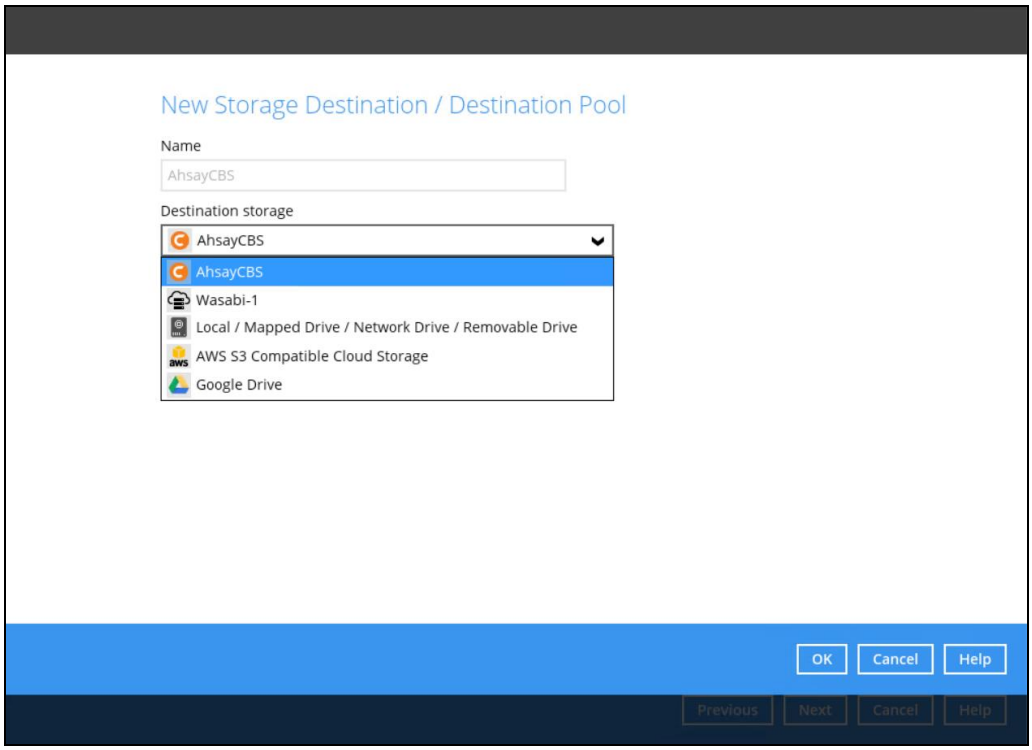
6. In the Destination menu, select a backup destination where the backup data will be stored. Click the "**+**" icon next to **Add new storage destination / destination pool**.



NOTE

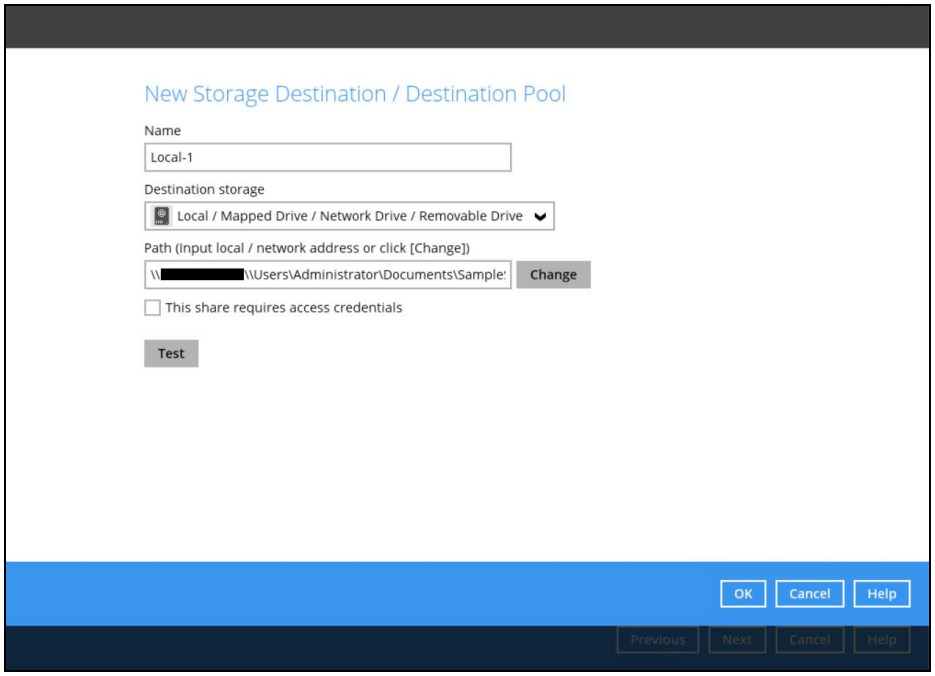
For more details on Backup Destination, refer to the following Wiki article for details:
FAQ: Frequently Asked Questions on Backup Destination

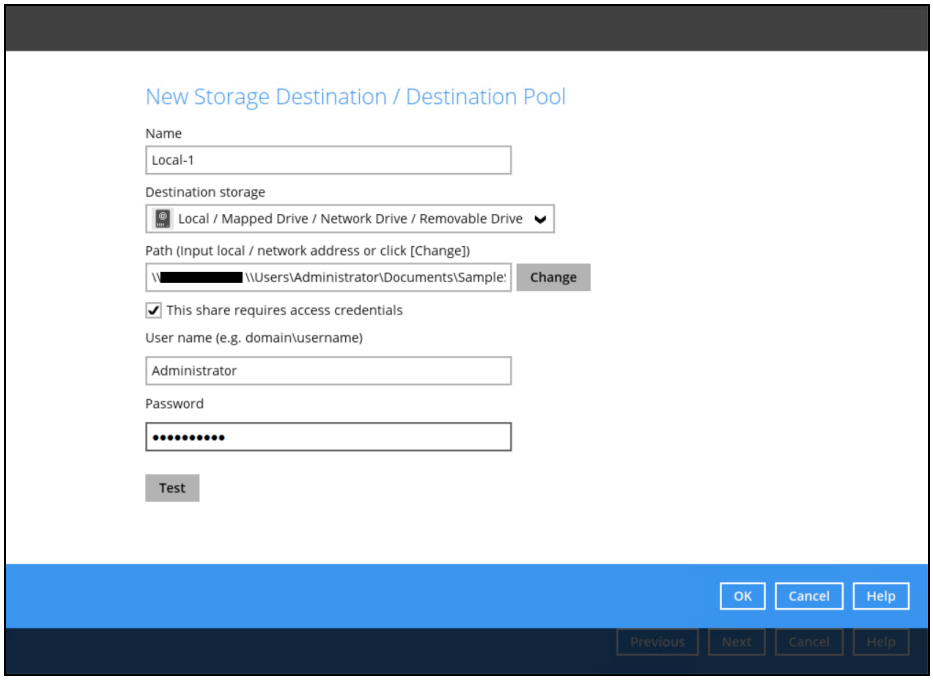
Select storage destinations.

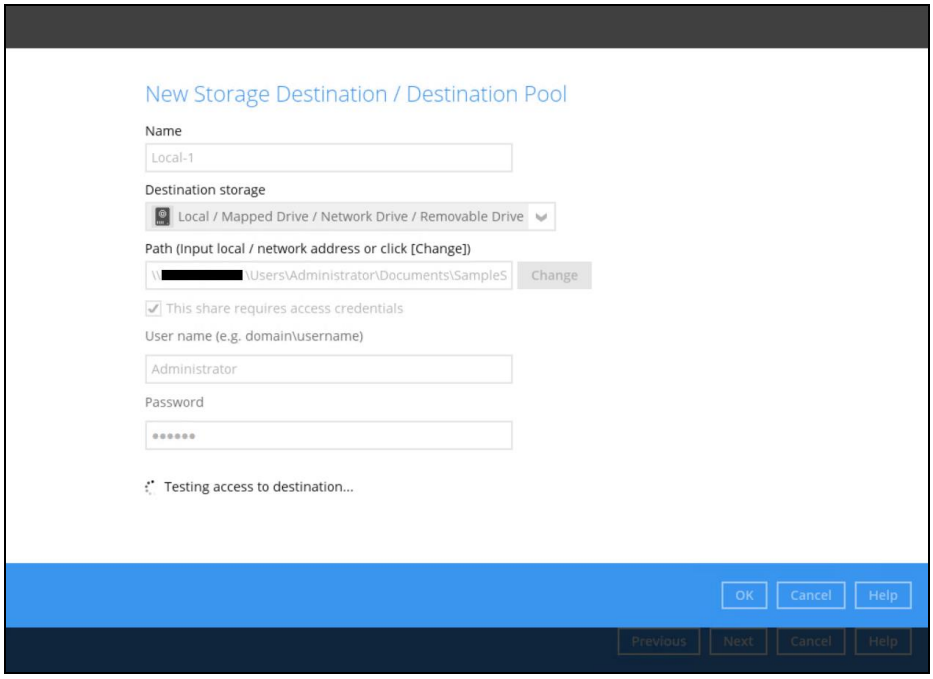


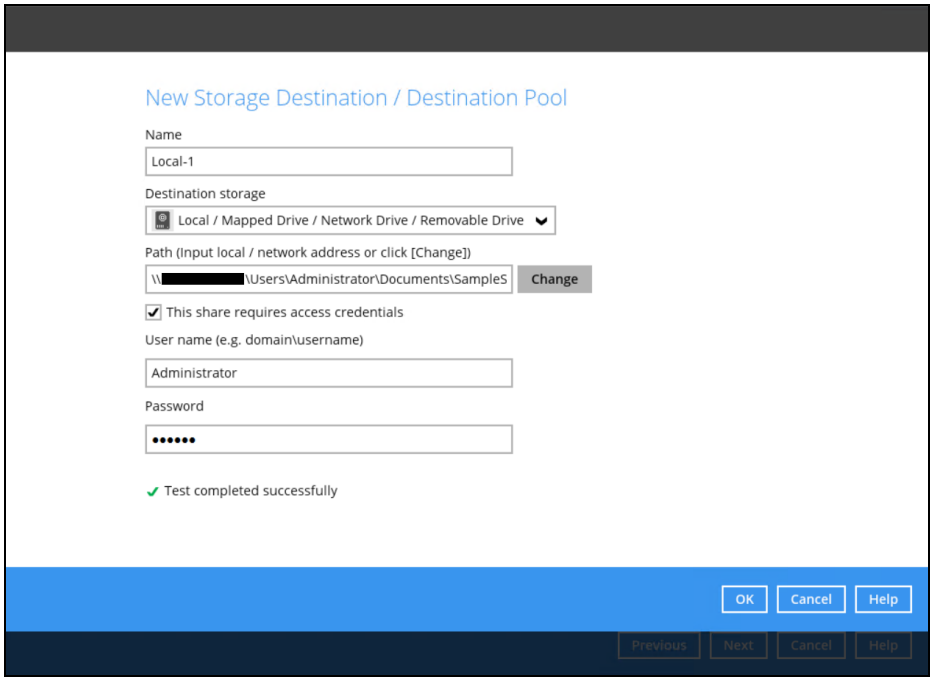
You can choose a storage combination of the Local/Mapped Drive/Network Drive/Removable Drive or Cloud storage. Click **OK** to proceed when you are done with the settings.

- If you have chosen the **Local / Mapped Drive / Network 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.

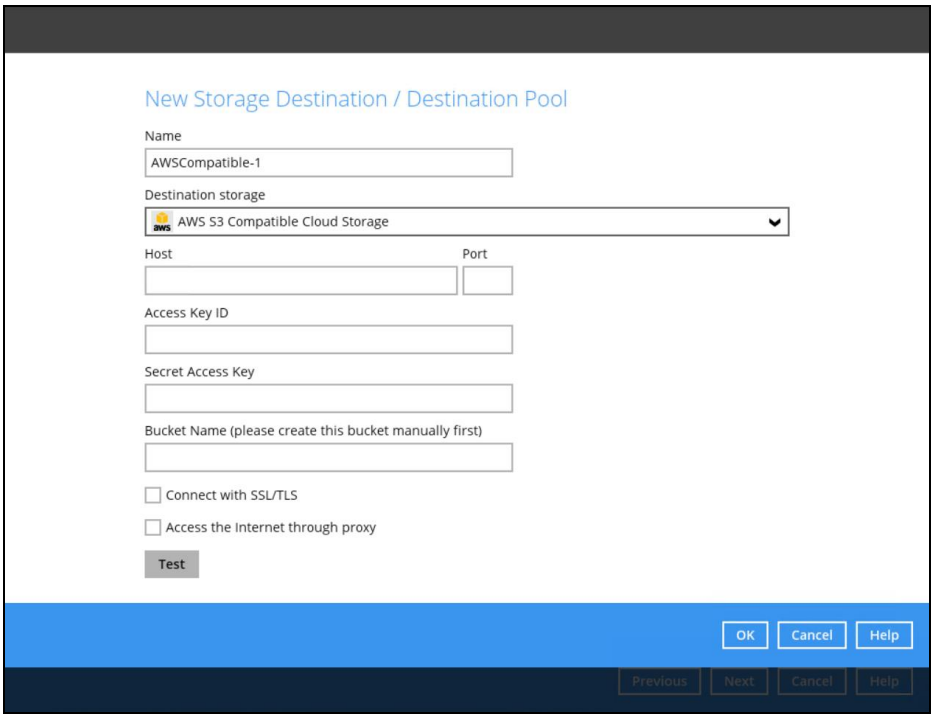


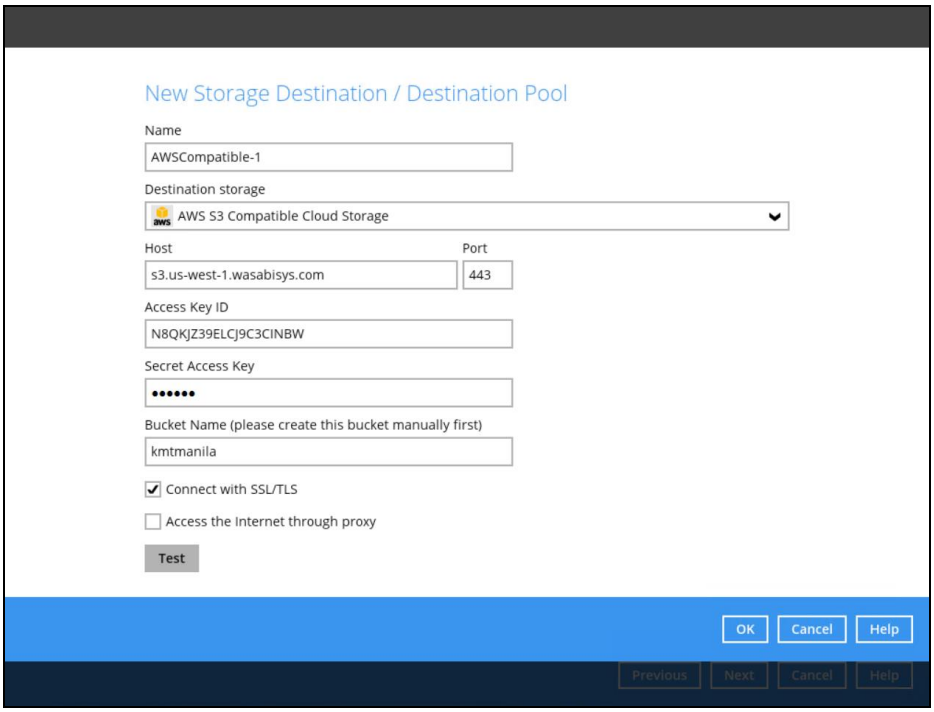


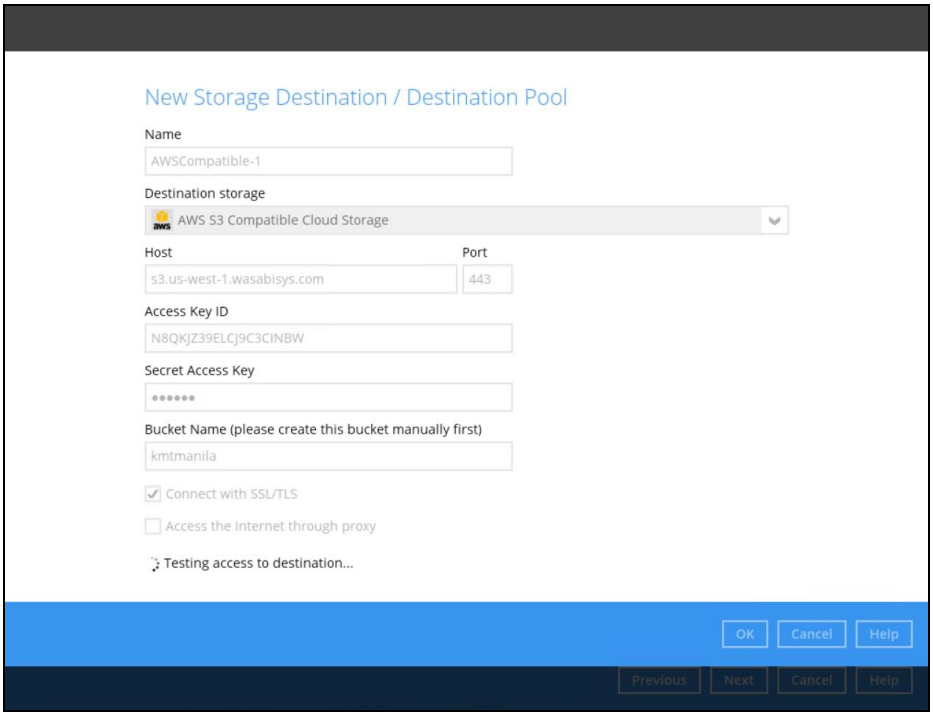

New Storage Destination / Destination Pool
Name
Local-1
Destination storage
Local / Mapped Drive / Network Drive / Removable Drive
Path (Input local / network address or click [Change])
\\[redacted]\Users\Administrator\Documents\SampleS
Change
This share requires access credentials
User name (e.g. domain\username)
Administrator
Password
Testing access to destination...
OK
Cancel
Help
Previous
Next
Cancel
Help

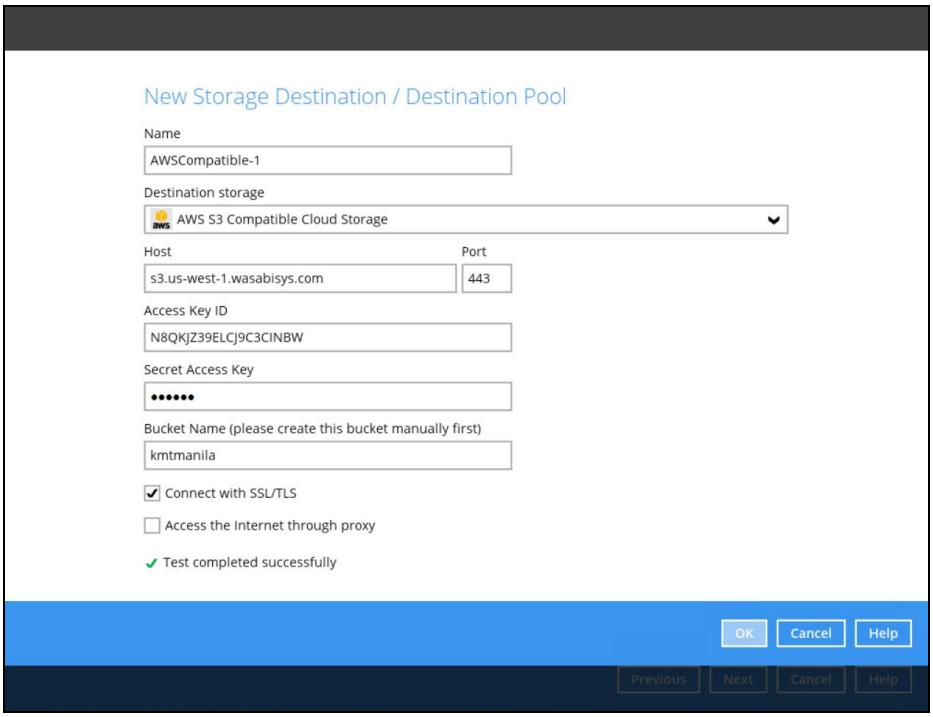

New Storage Destination / Destination Pool
Name
Local-1
Destination storage
Local / Mapped Drive / Network Drive / Removable Drive
Path (Input local / network address or click [Change])
\\[redacted]\Users\Administrator\Documents\SampleS
Change
This share requires access credentials
User name (e.g. domain\username)
Administrator
Password
Test completed successfully
OK
Cancel
Help
Previous
Next
Cancel
Help

- 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.

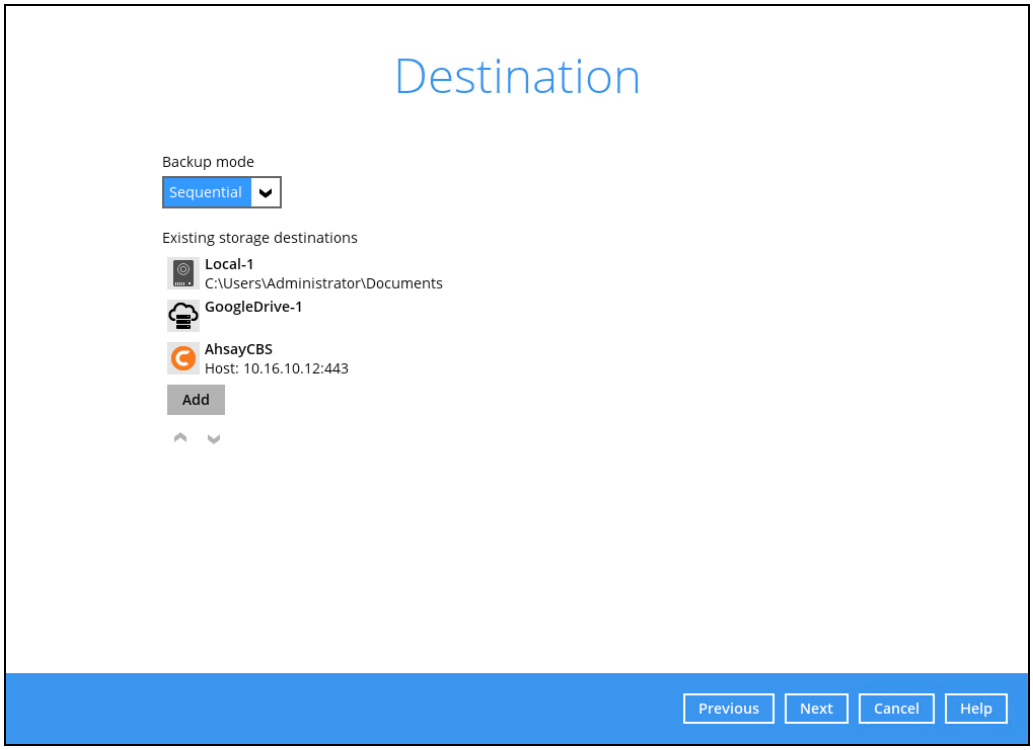


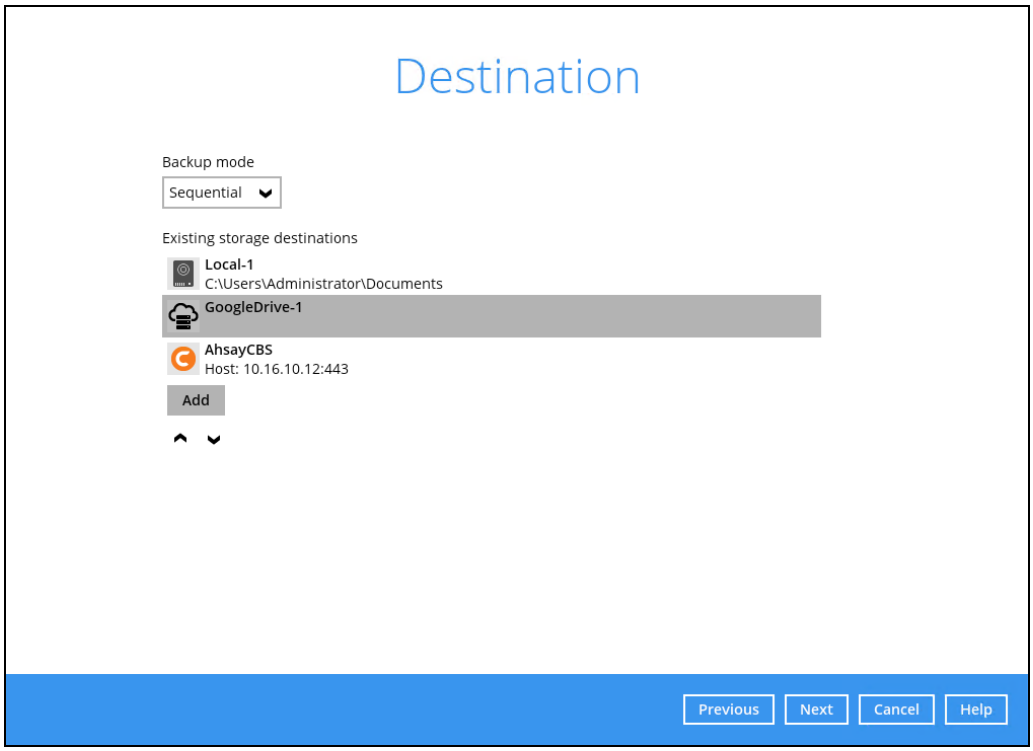




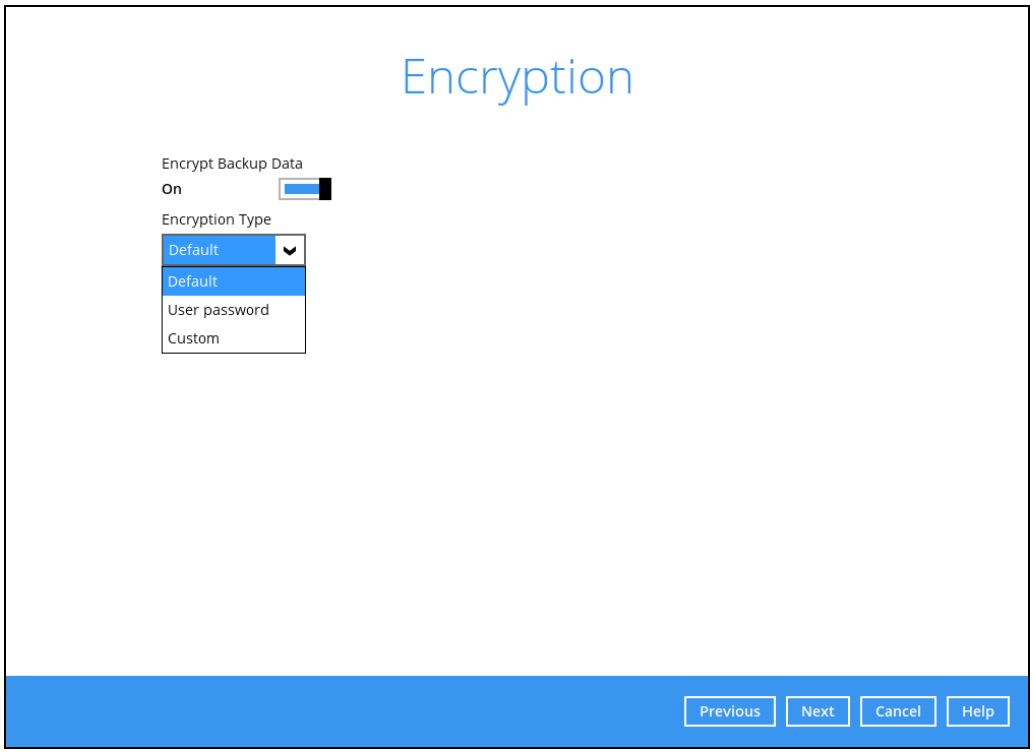


You can add multiple storage destinations. The backup data will be uploaded to all the destinations you have selected in the order you added them. Press the icon to alter the order. Click **Next** to proceed when you are done with the selection.


Destination
Backup mode
Sequential
Existing storage destinations
Local-1
C:\Users\Administrator\Documents
GoogleDrive-1
AhsayCBS
Host: 10.16.10.12:443
Add
Previous
Next
Cancel
Help

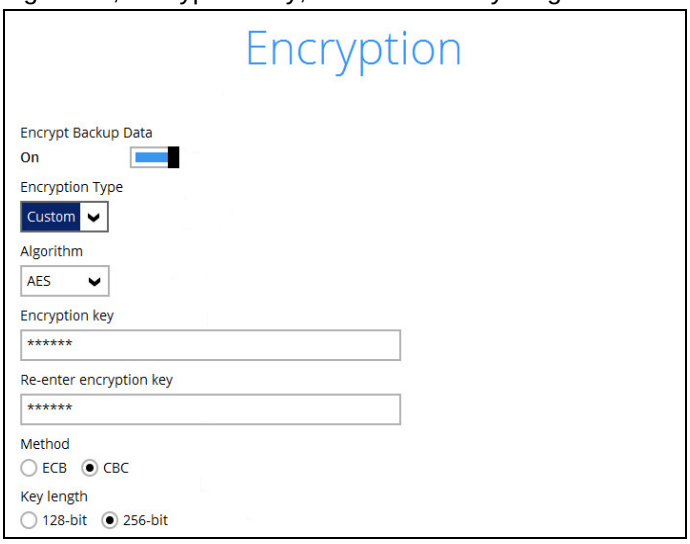

Destination
Backup mode
Sequential
Existing storage destinations
Local-1
C:\Users\Administrator\Documents
GoogleDrive-1
AhsayCBS
Host: 10.16.10.12:443
Add
Previous
Next
Cancel
Help

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 AhsayOBM at the time when this backup set is created. Please be reminded that if you change the AhsayOBM login password later, the encryption keys of the backup sets previously created with this encryption type will remain unchanged.
- **Custom** – you can customize your encryption key, where you can set your own algorithm, encryption key, method and key length.

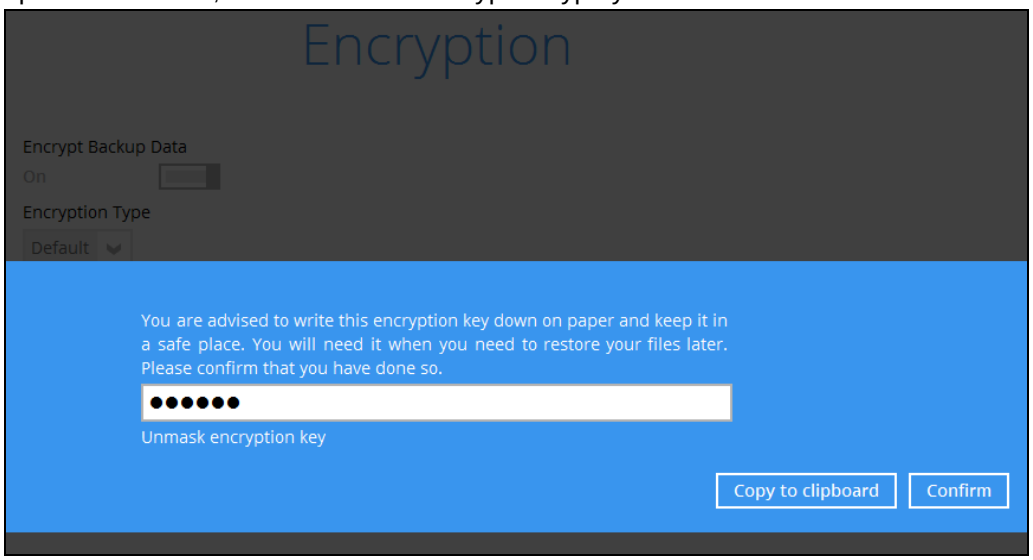


NOTE

For best practice on managing your encryption key, refer to the following Wiki article.
FAQ: Best practices for managing encryption key on AhsayOBM or AhsayACB?

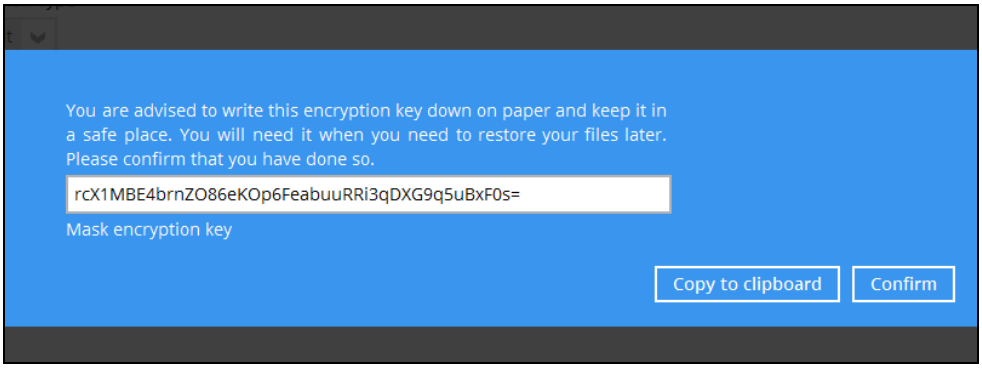
Click Next when you are done setting.

8. 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.



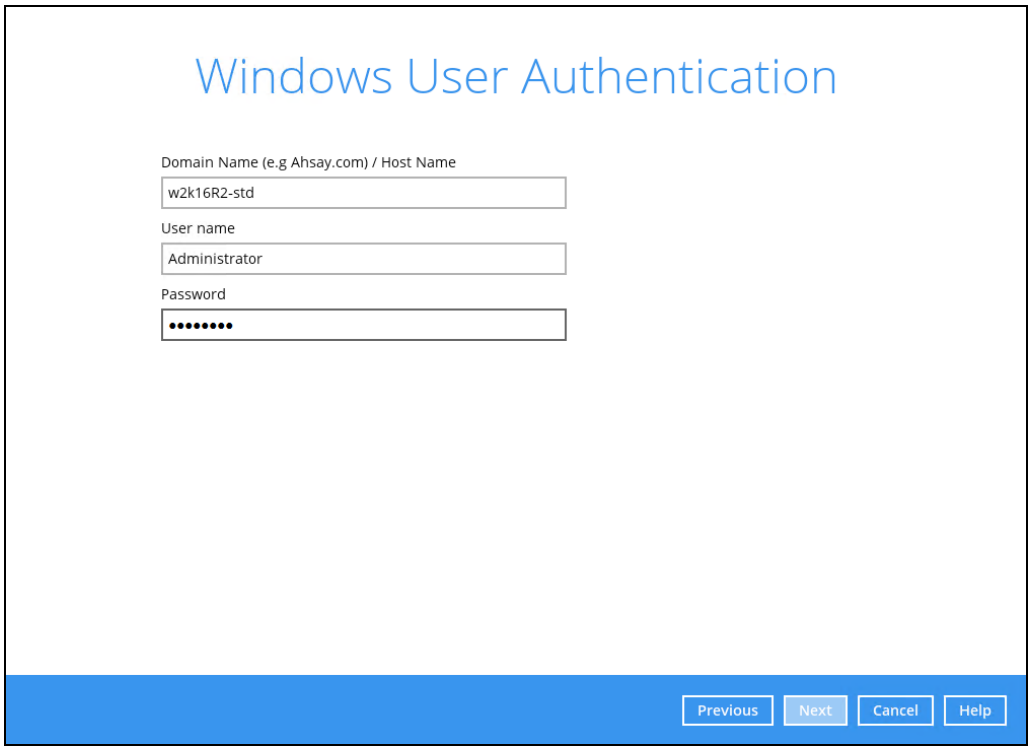
The pop-up window has the following three options to choose from:

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



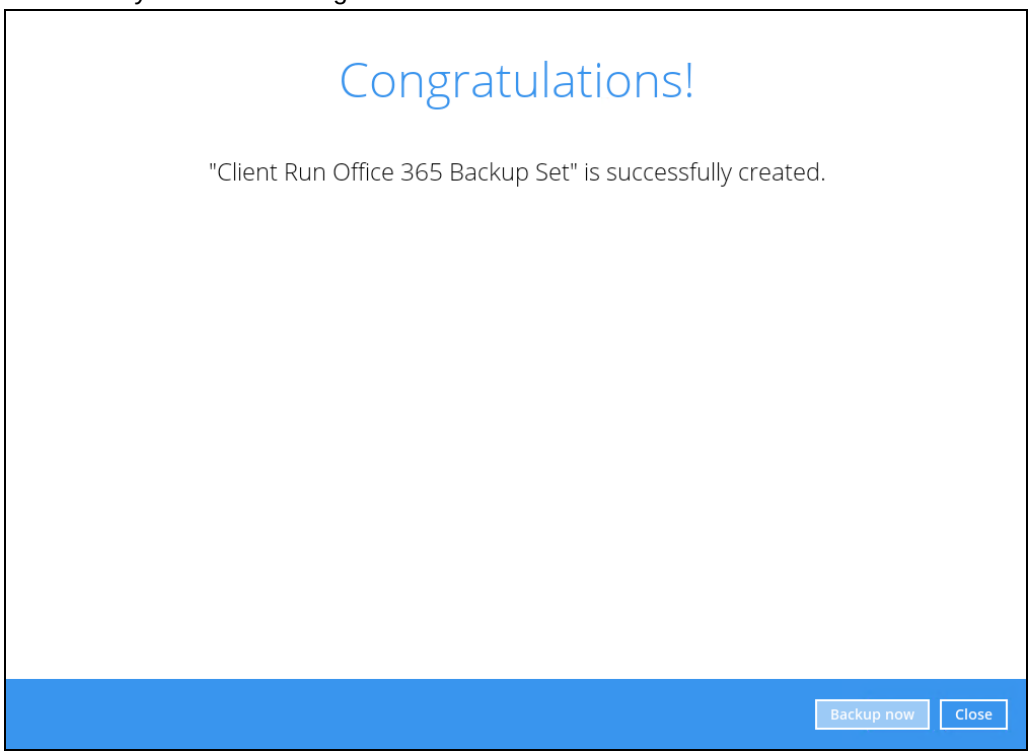
- **Copy to clipboard** – Click to copy the encryption key, then you can paste it in another location of your choice.
- **Confirm** – Click to exit this pop-up window and proceed to the next step.

9. If you have enabled the scheduled backup option, you will be prompted to enter the **User Name** and **Password** of the Windows account that will be running the backup.



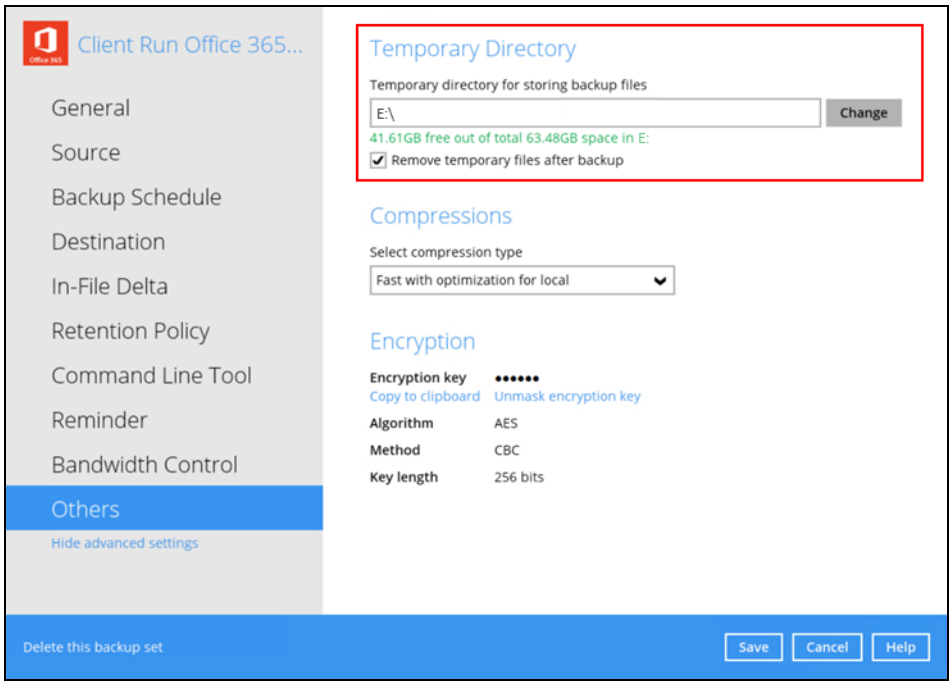
Click Next to create the backup set.

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



11. 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 Dive C.

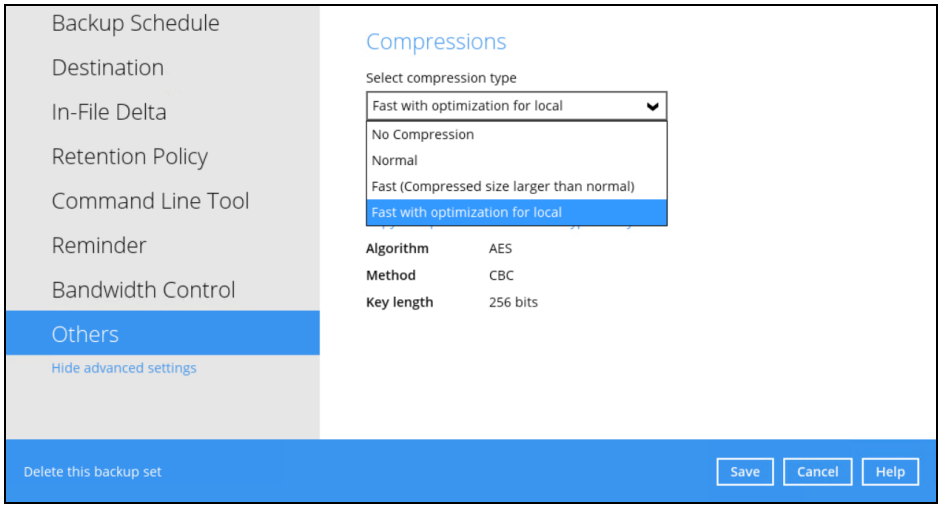
    Go to **Others** > **Temporary Directory**. Click **Change** to browse for another location.



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

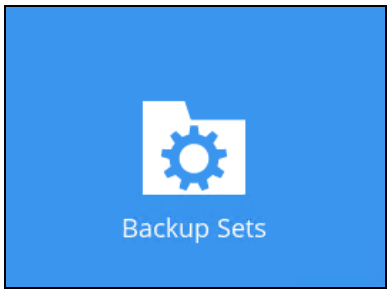
    Go to **Others** > **Compressions**. Select from the following list:

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

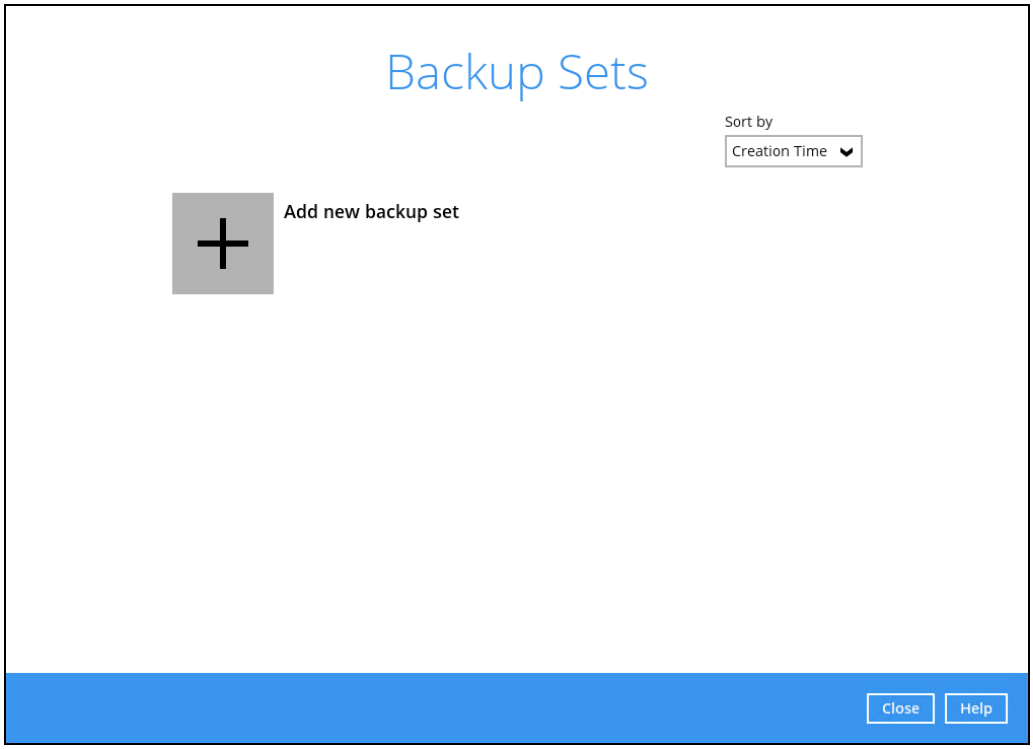


4.2 Hybrid Authentication

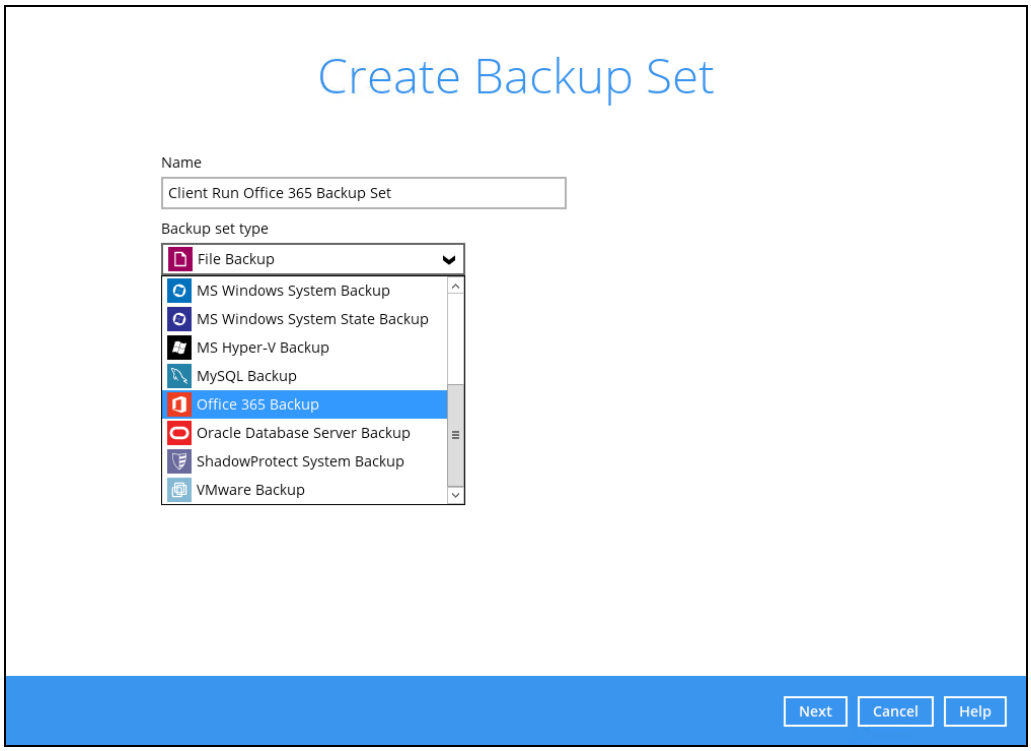
1. In the AhsayOBM main interface, click **Backup Sets**.



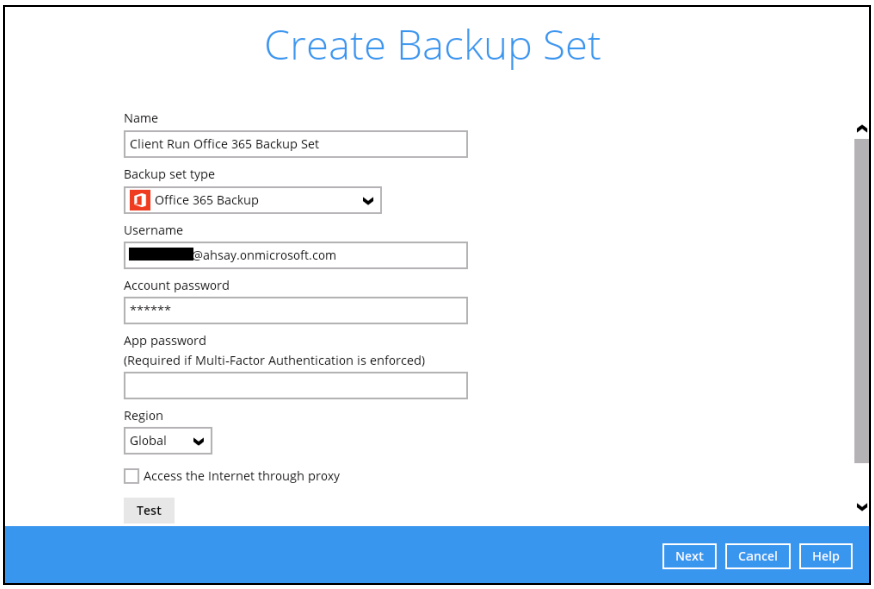
2. Click the "**+**" icon next to **Add new backup set**.



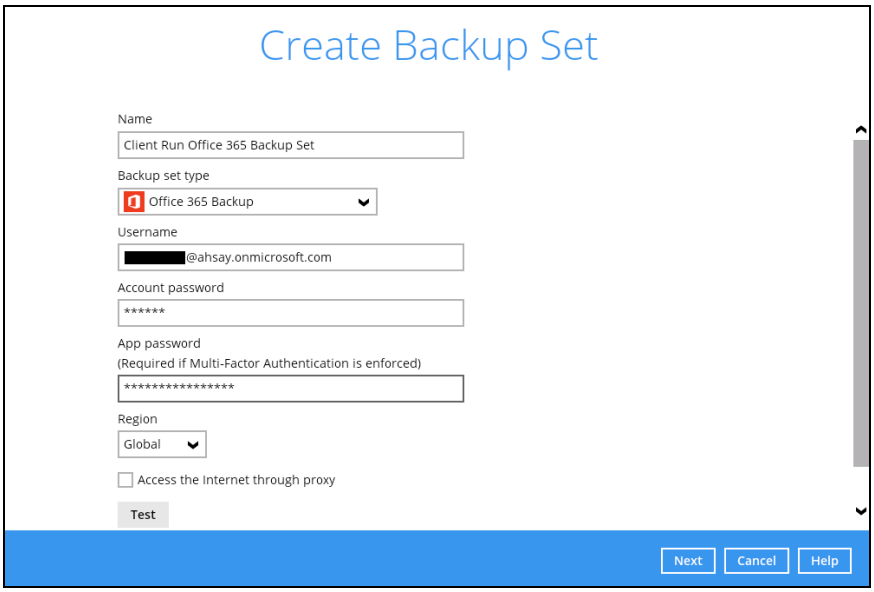
3. Enter a **Name** for your backup set and select **Office 365 Backup** as the **Backup set type**.



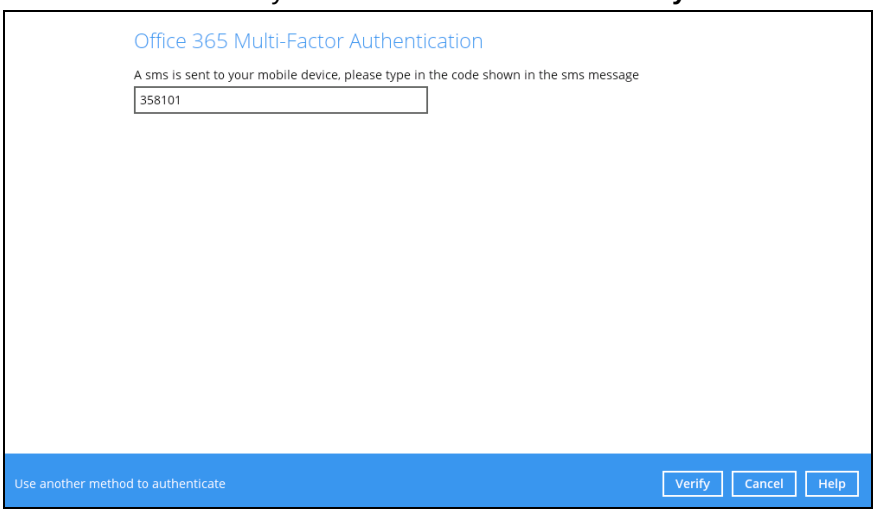
- If MFA is not enforced, enter the Username and Account password. Select the Region and click **Test**.



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



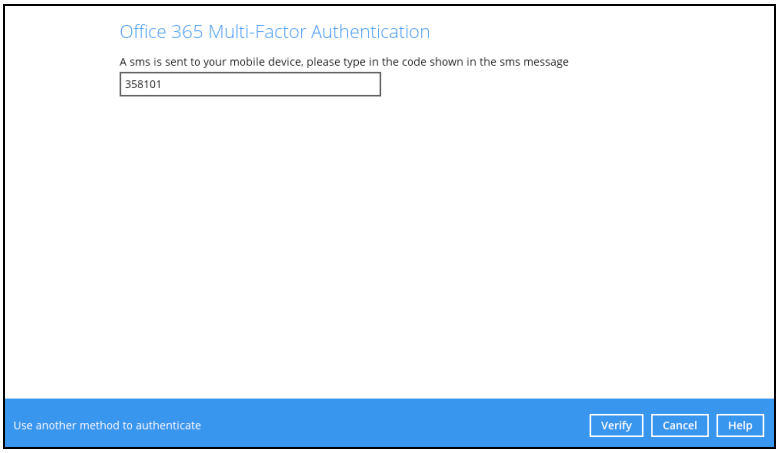
Enter the code sent to your mobile device and click **Verify**.



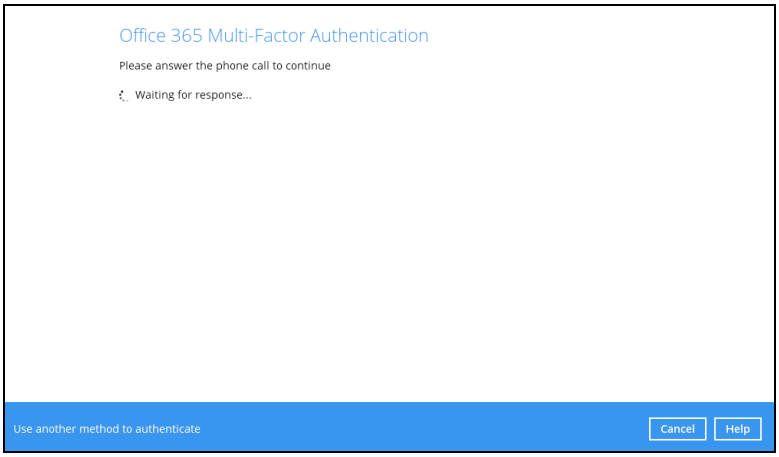
or

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.

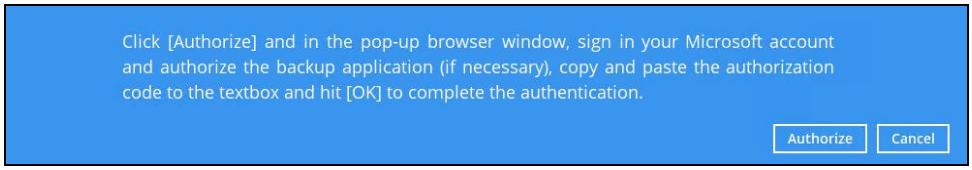


NOTE

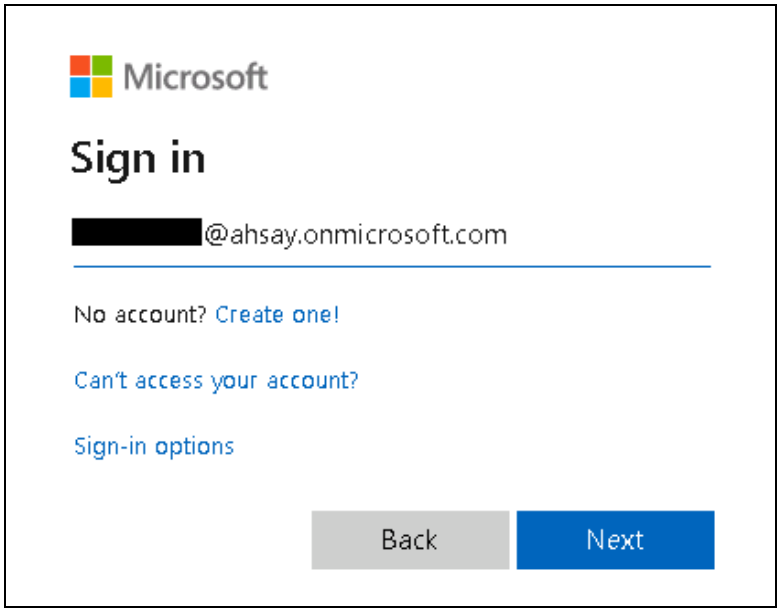
- The App password is only required if the MFA status of an Office 365 account is enforced.

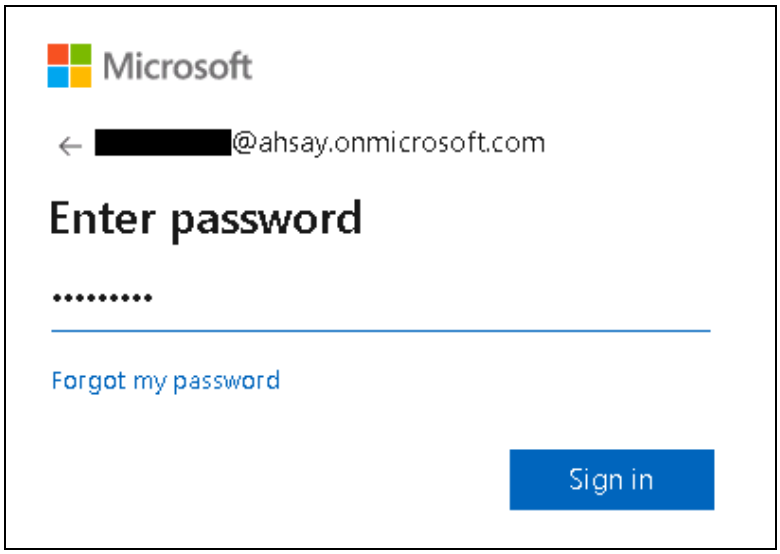
- If the MFA of the Office 365 user account will be enabled later on, it is highly advisable to login to AhsayOBM and re-authenticate the Office 365 user account's credential using the MFA App password. Otherwise the scheduled backups of the Office 365 backup set will stop working.

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

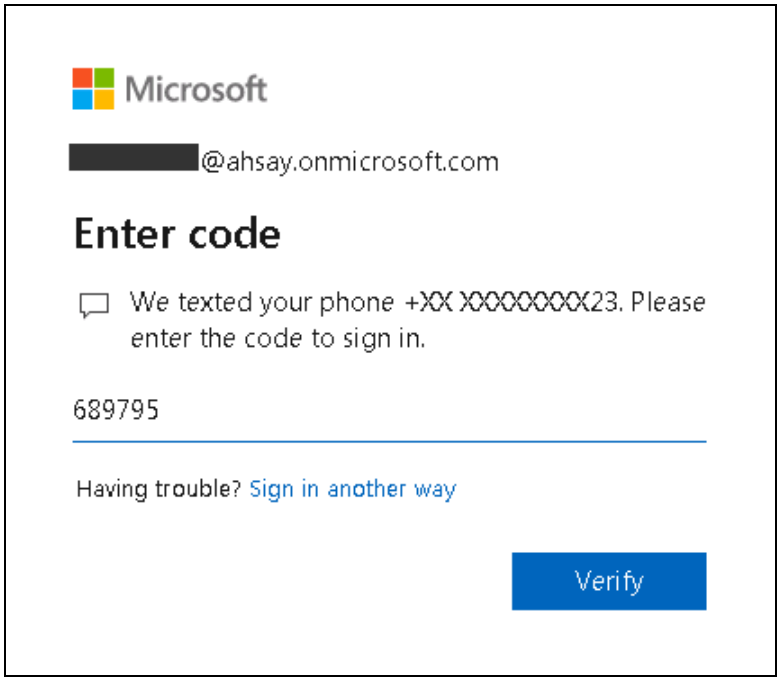


Sign in to your Microsoft account.





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



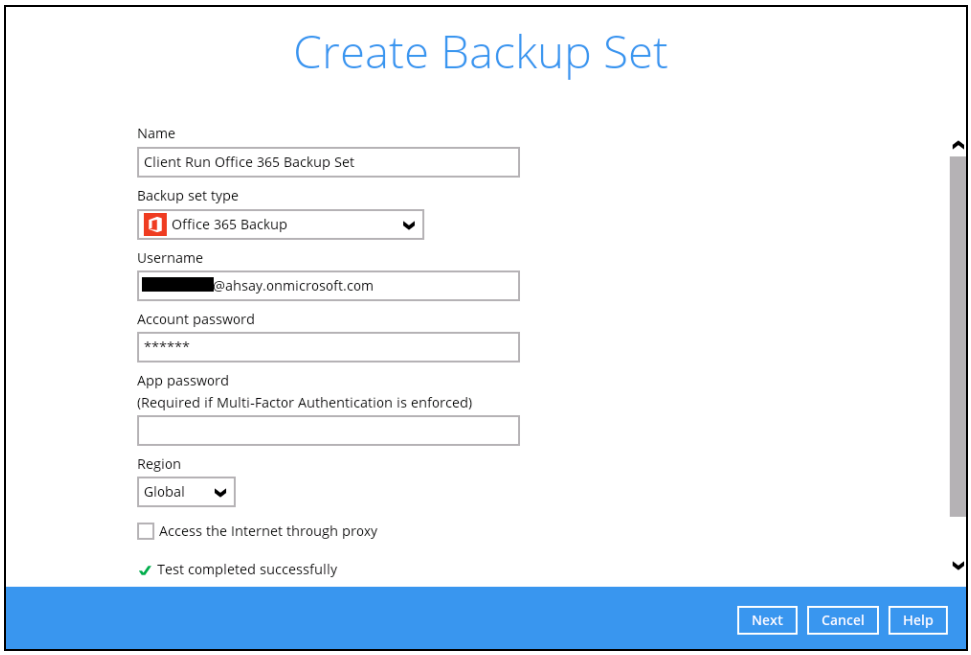
NOTE

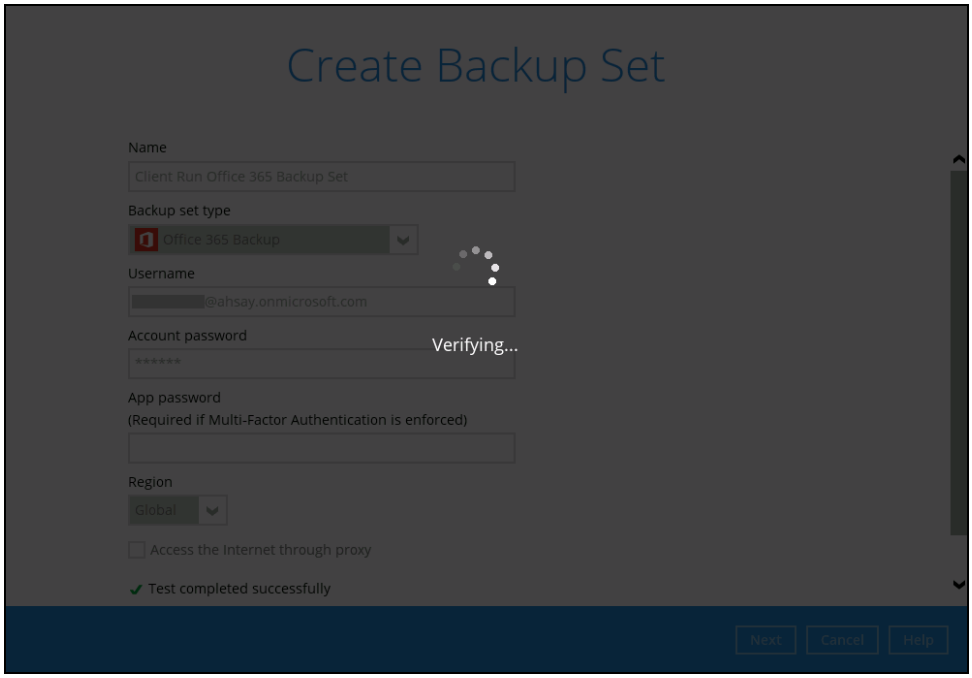
The verification code is only required if the MFA status of an Office 365 account is enforced.

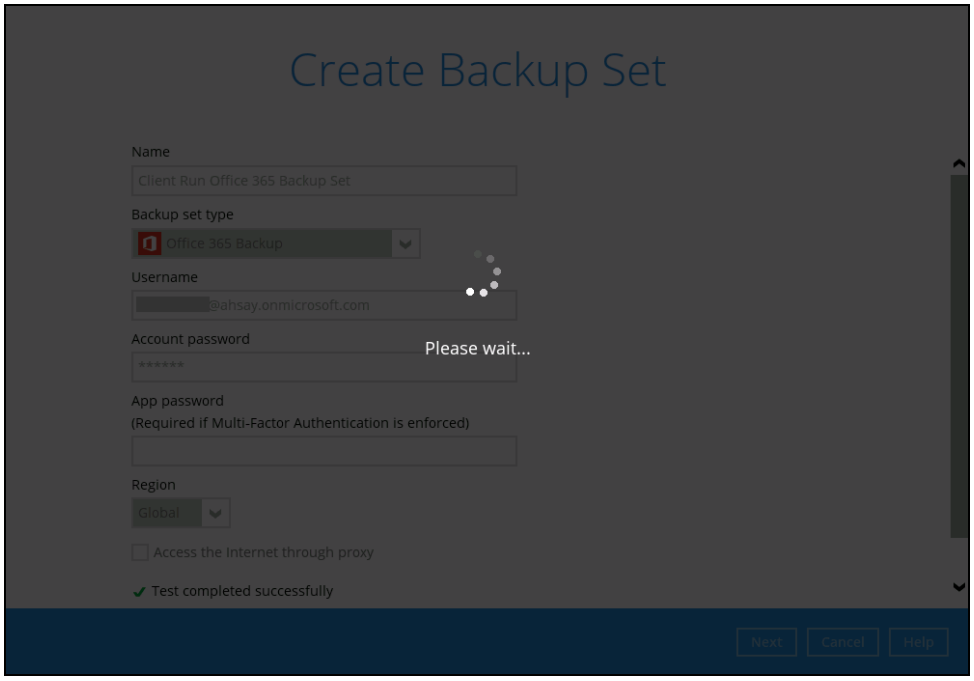
Copy the authorization code.

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

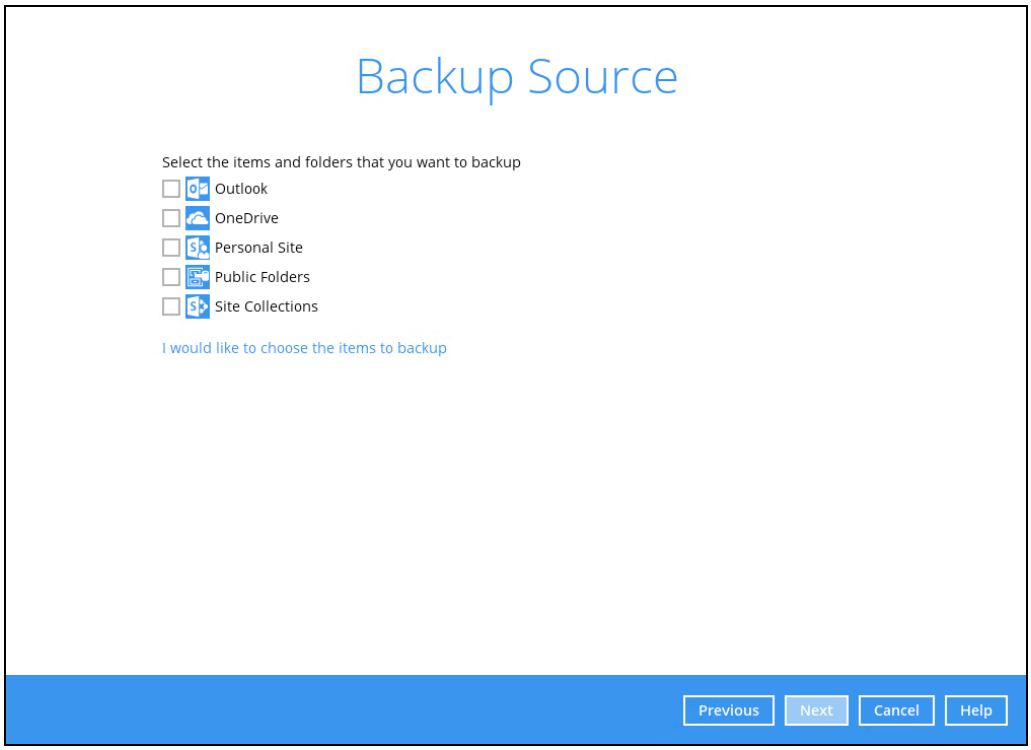
Test completed successfully shows when the validation is successful. Press **Next** to proceed to the next step.



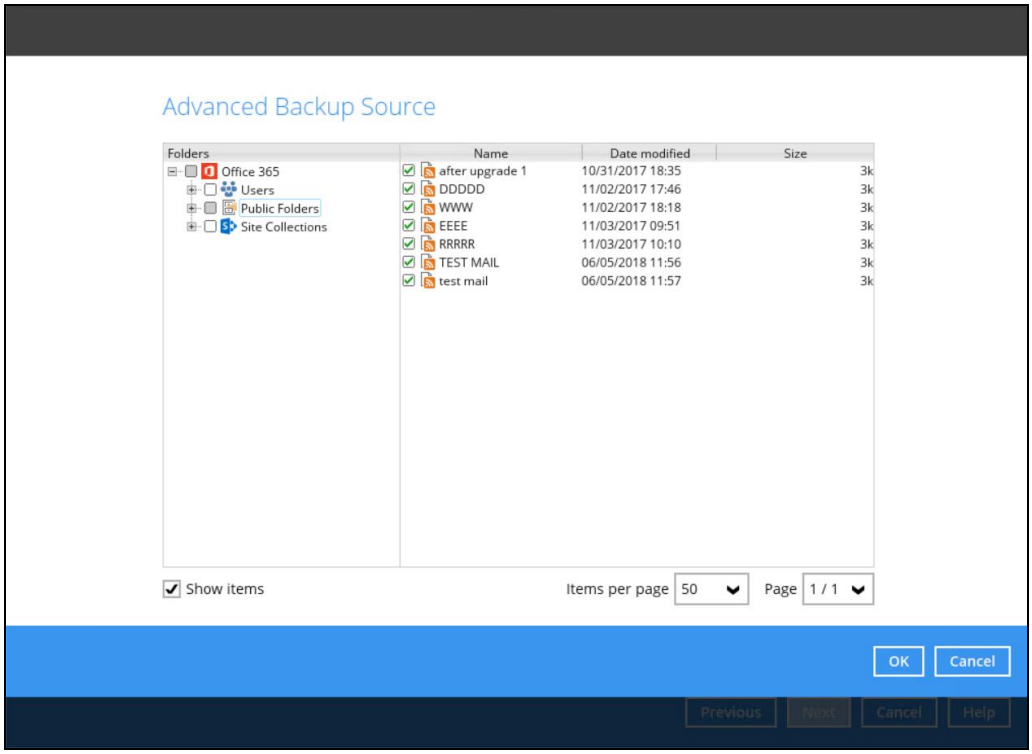



Create Backup Set
Name
Client Run Office 365 Backup Set
Backup set type
Office 365 Backup
Username
@ahsay.onmicrosoft.com
Account password
******
Please wait...
App password
(Required if Multi-Factor Authentication is enforced)
Region
Global
Access the Internet through proxy
Test completed successfully
Next
Cancel
Help

4. In the **Backup Source** menu, select the desired Outlook, OneDrive, Personal Site, Public Folders or Site Collections for backup.

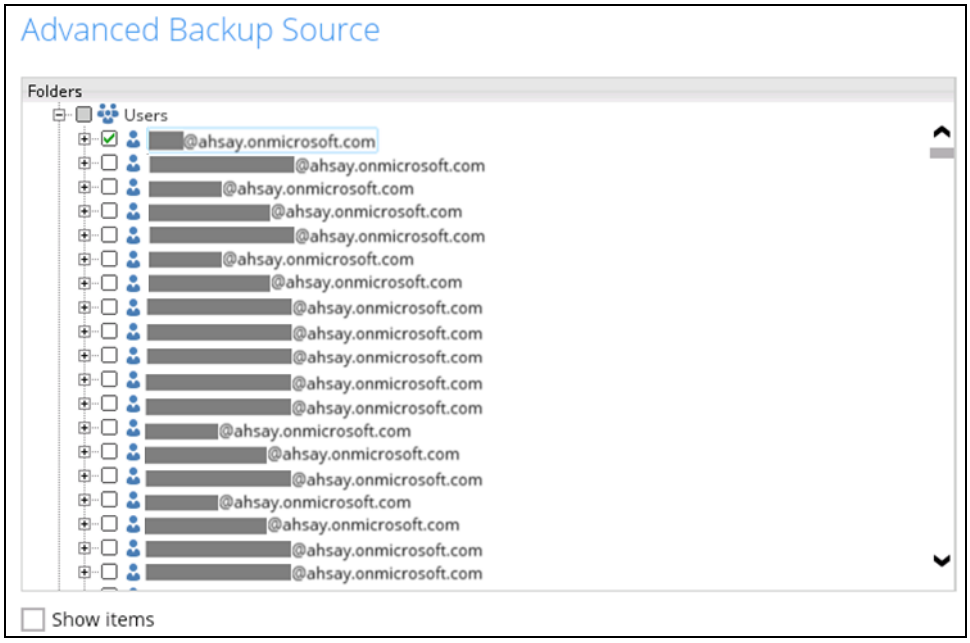


Or click **I would like to choose the items to backup** to choose the detailed items to backup. Enable the **Show items** checkbox at the bottom left corner if you would like to choose individual items for backup.



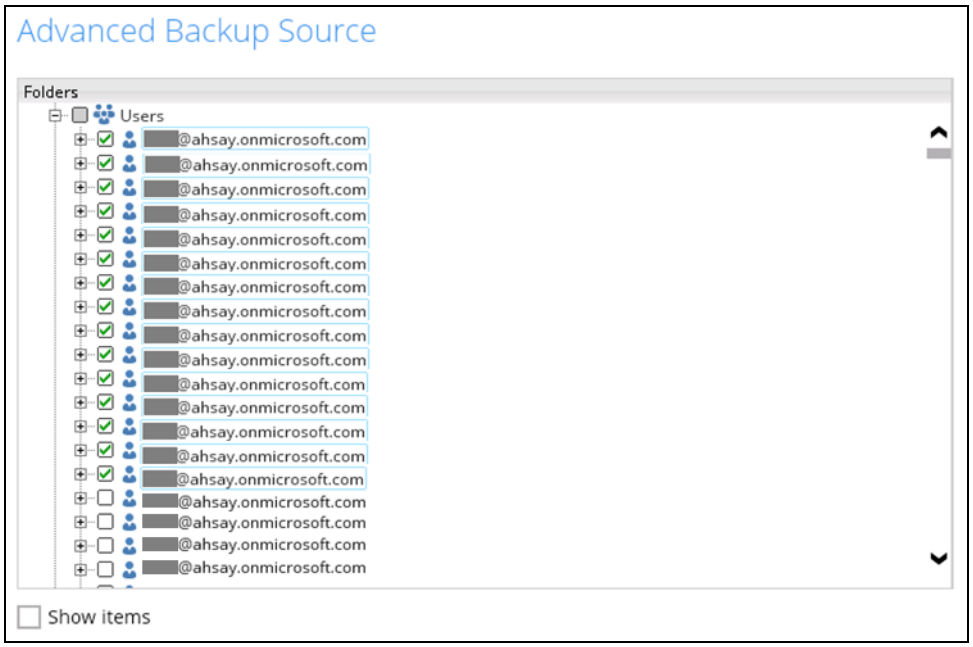
If you will select a large number of items to backup, like 1000 items, you need to click on these 1000 items to select/deselect them individually. Now there is a shortcut that you can use to lessen the burden of selecting/deselecting every 1000 item. You can select/deselect all 100 items at once by using the Shift key. As an example, we will only show how to do this by selecting only 15 users which would fit in our screen. Follow the steps below on how to do this:

i. Select the first user.



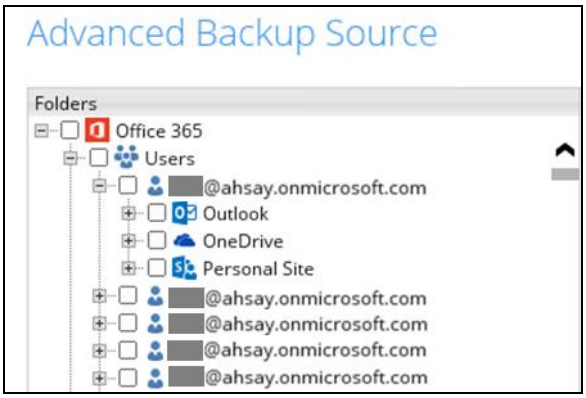
ii. Scroll down to the 15th user.

iii. Hold the **Shift key** then click the 15th user. All the 15 users are now selected.

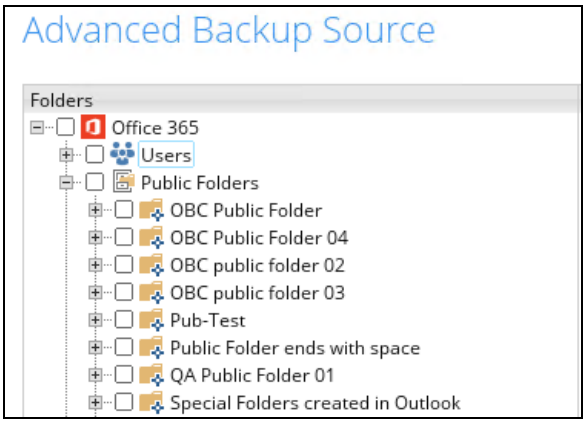


Below are example screenshots for the Users, Public Folders, and Site Collections.

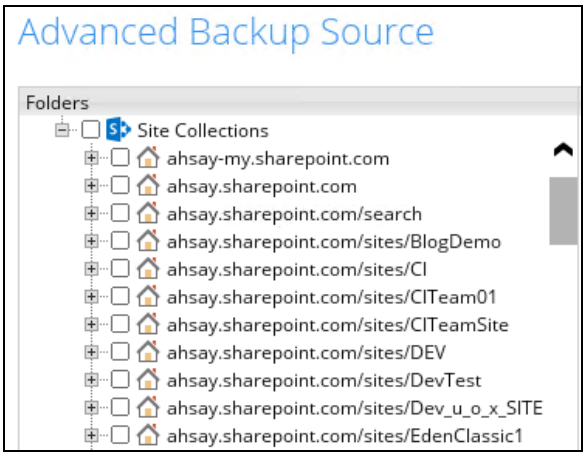
- Users: include Outlook, OneDrive and Personal Sites



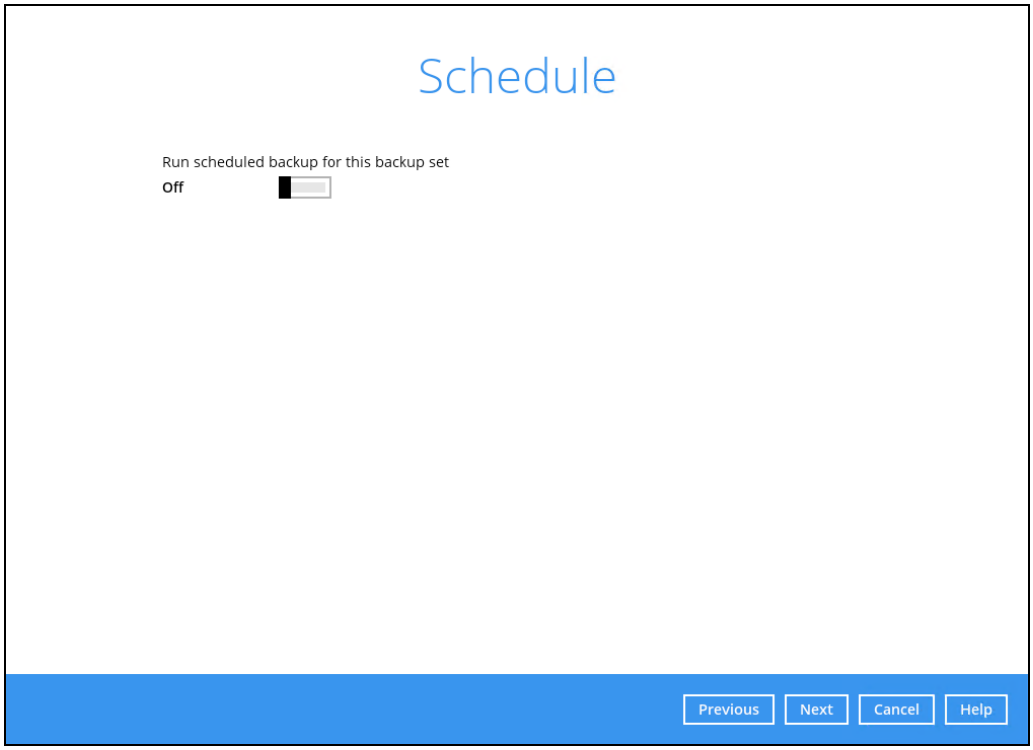
- Public Folders: include public folders

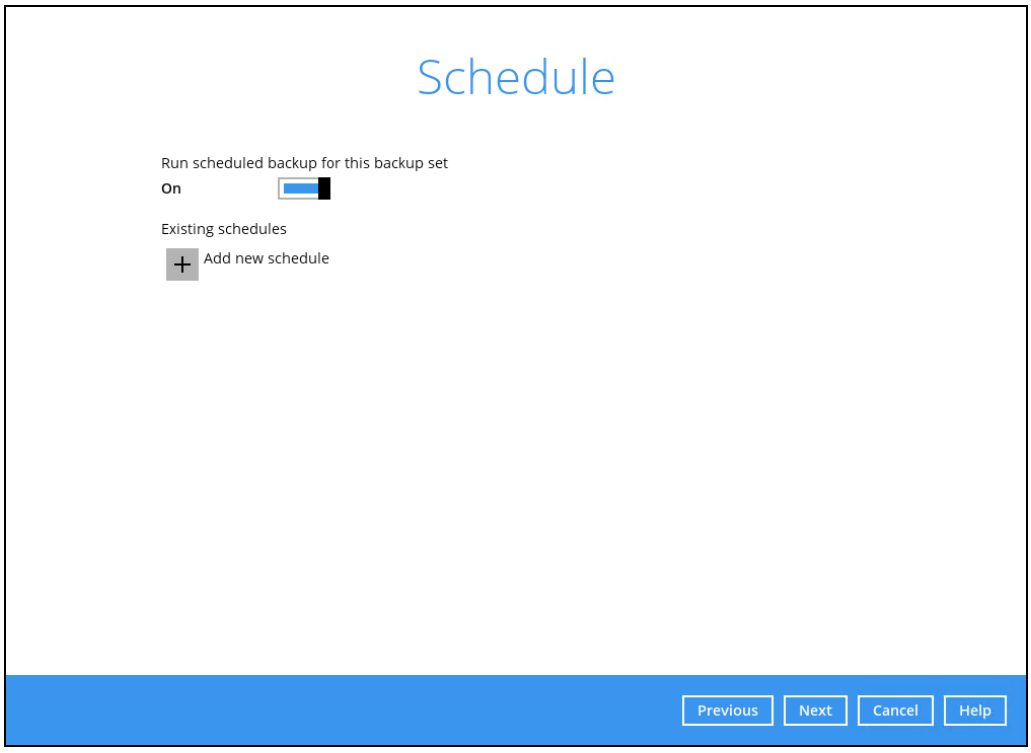


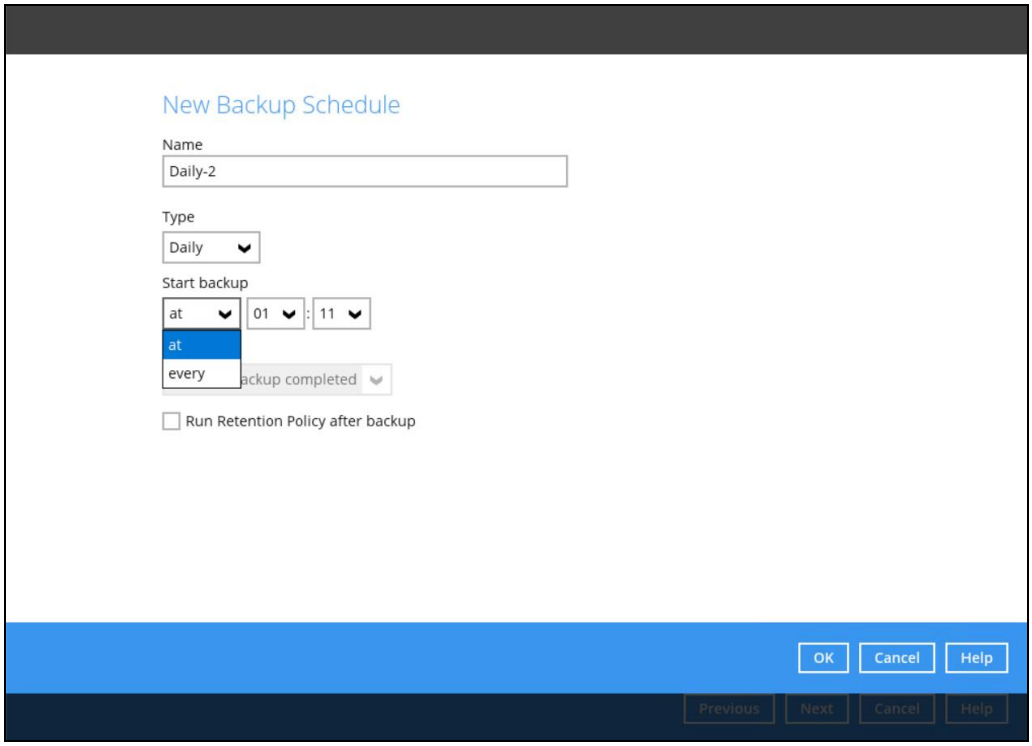
- Site Collections: include Personal Sites and Site Collections



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.

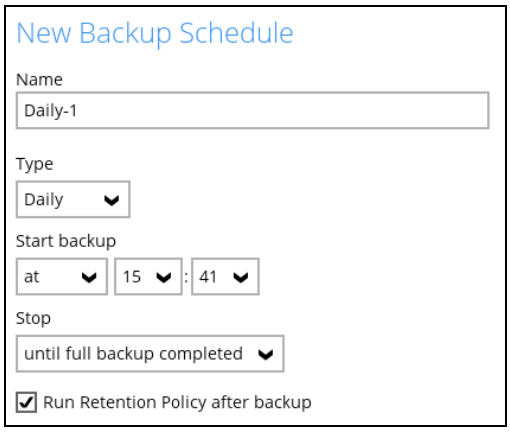




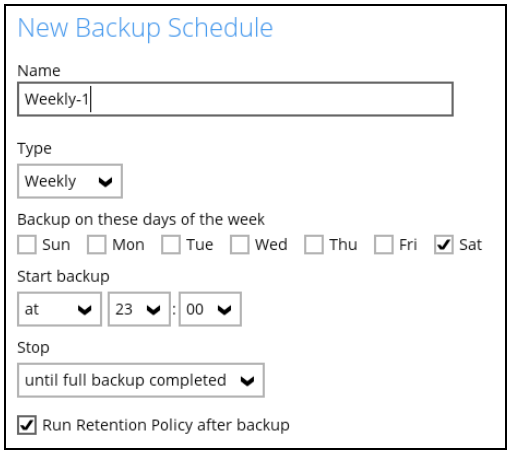


In the New Backup Schedule window, configure the following backup schedule settings.

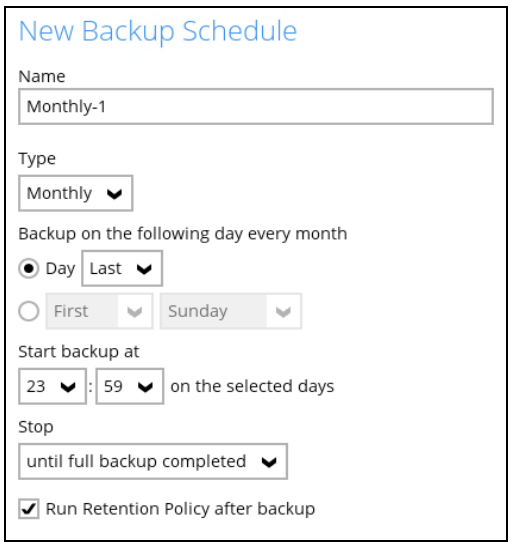
- **Name** – the name of the backup schedule.
- **Type** – the type of the backup schedule. There are four (4) different types of backup schedule: Daily, Weekly, Monthly and Custom.
  - **Daily** – the time of the day when the backup job will run.



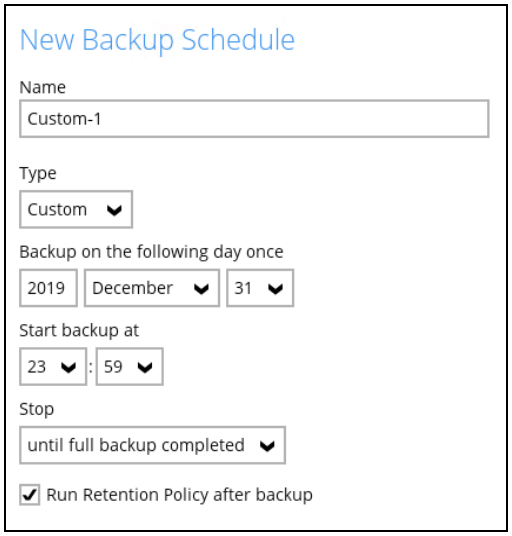
  - **Weekly** – the day of the week and the time of the day when the backup job will run.



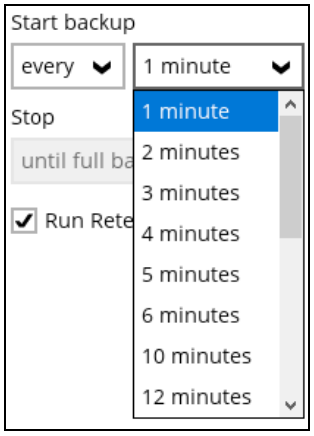
- **Monthly** – the day of the month and the time of the day when the backup job will run.

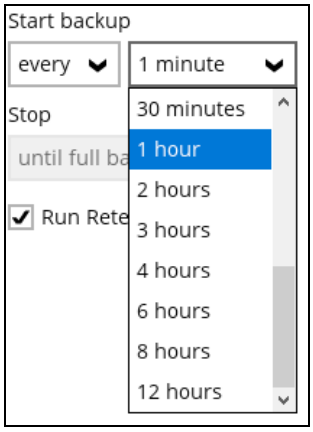


- **Custom** – a specific date and the time when the backup job will run.

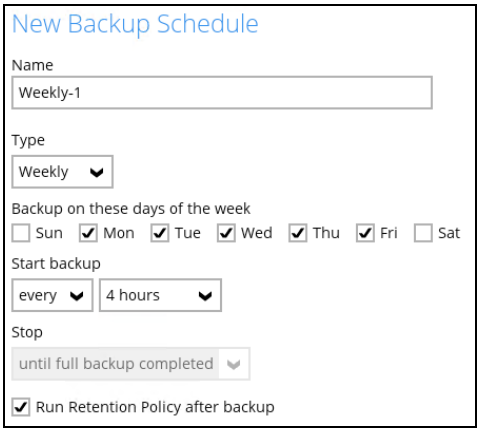


- **Start backup** – the start time of the backup job.
  - **at** – this option will start a backup job at a specific time.
  - **every** – this option will start a backup job in intervals of minutes or hours.





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



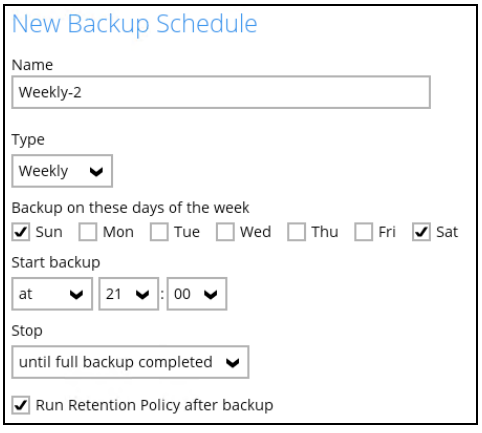


Figure 1.1 ***Figure 1.2***

Figure 1.1 – Periodic schedule every 4 hours Monday - Friday during business hours
Figure 1.2 – Normal schedule run at 21:00 or 9:00 PM on Saturday & Sunday on weekend during 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.

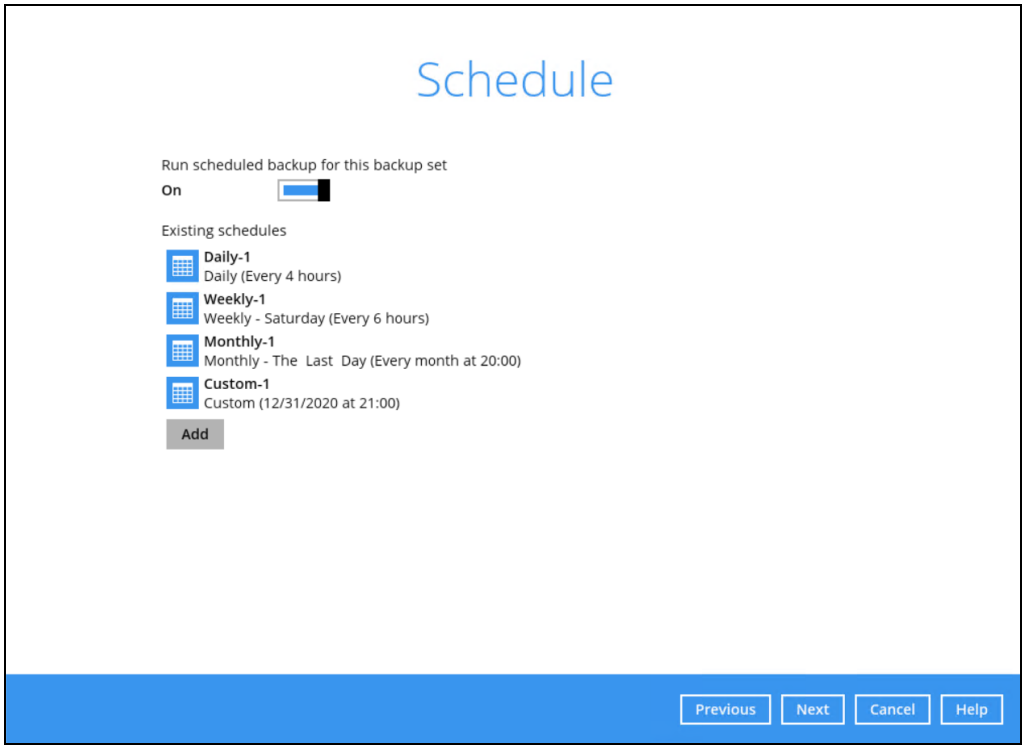
    The partially backed up data will have to be removed by running the data integrity check.

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

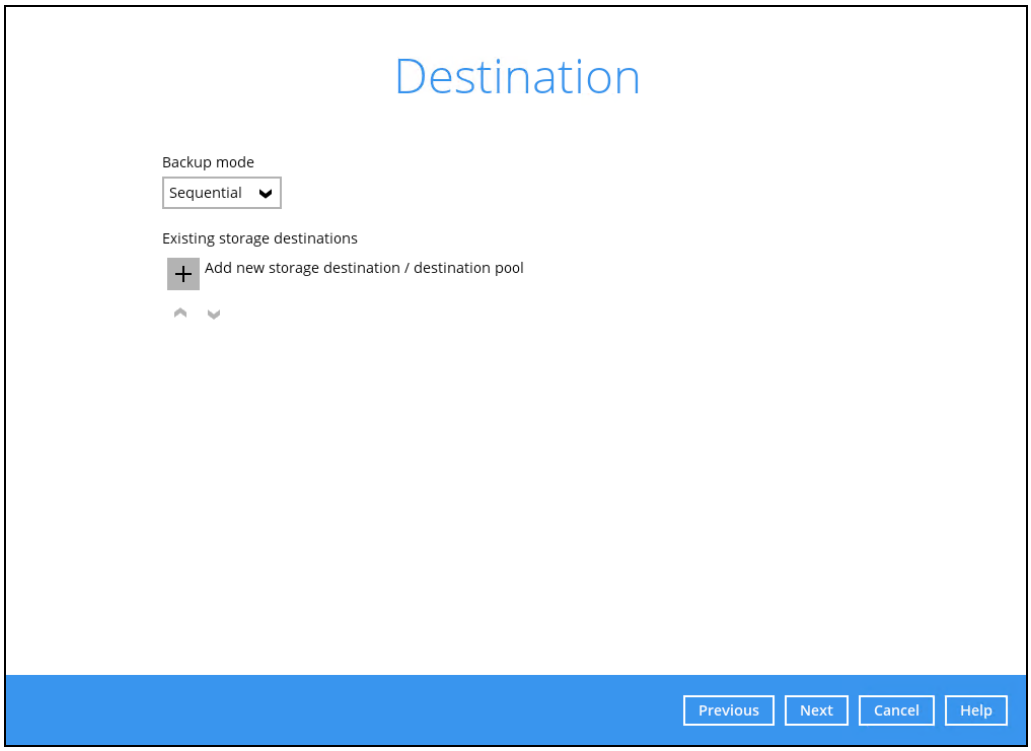
- **Run Retention Policy after backup** – if enabled, the AhsayOBM will run a retention policy job to remove files from the backup destination(s) which have exceeded the retention policy after performing a backup job.

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

Click the **[Next]** button to proceed. Multiple backup schedules can be created.

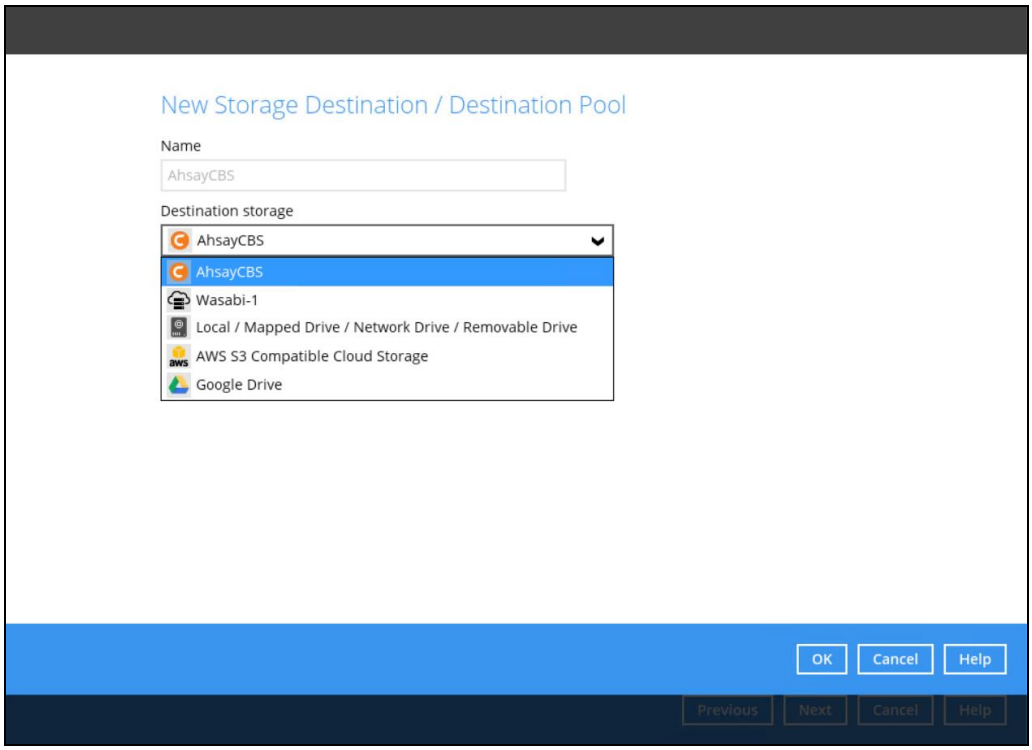


6. In the Destination menu, select a backup destination where the backup data will be stored. Click the "**+**" icon next to **Add new storage destination / destination pool**.



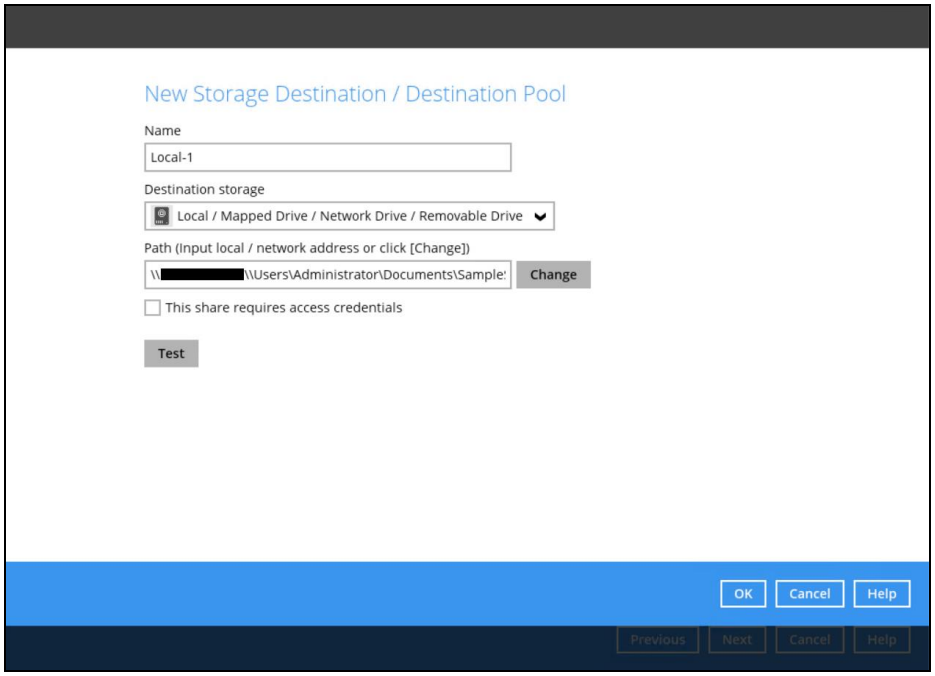
NOTE
For more details on Backup Destination, refer to the following Wiki article for details:
FAQ: Frequently Asked Questions on Backup Destination

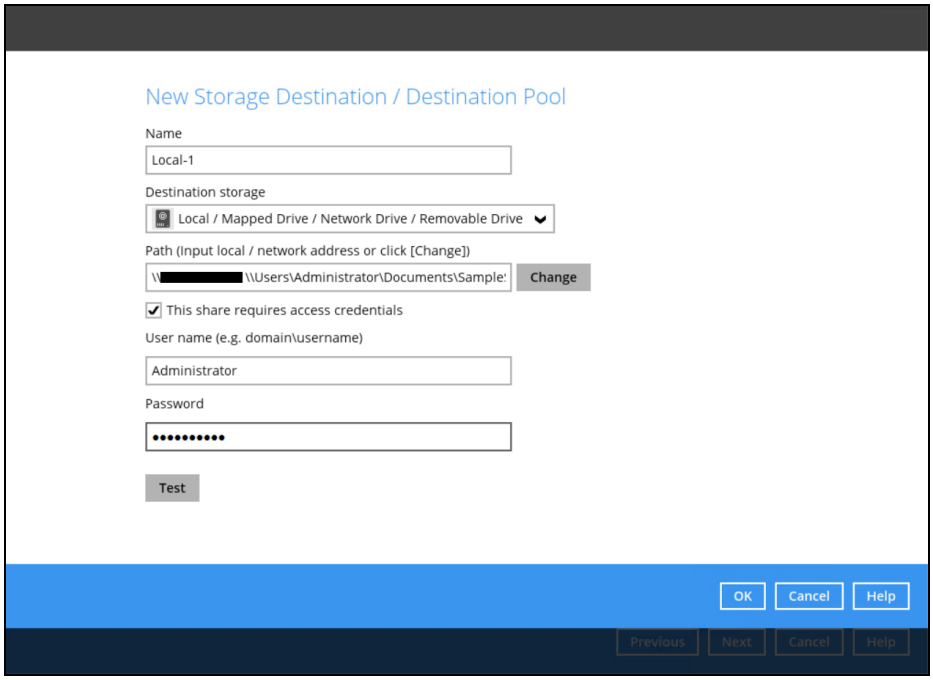
Select storage destinations.

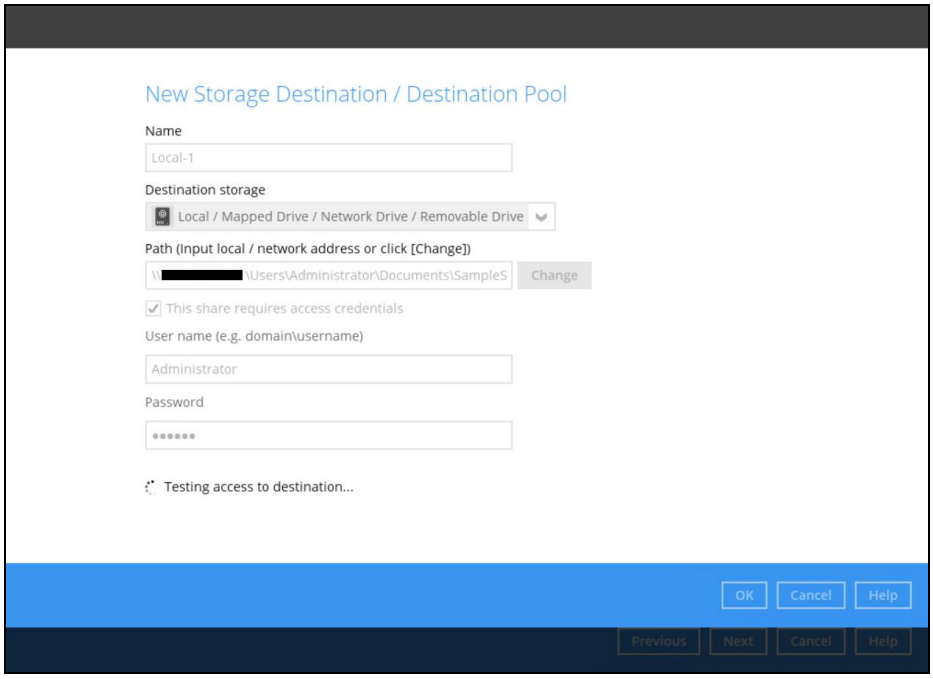


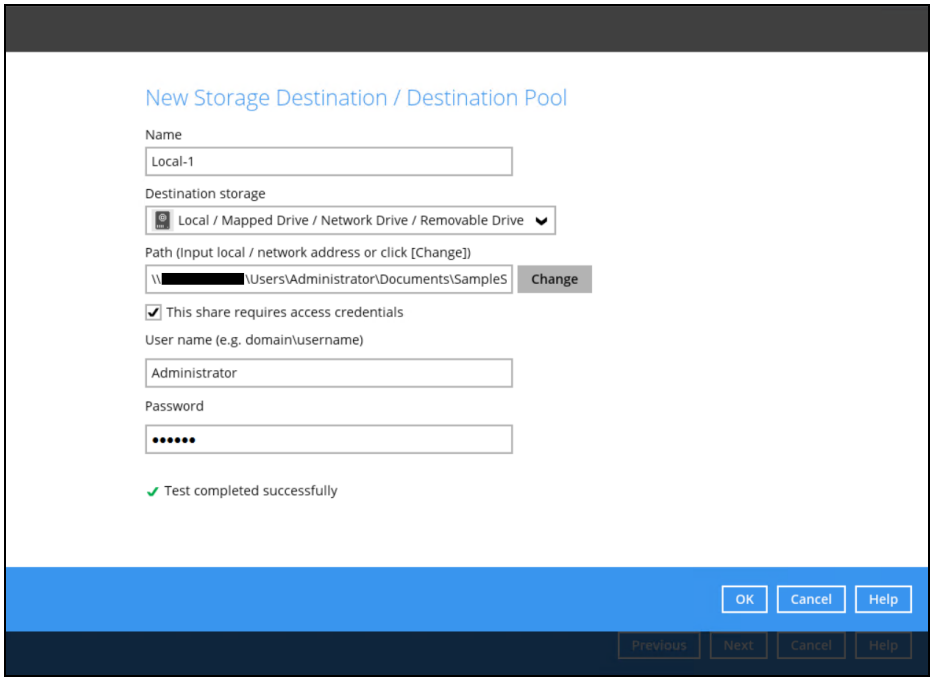
You can choose a storage combination of the Local/Mapped Drive/Network Drive/Removable Drive or Cloud storage. Click **OK** to proceed when you are done with the settings.

- If you have chosen the **Local / Mapped Drive / Network 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.

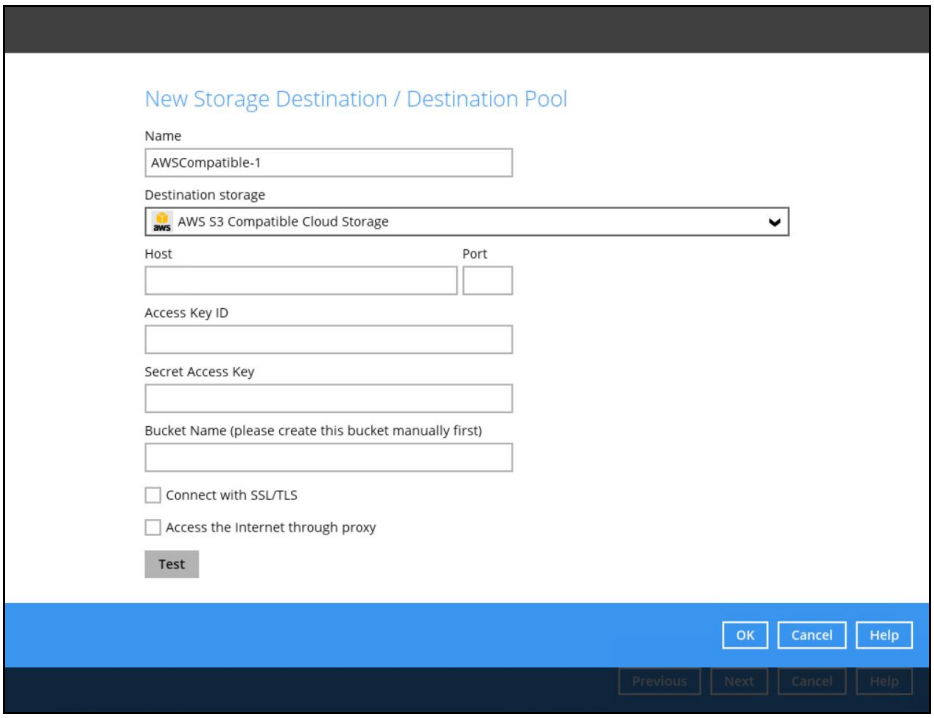


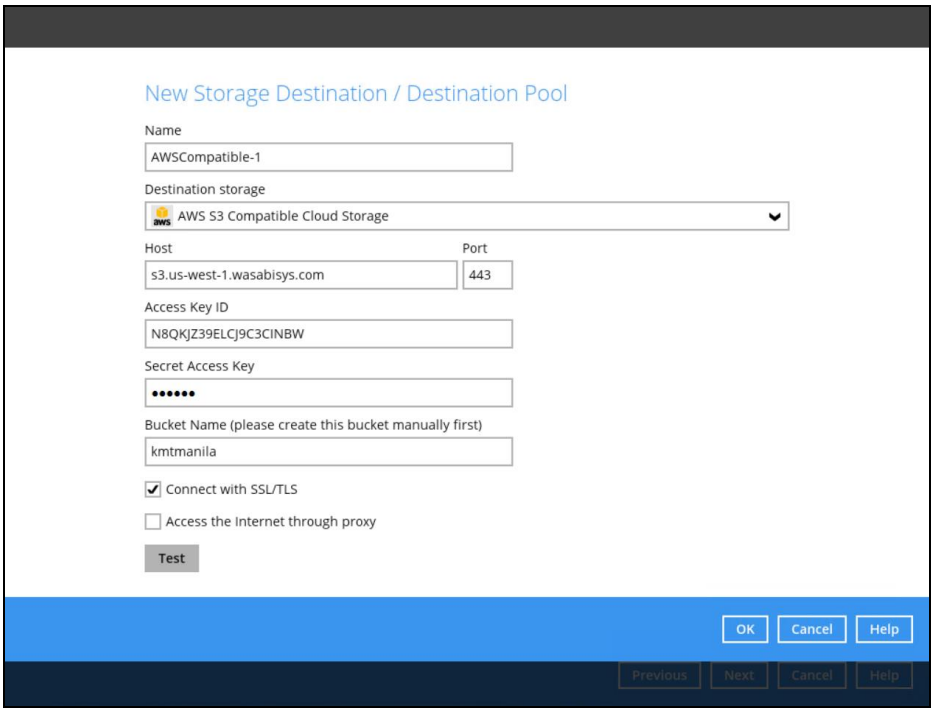


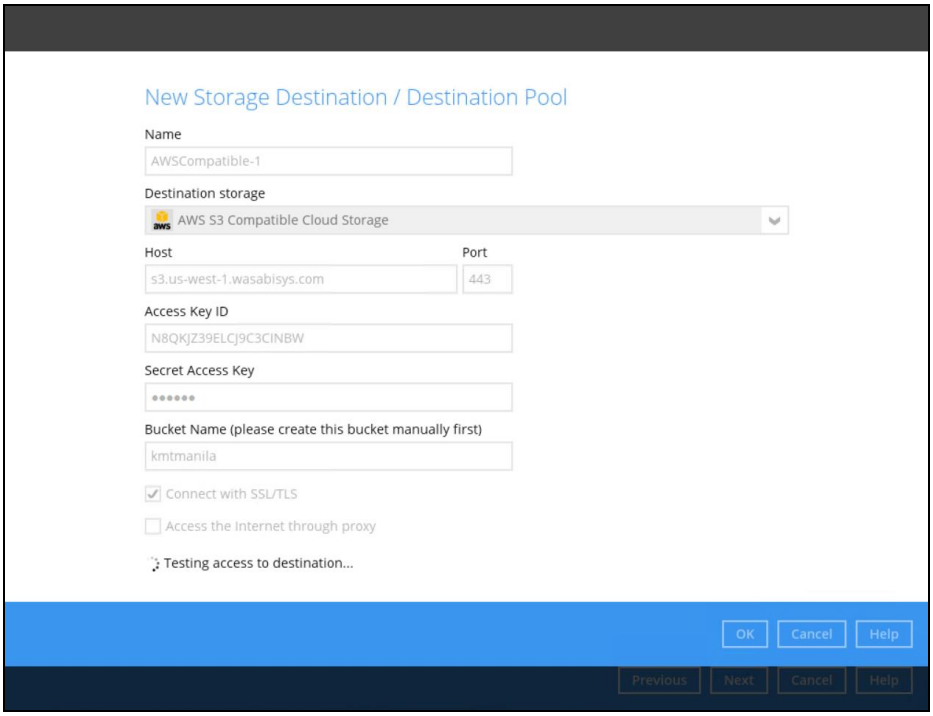

New Storage Destination / Destination Pool
Name
Local-1
Destination storage
Local / Mapped Drive / Network Drive / Removable Drive
Path (Input local / network address or click [Change])
\\[redacted]\Users\Administrator\Documents\SampleS
Change
This share requires access credentials
User name (e.g. domain\username)
Administrator
Password
Testing access to destination...
OK
Cancel
Help
Previous
Next
Cancel
Help

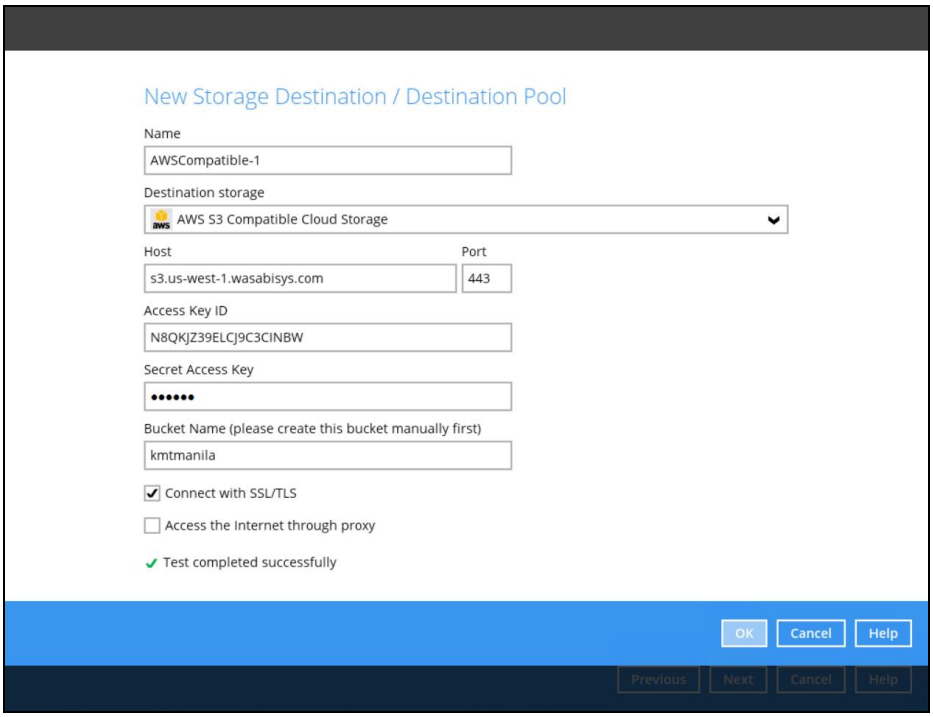

New Storage Destination / Destination Pool
Name
Local-1
Destination storage
Local / Mapped Drive / Network Drive / Removable Drive
Path (Input local / network address or click [Change])
\\[redacted]\Users\Administrator\Documents\SampleS
Change
This share requires access credentials
User name (e.g. domain\username)
Administrator
Password
Test completed successfully
OK
Cancel
Help
Previous
Next
Cancel
Help

- 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.

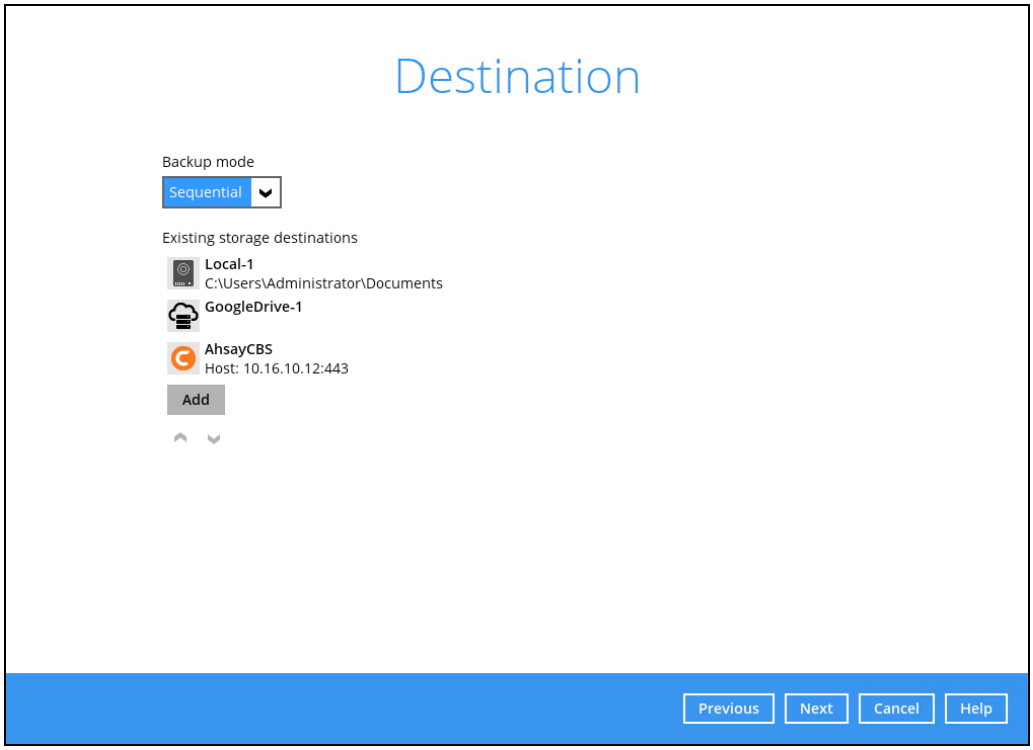


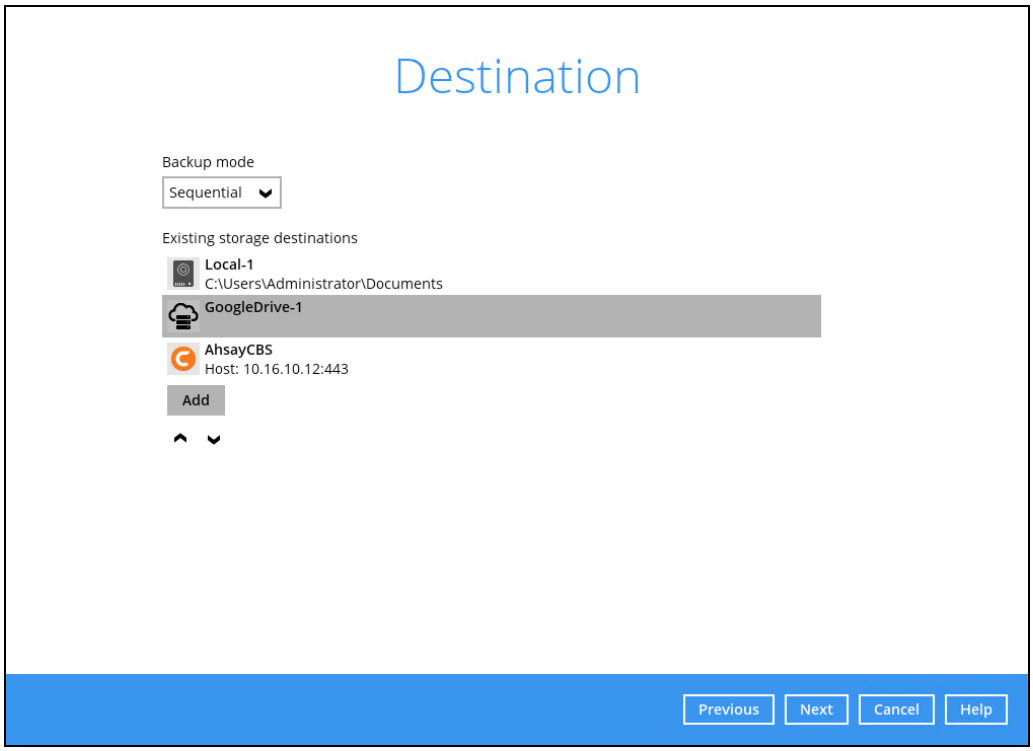




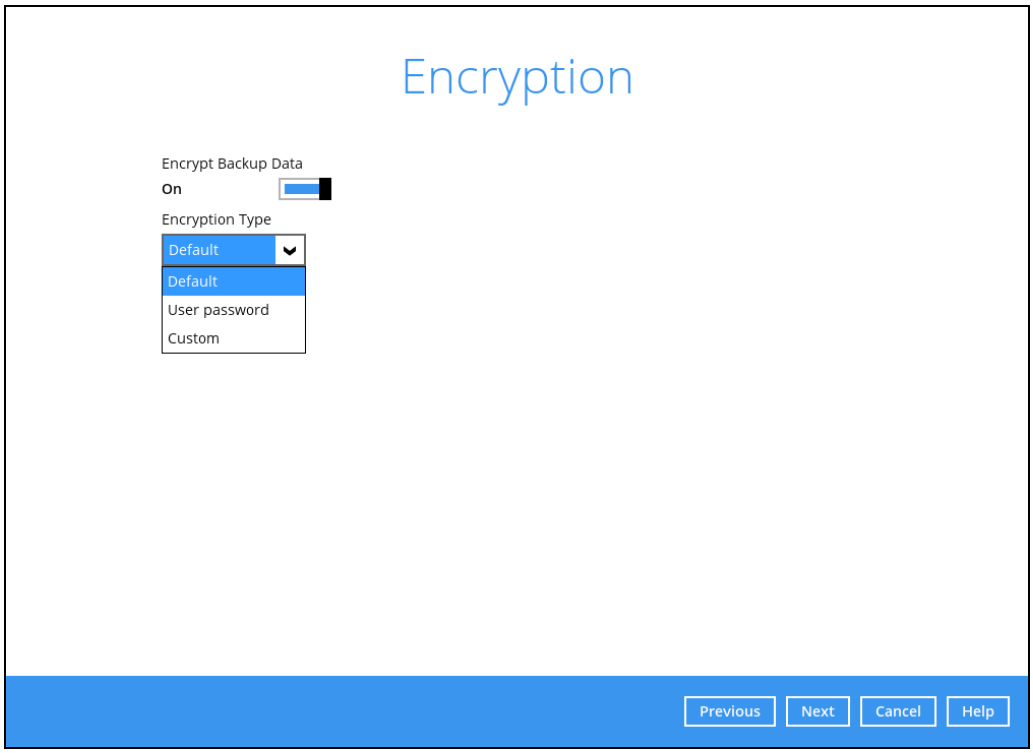


You can add multiple storage destinations. The backup data will be uploaded to all the destinations you have selected in the order you added them. Press the icon to alter the order. Click **Next** to proceed when you are done with the selection.


Destination
Backup mode
Sequential
Existing storage destinations
Local-1
C:\Users\Administrator\Documents
GoogleDrive-1
AhsayCBS
Host: 10.16.10.12:443
Add
Previous
Next
Cancel
Help

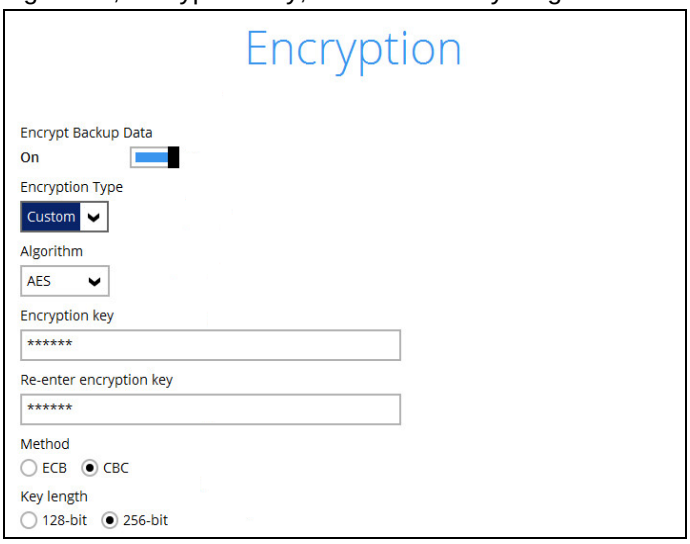

Destination
Backup mode
Sequential
Existing storage destinations
Local-1
C:\Users\Administrator\Documents
GoogleDrive-1
AhsayCBS
Host: 10.16.10.12:443
Add
Previous
Next
Cancel
Help

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 AhsayOBM at the time when this backup set is created. Please be reminded that if you change the AhsayOBM login password later, the encryption keys of the backup sets previously created with this encryption type will remain unchanged.
- **Custom** – you can customize your encryption key, where you can set your own algorithm, encryption key, method and key length.

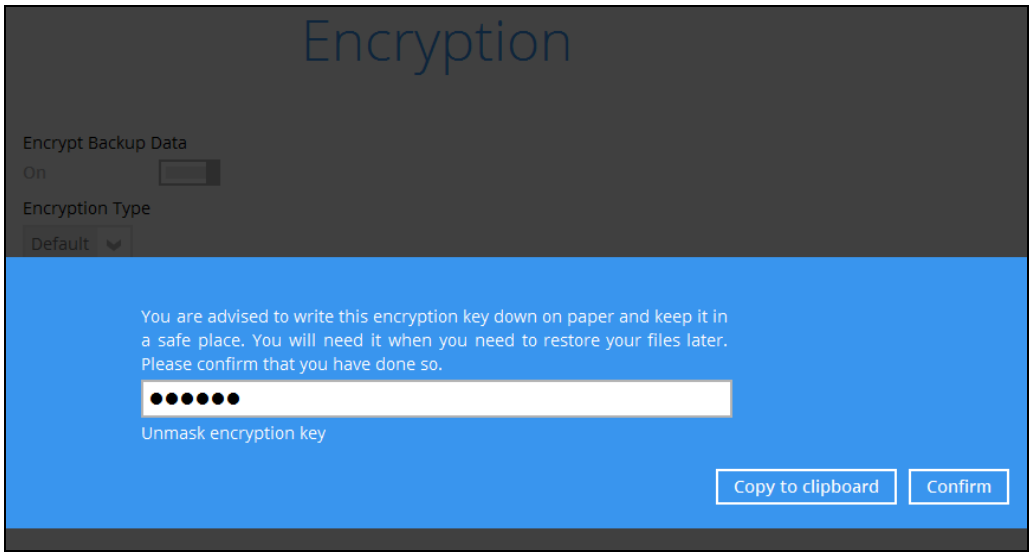


NOTE

For best practice on managing your encryption key, refer to the following Wiki article.
FAQ: Best practices for managing encryption key on AhsayOBM or AhsayACB?

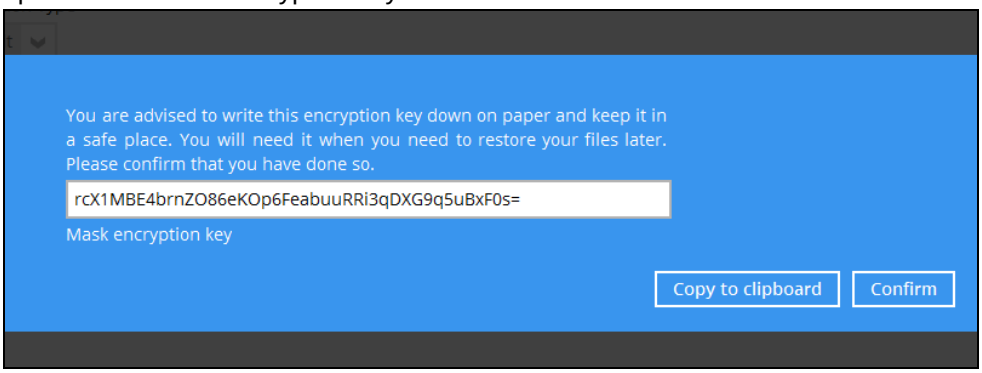
Click Next when you are done setting.

8. 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.



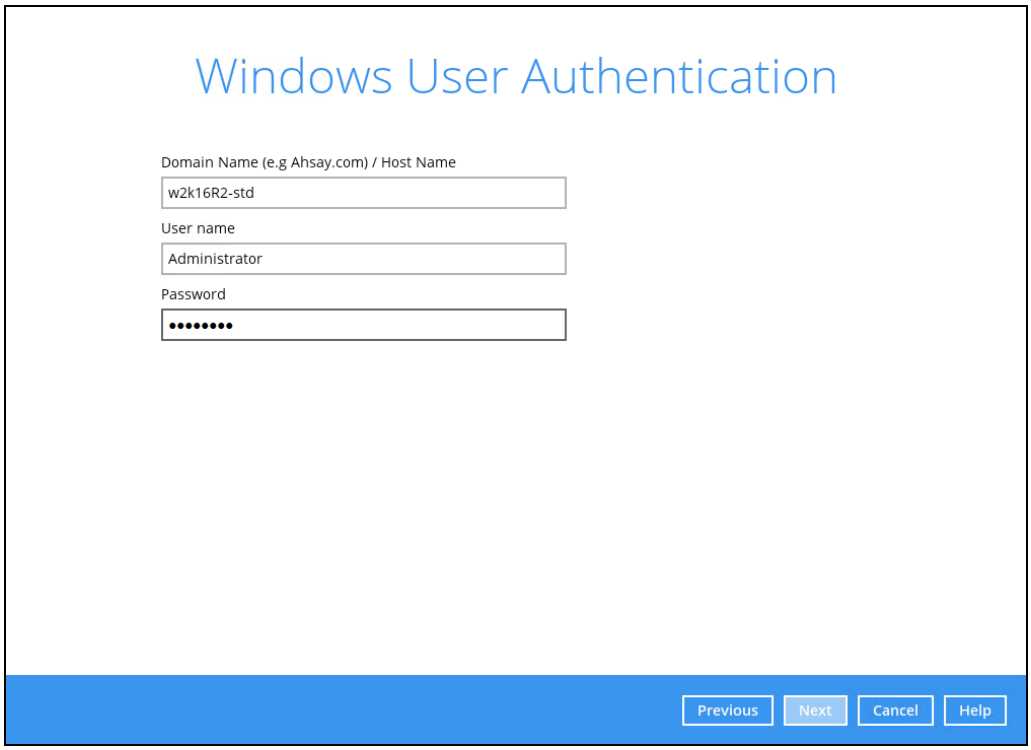
The pop-up window has the following three options to choose from:

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



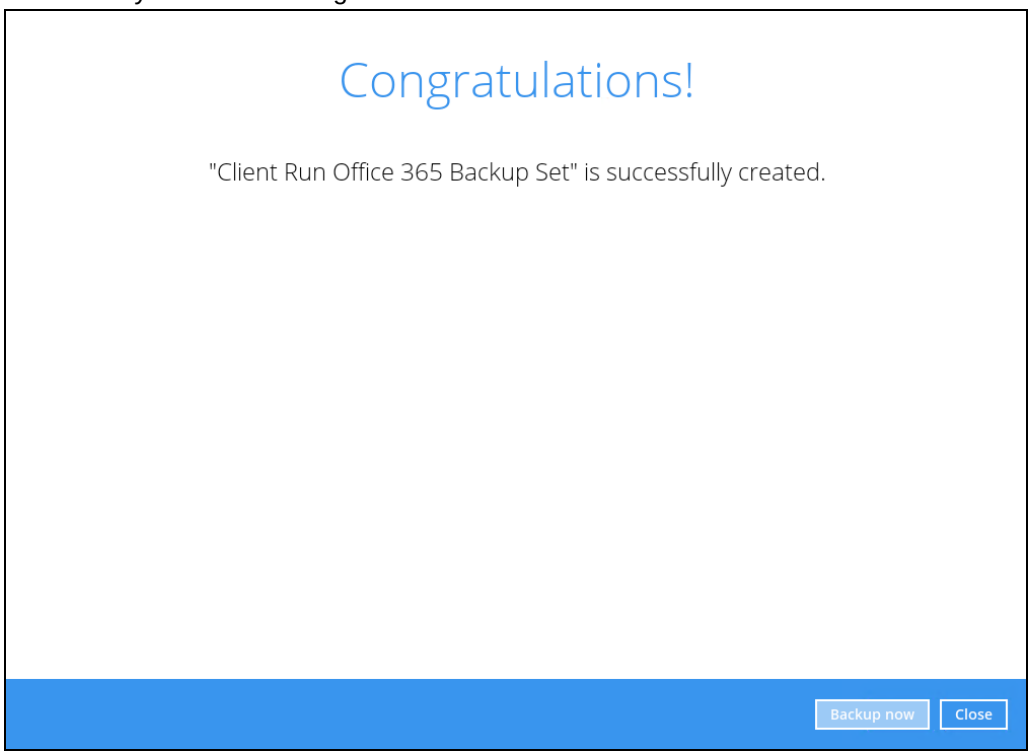
- **Copy to clipboard** – Click to copy the encryption key, then you can paste it in another location of your choice.
- **Confirm** – Click to exit this pop-up window and proceed to the next step.

9. If you have enabled the scheduled backup option, you will be prompted to enter the **User Name** and **Password** of the Windows account that will be running the backup.



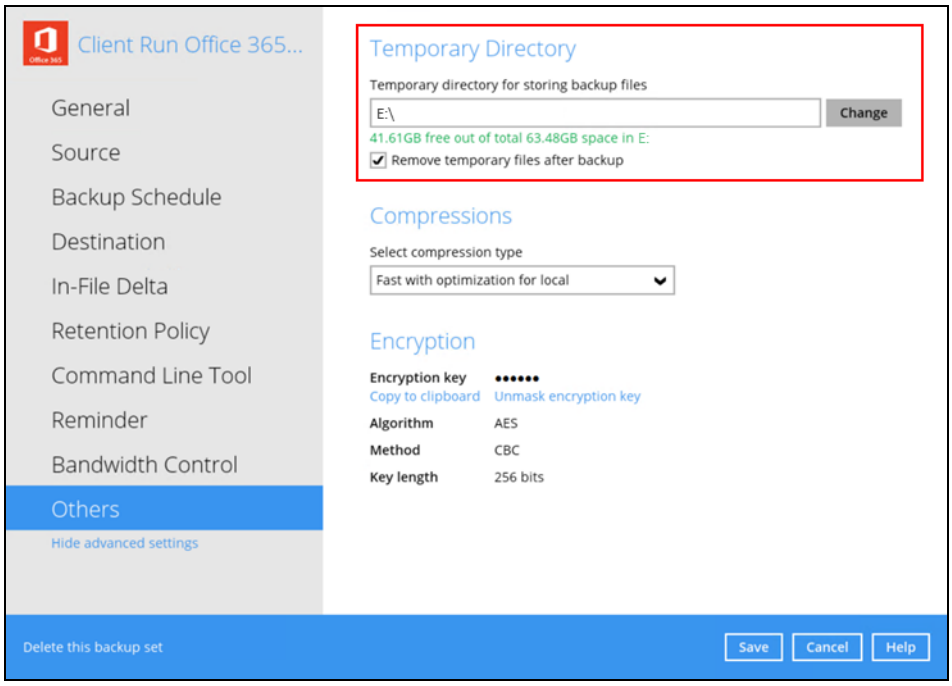
Click Next to create the backup set.

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



11. 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 Dive C.

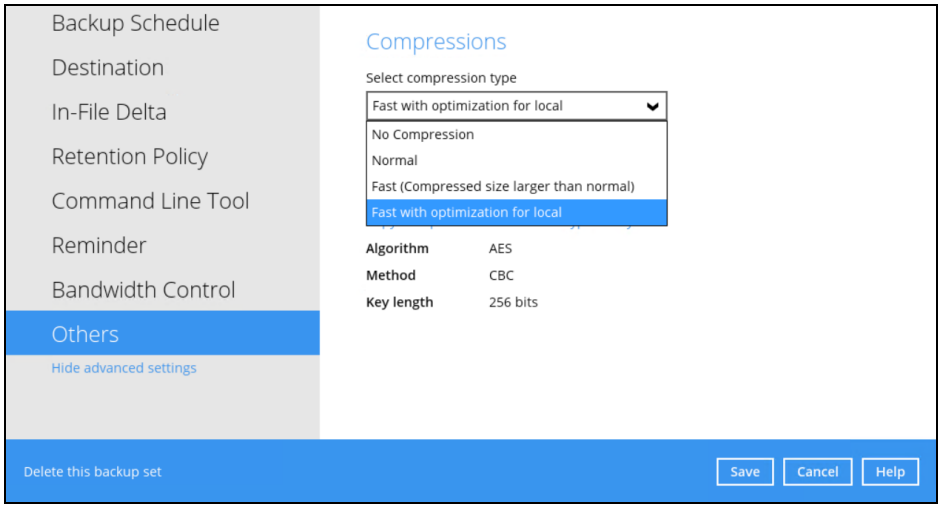
    Go to **Others** > **Temporary Directory**. Click **Change** to browse for another location.



12. 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:

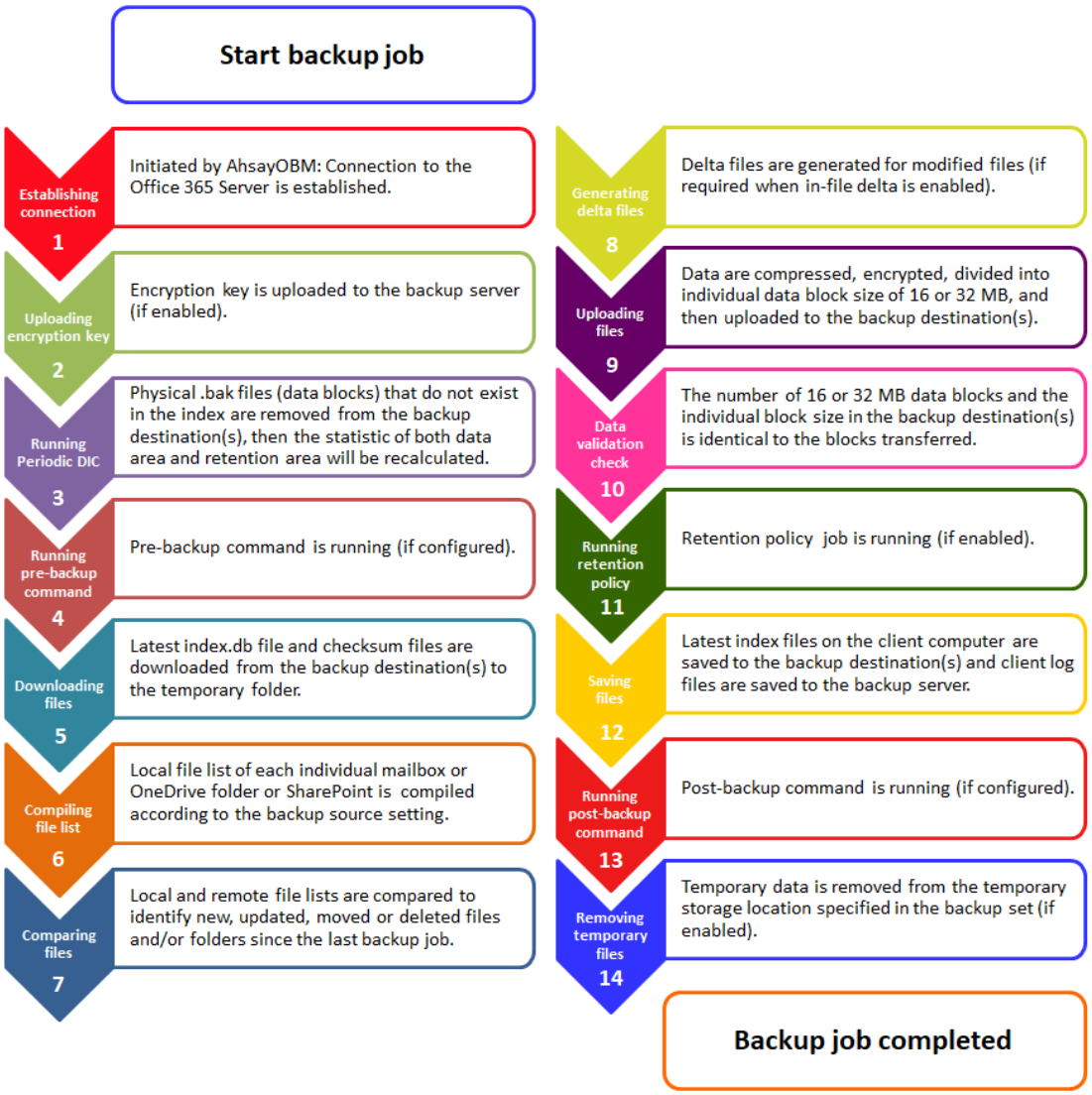
    - No Compression
    - Normal
    - Fast (Compressed size larger than normal)
    - Fast with optimization for local



5 Overview of Office 365 Backup Process

The following steps are performed during a backup job. For an overview of the detailed process for Steps **3**, **5**, **10**, and **12,** refer to the following chapters:

- Periodic Data Integrity Check (PDIC) Process **(Step 3)**
- Backup Set Index Handling Process
  - Start Backup Job **(Step 5)**
  - Completed Backup Job **(Step 12)**
- Data Validation Check **(Step 10)**



5.1 Periodic Data Integrity Check (PDIC) Process

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

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

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

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

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

NOTE: The PDIC schedule cannot be changed.

Example:

Backup set ID: 1594627447932

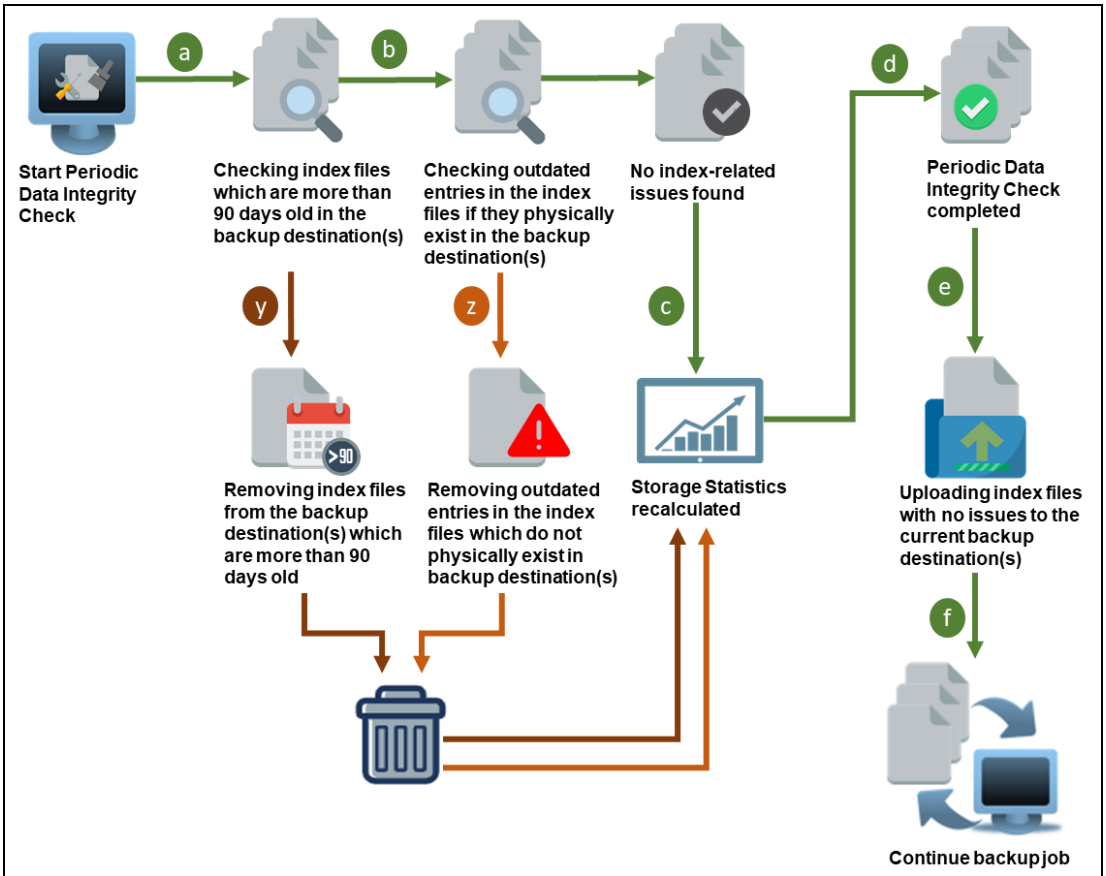
Calculation*:* 1594627447932 *mod 5* = ***2***

2	**Wednesday**

In this example:

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

NOTE
Although according to the PDIC formula for determining the schedule is ***%BackupSetID% mod 5***, this schedule only applies if the previous PDIC job was actually run more than 7 days prior. Under certain conditions, the PDIC may not run strictly according to this formula. For example: 1. If AhsayOBM was upgraded to v8.5 (or above) from an older version v6, v7, or pre-8.3.6.0 version. In this case, the PDIC job will run on the first backup job after upgrade. 2. If backup jobs for a backup set are not run on a regular daily backup schedule (for example: on a weekly or monthly schedule), then the PDIC job will run if it detects that the previous PDIC job was run more than 7 days ago.



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

→ If **YES**, proceed to y

→ If **NO**, proceed to b

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

→ If **YES**, proceed to c

→ If **NO**, proceed to z

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

d Periodic Data Integrity check is completed.

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

f The backup job process will continue.

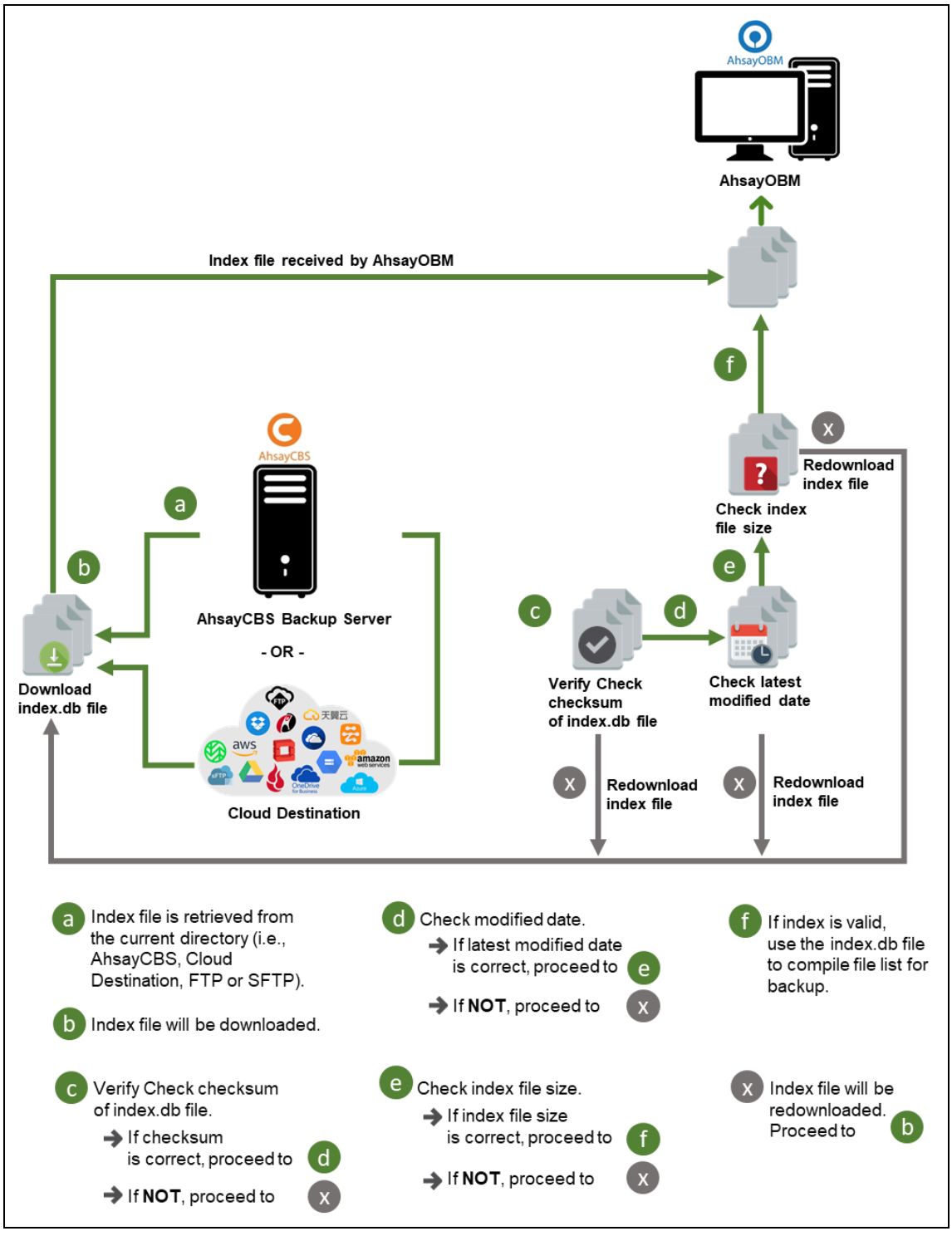
y Index files which are more than 90 days old will be removed from the backup destination(s).

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

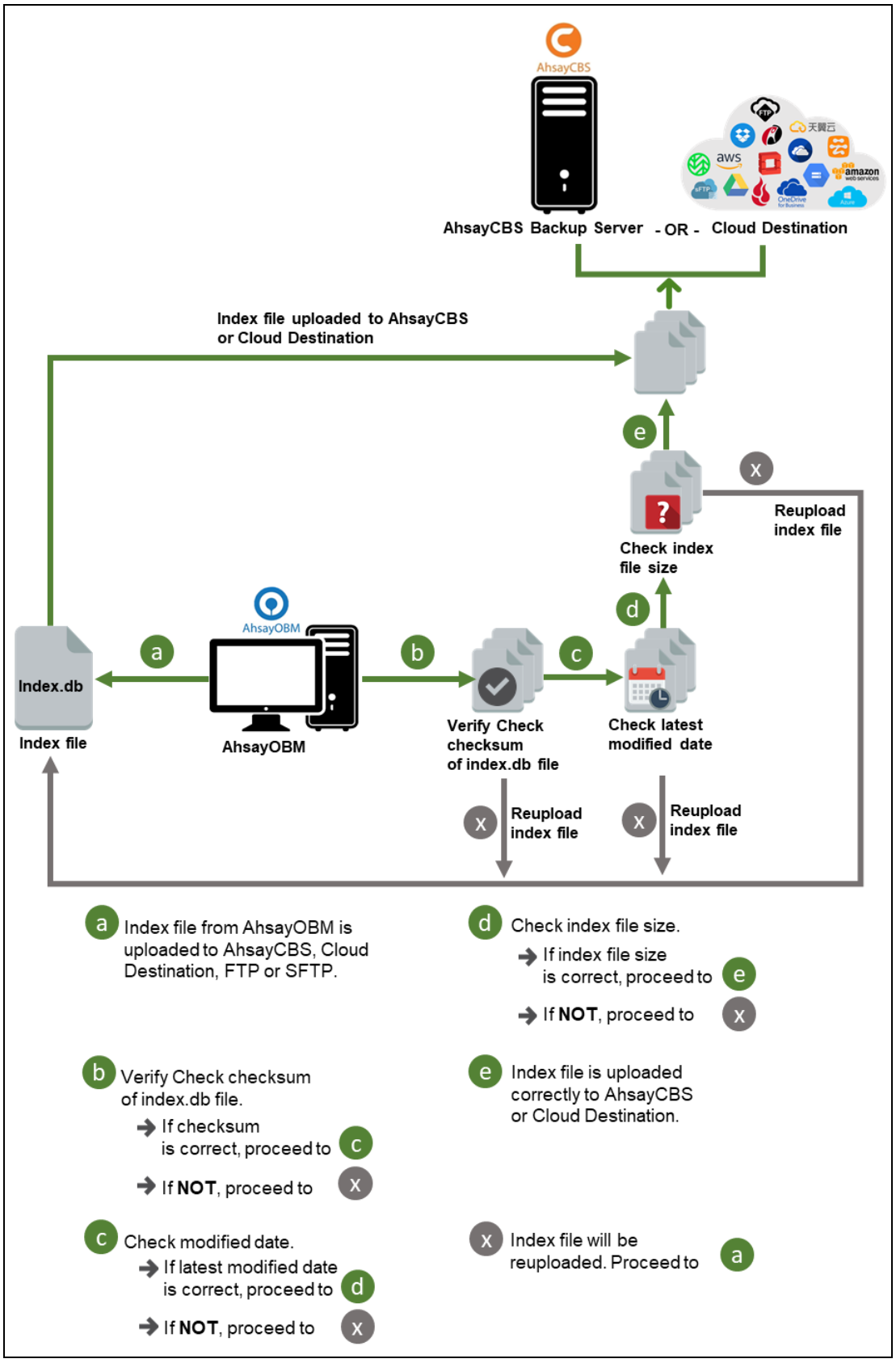
5.2 Backup Set Index Handling Process

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

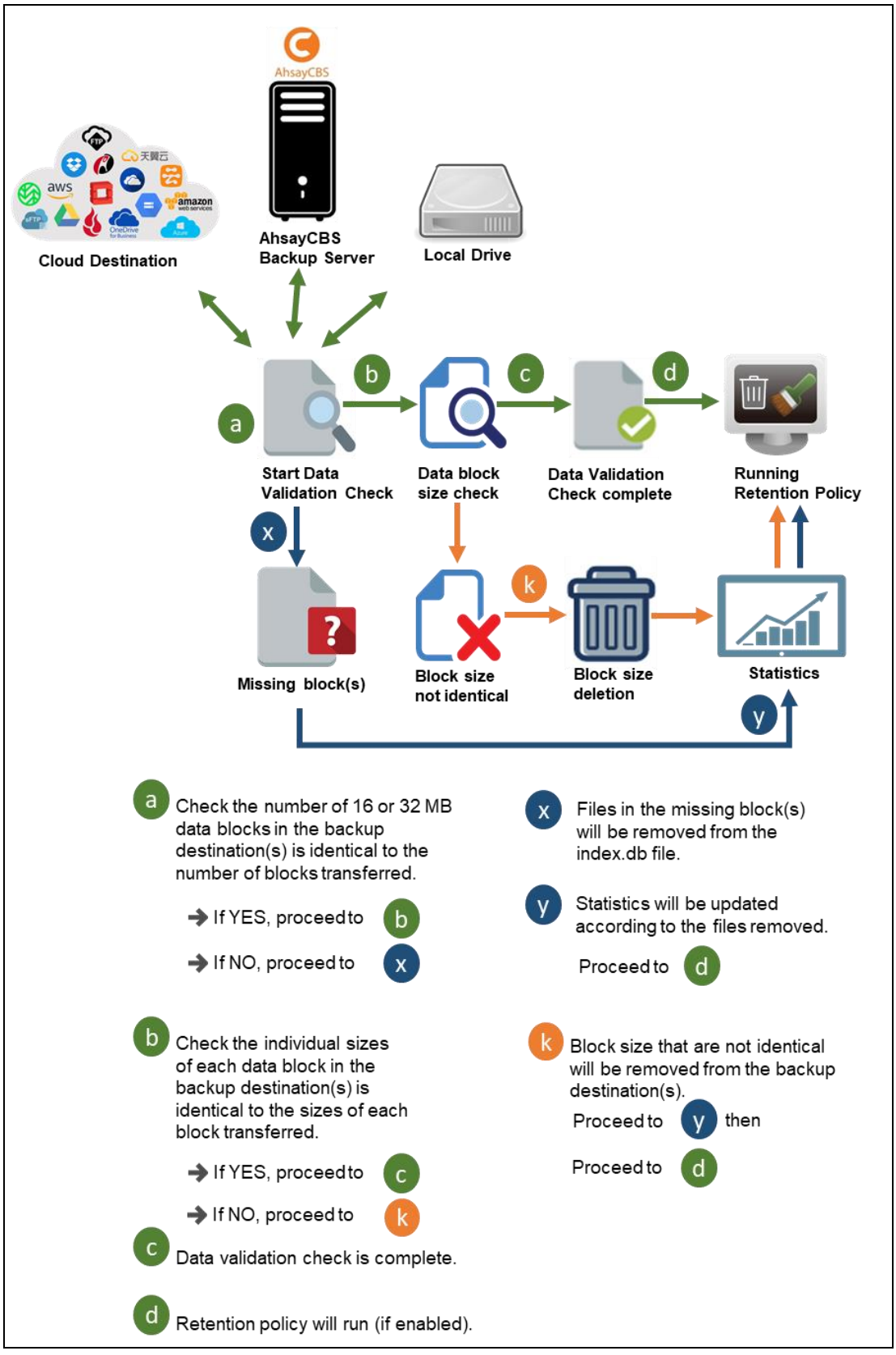


5.2.2 Completed Backup Job



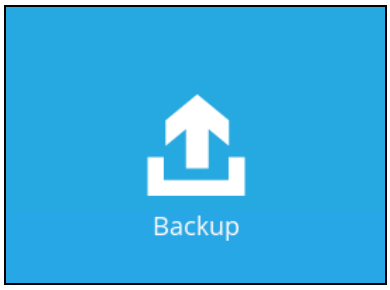
5.3 Data Validation Check Process

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.

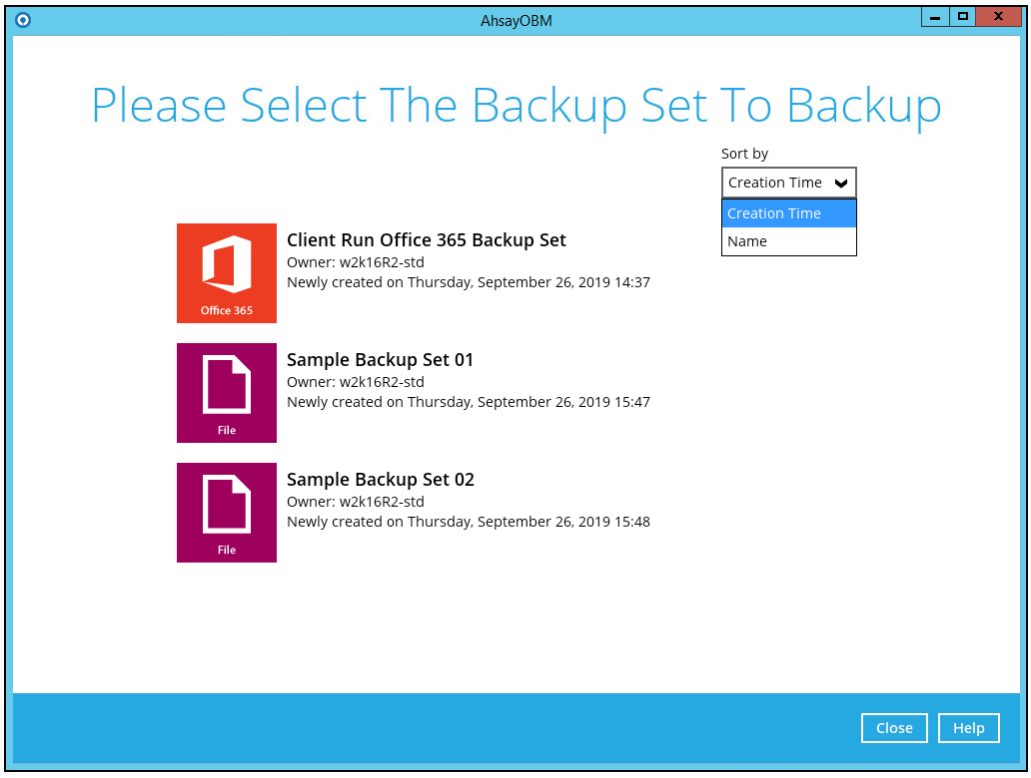


6 Running Backup Job

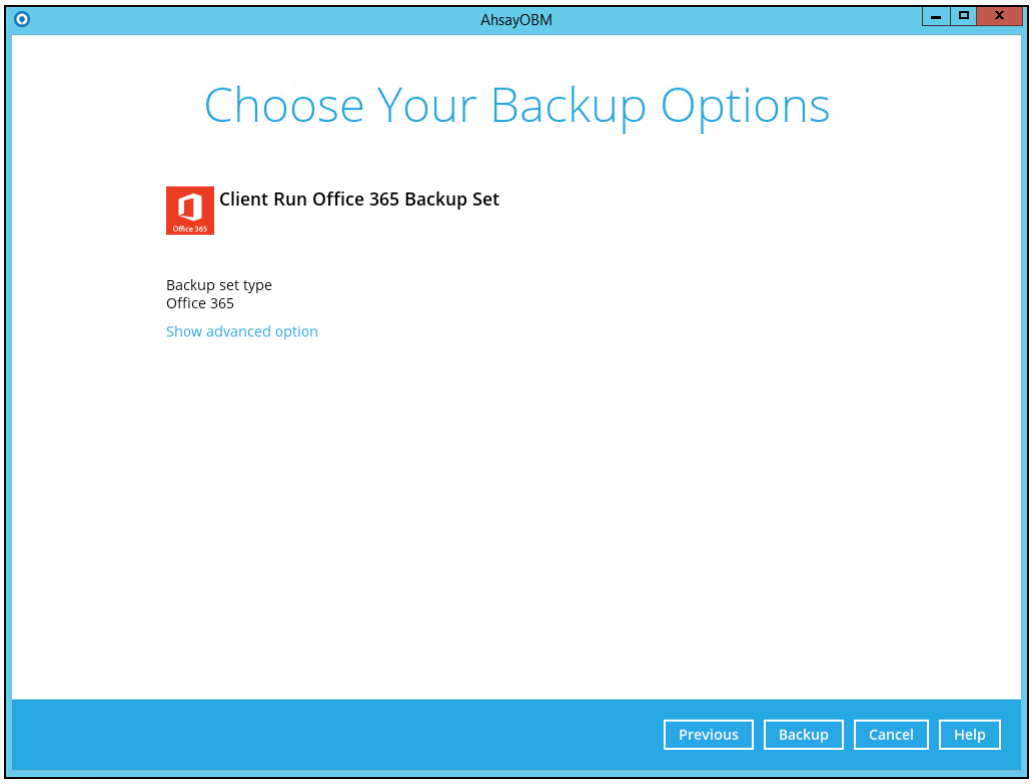
1. Login to AhsayOBM according to the instructions in Login to AhsayOBM.
2. Click the **Backup** icon on the main interface of AhsayOBM.

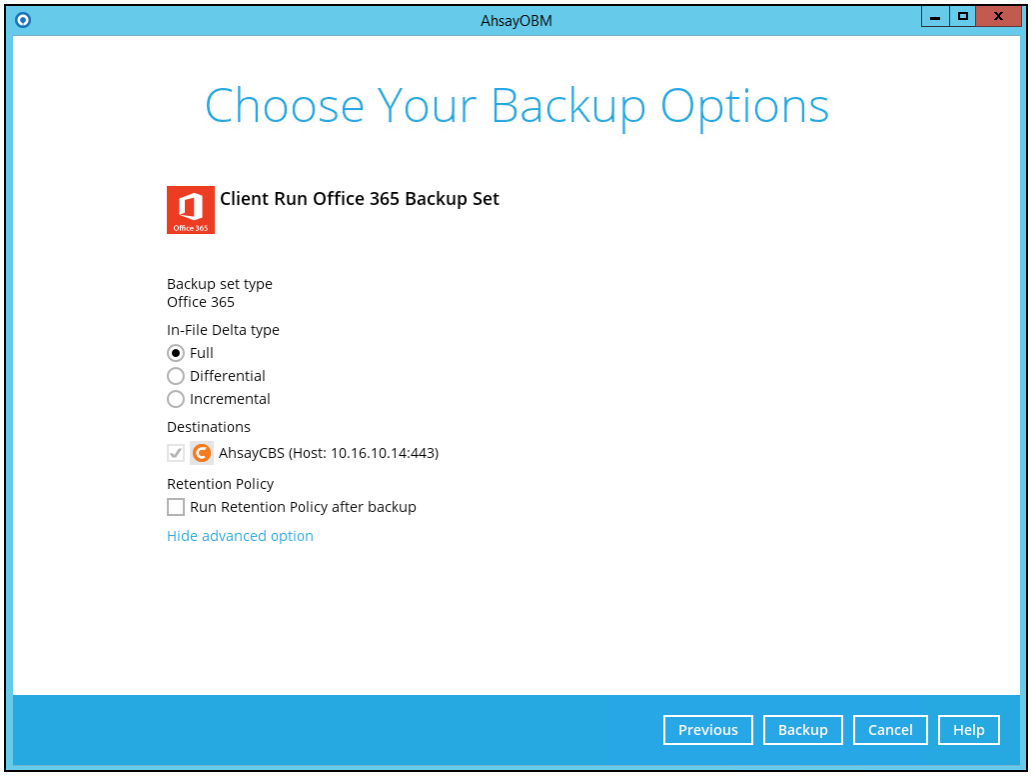


3. Backup sets can be sorted by Name or by Creation Time. By default, it is sorted by Name. Select the backup set which you would like to start a backup for. In case you want to modify the In-File Delta type, Destinations and Retention Policy settings, click **Show advanced option**.

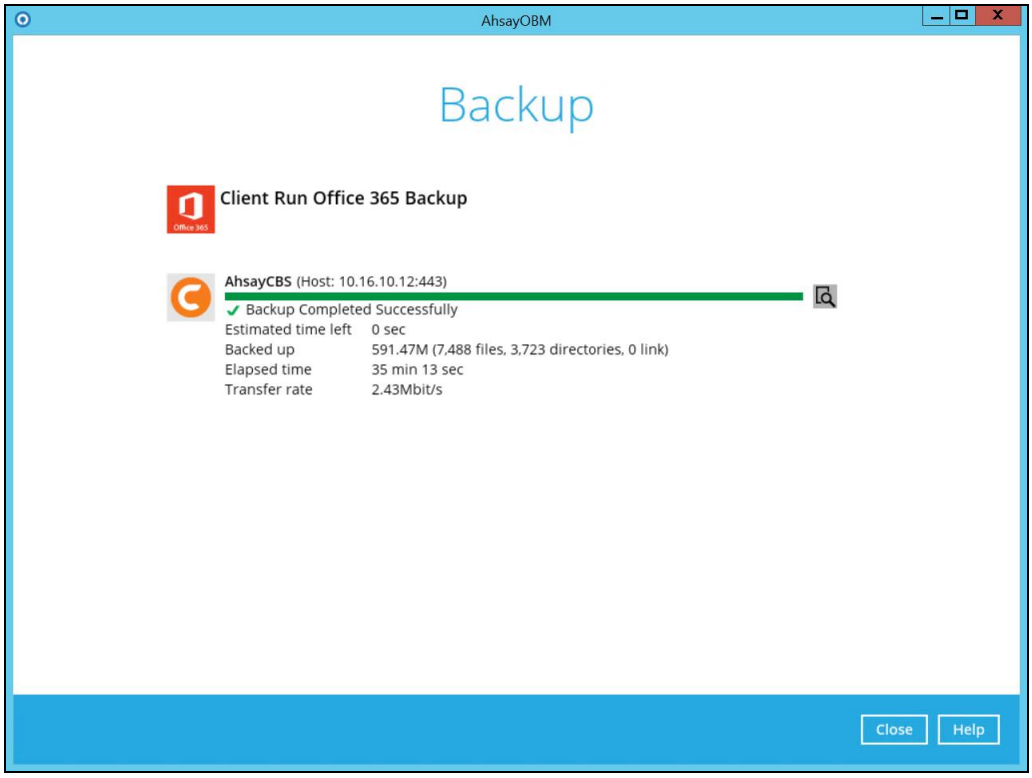


4. If you would like to modify the In-File Delta type, Destinations and Retention Policy Settings, click **Show advanced option**.

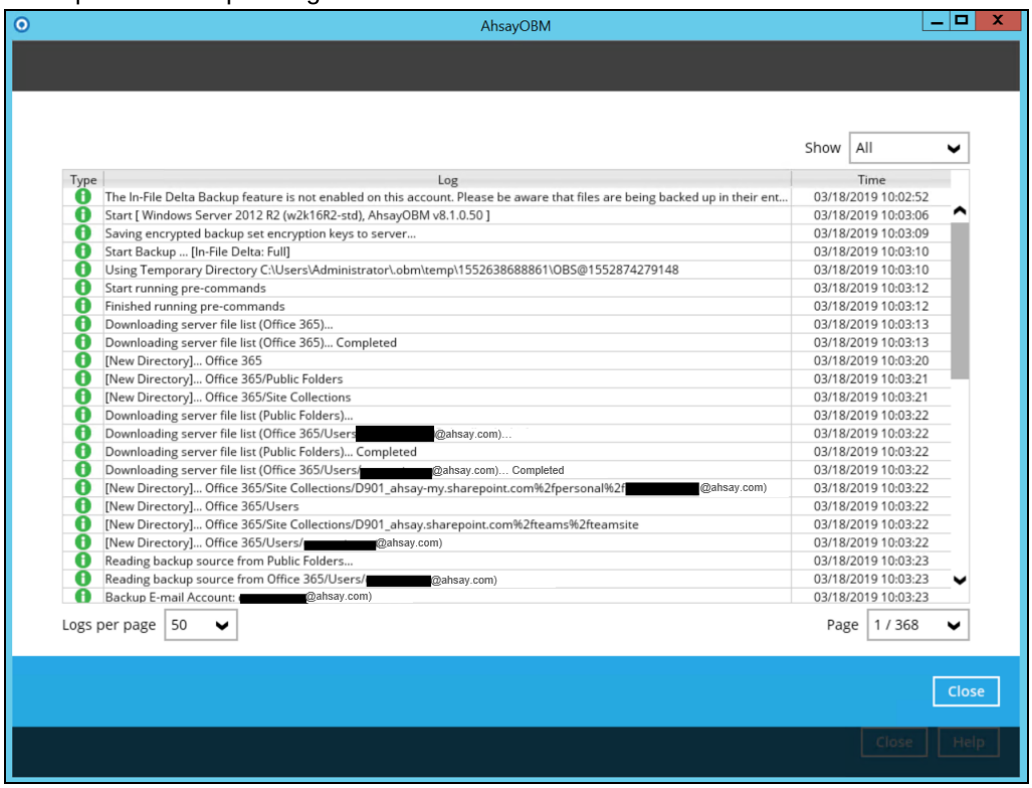




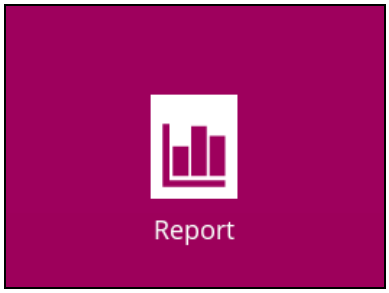
5. Click **Backup** to start the backup and wait until the backup is finished.



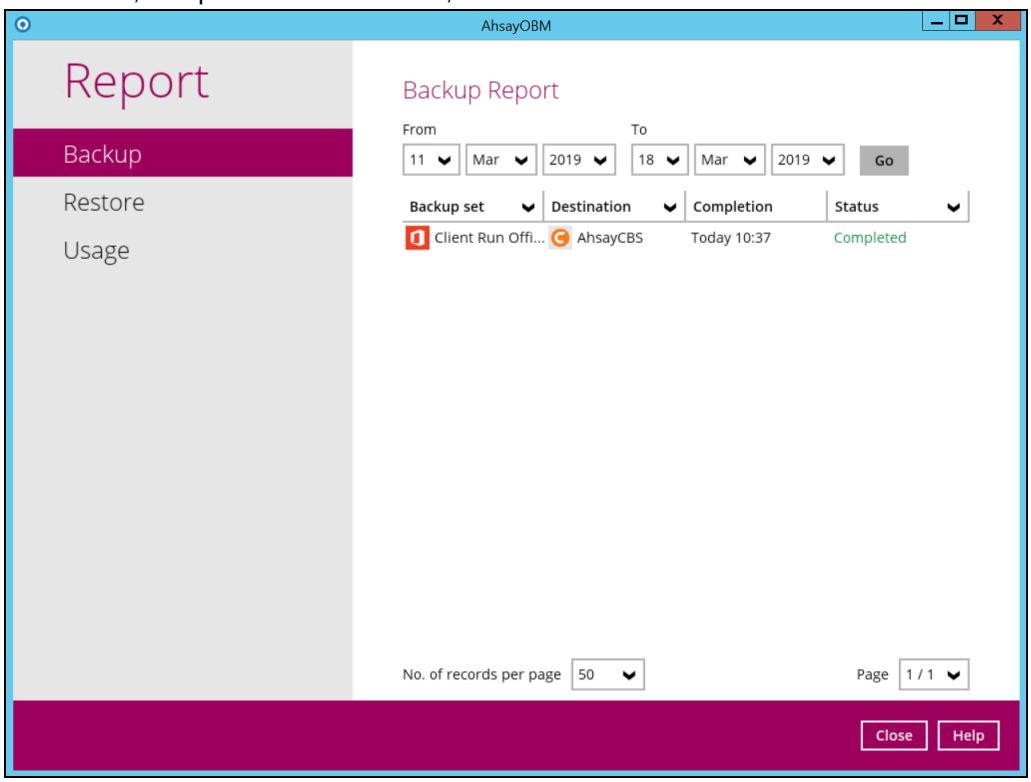
6. Check the log of your back up by clicking this icon . It will show you the log of your backup with corresponding date and time.



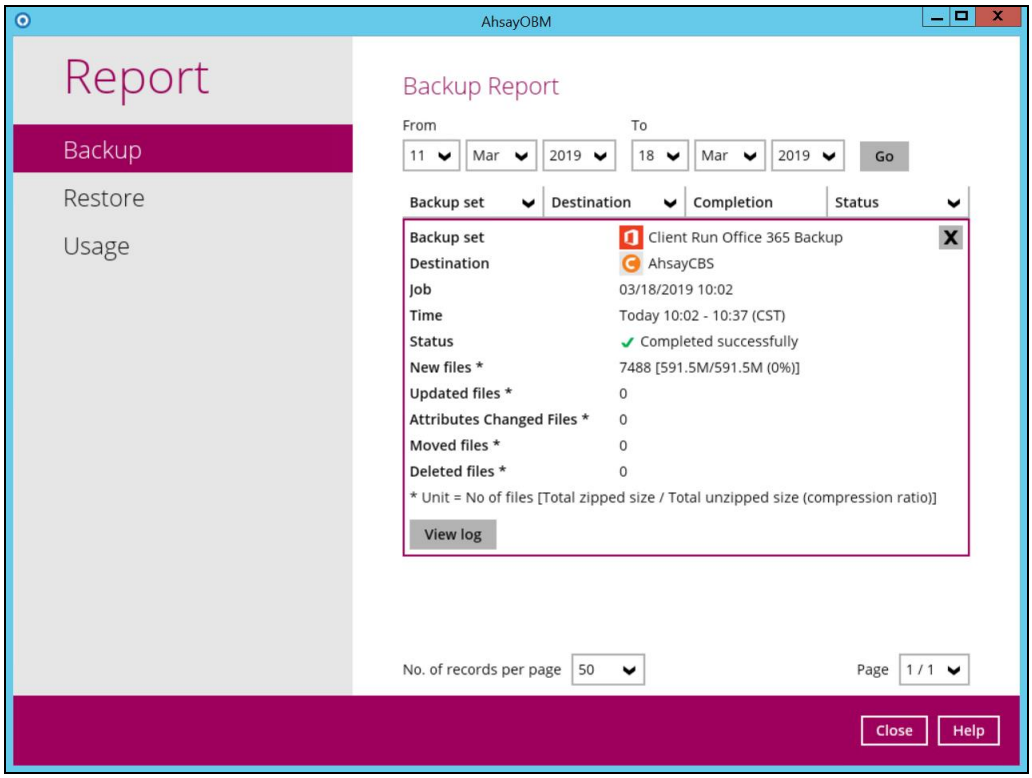
To view the report, go to the **Report > Backup**

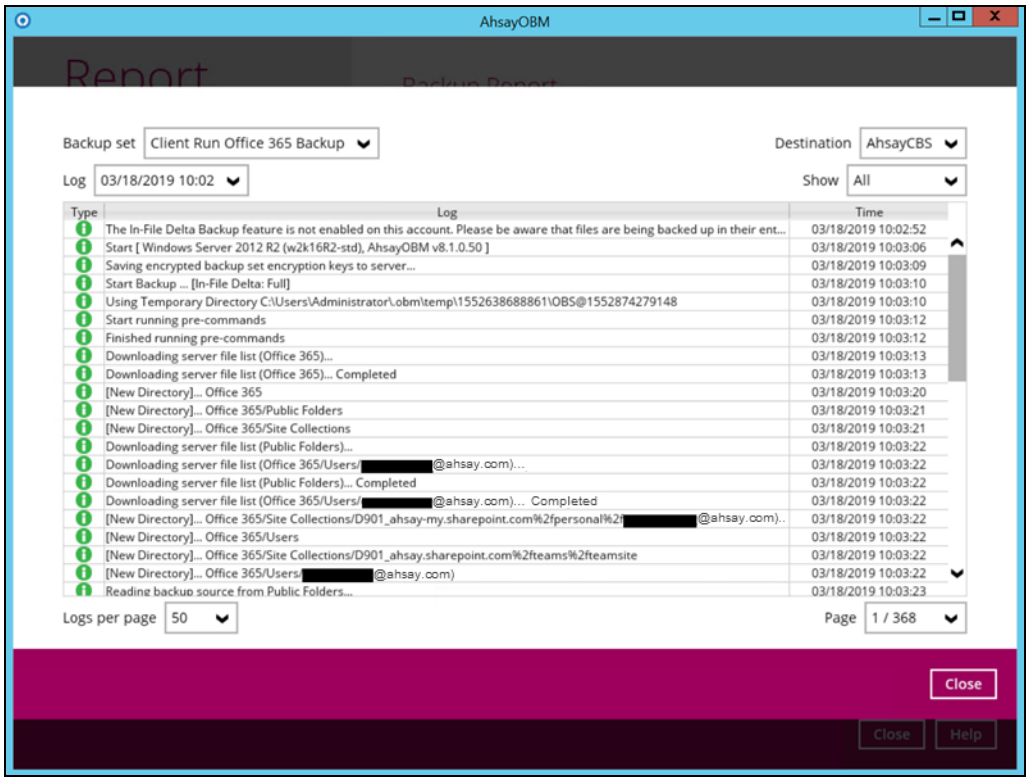


In this Backup Report screen, you can see the backup set with corresponding destination, completion date and time, and status.



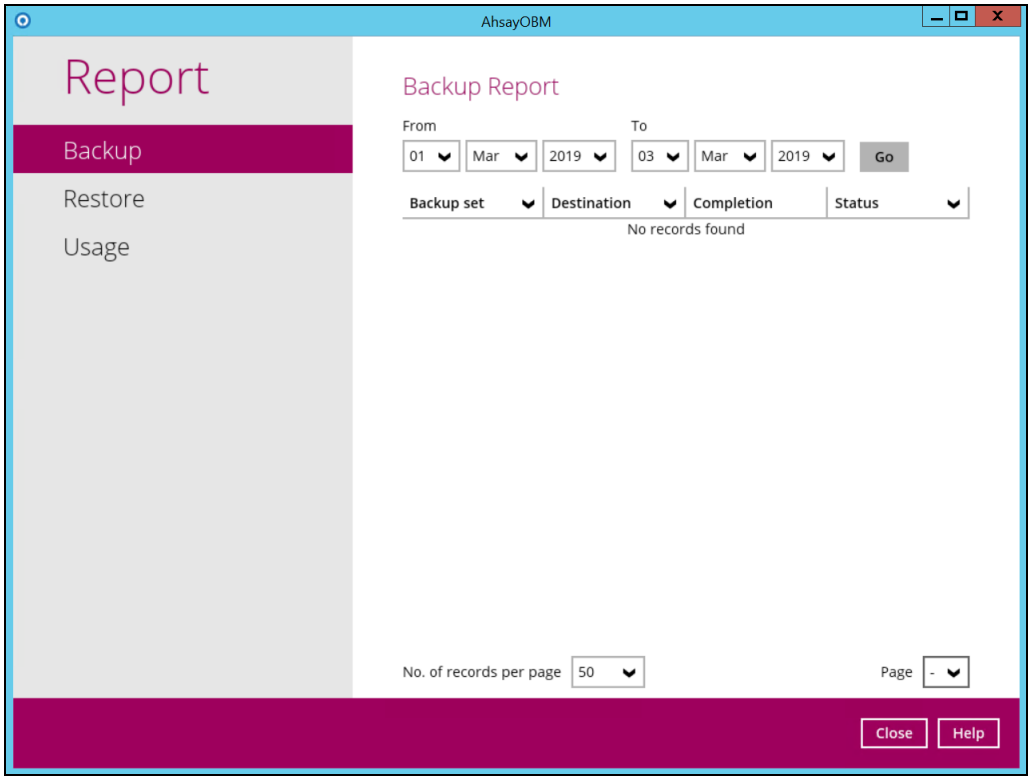
Click the backup report and the summary of the backup will be displayed. You can also click the **View Log**; this will redirect you to the log summary of your backup.





You can also search for backup reports from a specific period of date. For example, we have the **From** date which is, **01 Mar 2019** and the To date which is, **18 Mar 2019**. Then click the Go button to generate the available reports.

If this is a valid range of dates then backup reports will be displayed unless there were no backup running on the specified dates. A message of **No records found** will also be displayed.



7 Restoring Office 365 Backup Set

Prior to performing the restoration, it is best to be knowledgeable on the options that AhsayOBM can offer. Below are brief descriptions of the said features for you to be familiar with and utilize each function. After this quick walkthrough you will see the step-by-step instructions with corresponding screen shots on how to restore your data using the following options below.

For Office 365, you can restore items from,

- **Users**
  This is composed of data from Outlook, OneDrive, and Personal Site.
- **Site Collections**
  This is composed of one Top-level site, Subsites, and Public Folders.

Those items can be restored to,

- **Local Machine**
  Restore your data to your local computer where the AhsayOBM is running.

  Note: This option only applies to restore of items such as files, images, videos, music and more from OneDrive and not items from Outlook mailbox.
- **Original Location**
  Restore your data to the original Office 365 account.
- **Alternate Location**
  Restore your data to an alternate location, another O365 user account on the same 365 domain. Alternate location depends on source of the items. It can be from Users or Site Collections.

  Example #1:
  Restore Items from Users
  Office 365 Account: TestAccountABC@onecompany
  Users: TestUserAccount01@onecompany
  TestUserAccount02@onecompany
  TestUserAccount03@onecompany
  TestUserAccount04@onecompany
  TestUserAccount05@onecompany

  Explanation:
  For the example above, we have the **TestAccountABC@onecompany** as our Office 365 account. For the alternate location, a dropdown list will be available and from there you can choose from the following Office 365 accounts:
  - **TestUserAccount01@onecompany**
  - **TestUserAccount02@onecompany**
  - **TestUserAccount03@onecompany**
  - **TestUserAccount04@onecompany**
  - **TestUserAccount05@onecompany**

  Example #2:
  Restore Items from Site Collections
  Office 365 Account: SampleAccountXYZ@twosquaretower
  Site Collection / Site: blackbox.sharepoint.com/sites/EmptySite1
  blackbox.sharepoint.com/sites/EmptySite2
  blackbox.sharepoint.com/sites/EmptySite3

blackbox.sharepoint.com/sites/EmptySite4
blackbox.sharepoint.com/sites/EmptySite5

Explanation:
For the example above, we have the **SampleAccountXYZ@twosquaretower** as our Office 365 account. For the alternate location, a dropdown list will be available and from there you can choose from the following Site Collections / Sites:

- **blackbox.sharepoint.com/sites/EmptySite1**
- **blackbox.sharepoint.com/sites/EmptySite2**
- **blackbox.sharepoint.com/sites/EmptySite3**
- **blackbox.sharepoint.com/sites/EmptySite4**
- **blackbox.sharepoint.com/sites/EmptySite5**

- **Alternate Office 365 Account**
  Last but not the least, you can restore your data to an alternate Office 365 account that has a different domain.

  Example:
  Original Office 365 Account: TestAccountABC@onecompany
  Alternate Office 365 Account: SampleAccountXYZ@twosquaretower

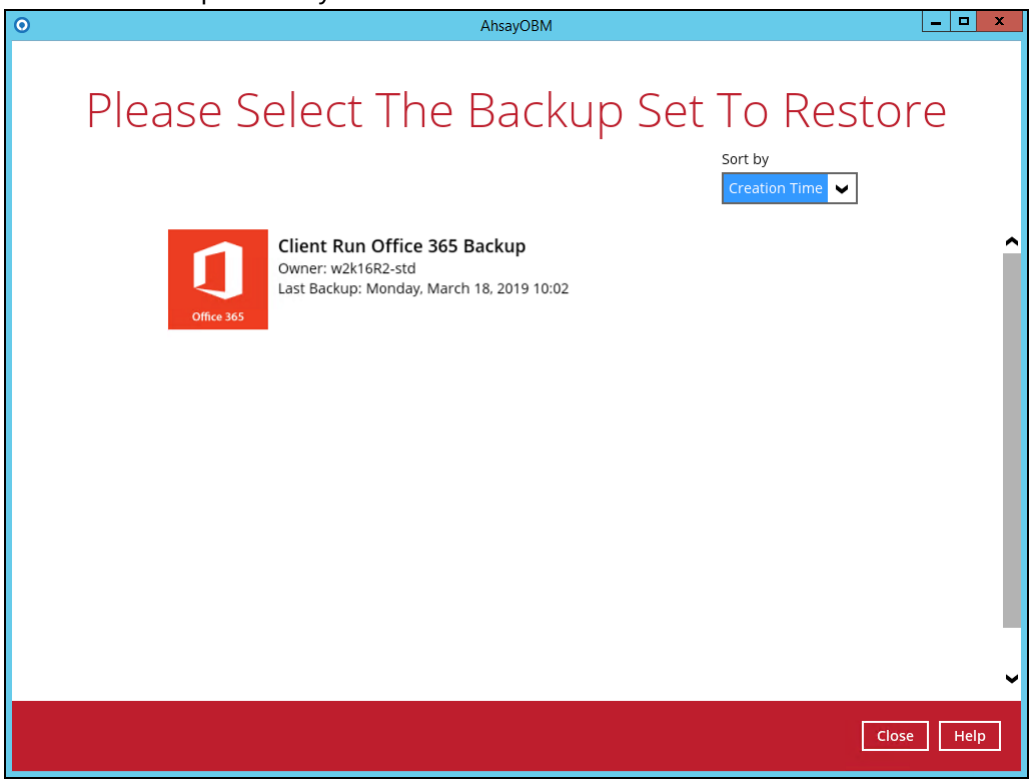
  Explanation:
  As you can see on the above example, we have two (2) Office 365 accounts with different domain. The Original Office 365 account is what we used as the source of our backup and can also use as the original location for restoration. For the alternate Office 365 account, we need to use another Office 365 account that has a different domain.

In case you also want to know how to restore an Office 365 backup using the AhsayCBS Web Console, please refer to this guide: **AhsayCBS v8 Run on Server Office 365 Backup & Restore Guide**

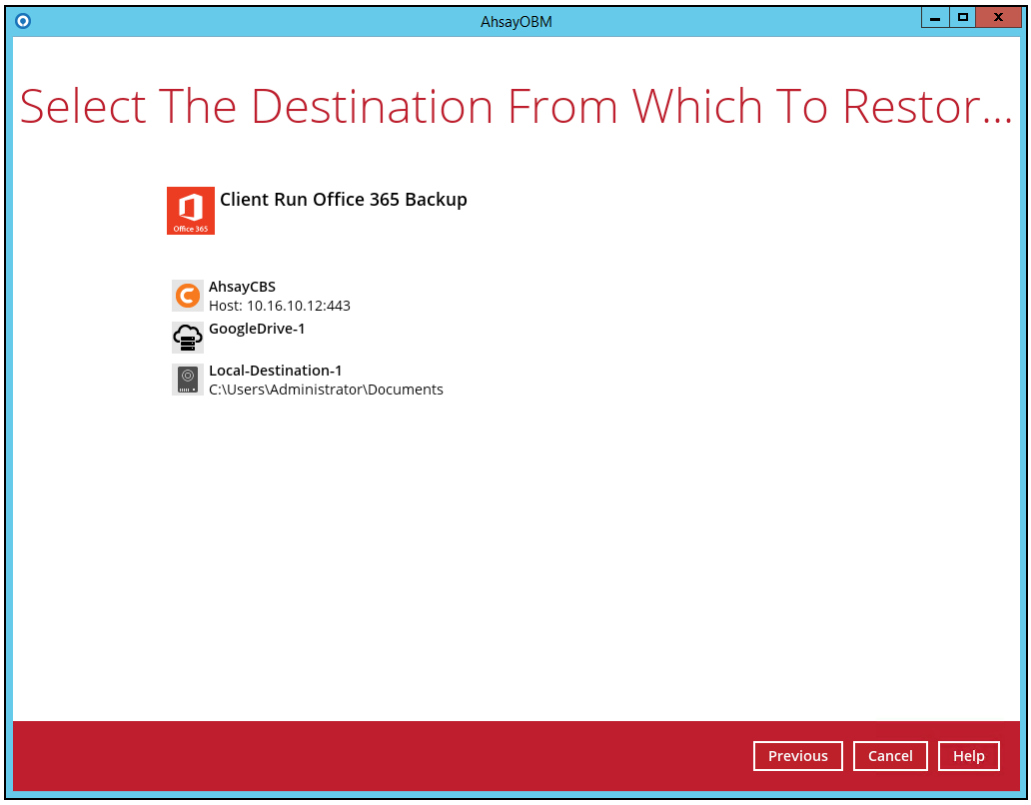
7.1 Restore Backup with AhsayOBM

1. Login to AhsayOBM according to the instructions in Login to AhsayOBM.
2. Click the **Restore** icon on the main interface of AhsayOBM.

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



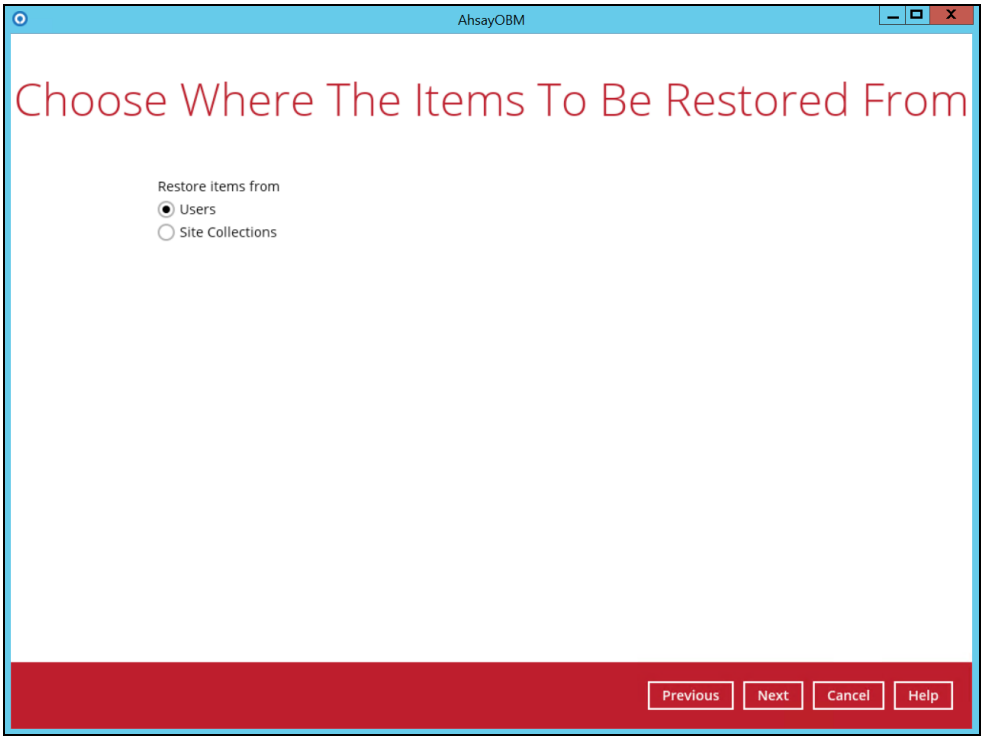
4. Select the backup destination that you would like to restore backed-up items to. In our screenshot below, we have three (3) options namely, **AhsayCBS**, **GoogleDrive-1**, and **Local-1**.



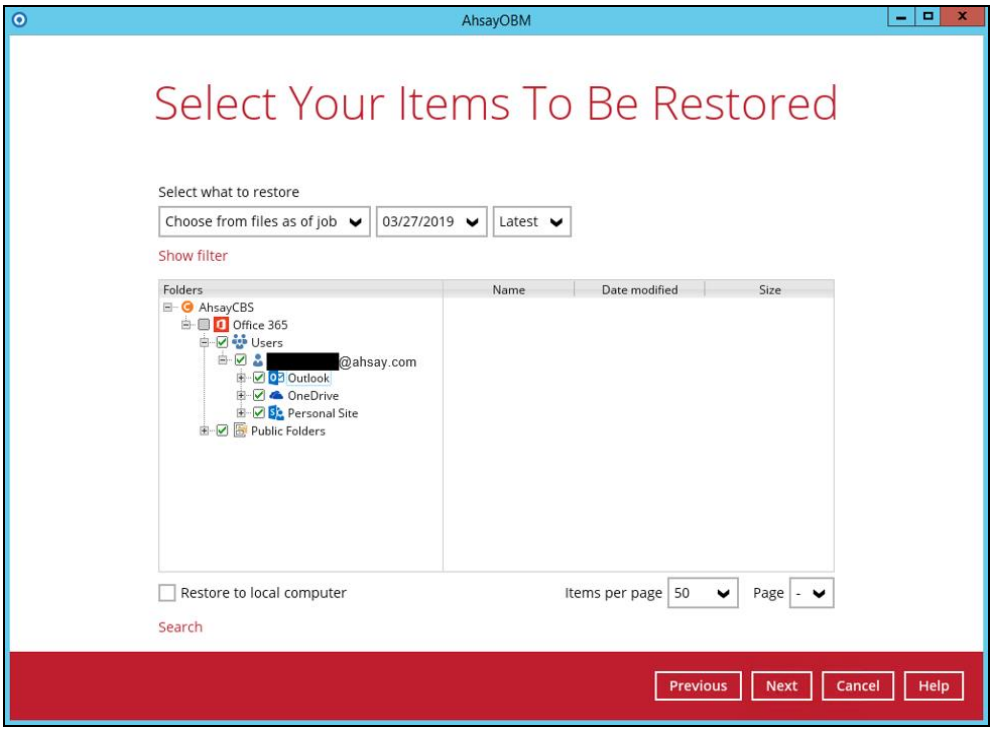
5. Select to restore from **Users** or **Site Collections**. Click **Next** to continue.

7.1.1. From Users

For the backup data from Users



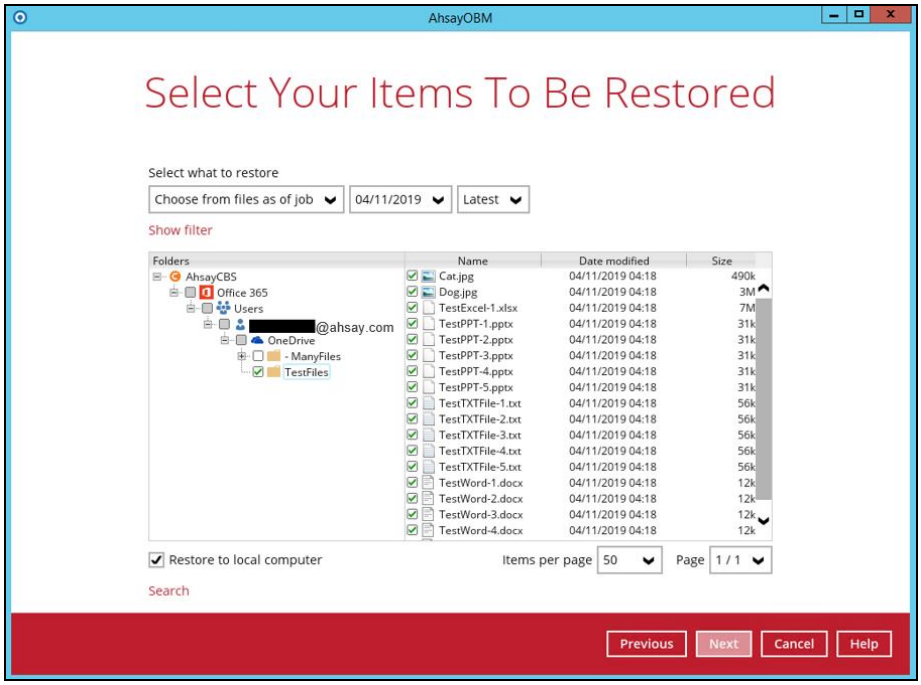
Select the item(s) you would like to restore. You can also choose to restore backed up file from a specific backup job of your choice using the **Select what to restore** drop-down menu at the top. Click **Next** to proceed when you are done with the selection.



Select the destination you would like the mail objects to be restored.

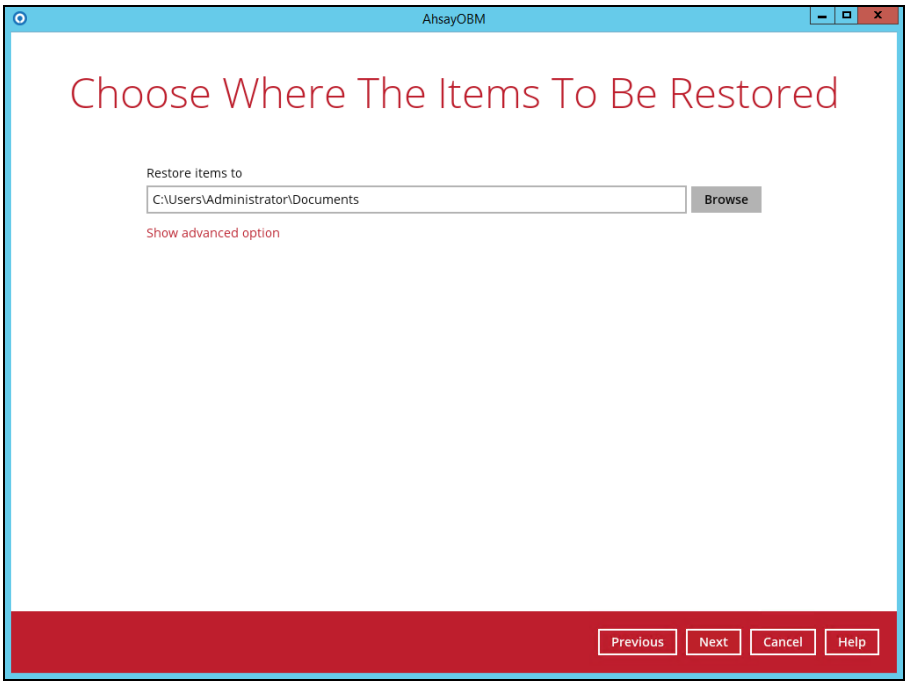
7.1.1.1. Local machine

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



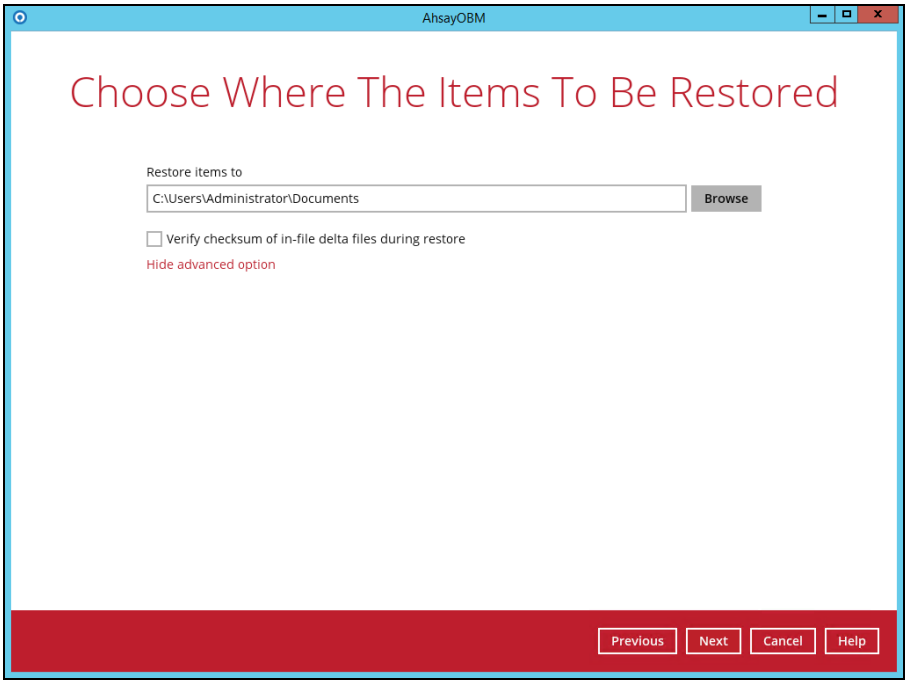
Click the **Browse** button to select a path on where you want the items to be restored on your local computer. Make sure it has enough space to accommodate your restoration.

Also click the **Show advanced option** to configure other restore settings.



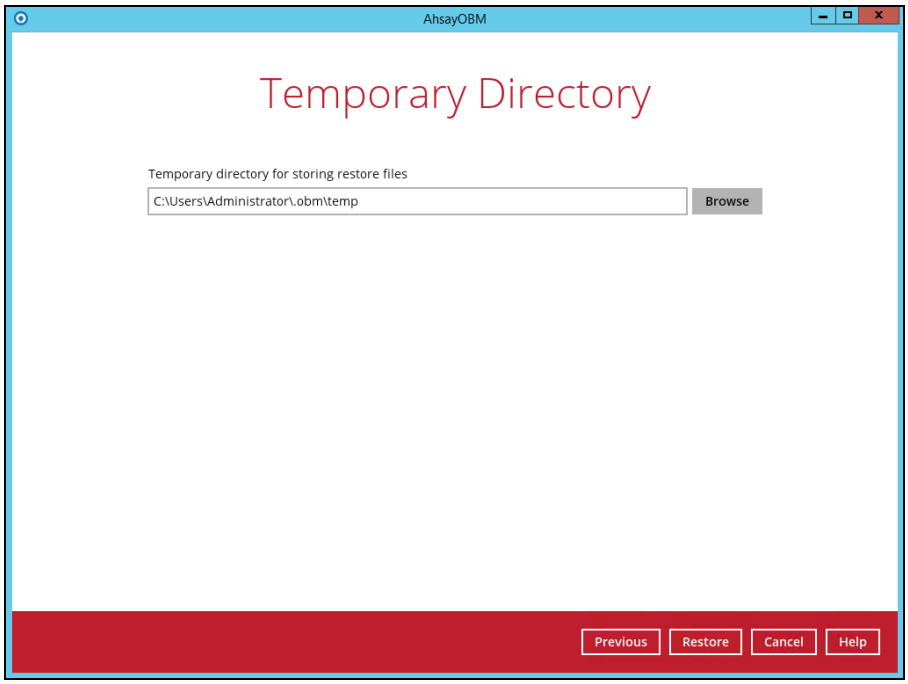
Verify checksum of in-file delta files during restore

By enabling this option, the checksum of in-file delta files will be verified during the restore process. This will check the data for errors during the restore process and create a data summary of the in-file delta files which will be included in the report.

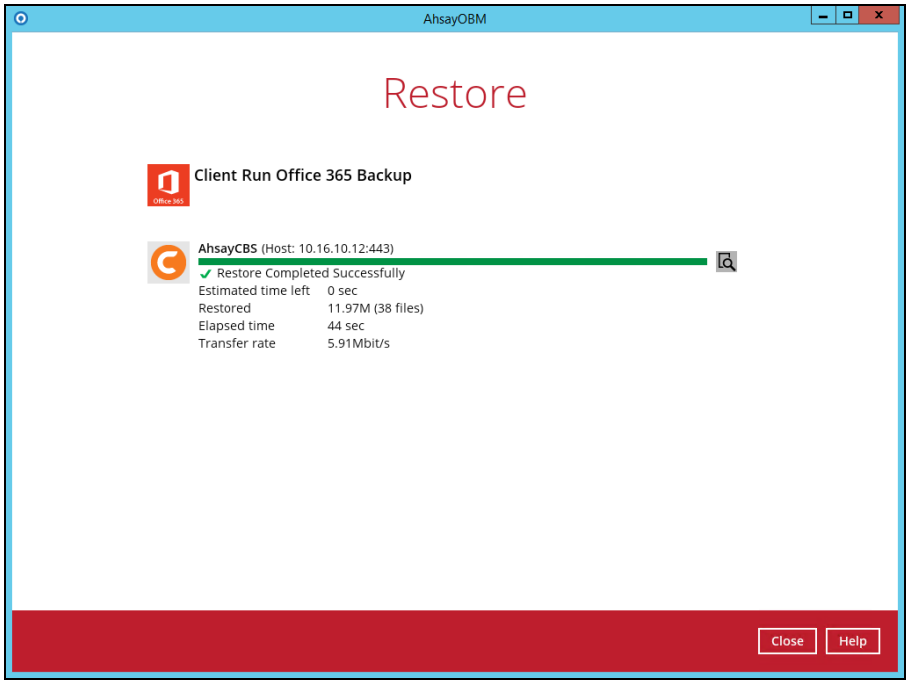


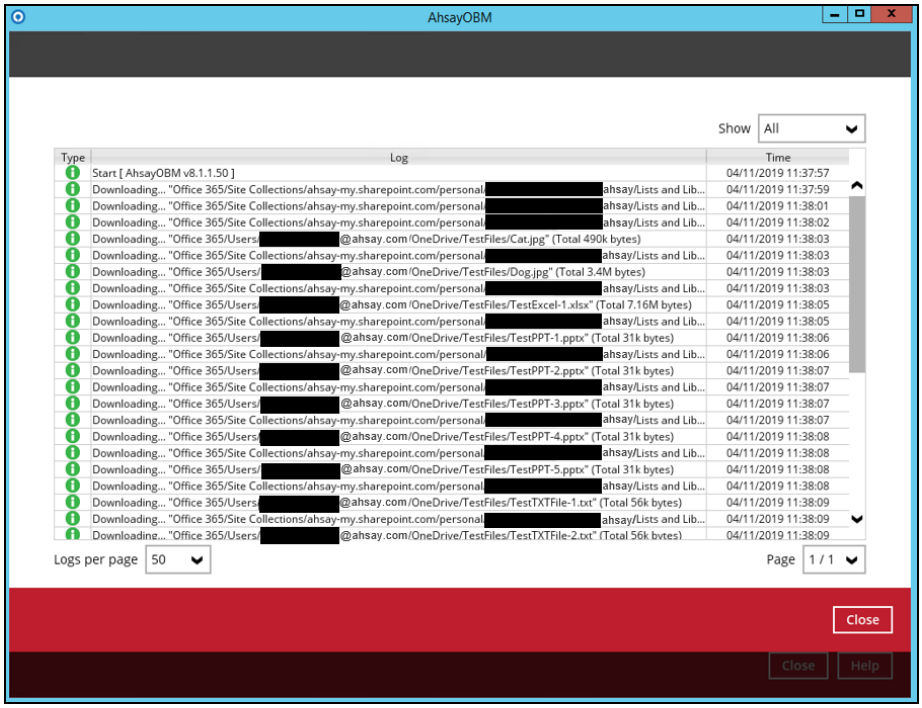
Click **Next** to proceed.

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

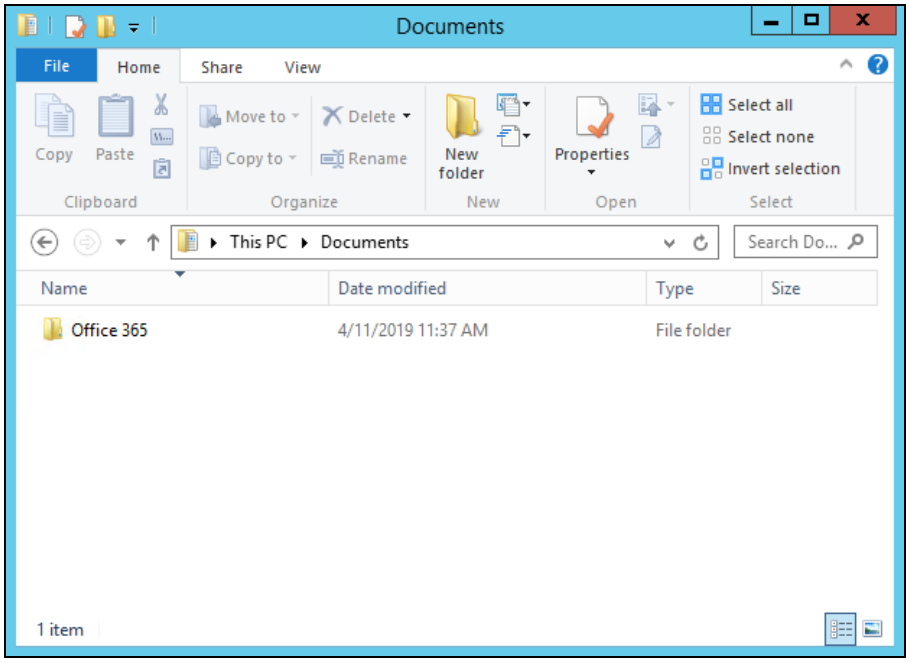


Restore is completed. Click the to show the log of the restoration.



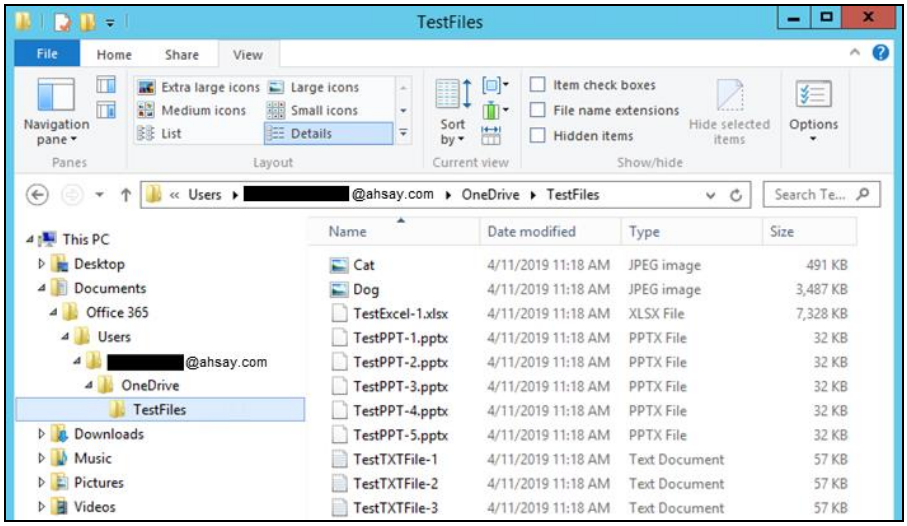


To check if the files from OneDrive are fully restored in the location machine on the selected directory which is **C:\Users\Administrator\Documents,** go to the Documents folder. There should be an available **Office 365** folder.

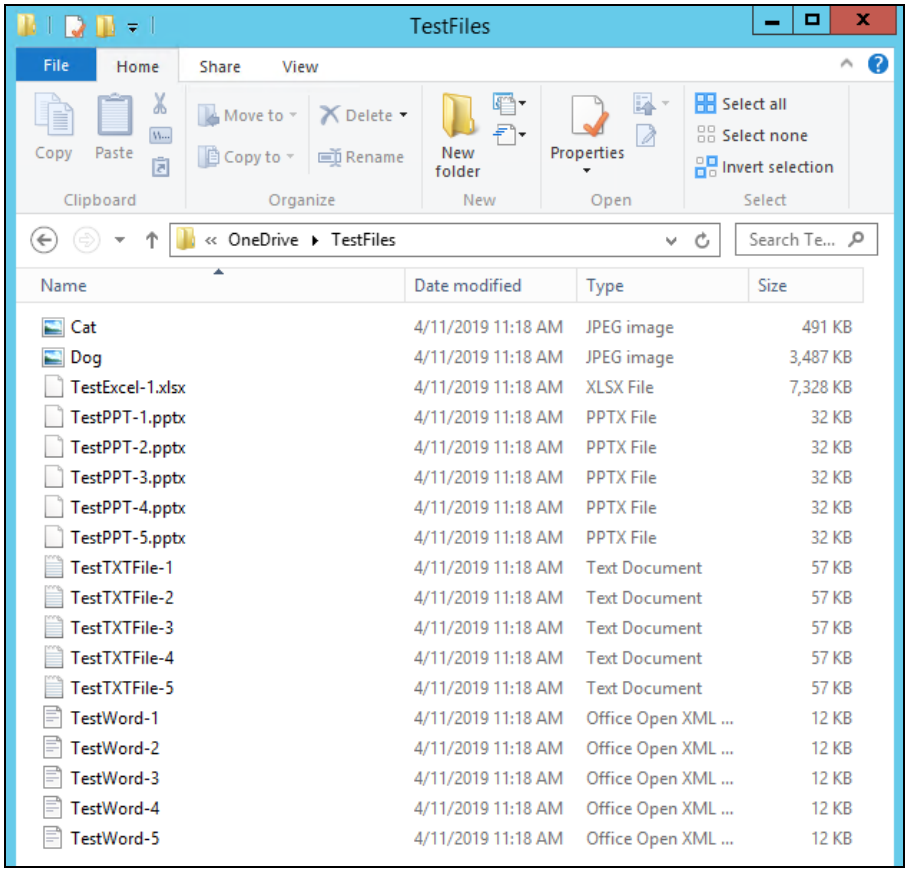


Open the Office 365 folder and you will see a **User** folder. This includes the selected Office 365 user account which is **abc@ahsay.com** and when you open the Office 365 user account folder, you will see the **OneDrive** folder.

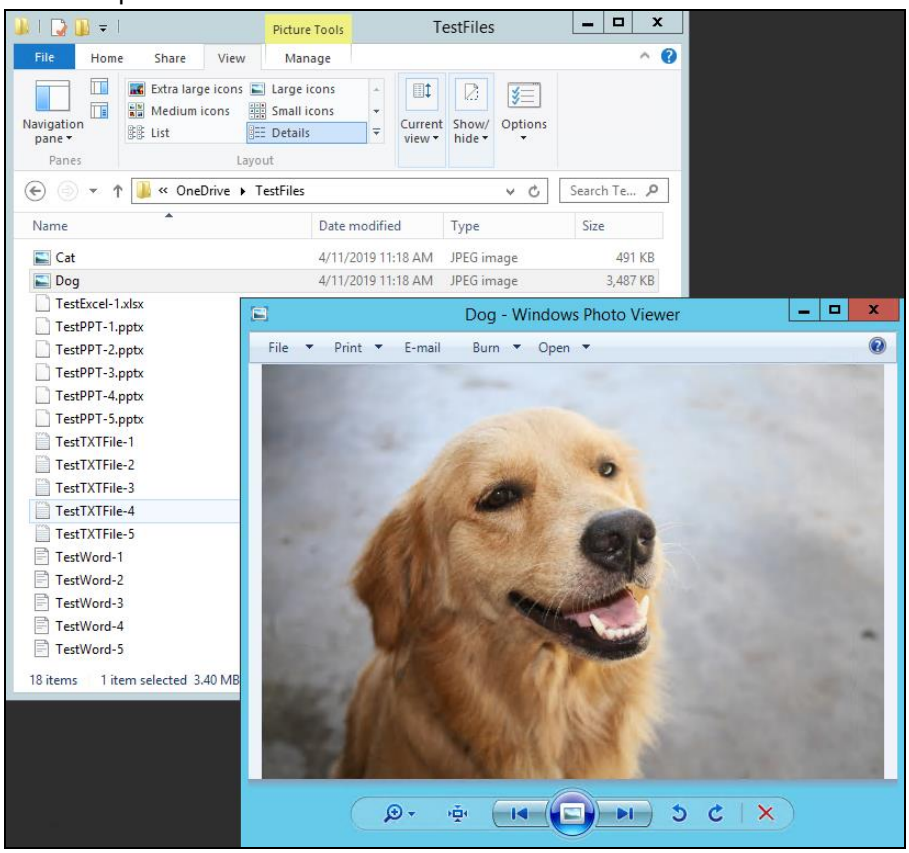
Click the OneDrive folder and you will see the **TestFiles** folder.



Inside the TestFiles folder are files we have restored from OneDrive. This includes Images, Microsoft Excel. Microsoft Word, PowerPoint Presentations, and Text.

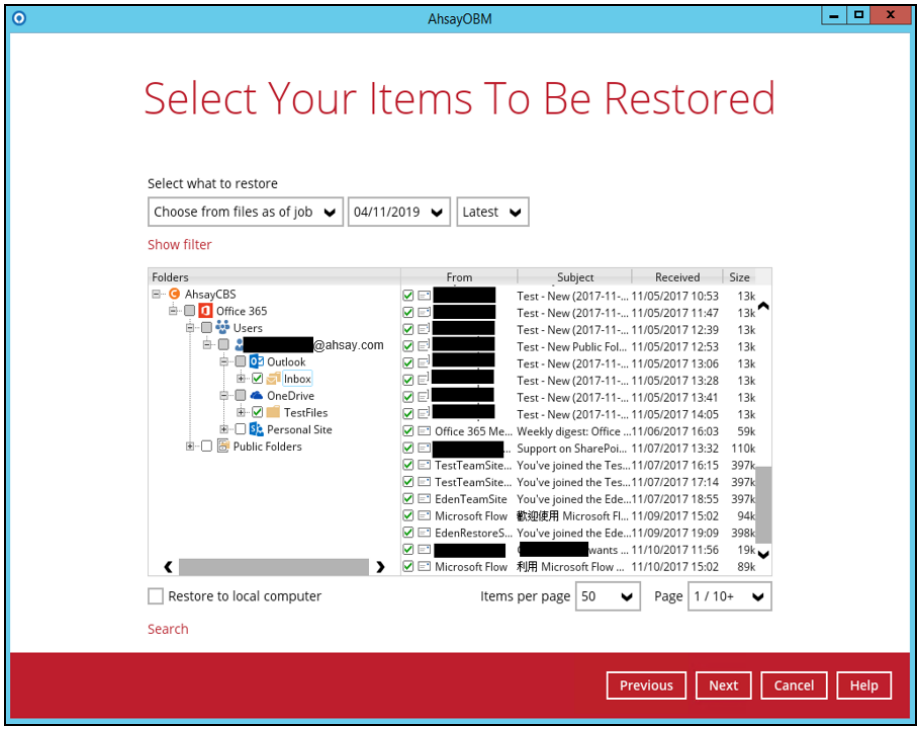


Here is a preview of one of restored files from OneDrive.



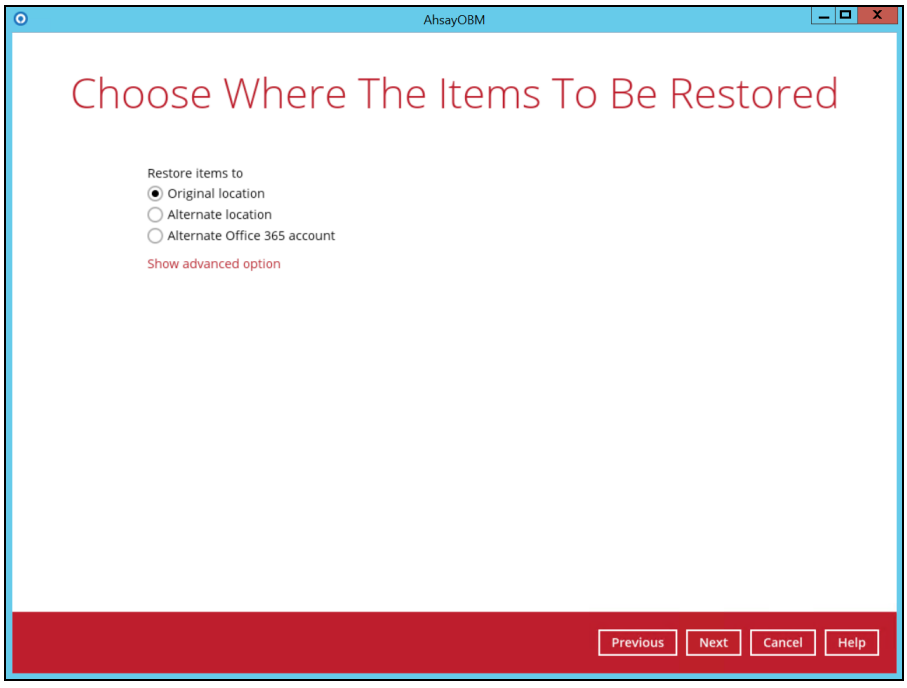
7.1.1.2 Original location

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.



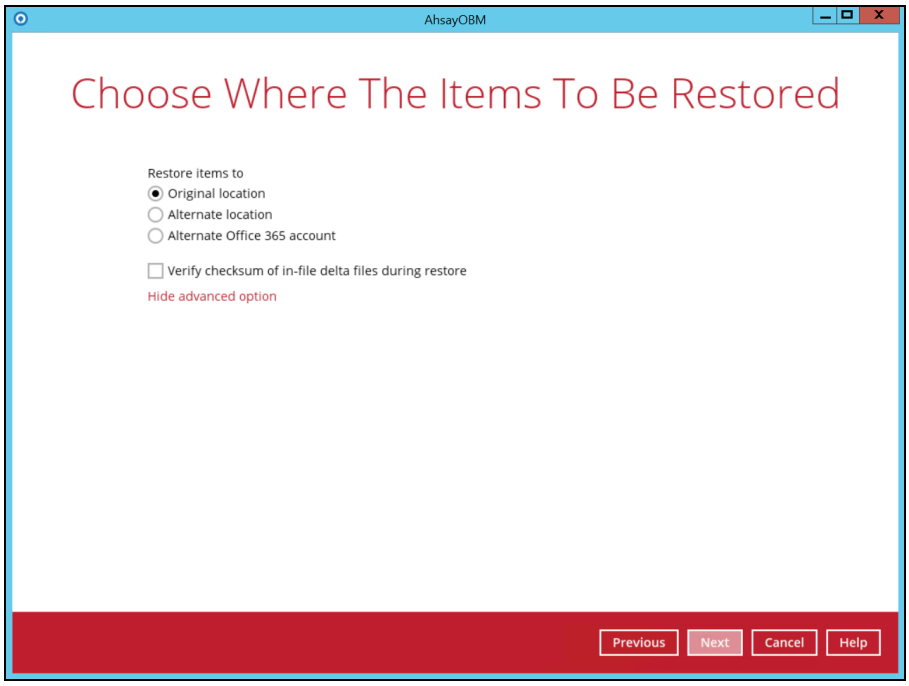
Choose from the following three (3) options on where you want your items to be restored. Select the **Original location**.

Also click the **Show advanced option** to configure other restore settings.

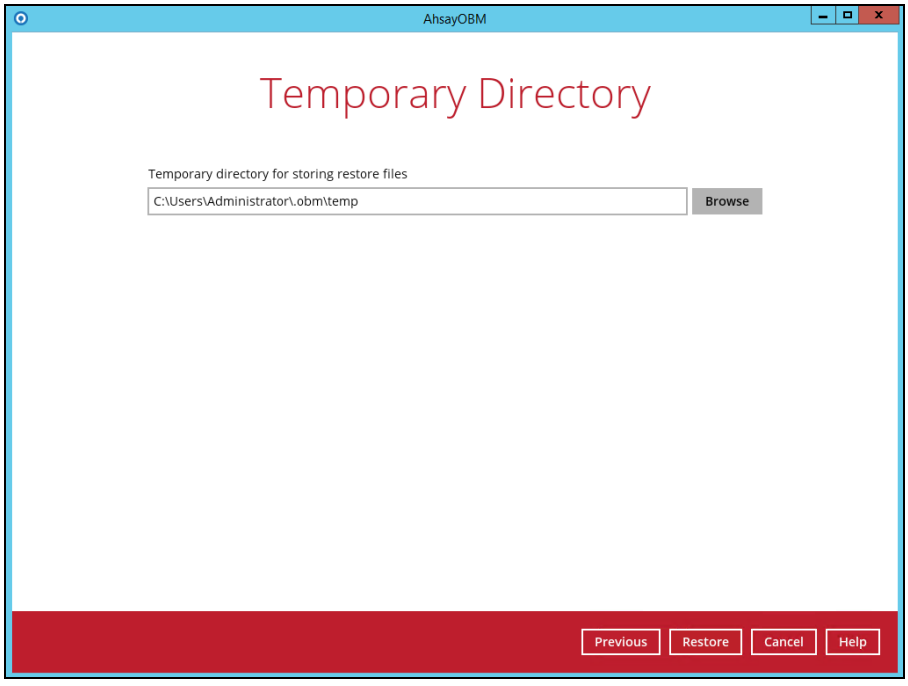


Verify checksum of in-file delta files during restore

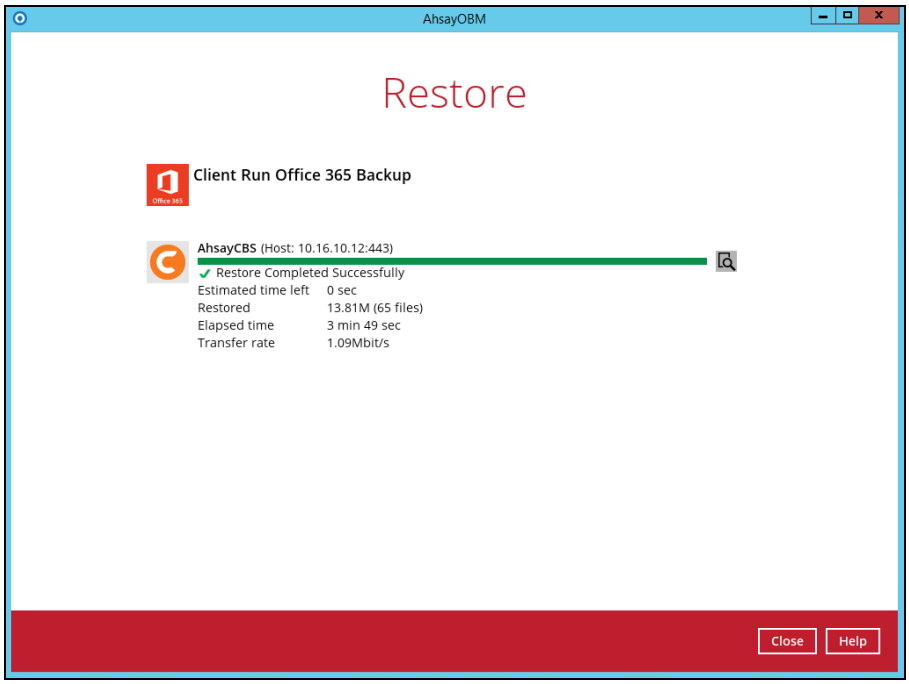
By enabling this option, the checksum of in-file delta files will be verified during the restore process. This will check the data for errors during the restore process and create a data summary of the in-file delta files which will be included in the report. Click **Next** to proceed.

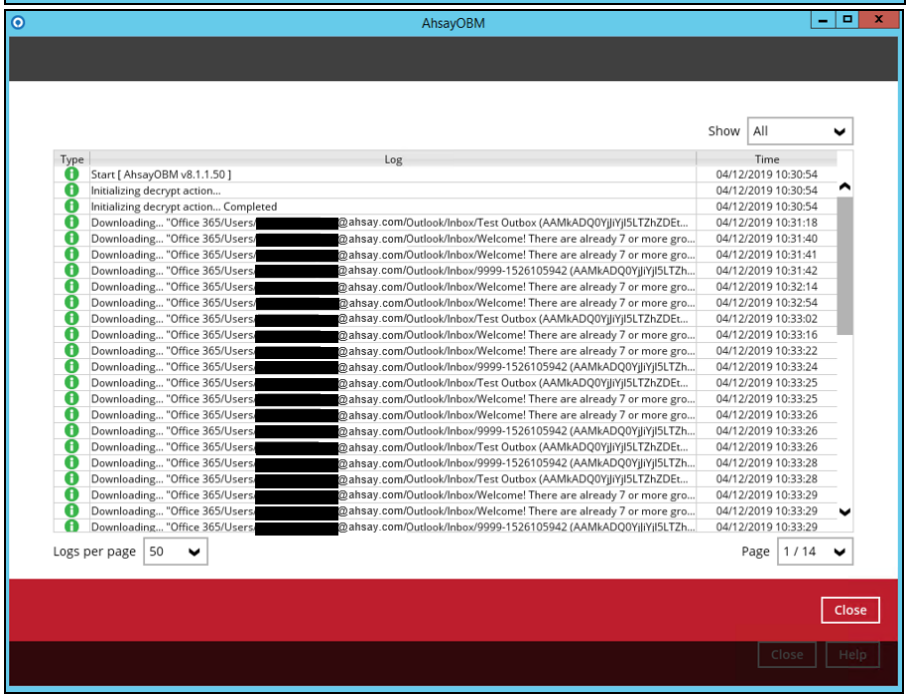


Select the temporary directory for storing temporary files, such as delta files when they are being merged, click **Restore** to start the restoration

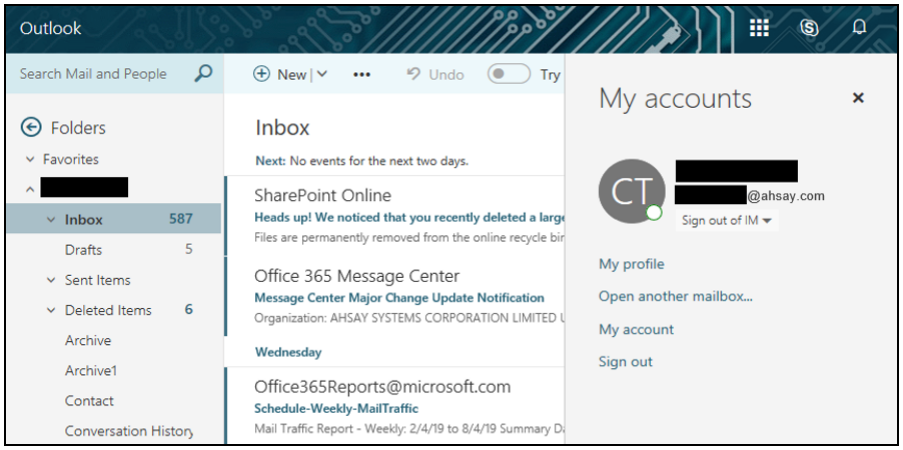


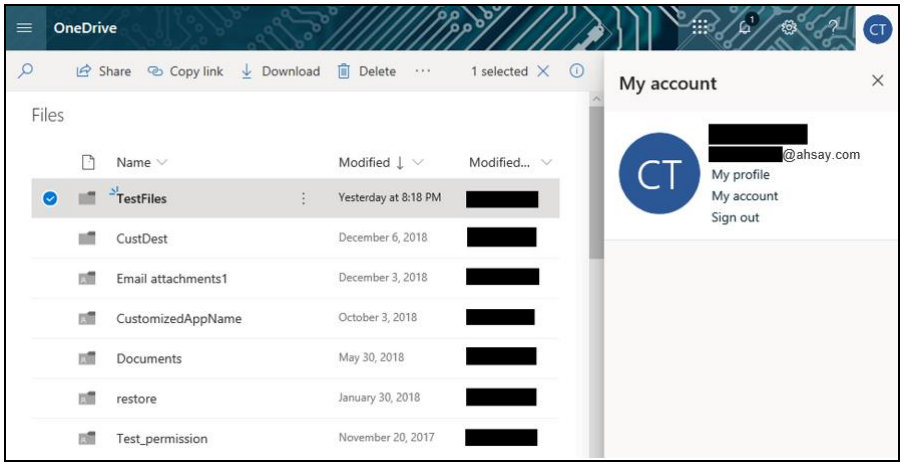
Restore is completed. Click the to show the log of the restoration.



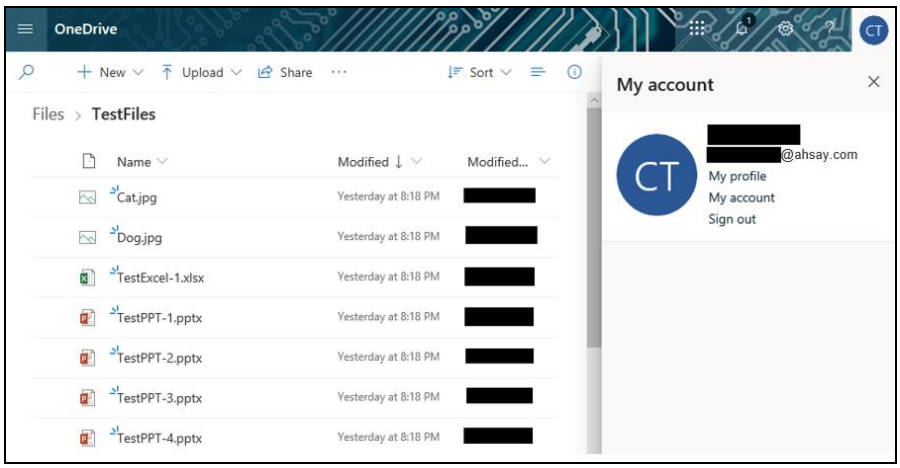


To check if the mails from Outlook and files from OneDrive are fully restored in the original location, login and check the files in Outlook and OneDrive. As you can see on our example screen shot below, **CT** account is logged in and the **Inbox** from Outlook and **TestFiles** folder from OneDrive are available.

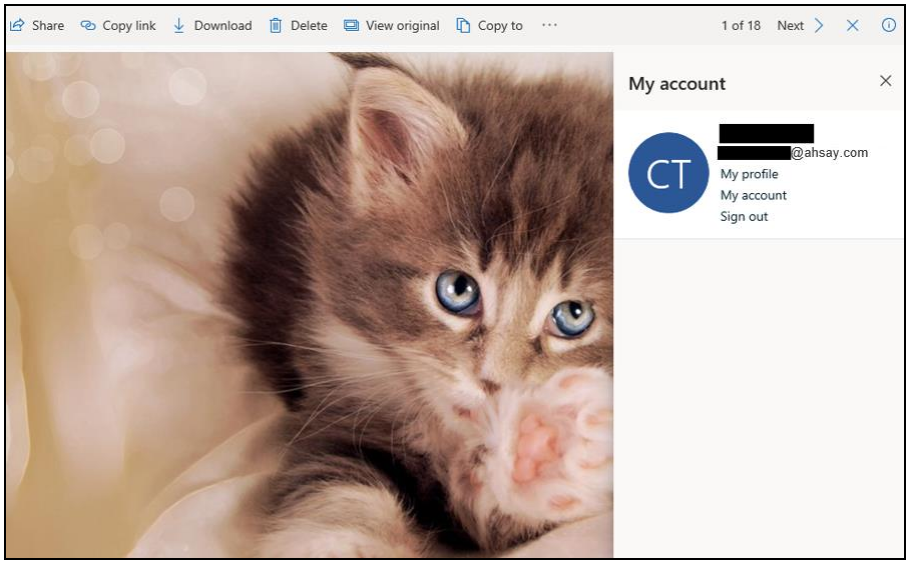




Open the TestFiles folder to check if the files are completely restored.

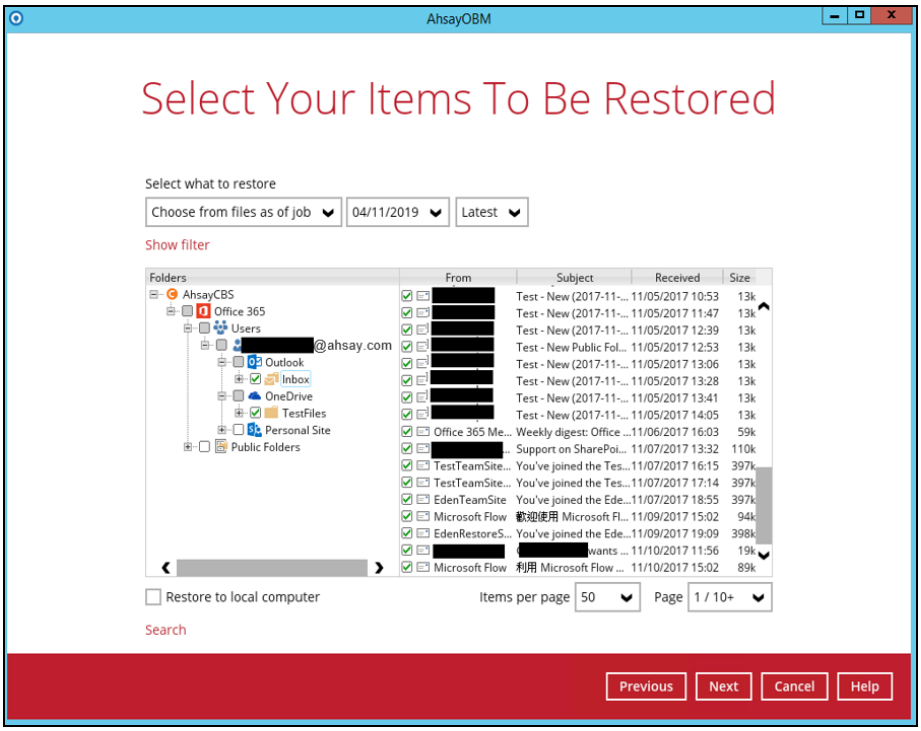


Here is a preview of one of the restored files from OneDrive.



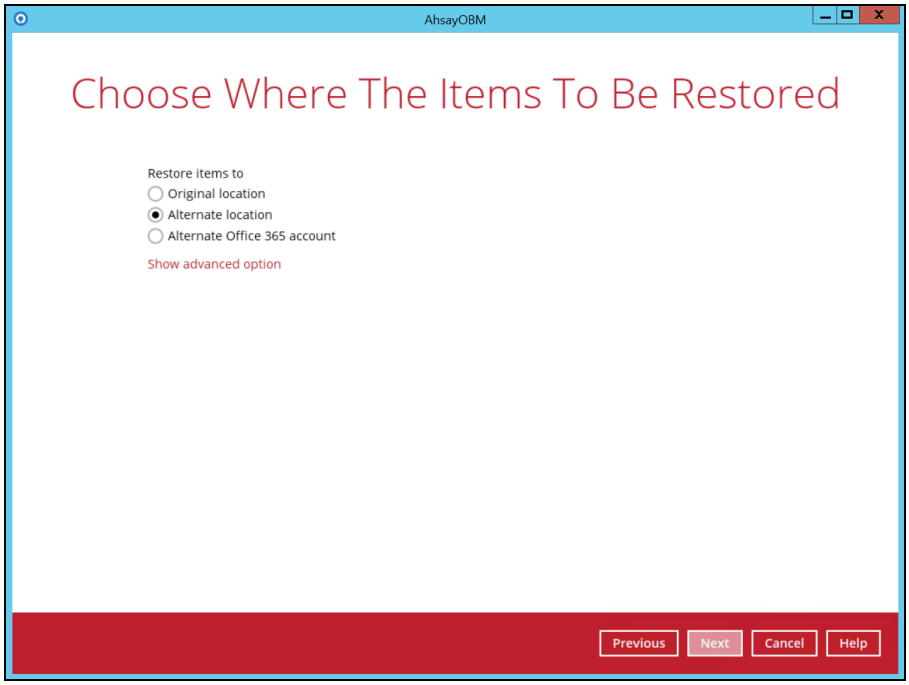
7.1.1.3. Alternate location

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.



Choose from the following three (3) options on where you want your items to be restored. Select the **Alternate location**.

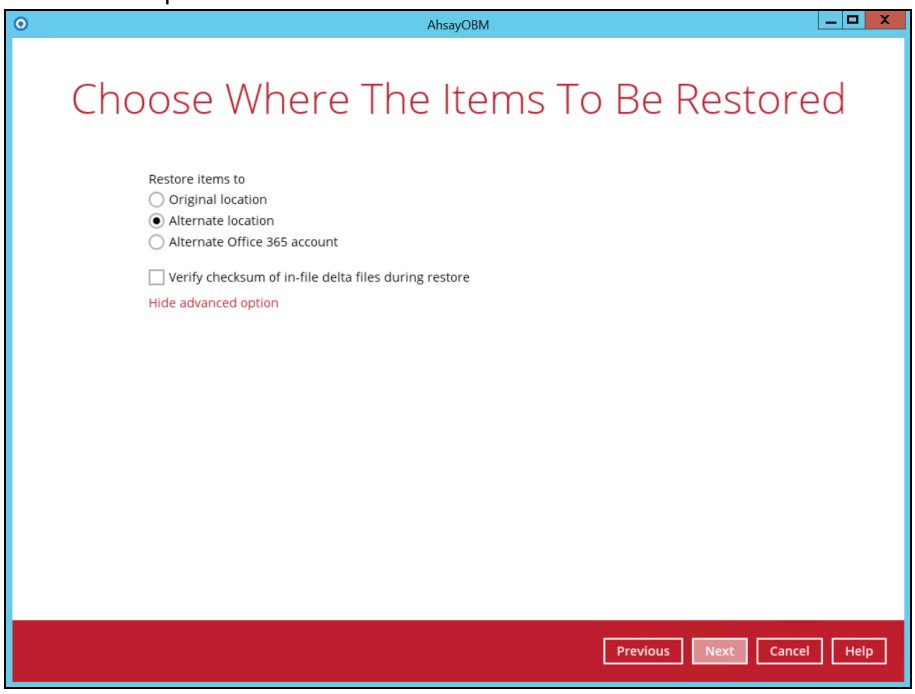
Also click the **Show advanced option** to configure other restore settings.



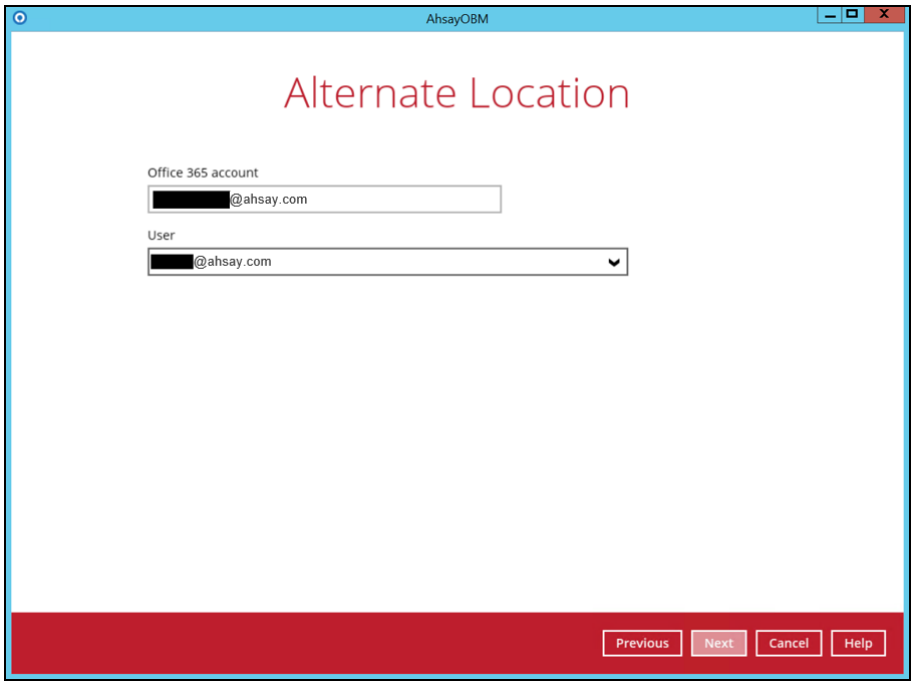
Verify checksum of in-file delta files during restore

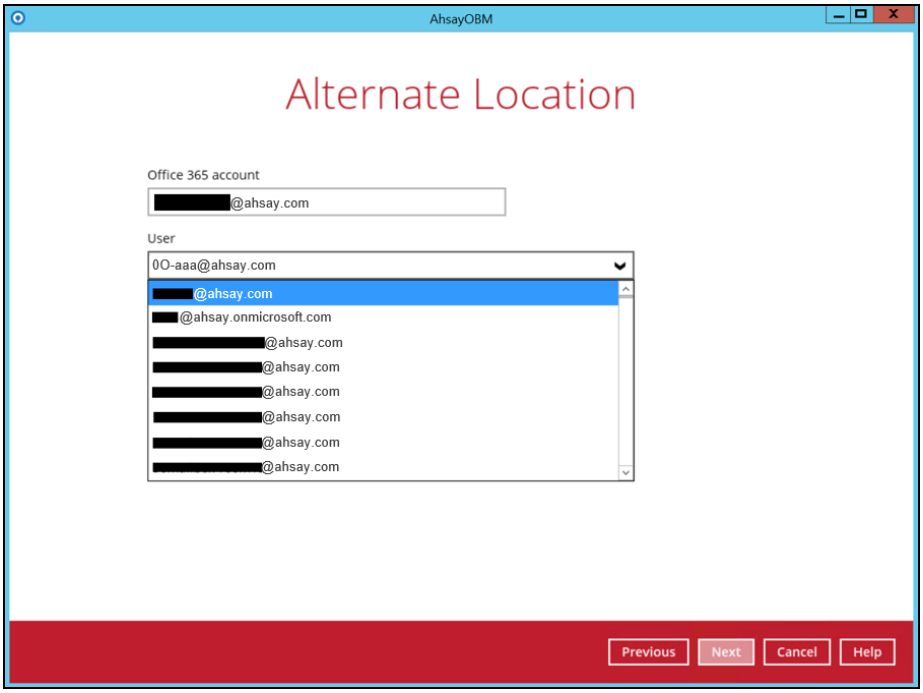
By enabling this option, the checksum of in-file delta files will be verified during the restore process. This will check the data for errors during the restore process and create a data summary of the in-file delta files which will be included in the report.

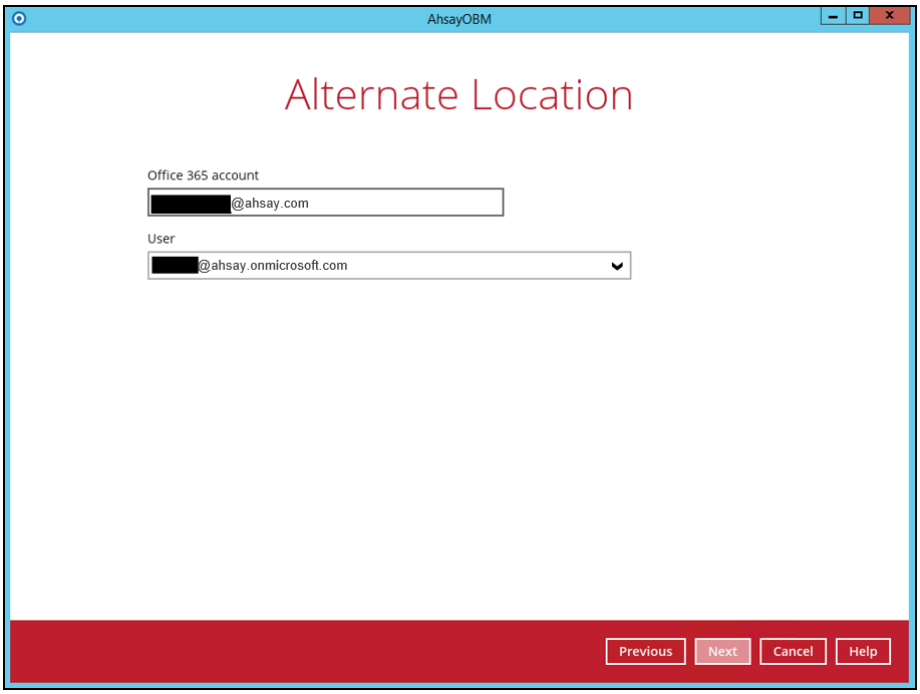
Click **Next** to proceed.



Select an Office 365 user account on which the data will be restored. Click on the dropdown arrow to view the available Office 365 user accounts.

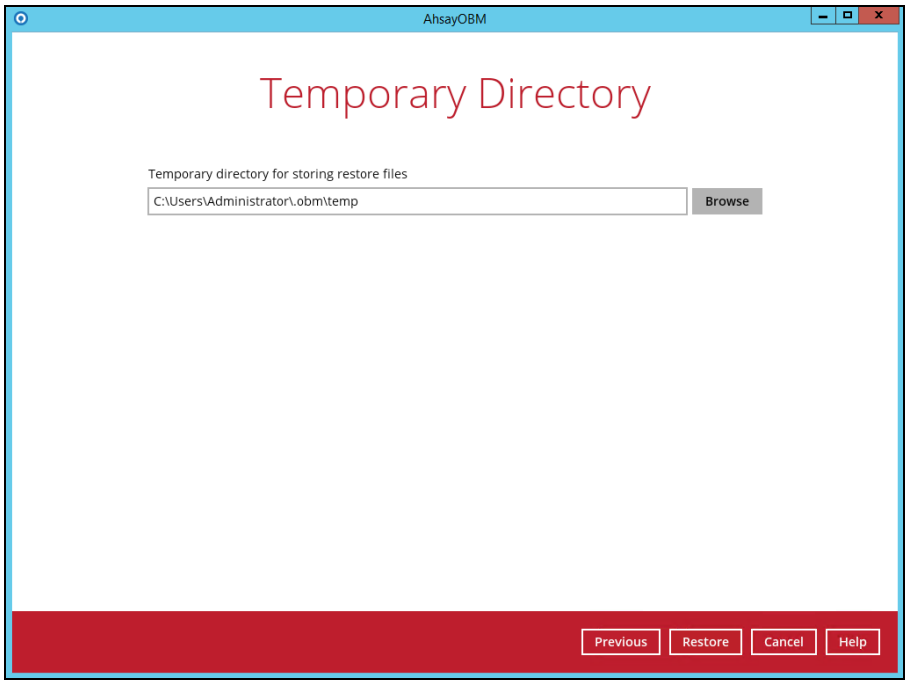




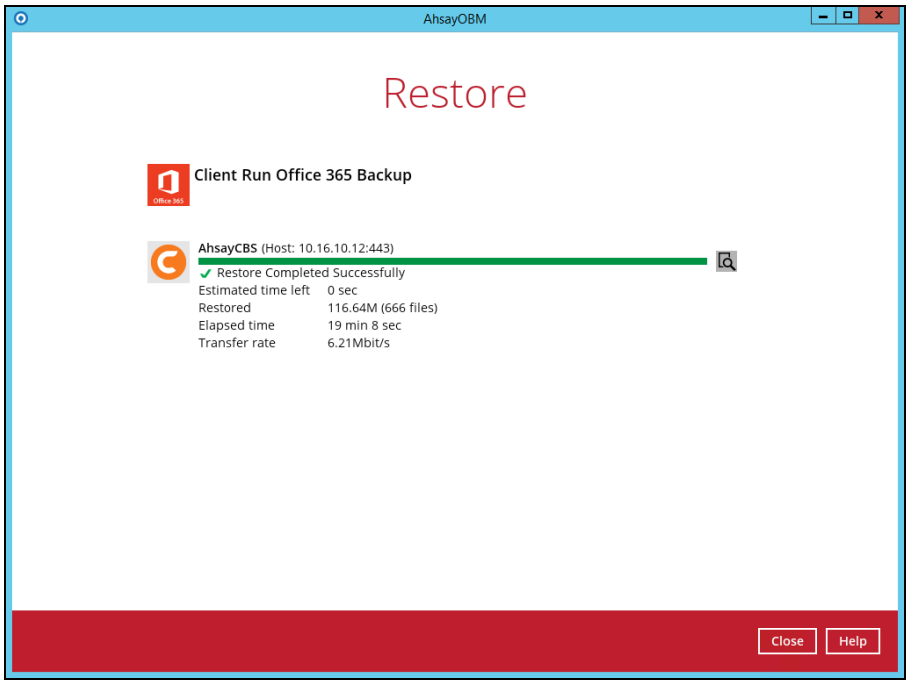


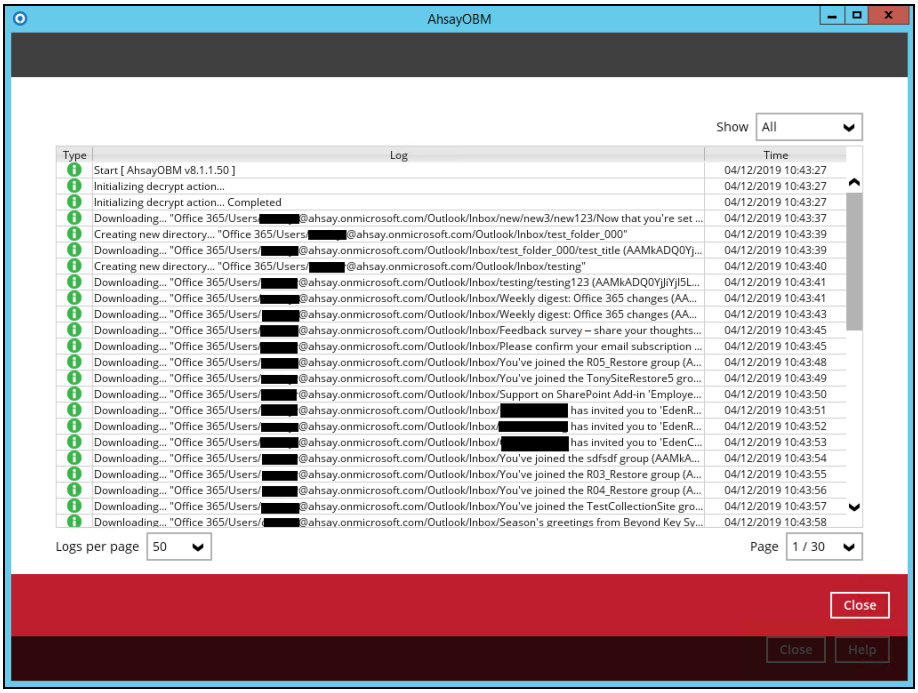
Click **Next** to proceed.

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

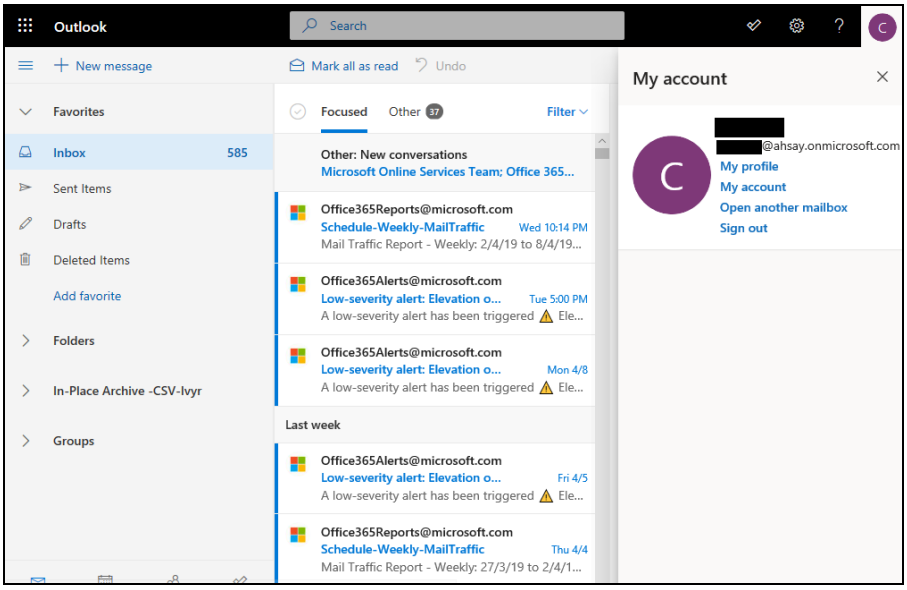


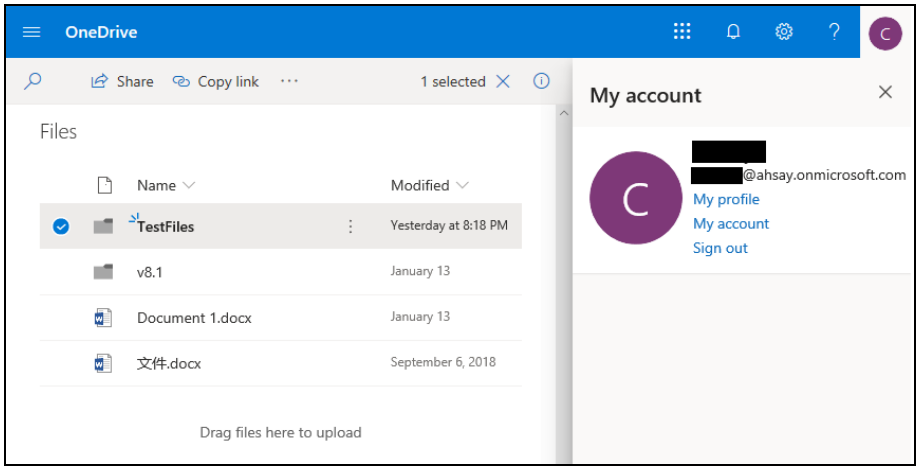
Restore is completed. Click the to show the log of the restoration.

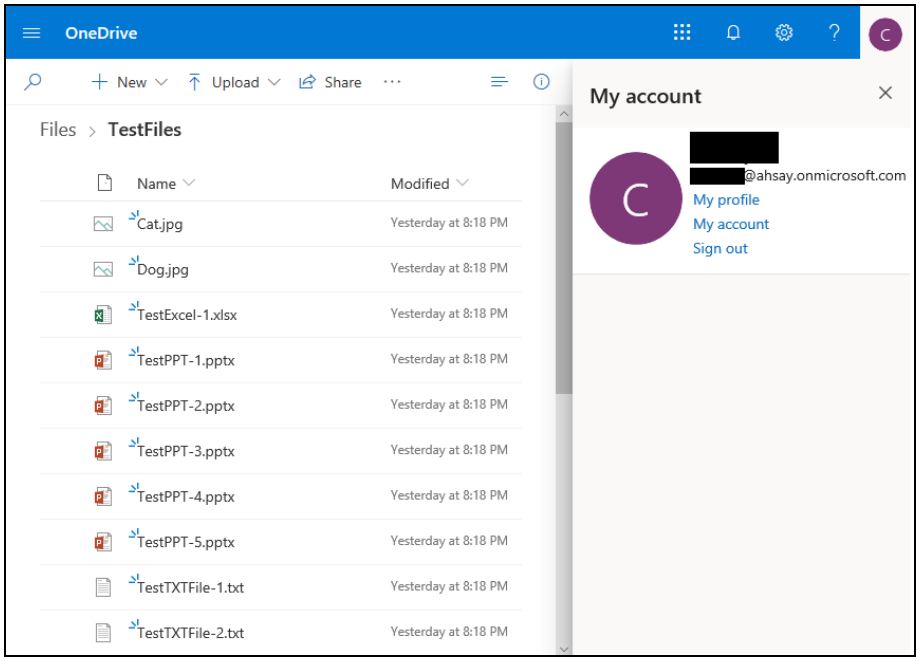




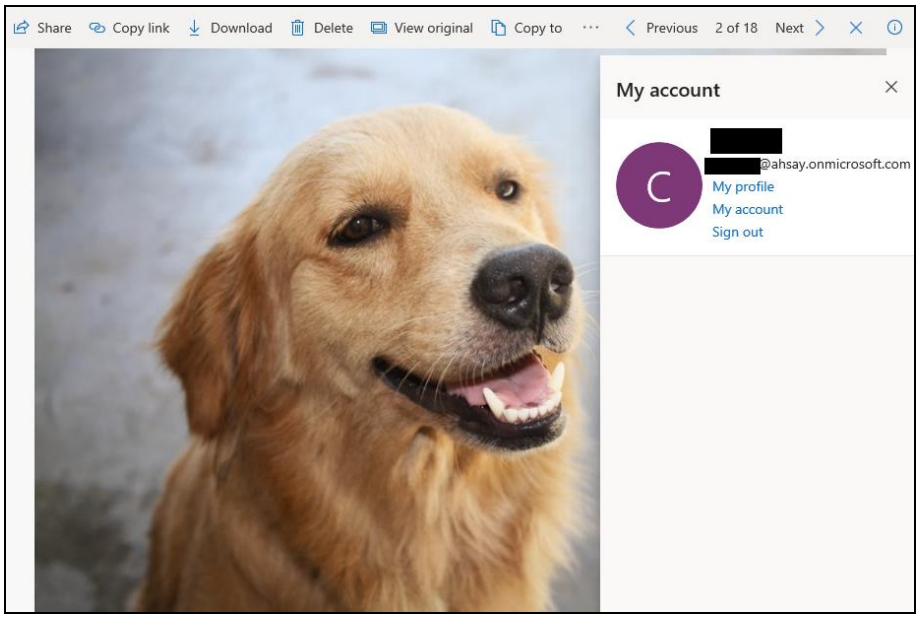
To check if the mails from Outlook and files from OneDrive are fully restored in the original location, login and check the files in Outlook and OneDrive. As you can see on our example screen shot below, **cde** is logged in and the **Inbox** from Outlook and **TestFiles** folder from OneDrive are available.





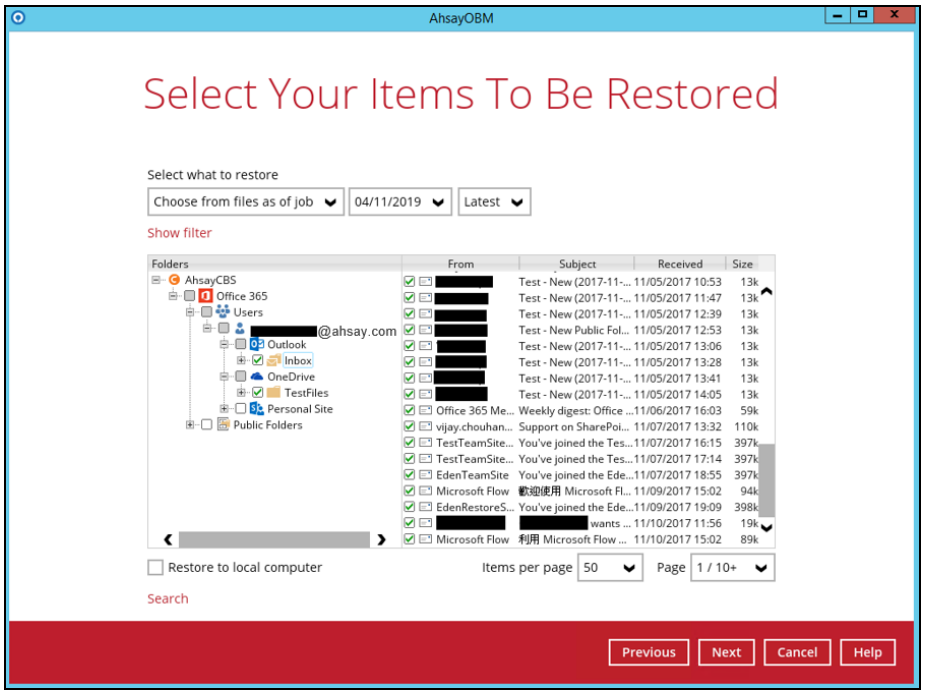


Here is a preview of one of restored files from OneDrive.



7.1.1.4. Alternate Office 365 Account

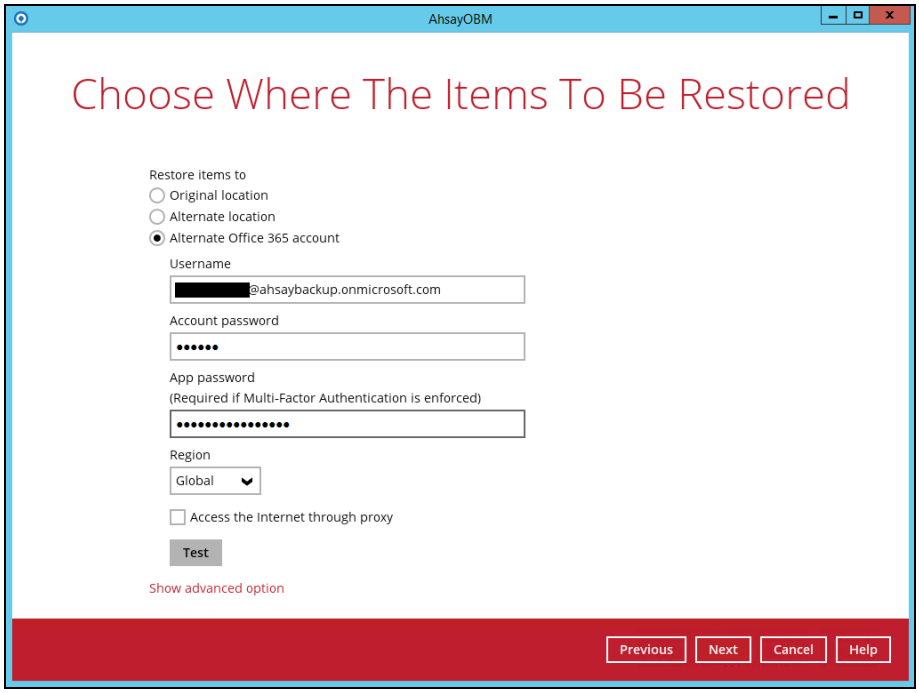
Select the item(s) you would like to restore. You can also choose to restore backed up file from a specific backup job of your choice using the **Select what to restore** drop-down menu at the top. Click **Next** to proceed when you are done with the selection



Choose from the following three (3) options on where you want your items to be restored. Select the **Alternate Office 365 Account**.

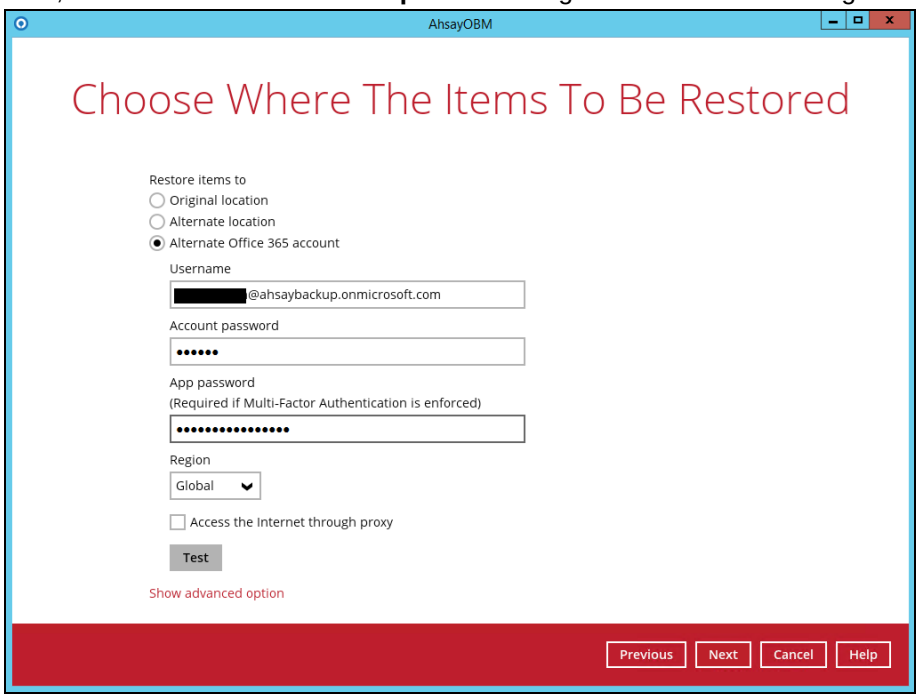
Input the Username, Password, App password, and choose the region for the other Office 365 account.

If the MFA of an alternate Office 365 account is enabled, then you are required to input the App password. Otherwise, restoration will not be able to proceed as it is mandatory.

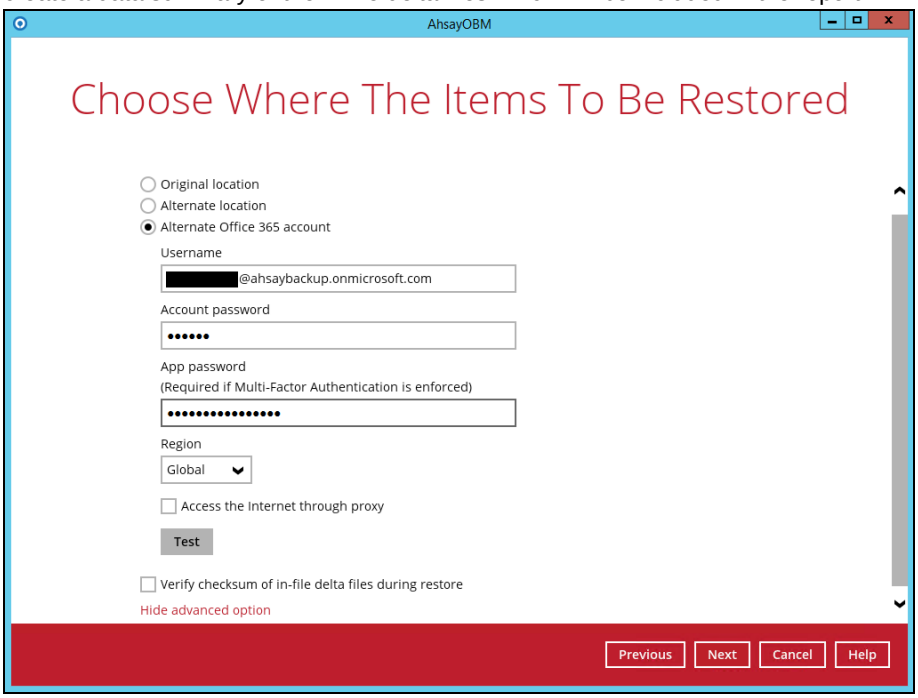


Choose from the following **Region**:

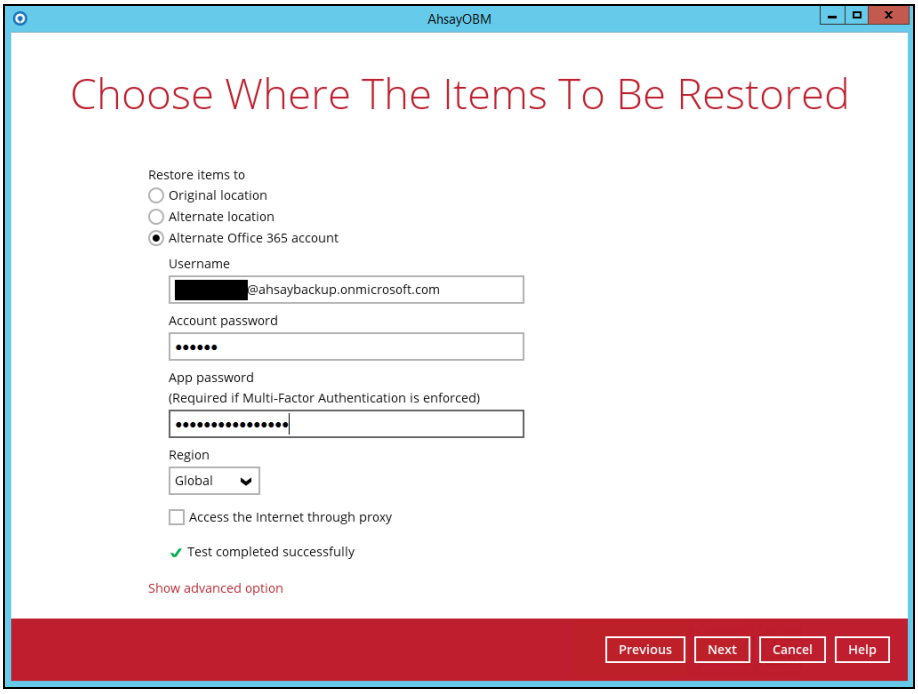
Also, click the **Show advanced option** to configure other restore settings.



Verify checksum of in-file delta files during restore
By enabling this option, the checksum of in-file delta files will be verified during the restore process. This will check the data for errors during the restore process and create a data summary of the in-file delta files which will be included in the report.

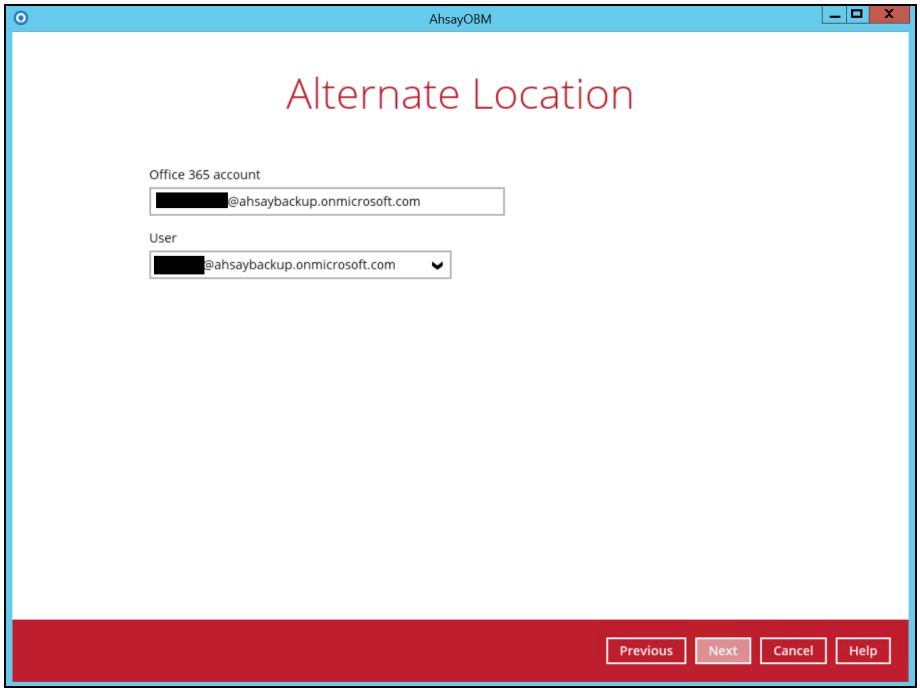


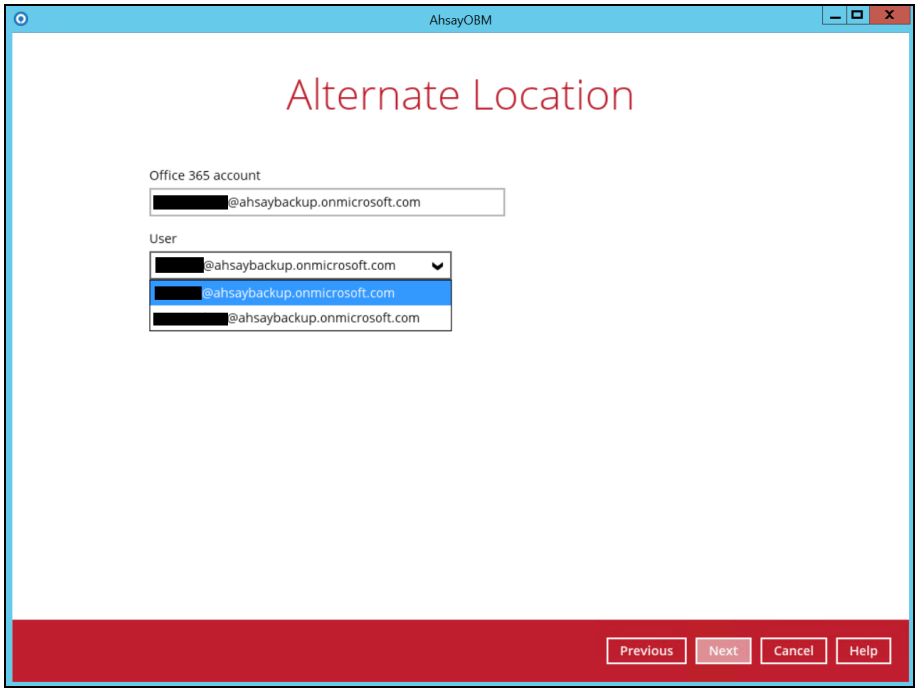
Test completed successfully shows when the validation is successful, then click **Next** to continue.

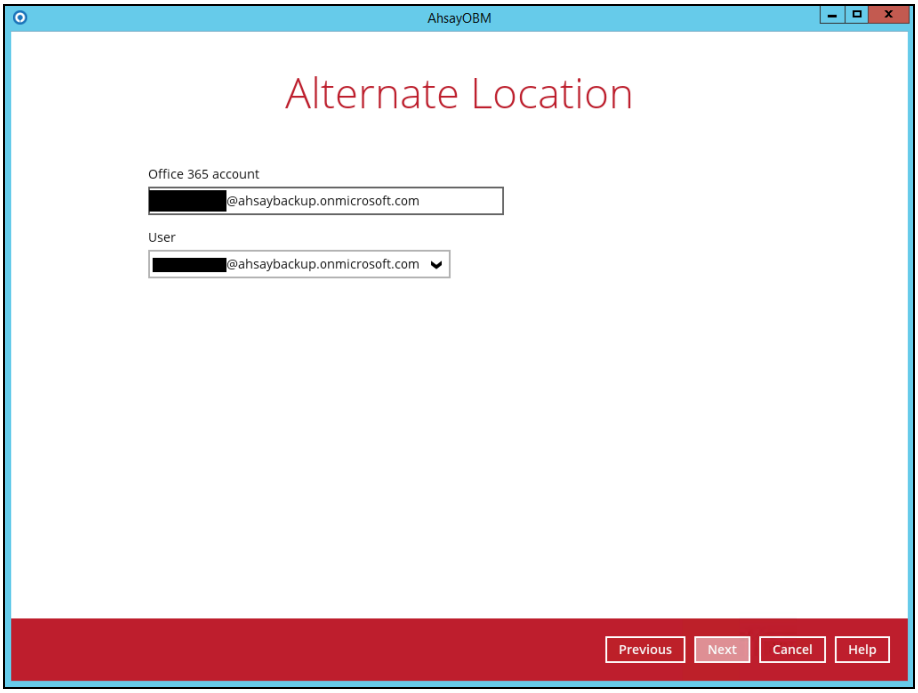


Click **Next** to proceed.

Select an Office 365 user account on which the data will be restored. Click on the dropdown arrow to view the available Office 365 user accounts.

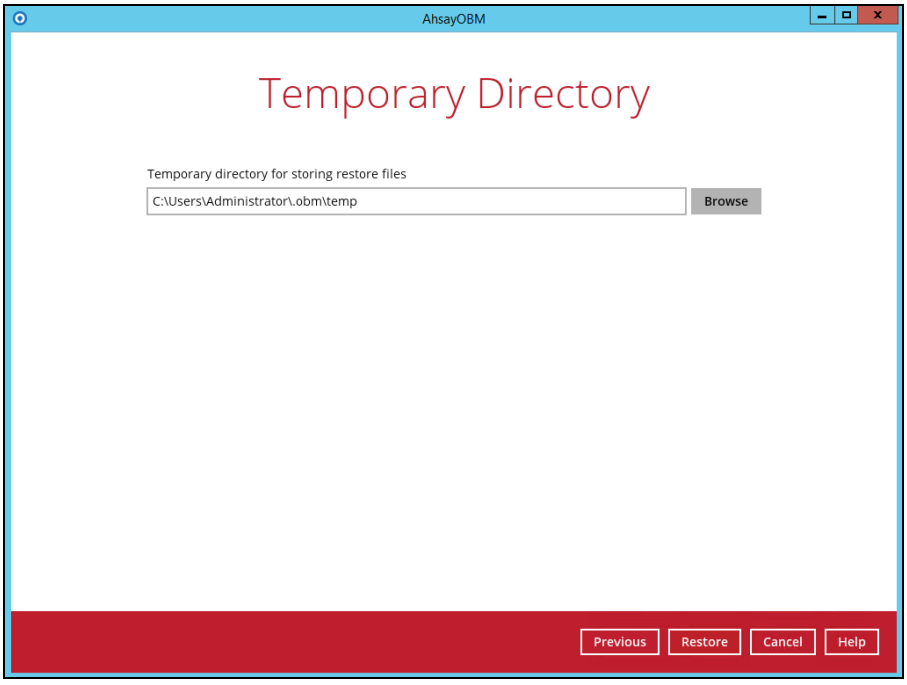

AhsayOBM
Alternate Location
Office 365 account
[redacted]@ahsaybackup.onmicrosoft.com
User
[redacted]@ahsaybackup.onmicrosoft.com
Previous
Next
Cancel
Help


AhsayOBM
Alternate Location
Office 365 account
[redacted]@ahsaybackup.onmicrosoft.com
User
[redacted]@ahsaybackup.onmicrosoft.com
[redacted]@ahsaybackup.onmicrosoft.com
[redacted]@ahsaybackup.onmicrosoft.com
Previous
Next
Cancel
Help

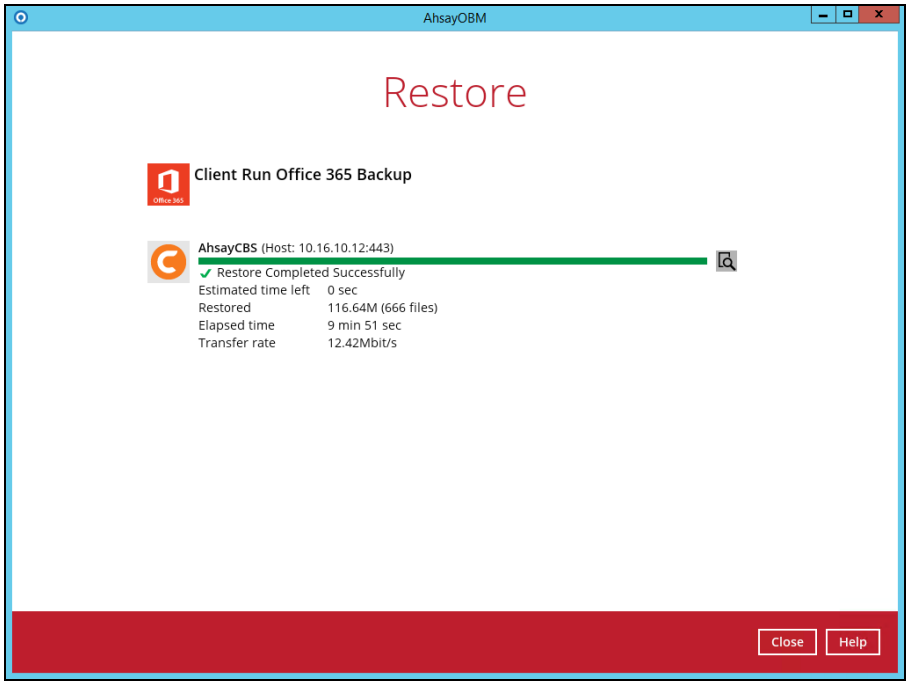


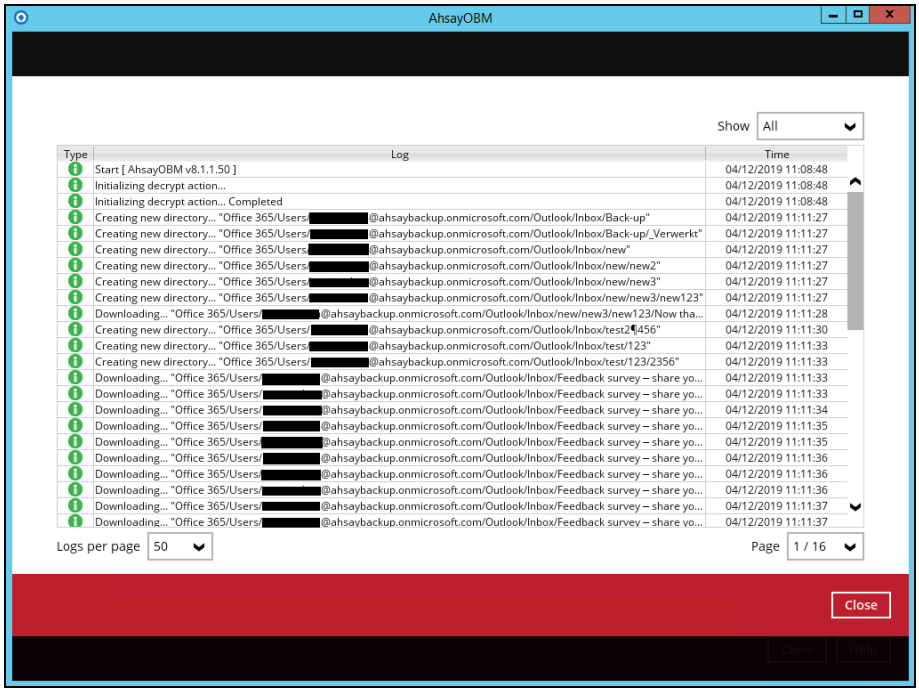
Click **Next** to proceed.

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

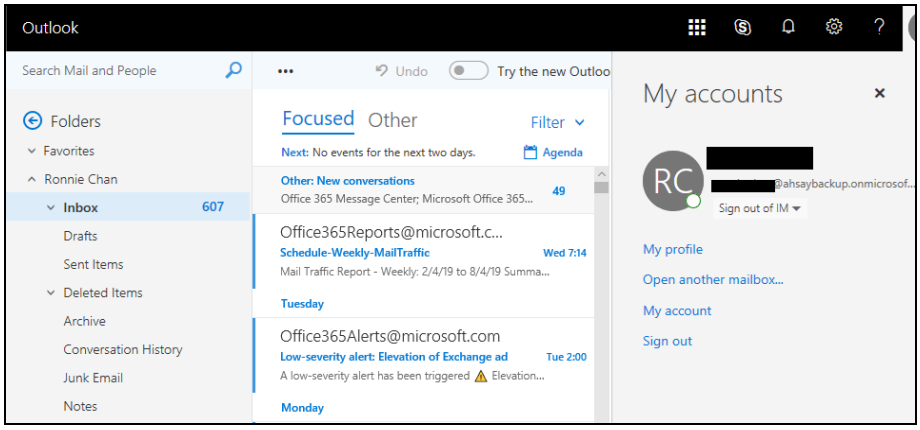


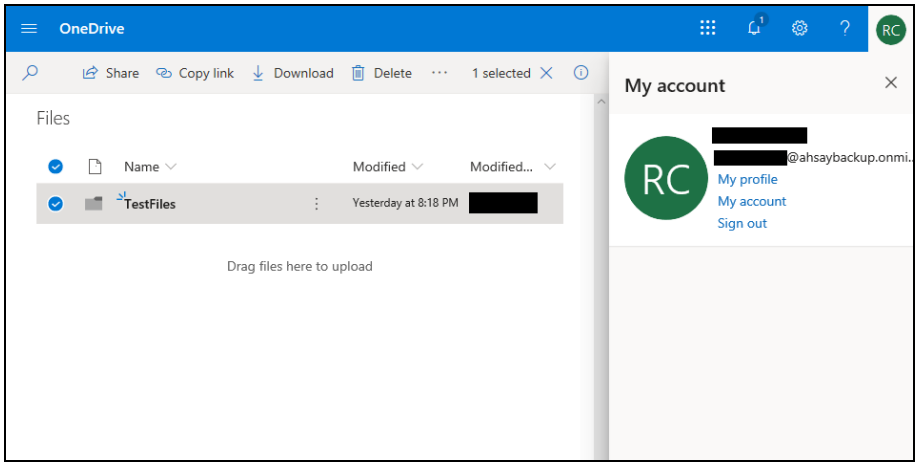
Restore is completed. Click the to show the log of the restoration.

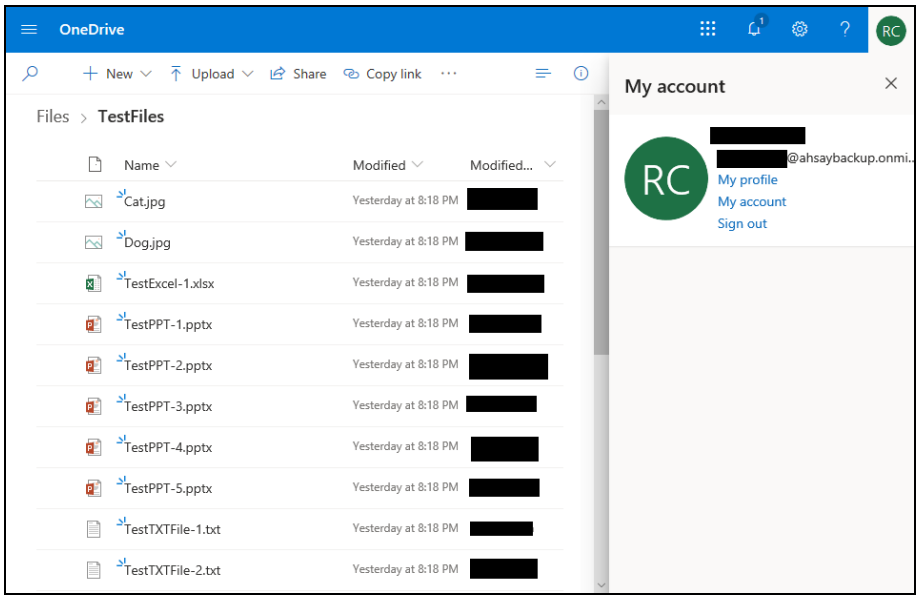




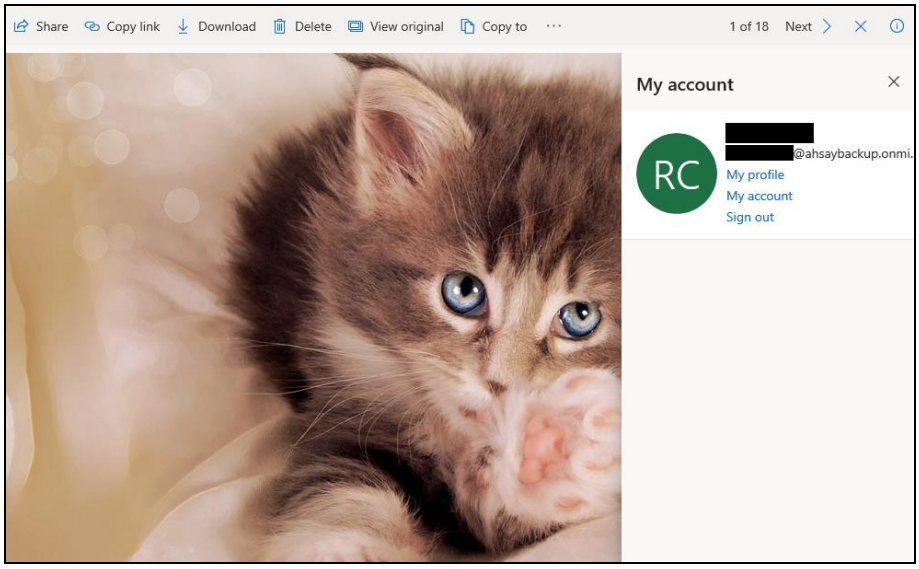
To check if the mails from Outlook and files from OneDrive are fully restored in the original location, login and check the files in Outlook and OneDrive. As you can see on our example screen shot below, **RC** is logged in and the **Inbox** from Outlook and **TestFiles** folder from OneDrive are available.



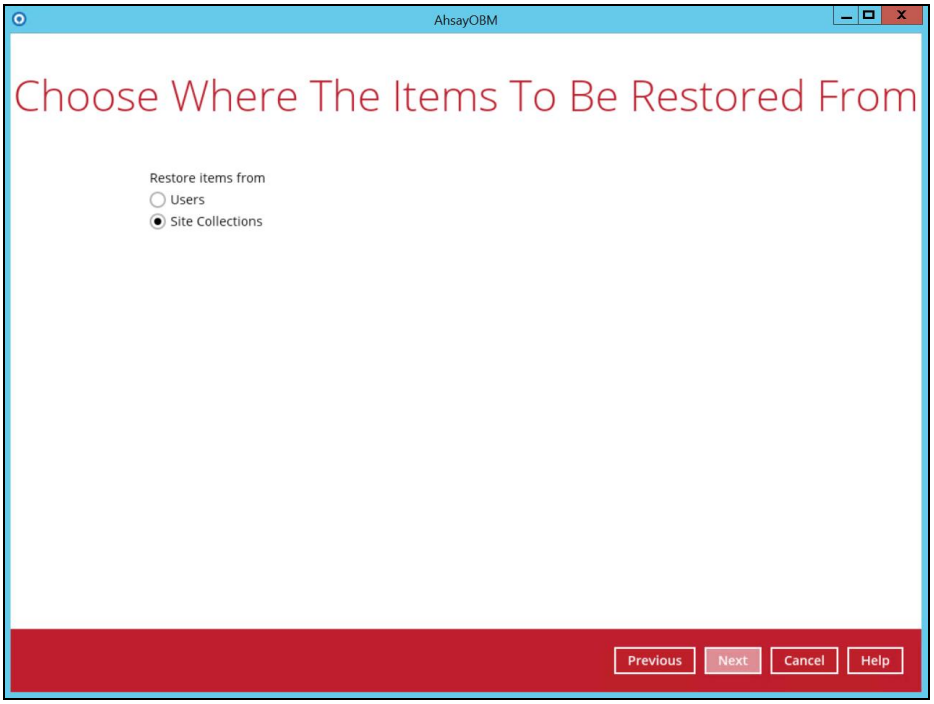




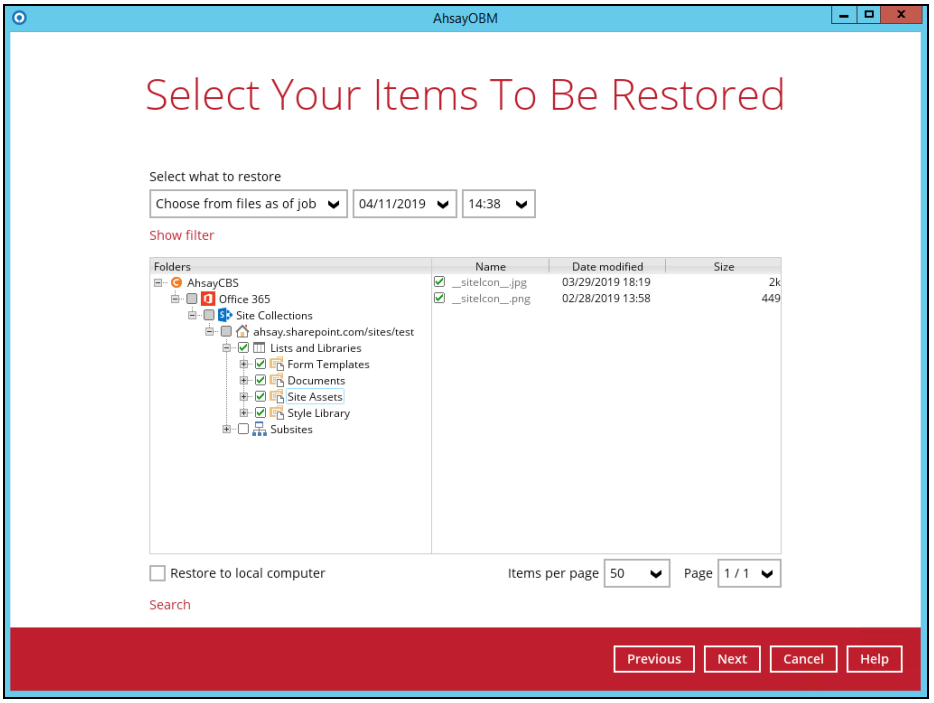
Here is a preview of one of restored files from OneDrive.


Share
Copy link
Download
Delete
View original
Copy to
1 of 18
Next
My account
RC
[redacted]@ahsaybackup.onmi...
My profile
My account
Sign out

7.1.2. From Site Collections



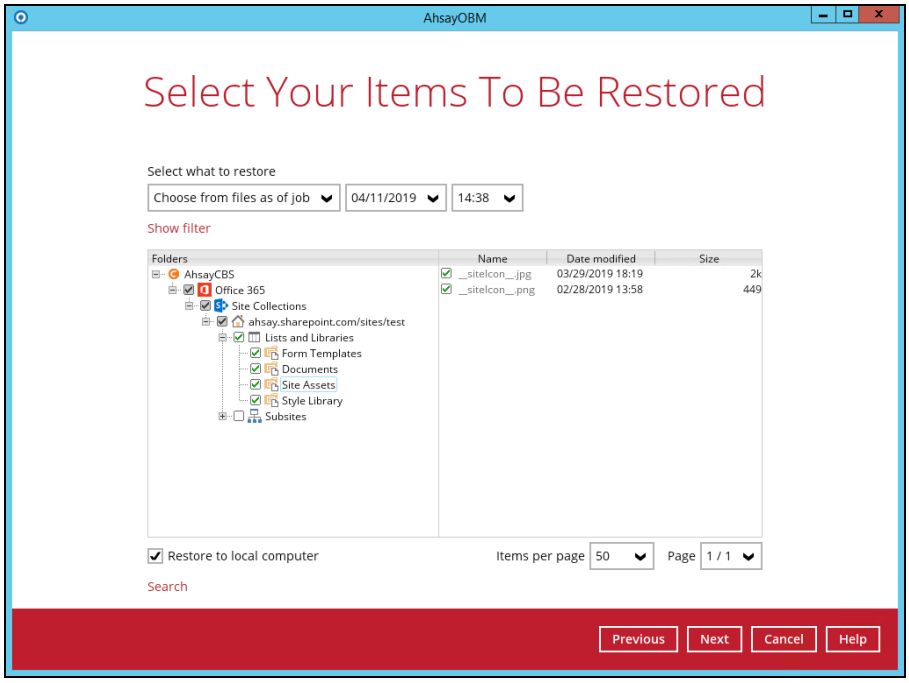
Select the item(s) you would like to restore. You can also choose to restore backed up file from a specific backup job of your choice using the **Select what to restore** drop-down menu at the top. Click **Next** to proceed when you are done with the selection.



Select the destination you would like the mail objects to be restored.

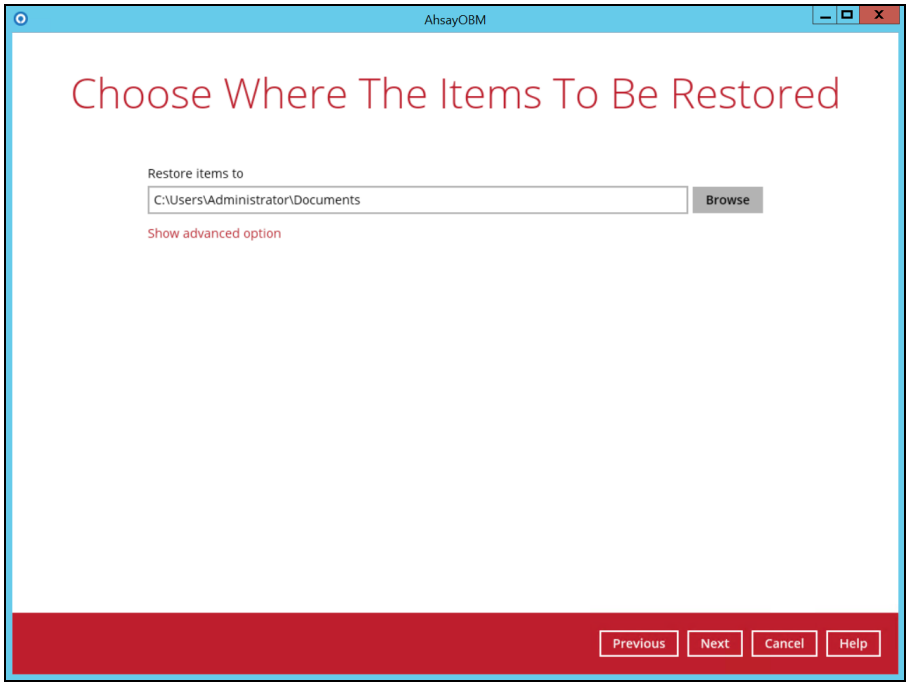
7.1.2.1. Local machine

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



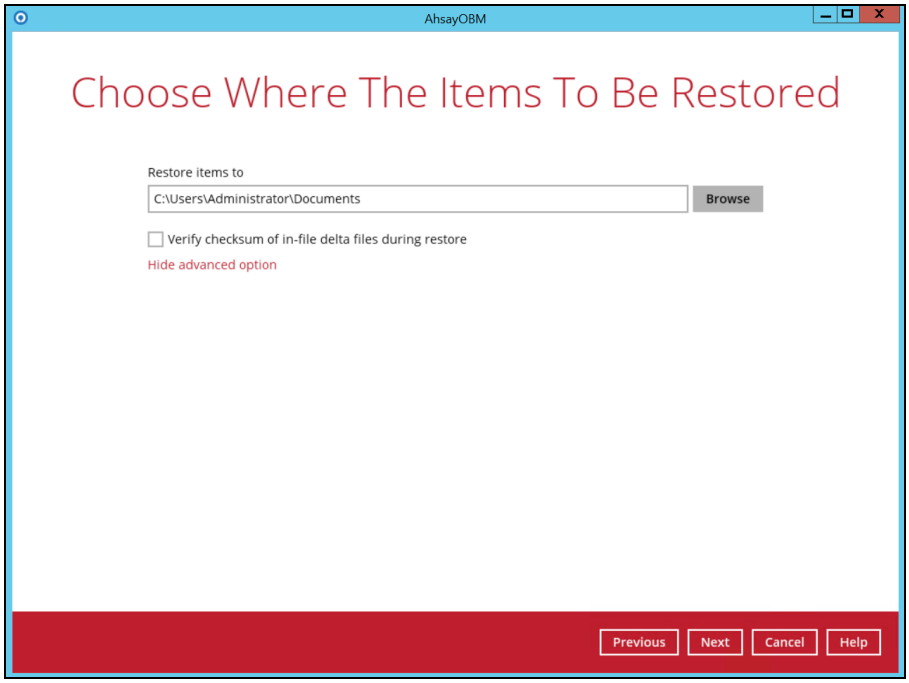
Click the **Browse** button to select a path on where you want the items to be restored on your local computer. Make sure it has enough space to accommodate your restoration.

Also, click the **Show advanced option** to configure other restore settings.

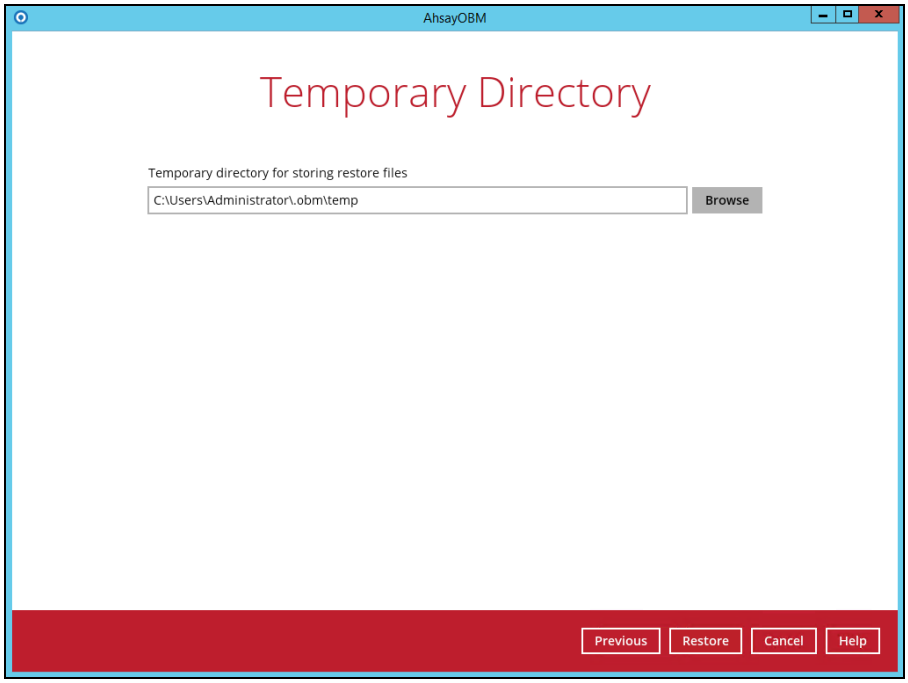


Verify checksum of in-file delta files during restore
By enabling this option, the checksum of in-file delta files will be verified during the restore process. This will check the data for errors during the restore process and create a data summary of the in-file delta files which will be included in the report.

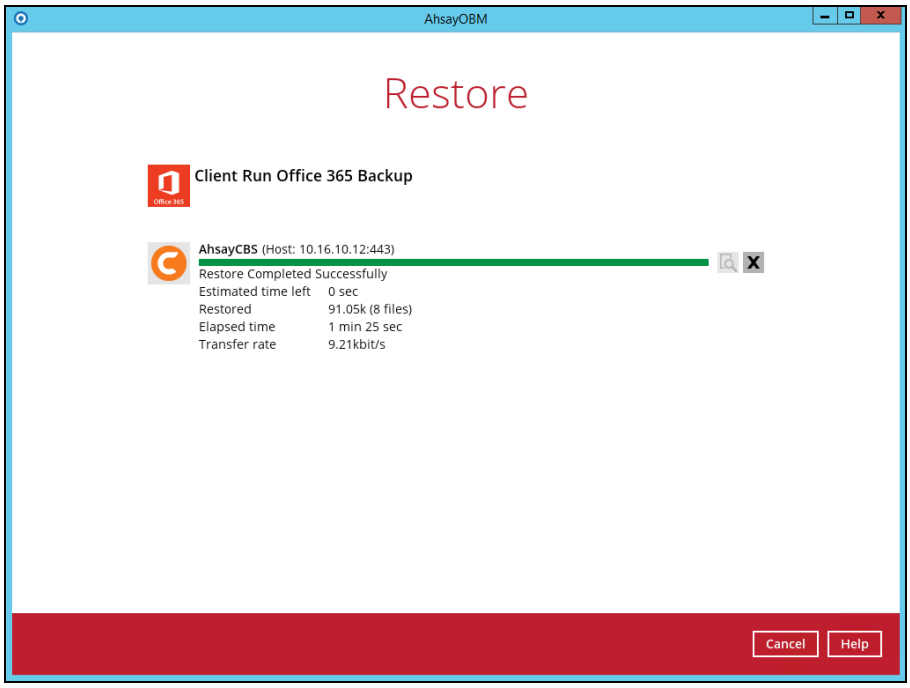
Click **Next** to proceed.

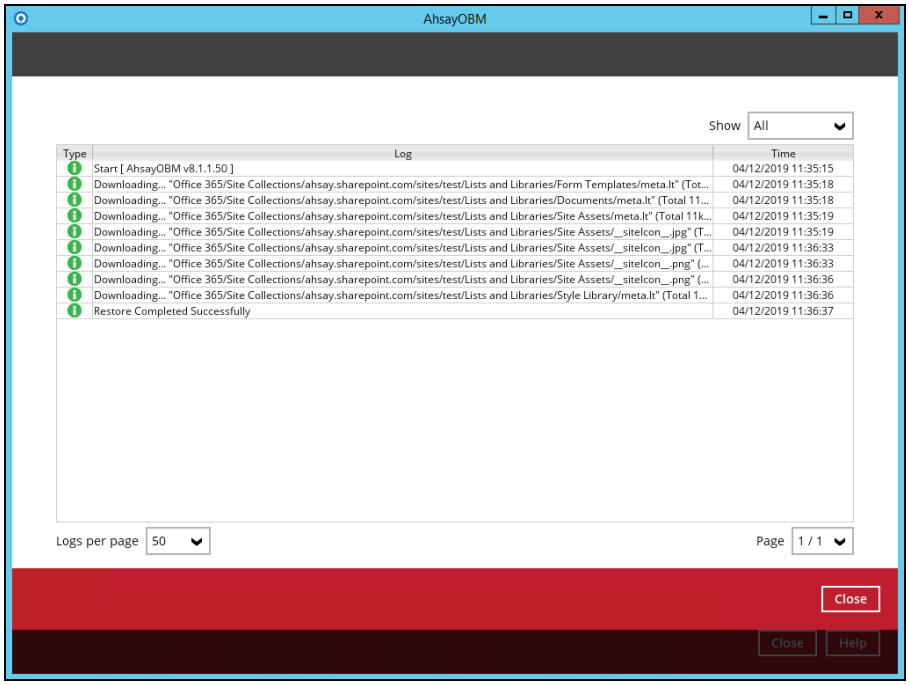


Select the temporary directory for storing temporary files, such as delta files when they are being merged, click **Restore** to start the restoration

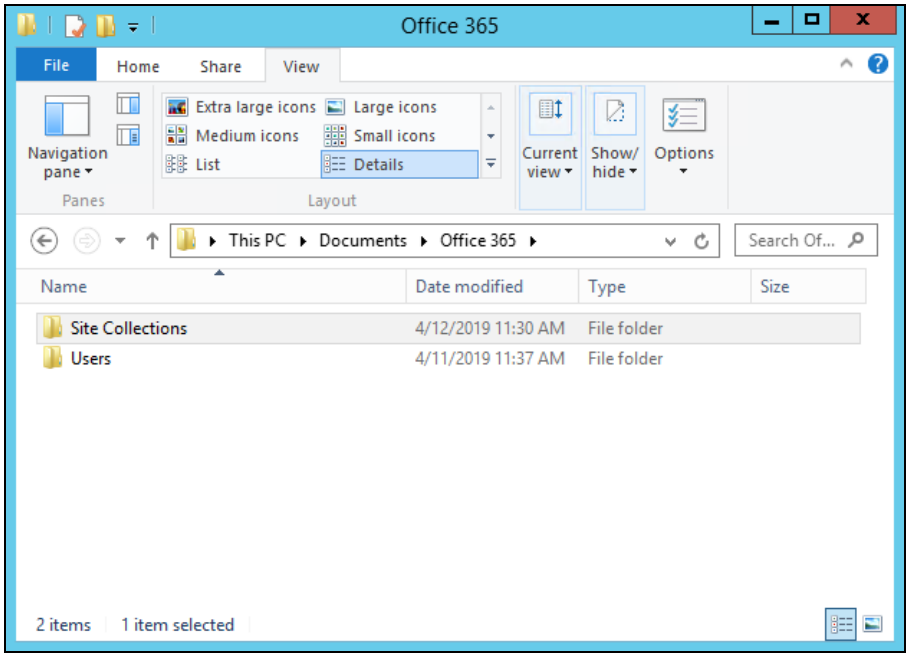


Restore is completed. Click the to show the log of the restoration.

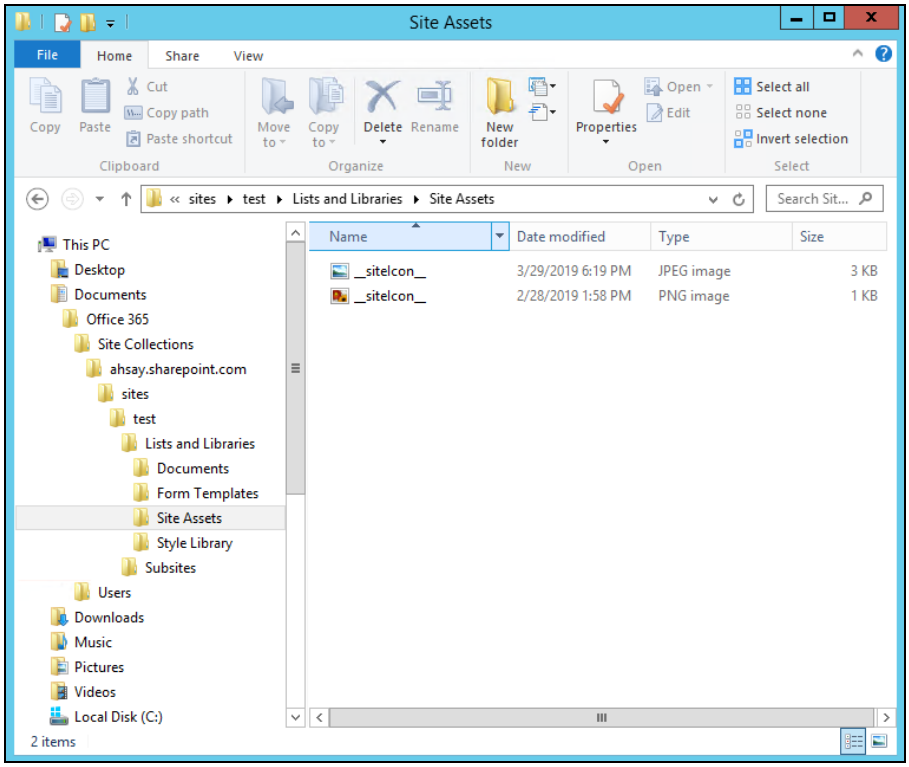




To check if the files from the Site Collections are fully restored in the location machine on the selected directory which is **C:\Users\Administrator\Documents,** go to the Documents folder. There should be an available **Office 365** folder.

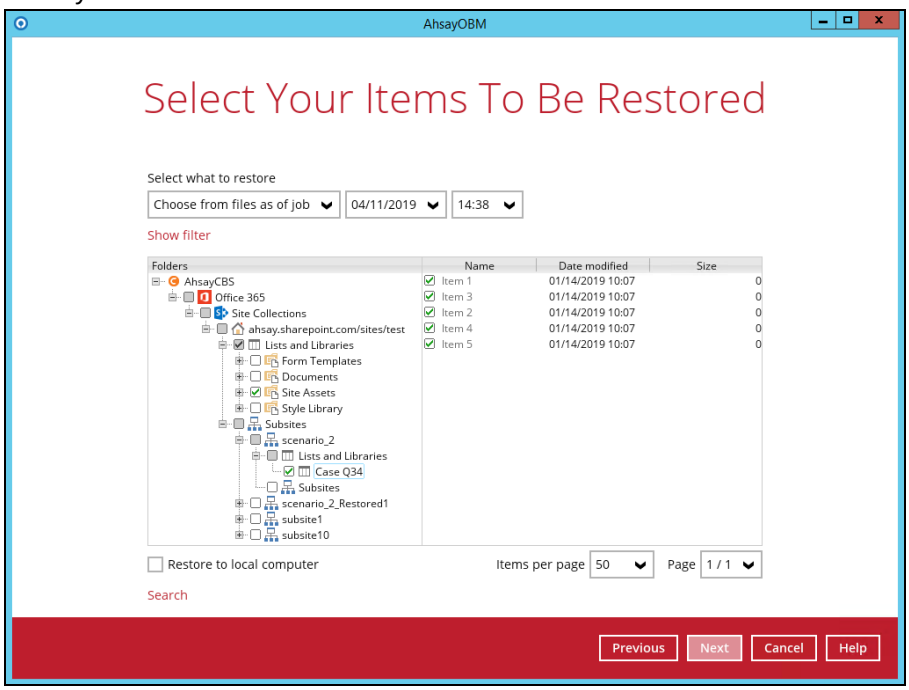


Open the Office 365 folder and you will see a **Site Collections** folder. This includes the selected SharePoint site which is the **ahsay.sharepoint.com.** Open the folder and you will see the sites, list and libraries, and subsites.

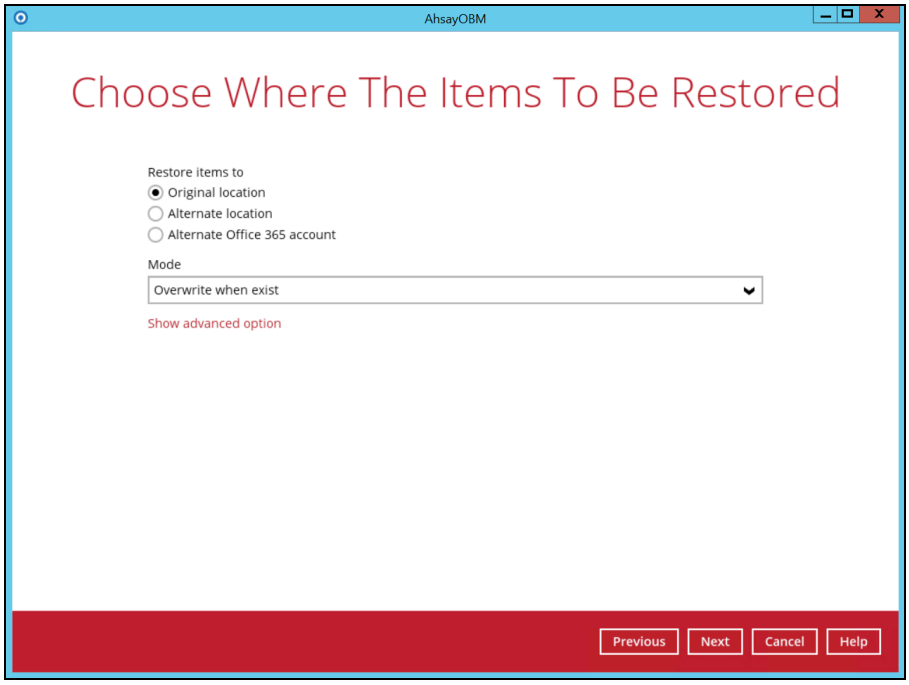


7.1.2.2. Original location

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.



Choose from the following three (3) options on where you want your items to be restored. Select the **Original location**.



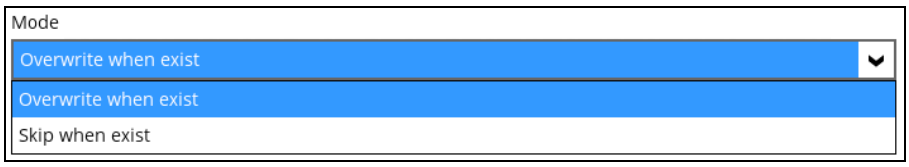
Select a **Mode**.

- **Overwrite when exist**

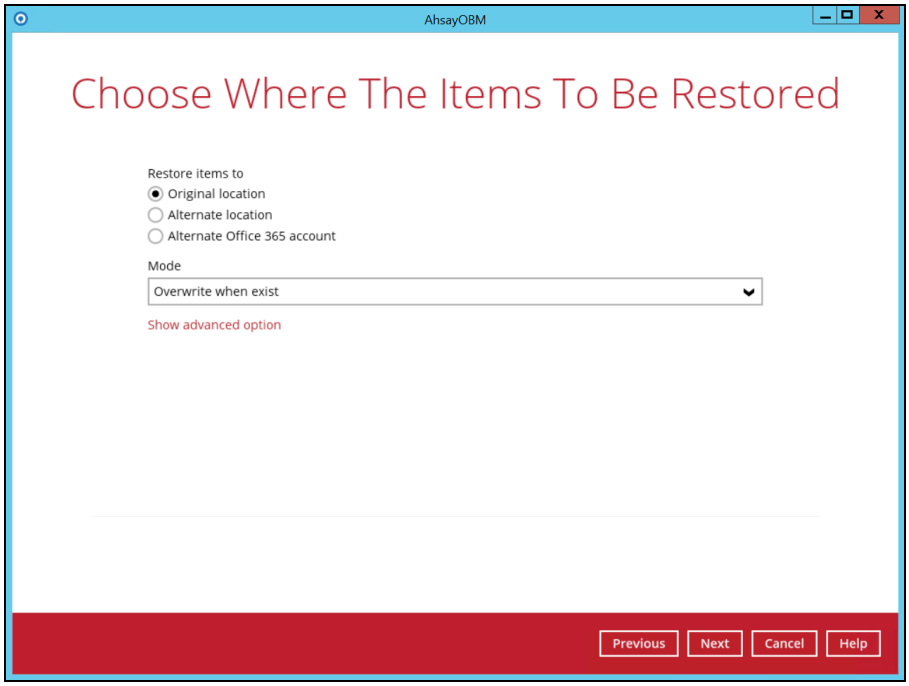
If the data that you will be restoring is already available in the Office 365 account, then you have a choice to still overwrite the existing data.

- **Skip when exist**

  If the data you will be restoring is already available in the Office 365 account, then you have a choice to skip and move to the next one.

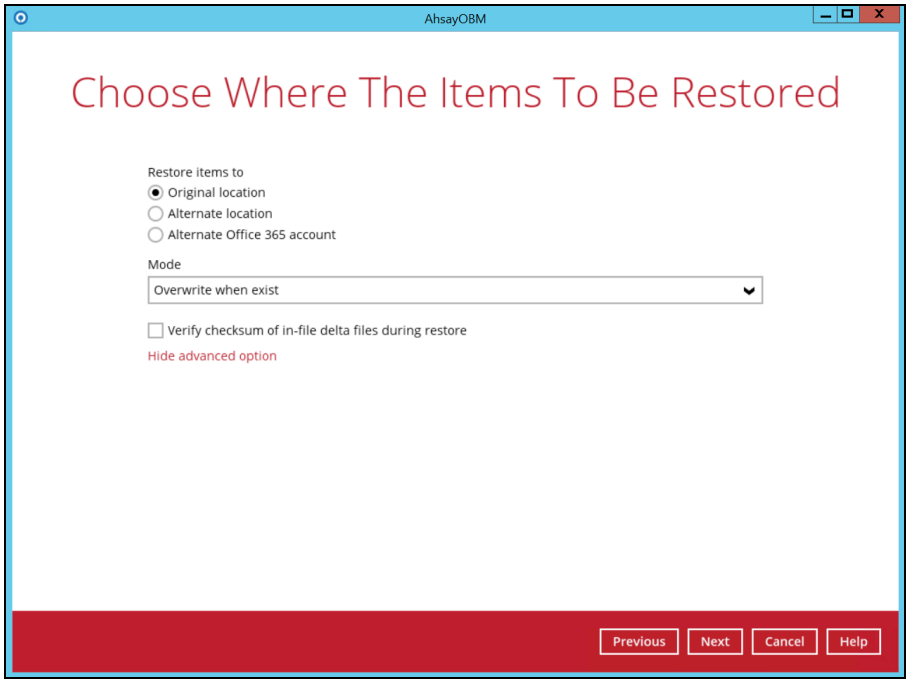


Click the **Show advanced option** to configure other restore settings.

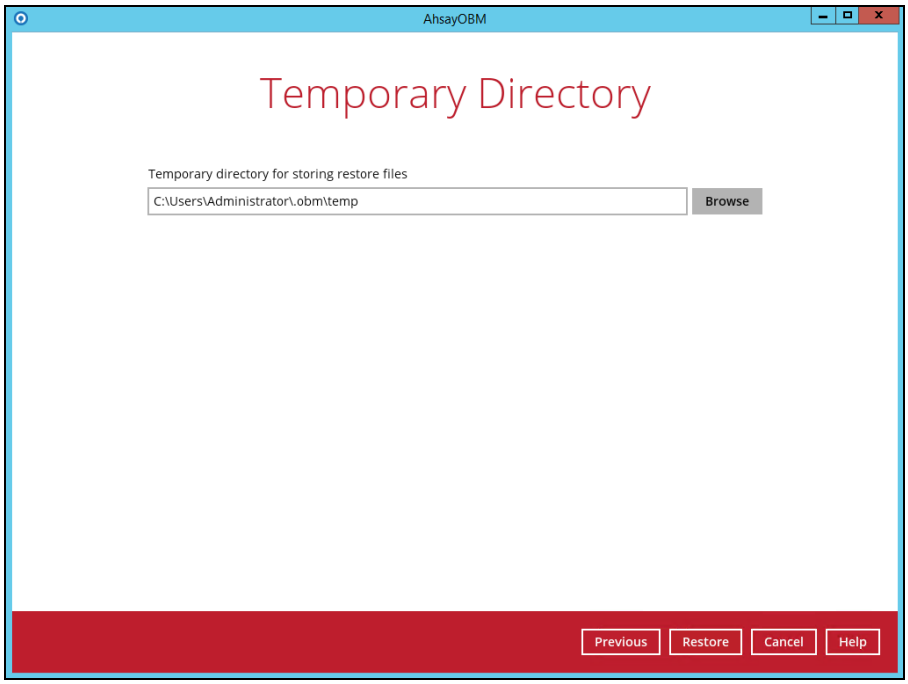


Verify checksum of in-file delta files during restore
By enabling this option, the checksum of in-file delta files will be verified during the restore process. This will check the data for errors during the restore process and create a data summary of the in-file delta files which will be included in the report.

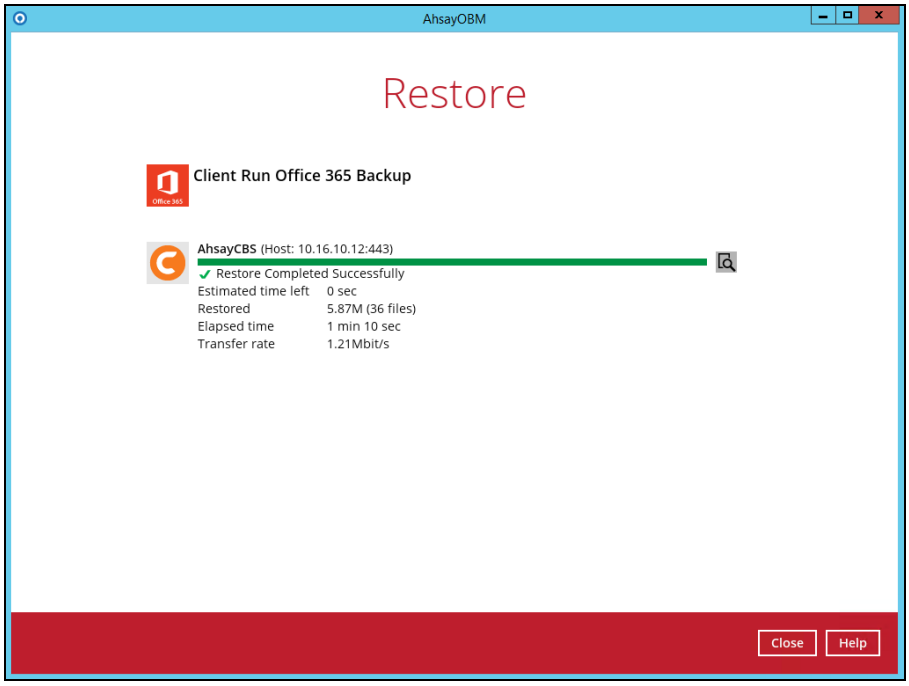
Click **Next** to proceed.

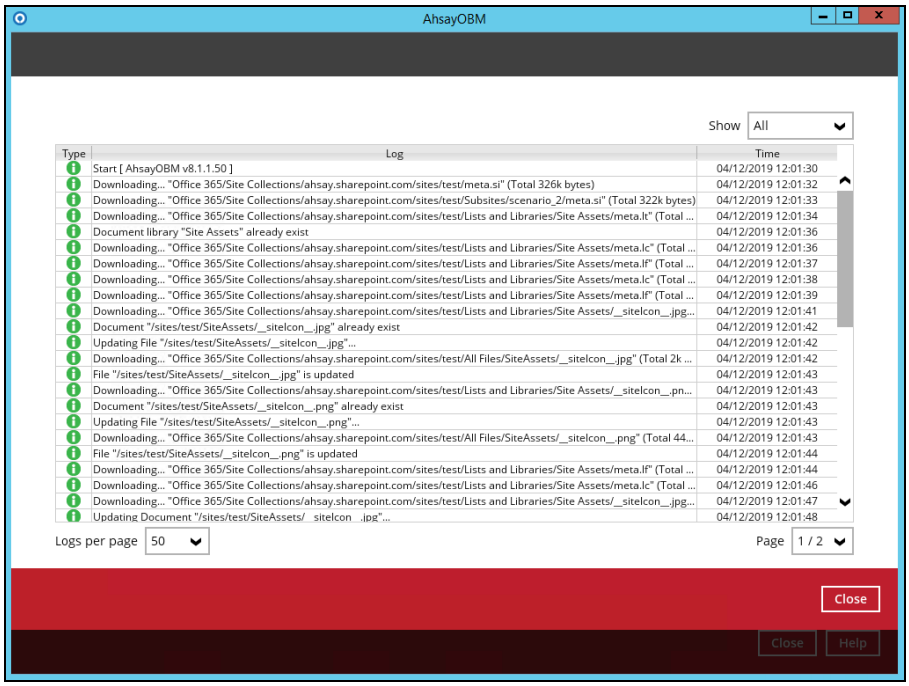


Select the temporary directory for storing temporary files, such as delta files when they are being merged, click **Restore** to start the restoration

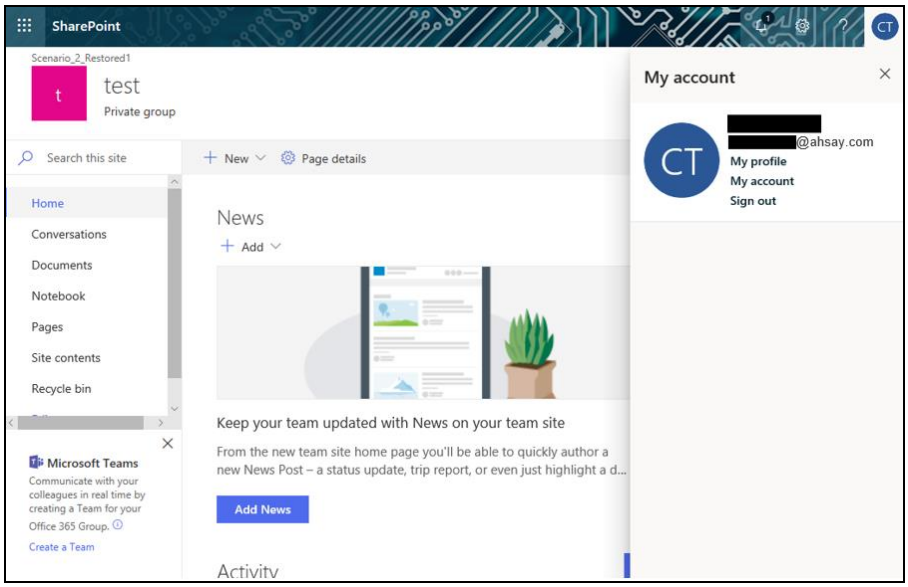


Restore is completed. Click the to show the log of the restoration.



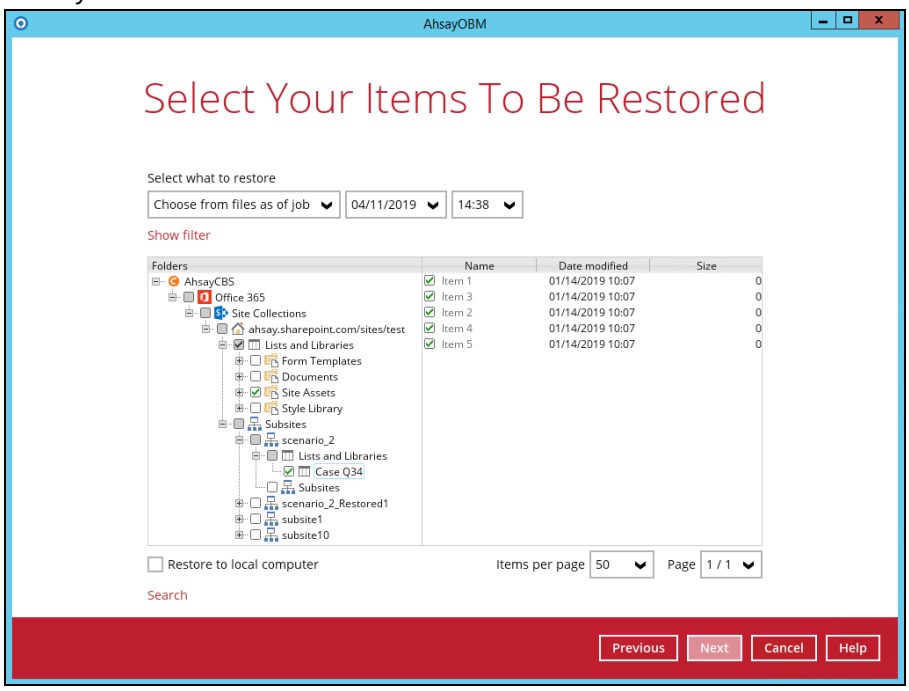


To check if the selected site from Site Collections is fully restored, login and check the SharePoint. As you can see on our example screen shot below, **abc** is logged in and the ahsay.sharepoint.com/sites/test is completely restored.

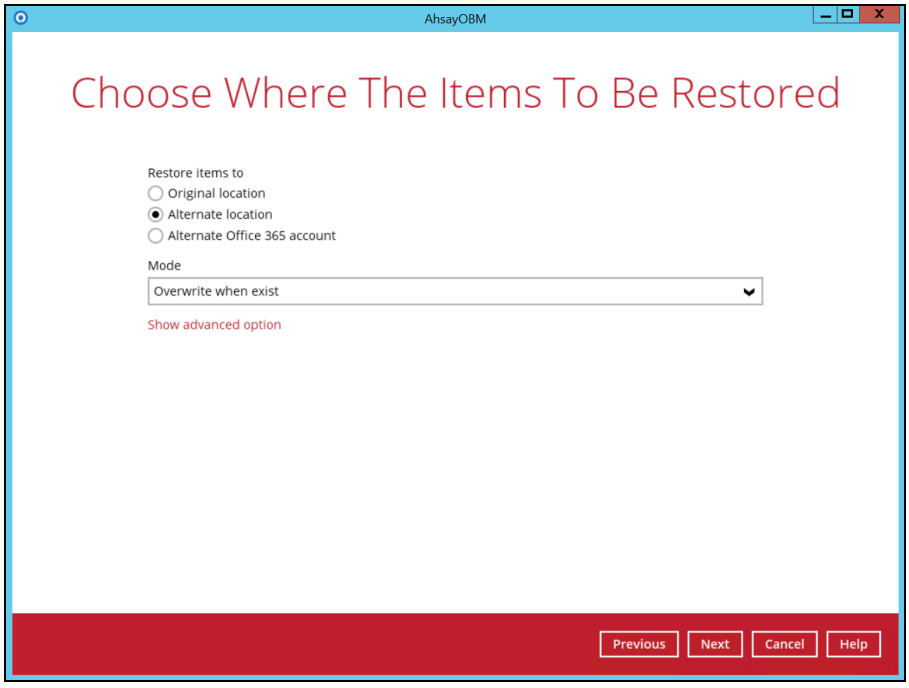


7.1.2.3. Alternate Location

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



Choose from the following three (3) options on where you want your items to be restored. Select the **Alternate location**.



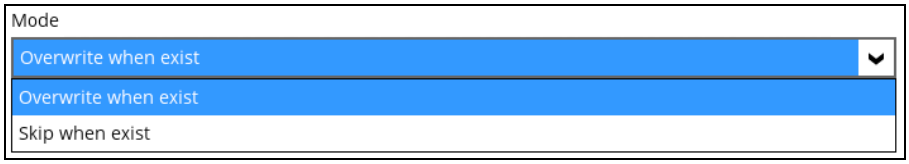
Select a **Mode**.

- **Overwrite when exist**

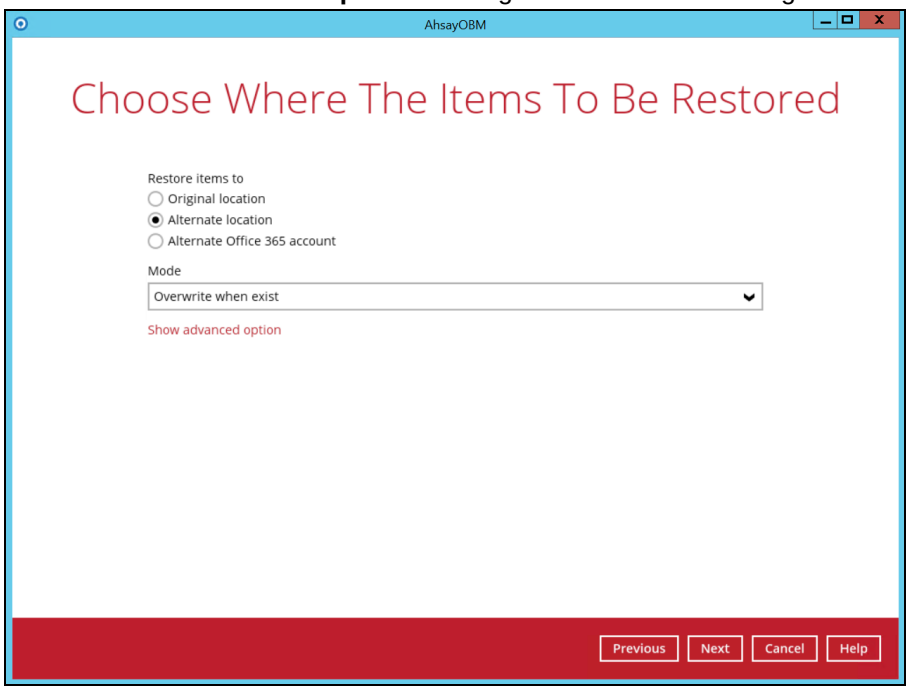
  If the data that you will be restoring is already available in the alternate location in the Office 365 account, then you have a choice to still overwrite the existing data.

- **Skip when exist**

  If the data you will be restoring is already available in the alternate location in the Office 365 account, then you have a choice to skip and move to the next one.

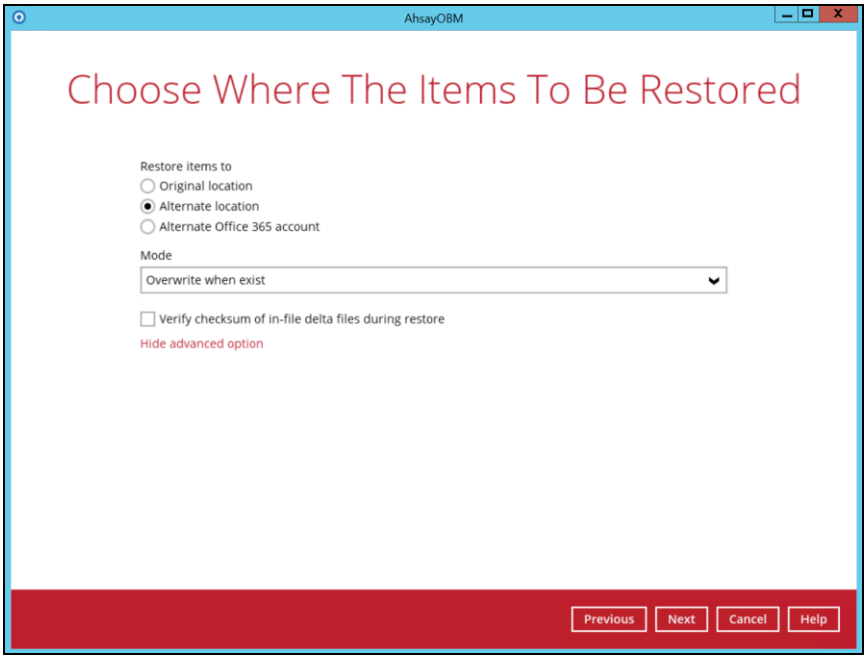


Click the **Show advanced option** to configure other restore settings.

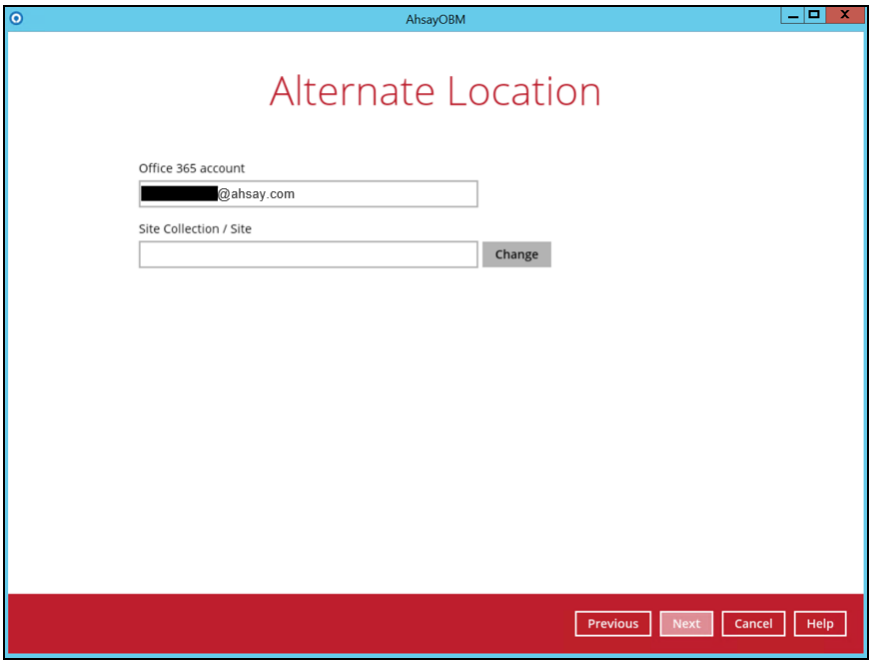


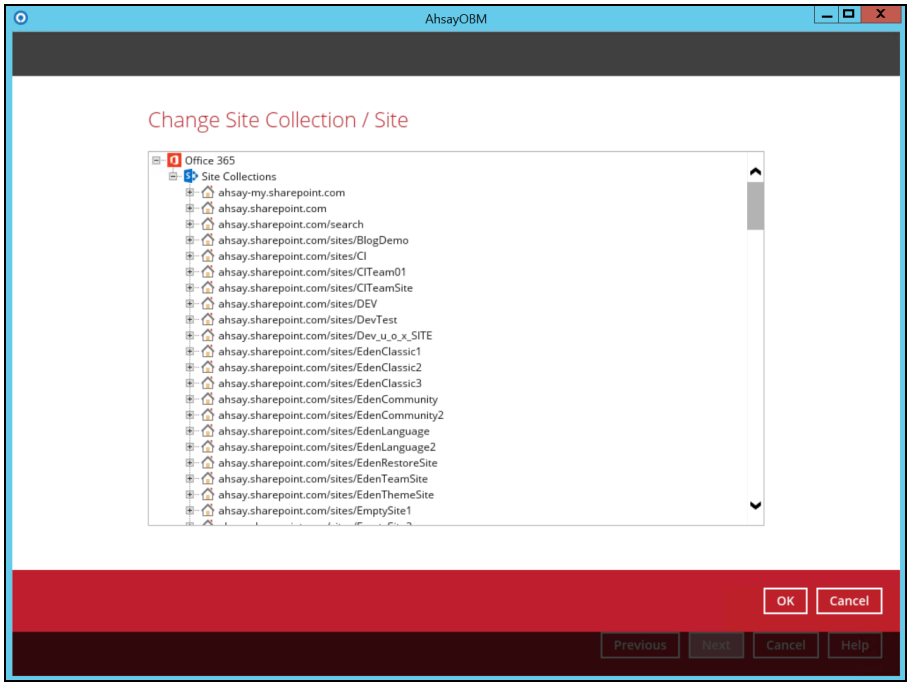
Verify checksum of in-file delta files during restore
By enabling this option, the checksum of in-file delta files will be verified during the restore process. This will check the data for errors during the restore process and create a data summary of the in-file delta files which will be included in the report.

Click **Next** to proceed.

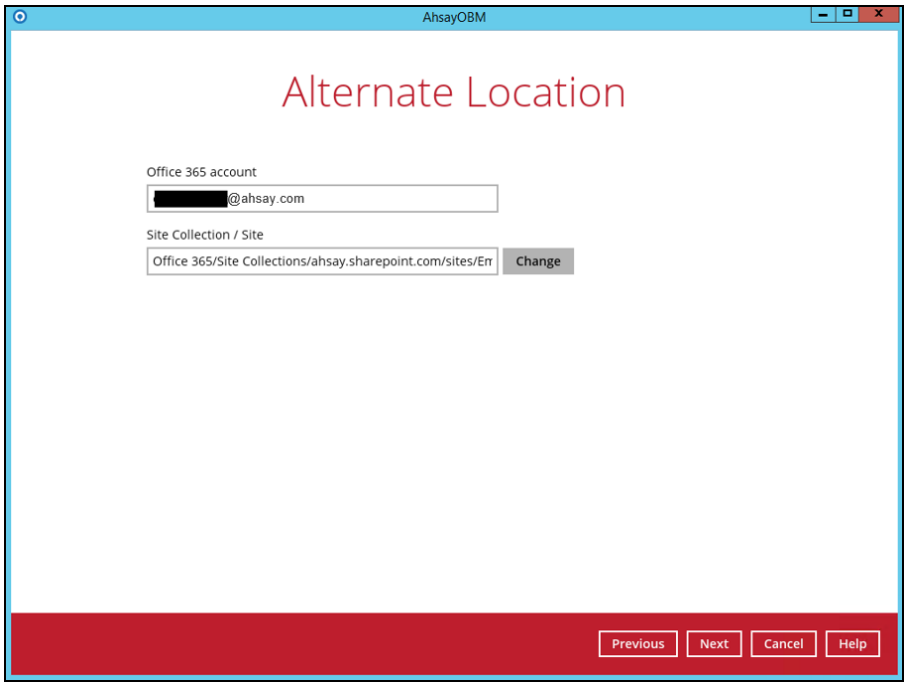


Click **Change** to select an alternate Site Collection / Site on which the data will be restored. Click on the dropdown arrow to view the available Sites.

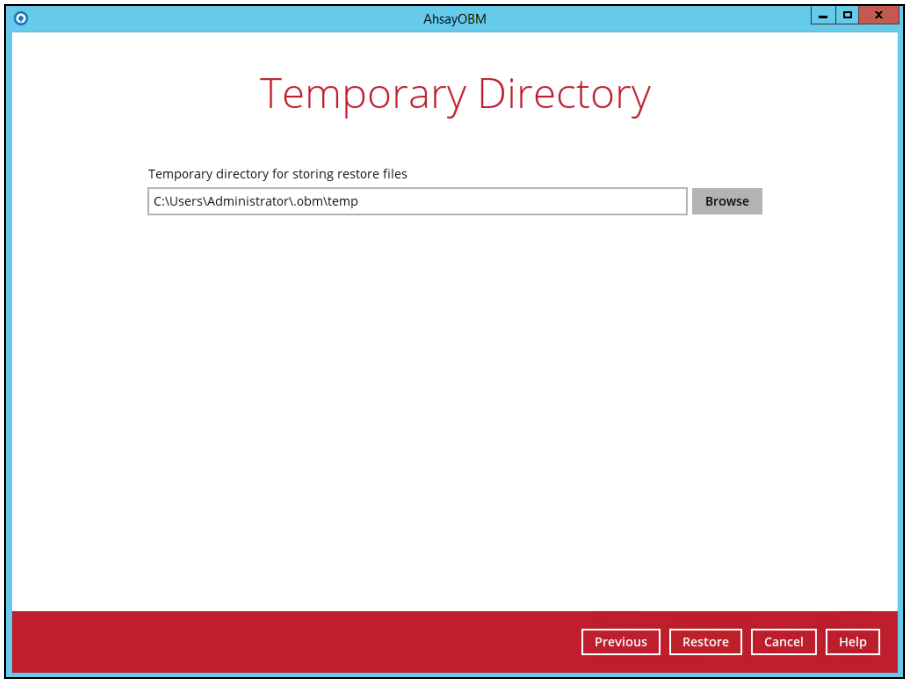




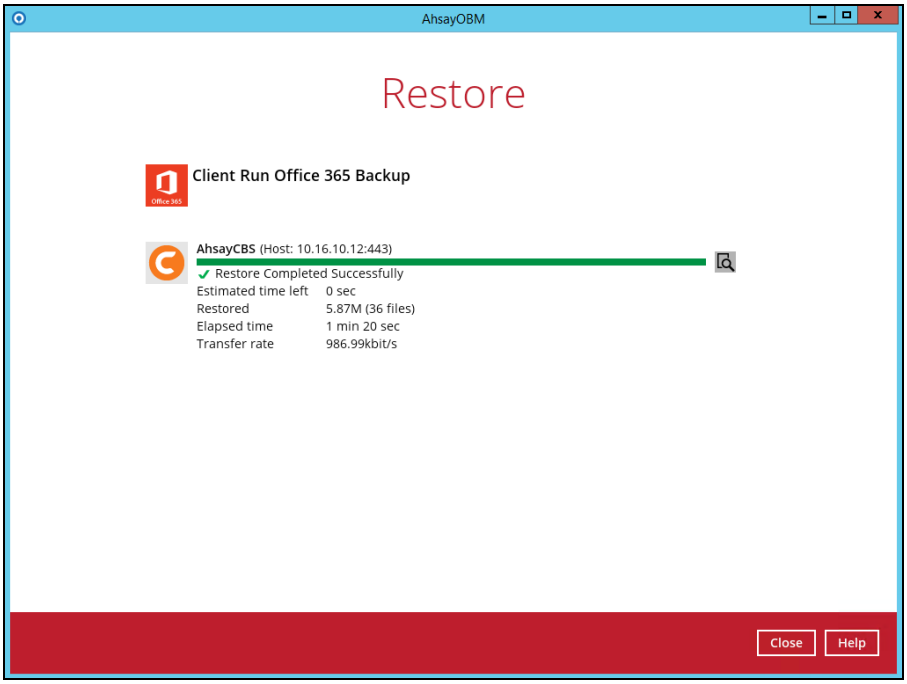
Click **Next** to proceed.

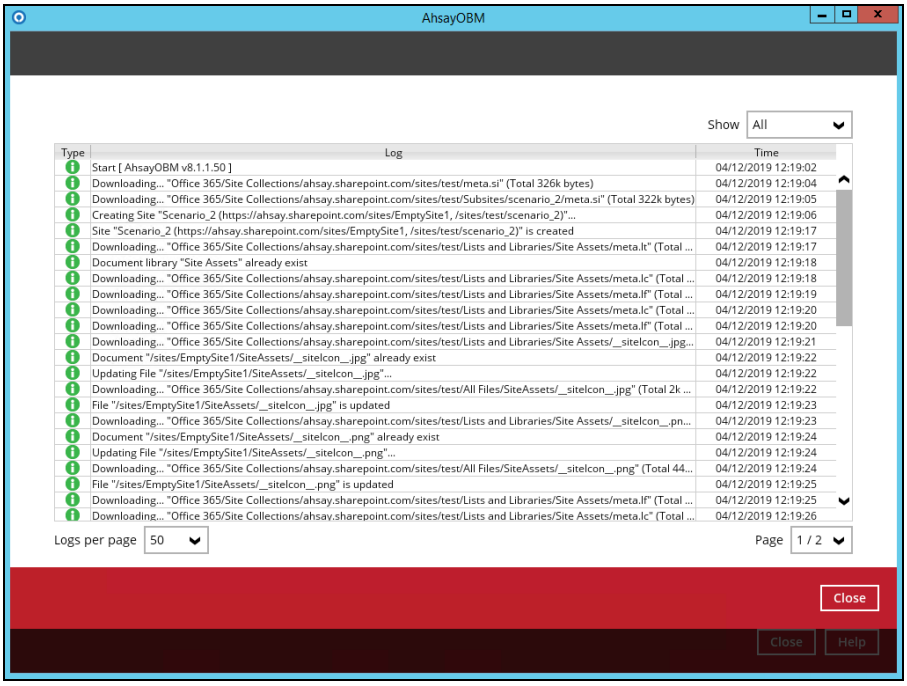


Select the temporary directory for storing temporary files, such as delta files when they are being merged, click **Restore** to start the restoration

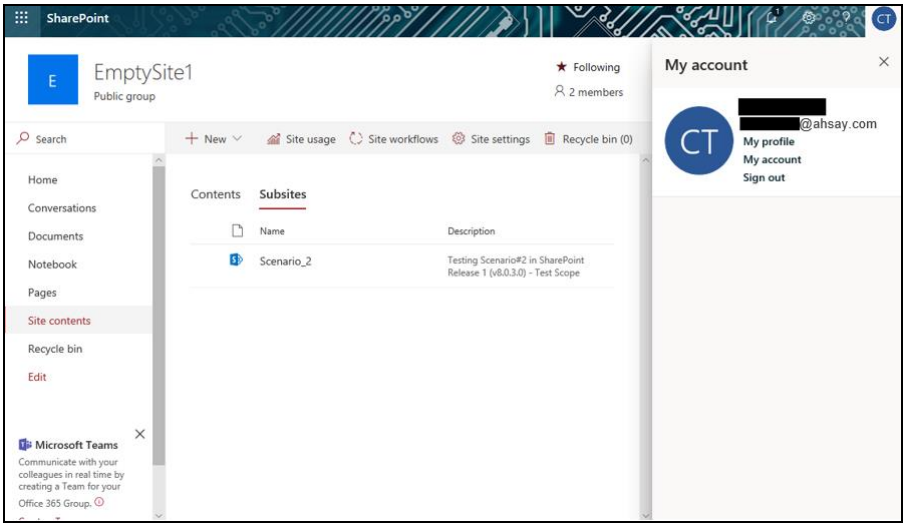


Restore is completed. Click the to show the log of the restoration.



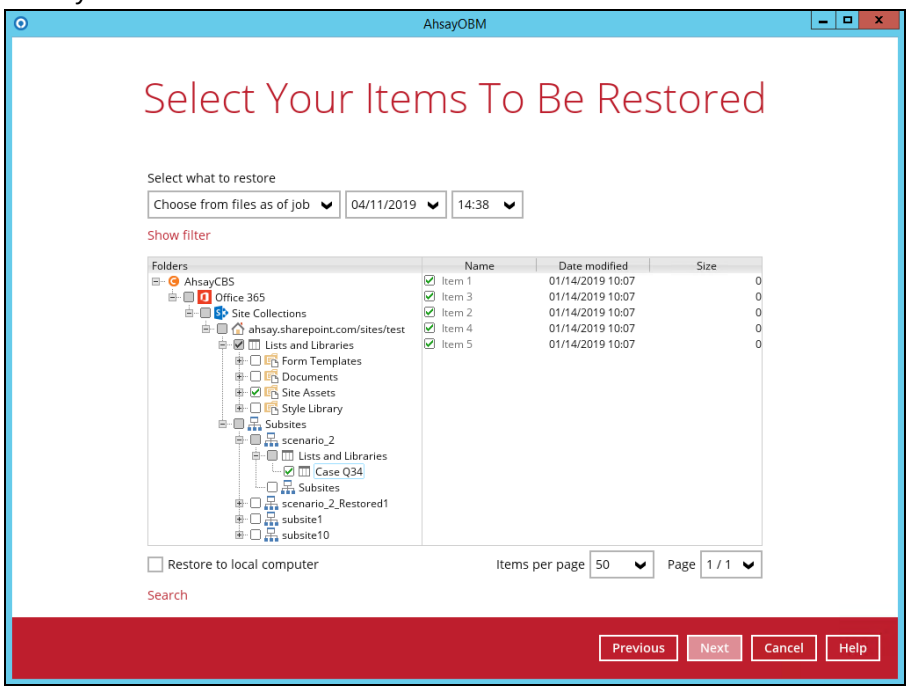


To check if the selected site from Site Collections is fully restored, login and check the SharePoint. As you can see on our example screen shot below, **abc** is logged in and the contents in ahsay.sharepoint.com/sites/test is completely restored in ahsay.sharepoint.com/sites/EmptySite1.



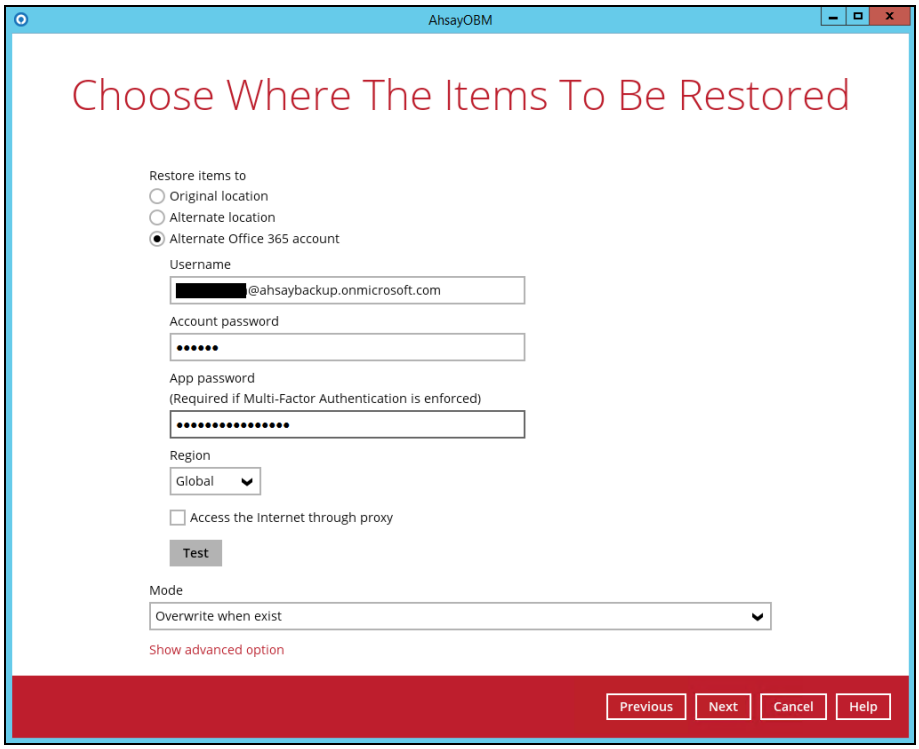
7.1.2.4. Alternate Office 365 Account

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.



Choose from the following three (3) options on where you want your items to be restored. Select the **Alternate Office 365 Account**.

Input the Username, Password, App password, and choose the region for the other Office 365 account.



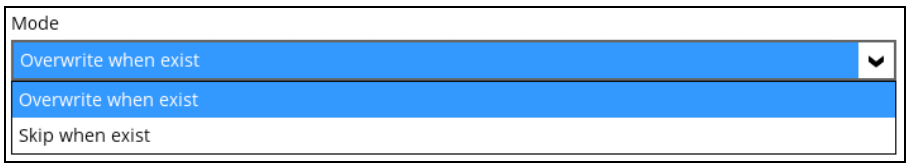
Select a **Mode**.

- **Overwrite when exist**

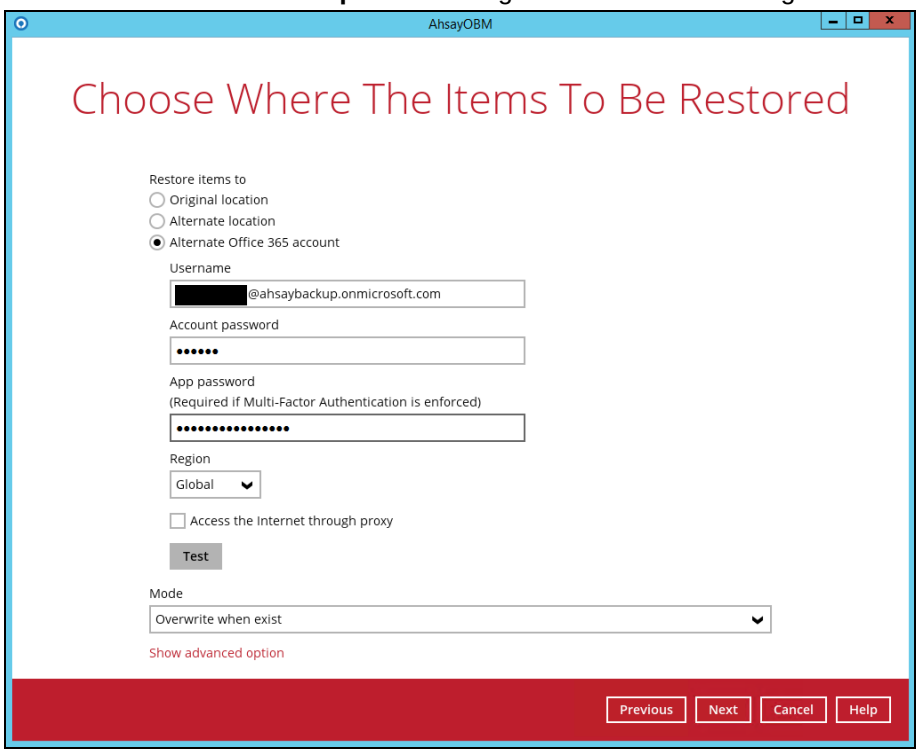
  If the data that you will be restoring is already available in the alternate Office 365 account, then you have a choice to still overwrite the existing data.

- **Skip when exist**

  If the data you will be restoring is already available in the alternate Office 365 account, then you have a choice to skip and move to the next one.

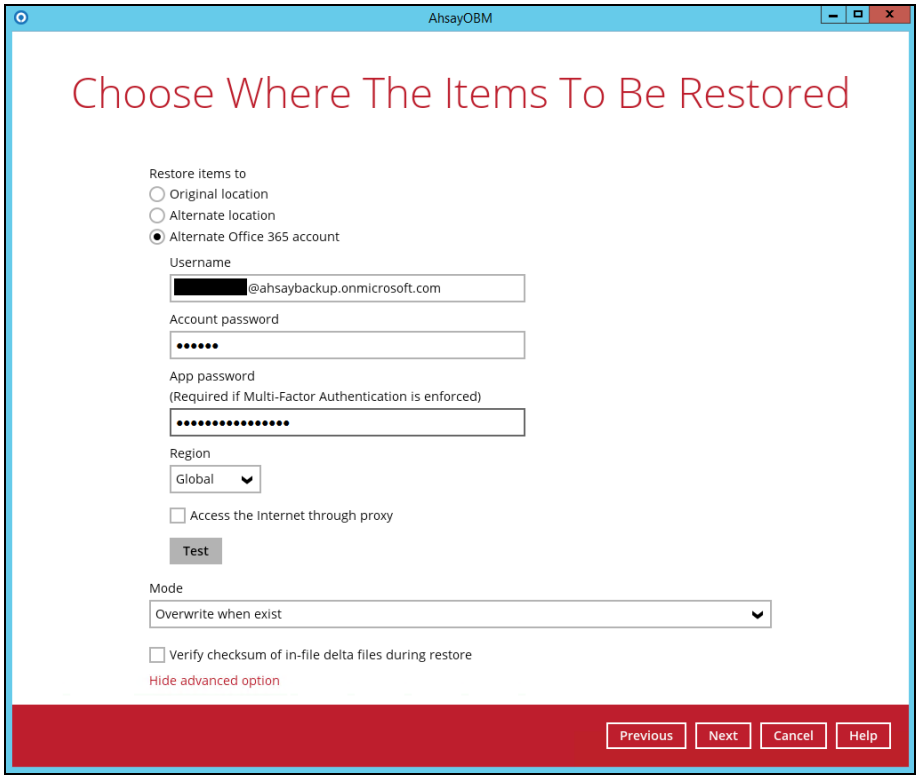


Click the **Show advanced option** to configure other restore settings.

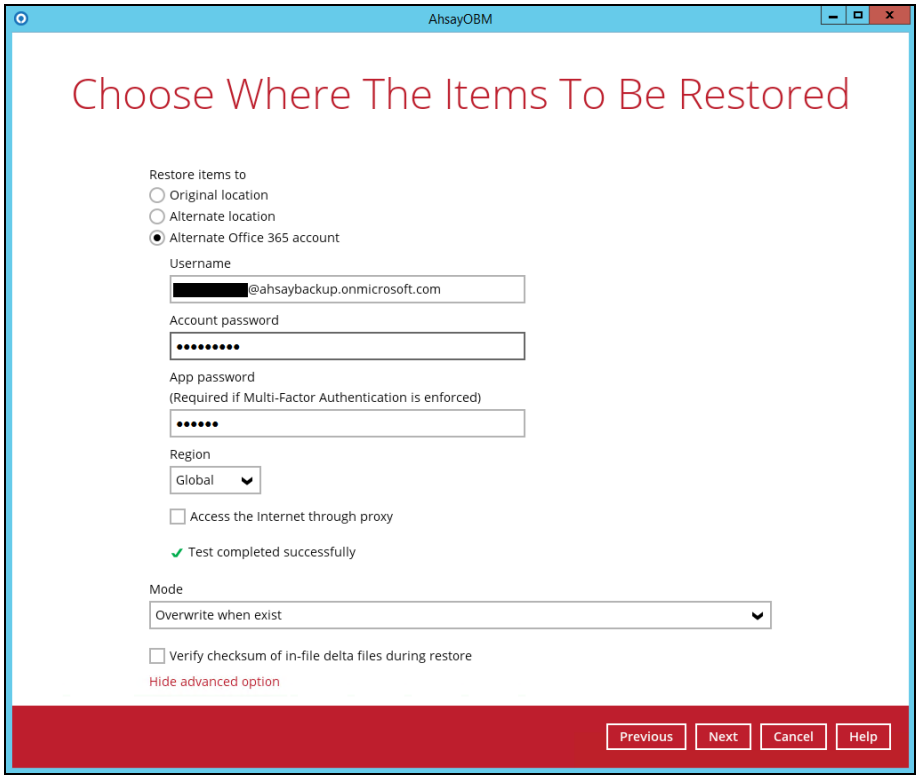


Verify checksum of in-file delta files during restore
By enabling this option, the checksum of in-file delta files will be verified during the restore process. This will check the data for errors during the restore process and create a data summary of the in-file delta files which will be included in the report.

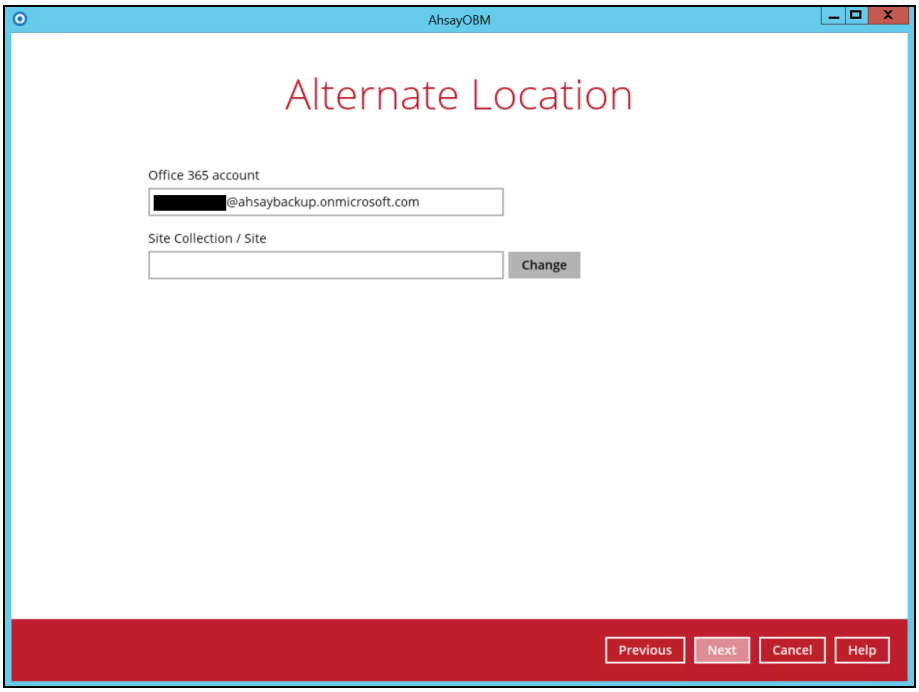
Click **Next** to proceed.

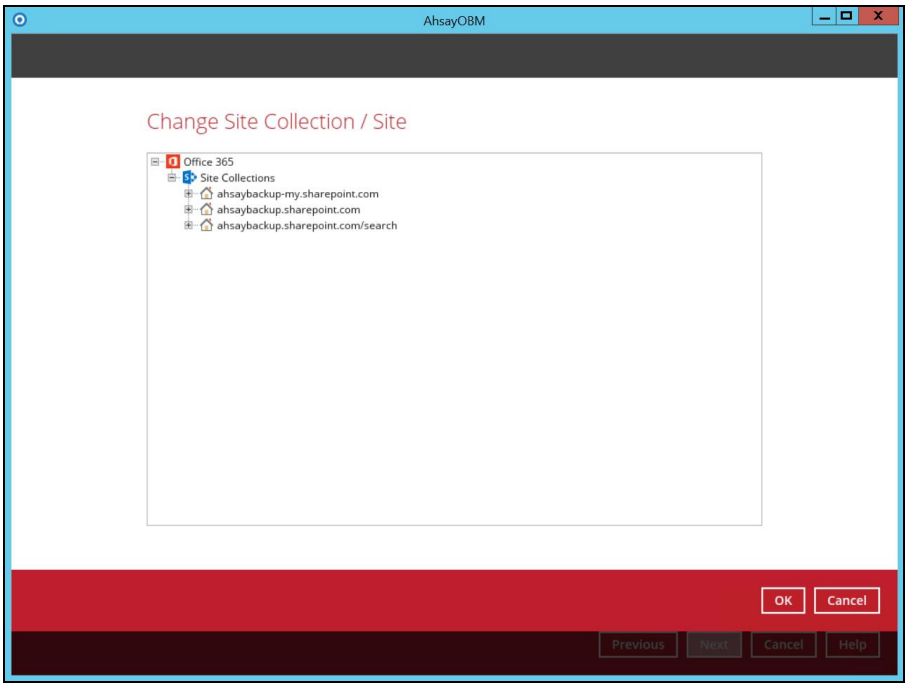


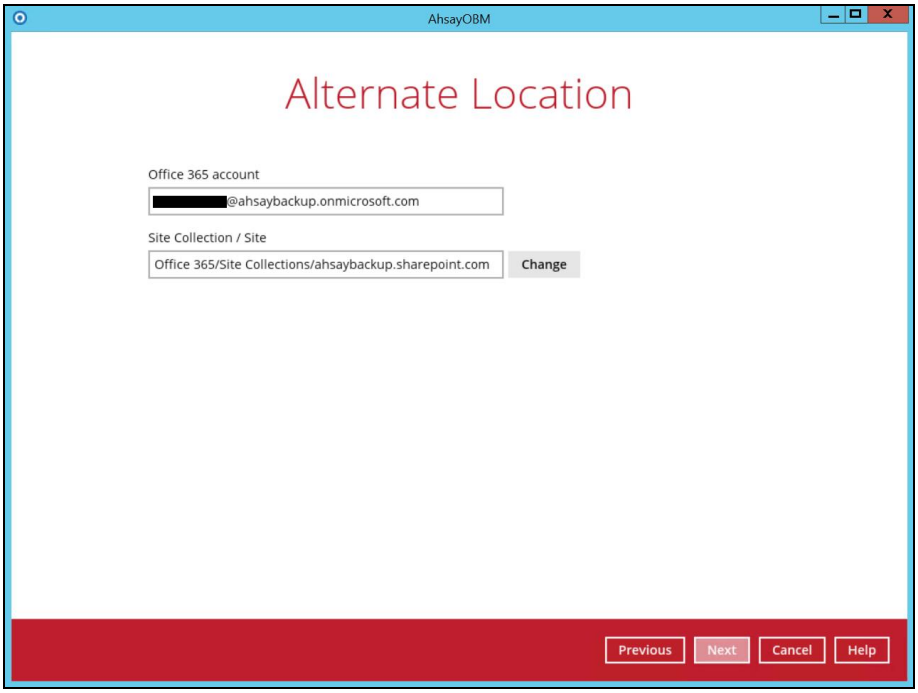
Test completed successfully shows when the validation is successful, then click **Next** to continue.



Click **Change** to select an alternate Site Collection / Site on which the data will be restored. Click on the dropdown arrow to view the available Sites.

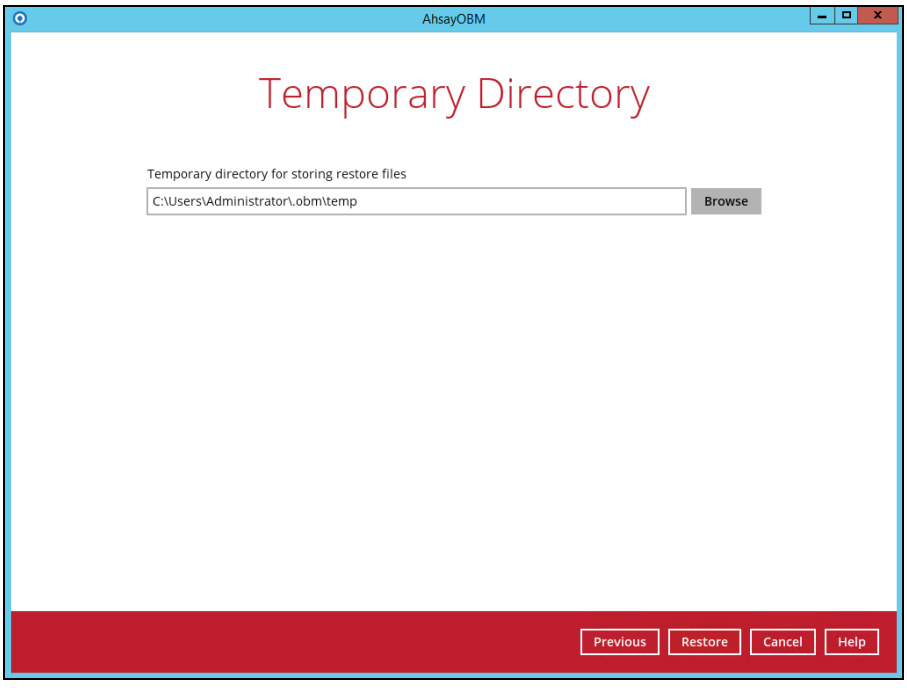




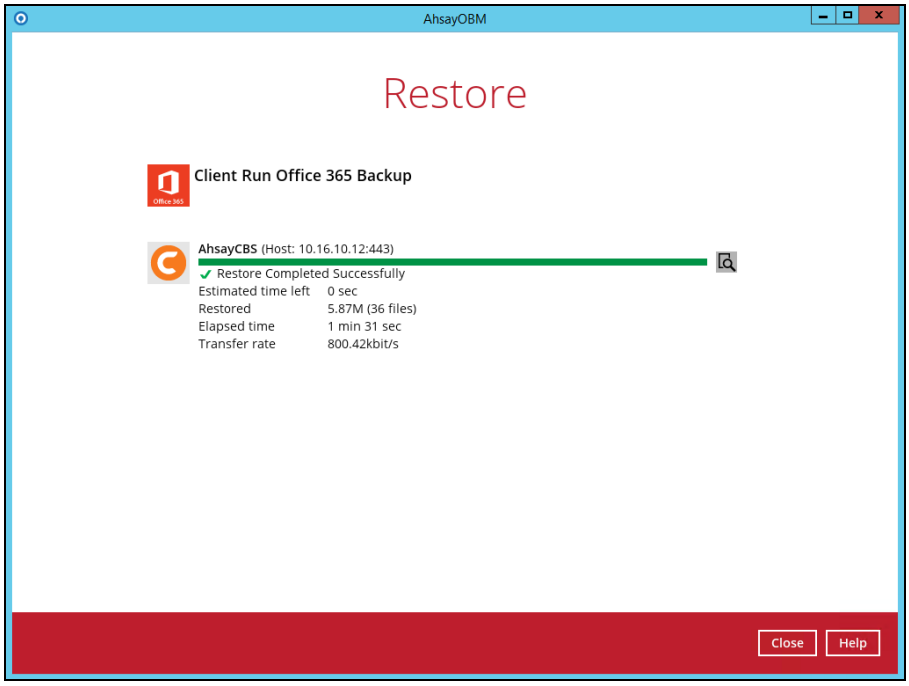


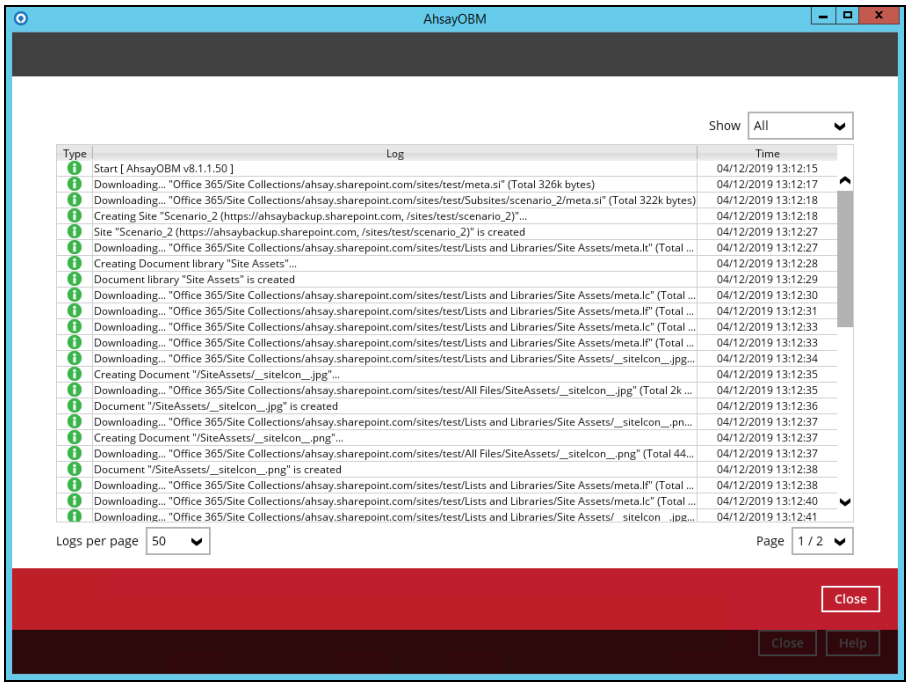
Click **Next** to proceed.

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

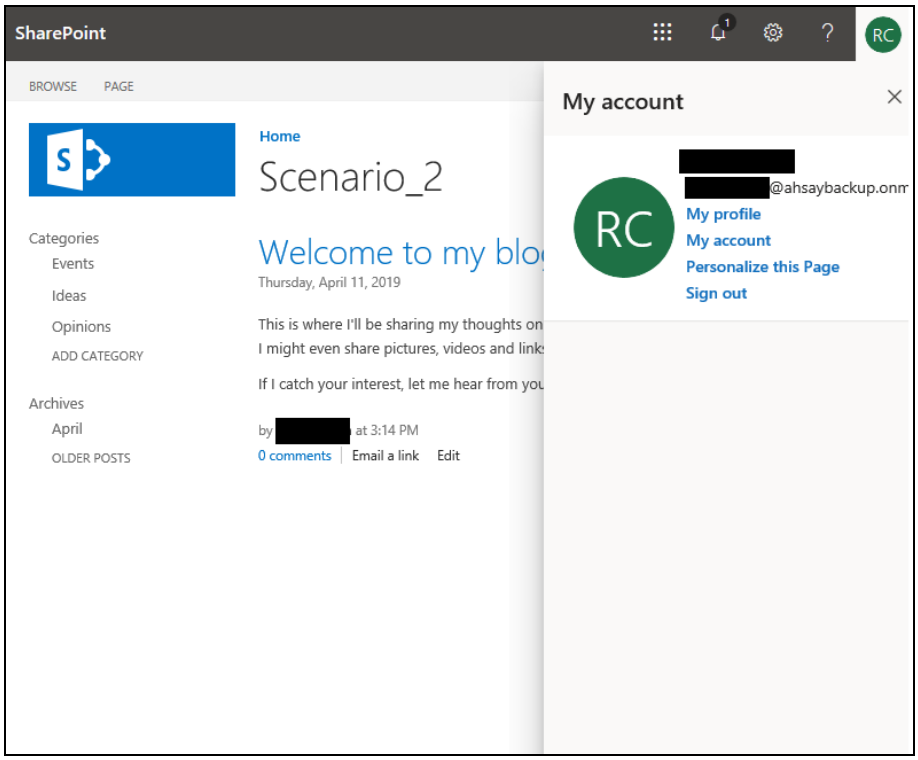


Restore is completed. Click the to show the log of the restoration.





To check if the selected site from Site Collections is fully restored, login and check the SharePoint. As you can see on our example screen shot below, Ronnie Chan is logged in and the ahsay.sharepoint.com/sites/test is completely restored in another Office 365 account.



7.2 Restore Filter with AhsayOBM

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

- For Users, you can search **Files**, **Folders**, and **Mails**.
- For Site Collections, you can search **Directories** and **Files**.

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**

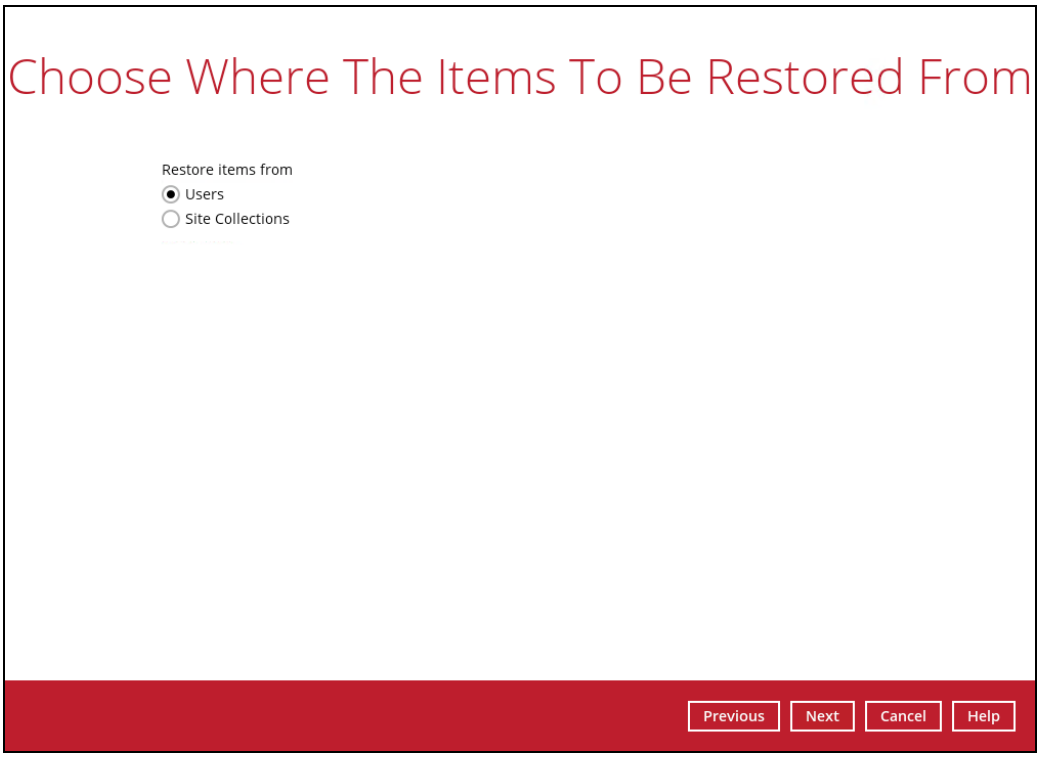
  These are Directories, Files, Folders, and Mails with the name **ending** with a specific letter or word.

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

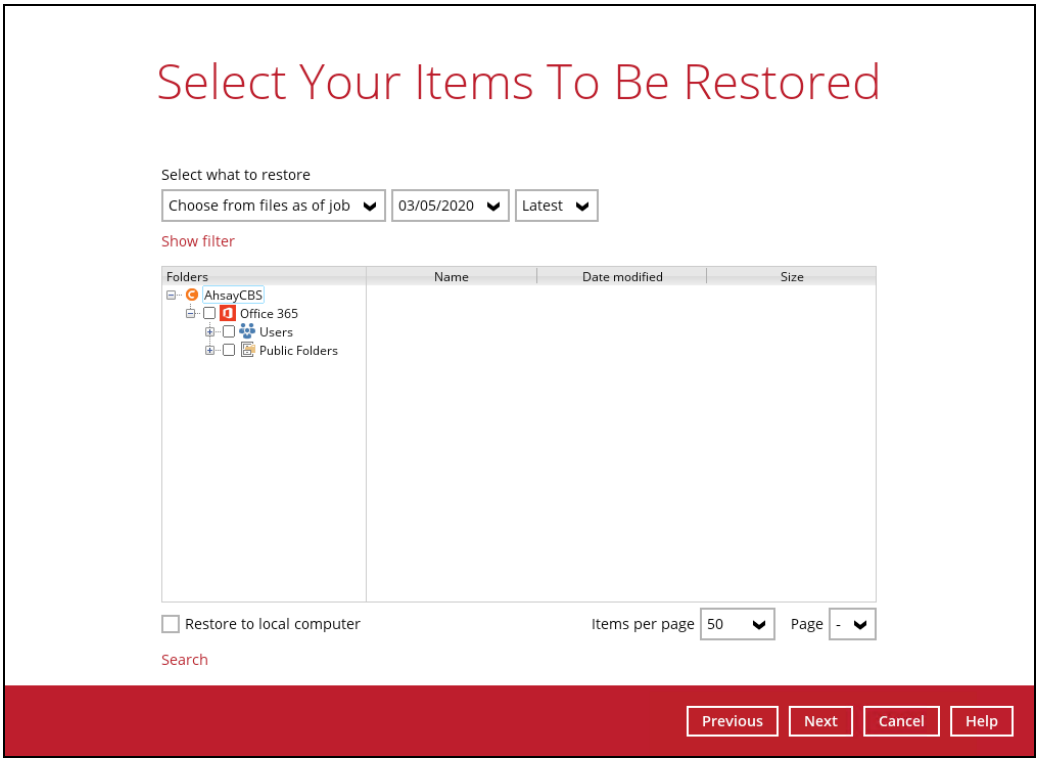
For more detailed examples using the restore filter on AhsayOBM, refer to Appendix C: Example Scenarios for Restore Filter using AhsayOBM.

1. Login to AhsayOBM according to the instructions in Login to AhsayOBM.
2. Click the Restore icon on the main interface of AhsayOBM.
3. Select the backup set the you would like to restore.
4. Select the backup destination that you would like to restore backed-up items to.
5. Select to restore from Users or Site Collections. Click Next to continue.

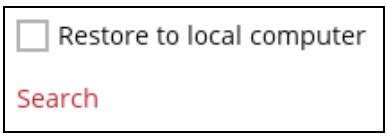
7.2.1. From Users



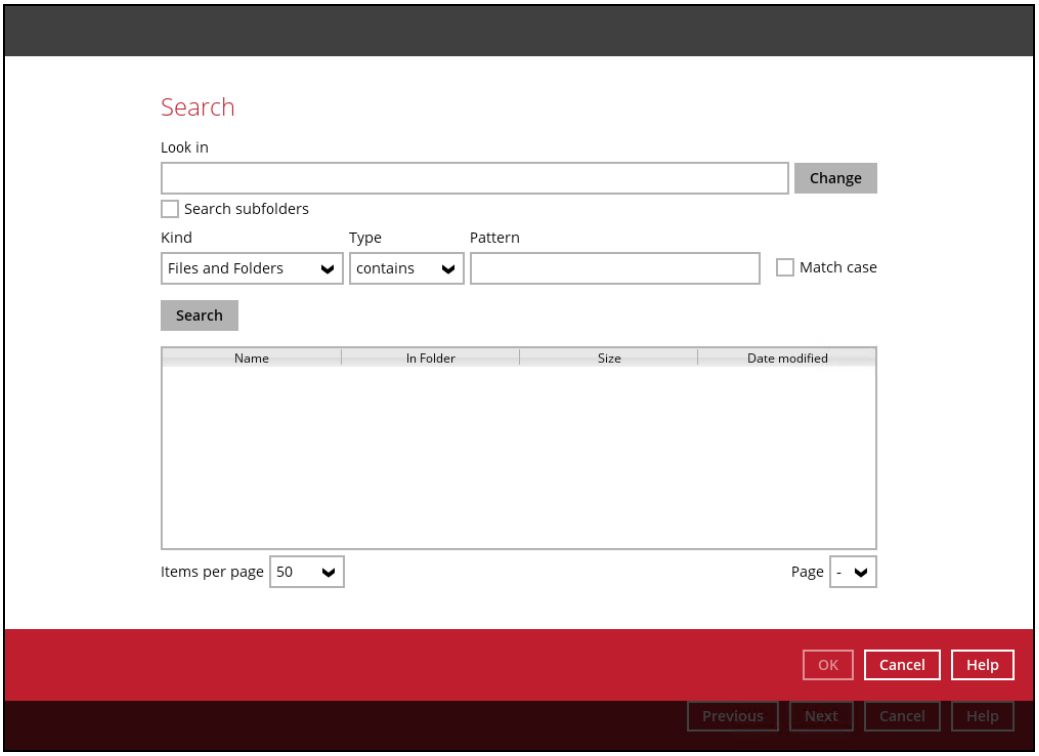
Select the item(s) you would like to restore. You can also choose to restore backed-up file from a specific backup job of your choice using the Select what to restore drop-down menu at the top. Click Next to proceed.

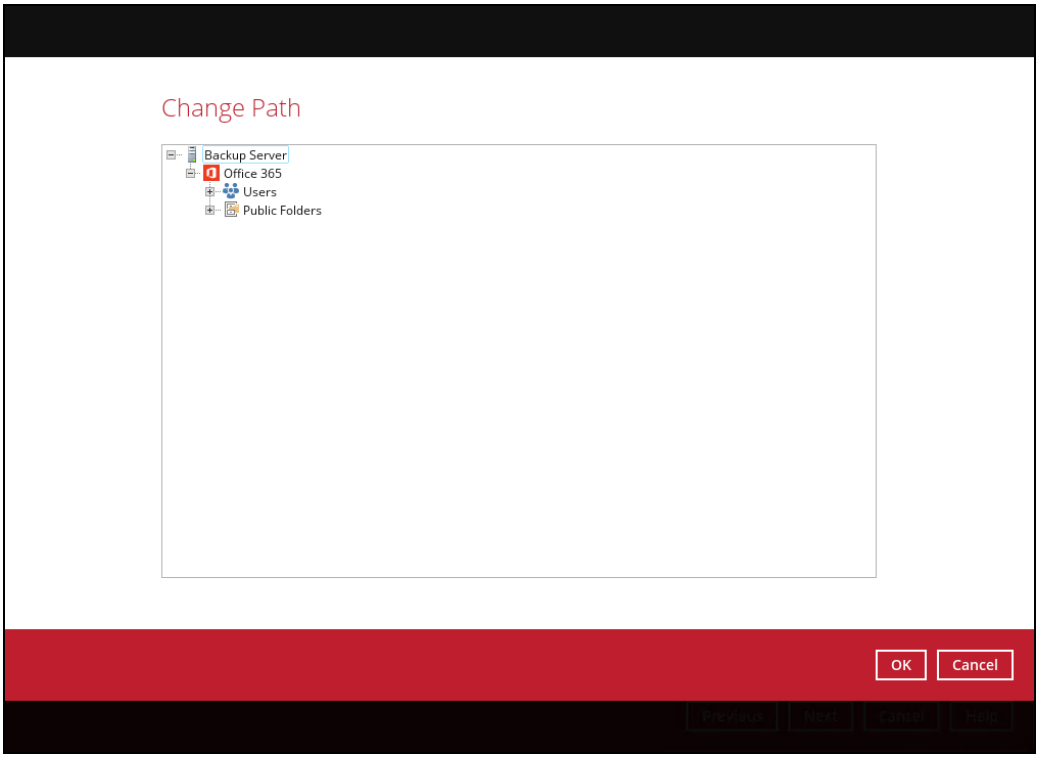


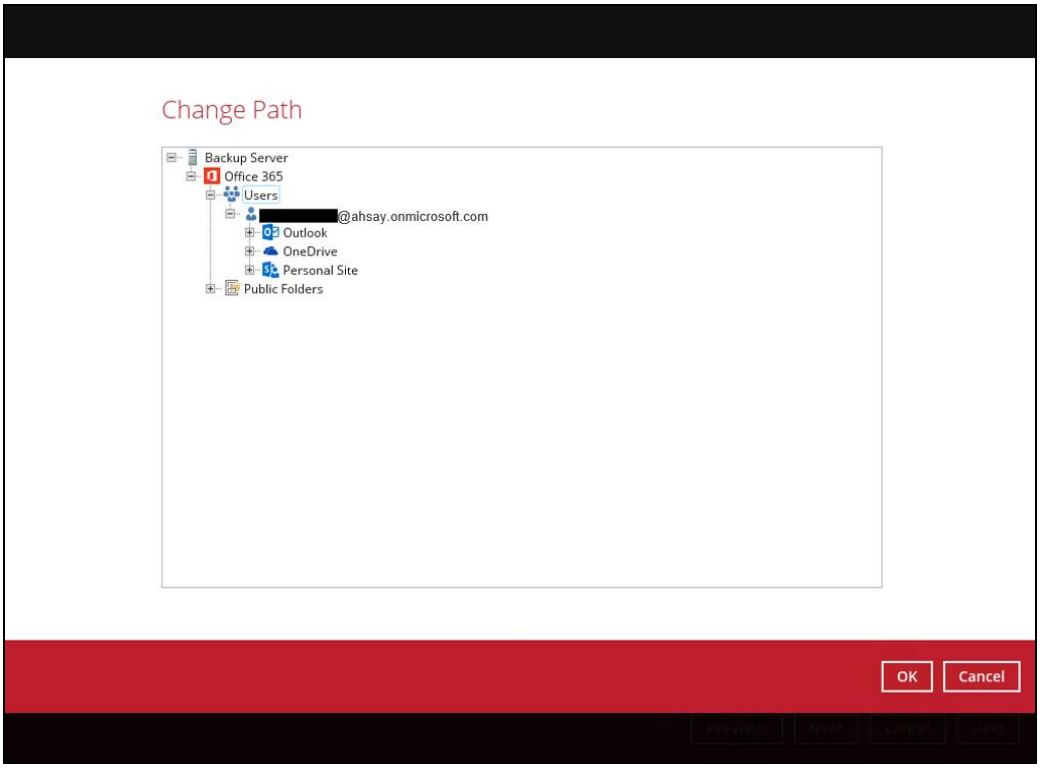
Click the Search located below the Restore to local computer checkbox.



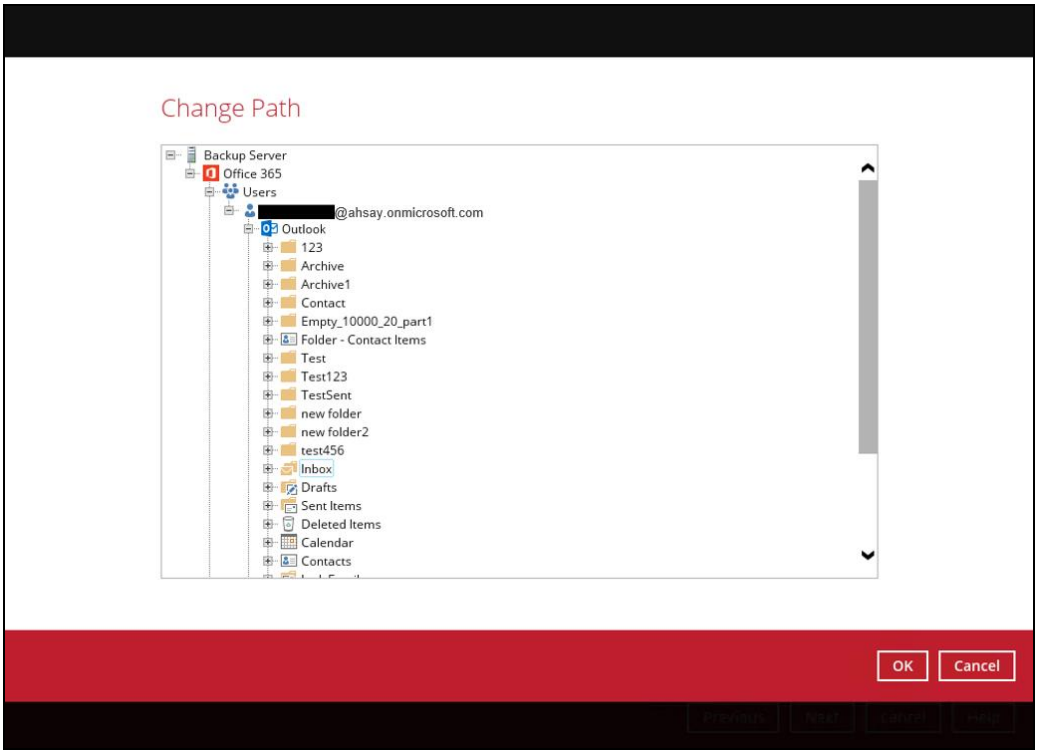
Change the path if you want to restore items from other location. Click the Change button then click OK to proceed.

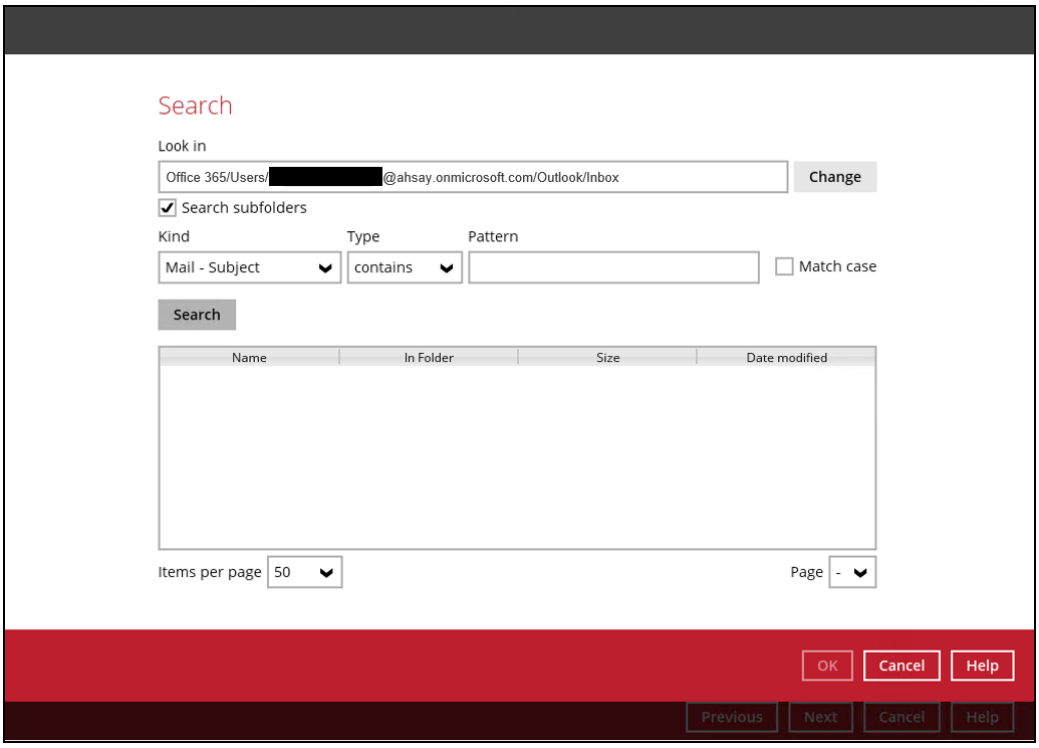






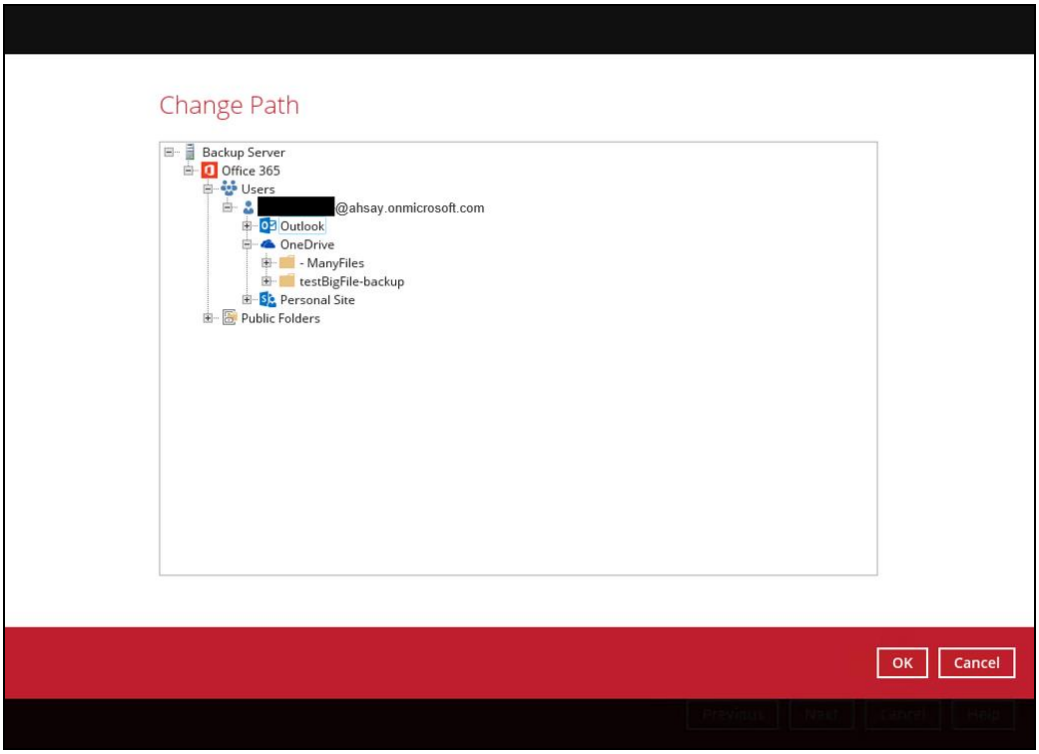
If you are going to search for specific mails, then click the Outlook to expand for more selection. In our example below, **Inbox** of **abc@ahsay.onmicrosoft.com** is selected.

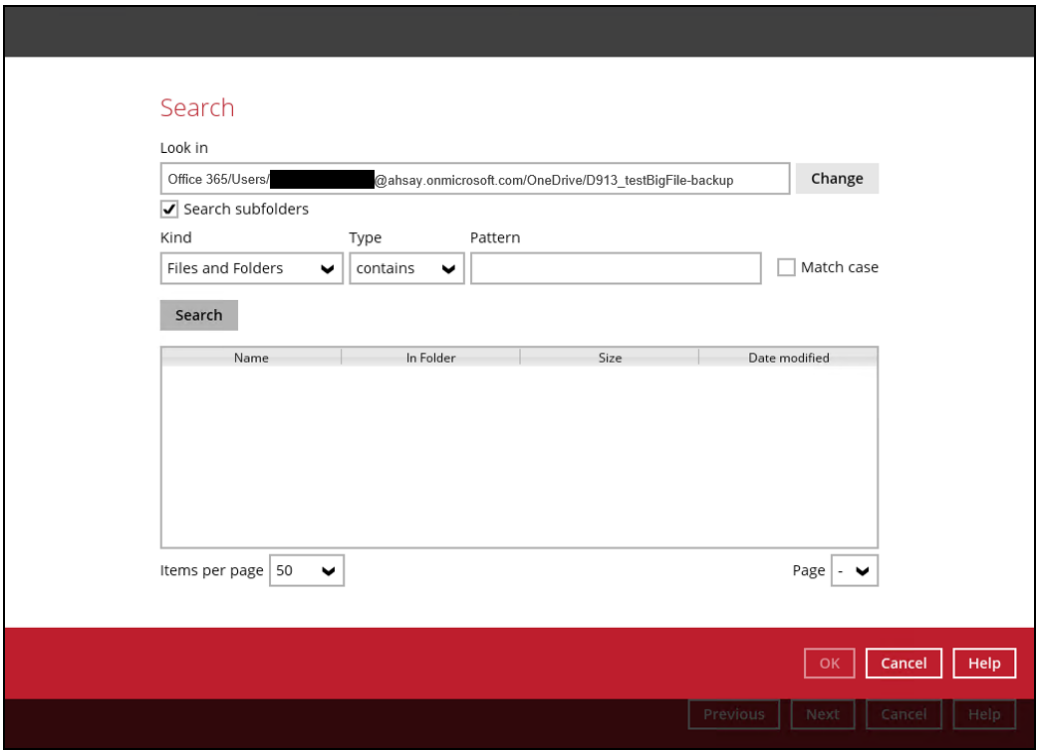




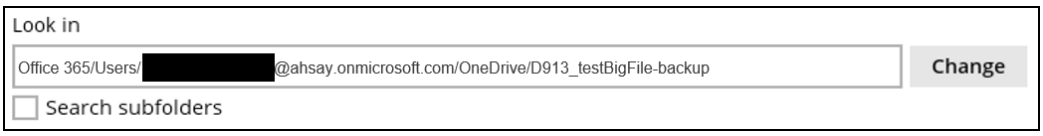
OR

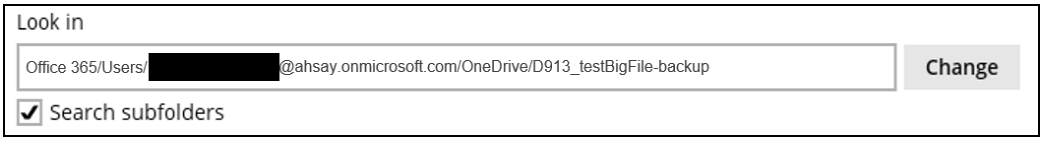
If you are going to search for specific files and/or folders, then click the OneDrive to expand for more selection. In our example below, **testBigFile-backup** folder in **OneDrive** is selected.





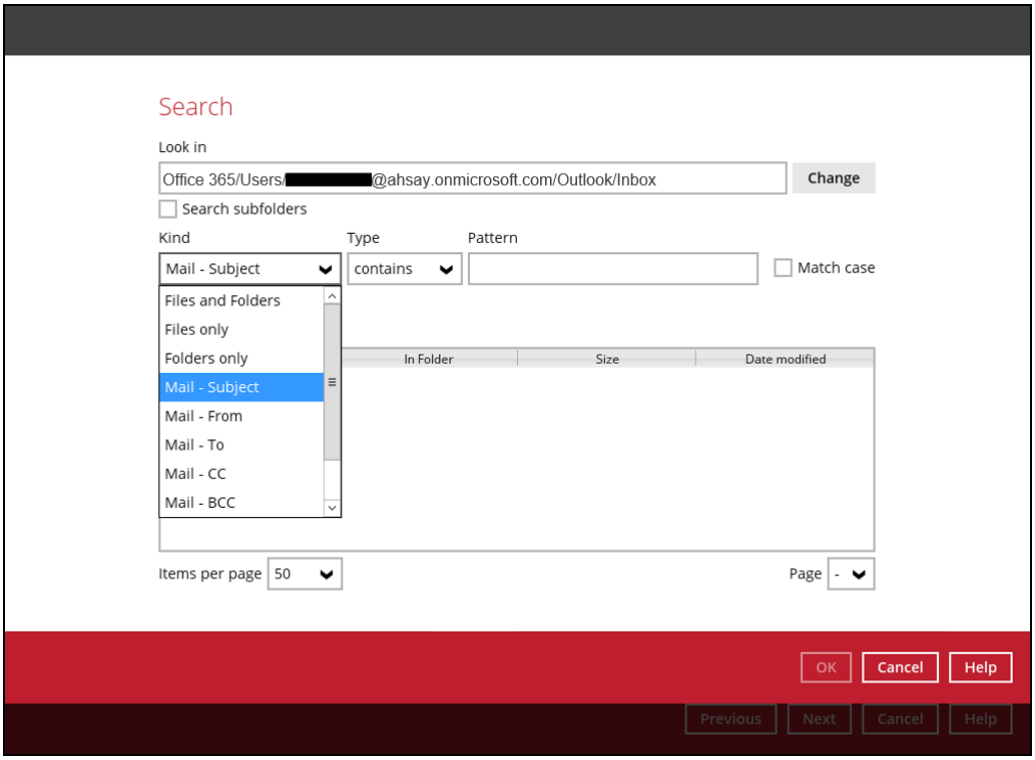
Tick the **Search subfolders** checkbox if you want to include available subfolders upon searching.





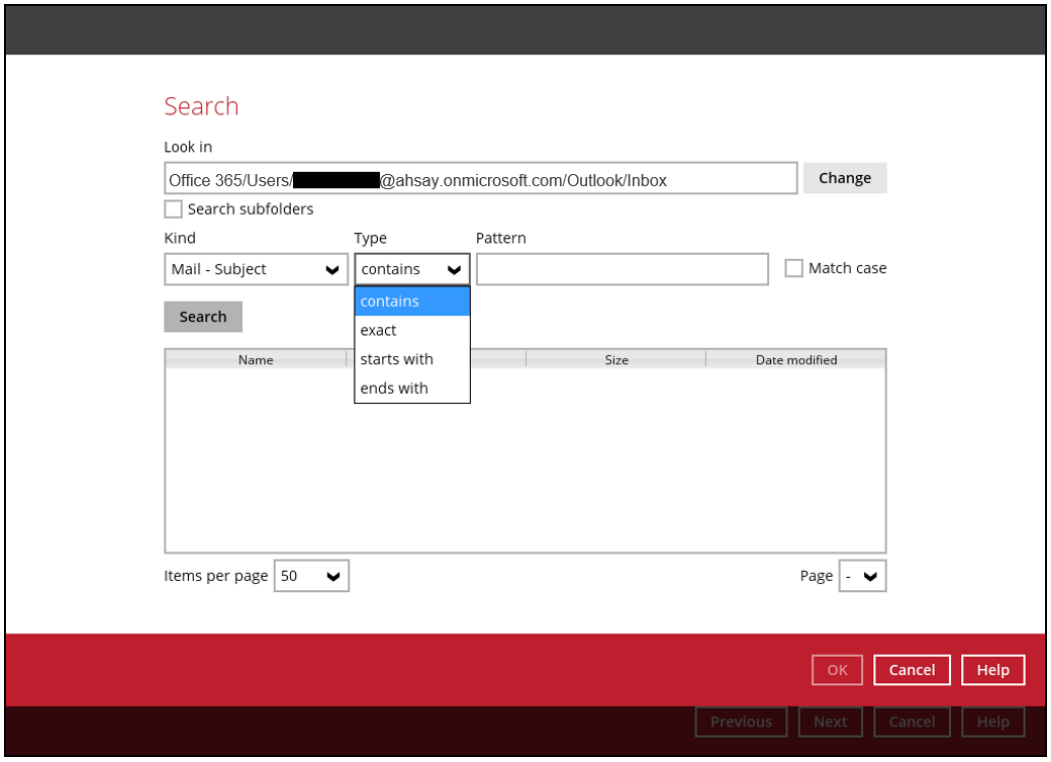
Select from the following kind of files you want to search.

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

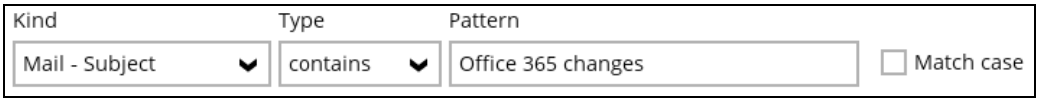


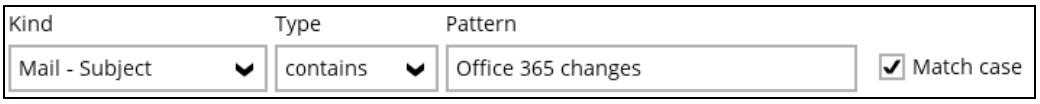
Select from the following type of filtering you want to search.

- Contains
- Exact
- Starts With
- Ends With

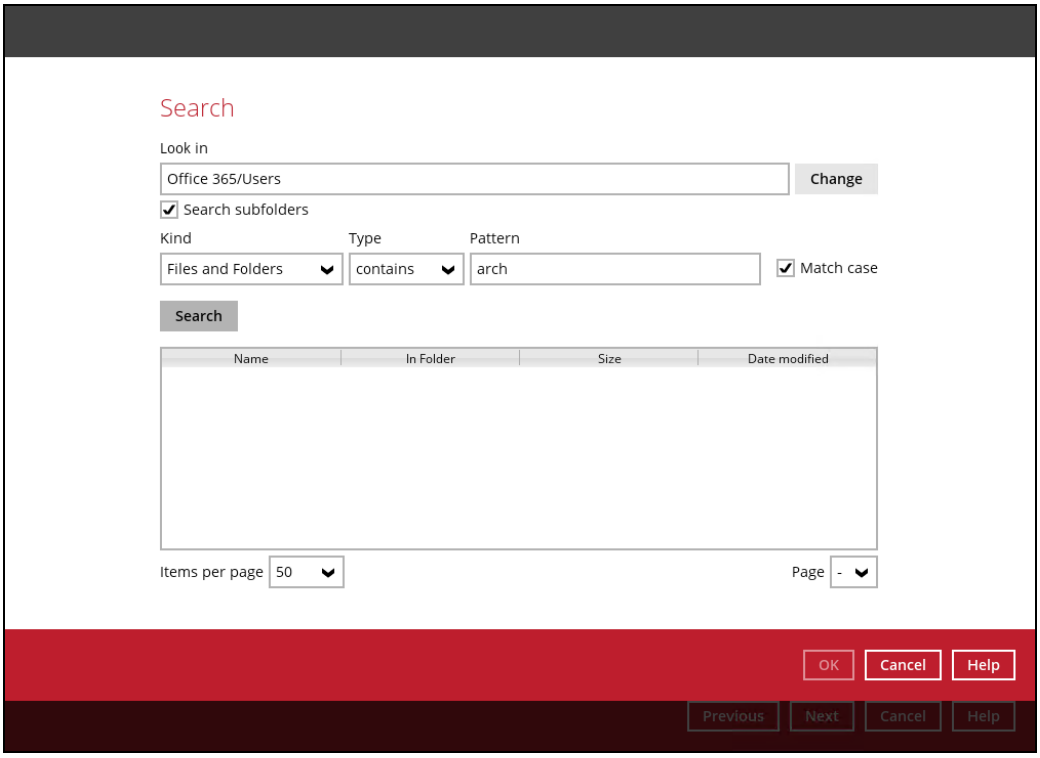


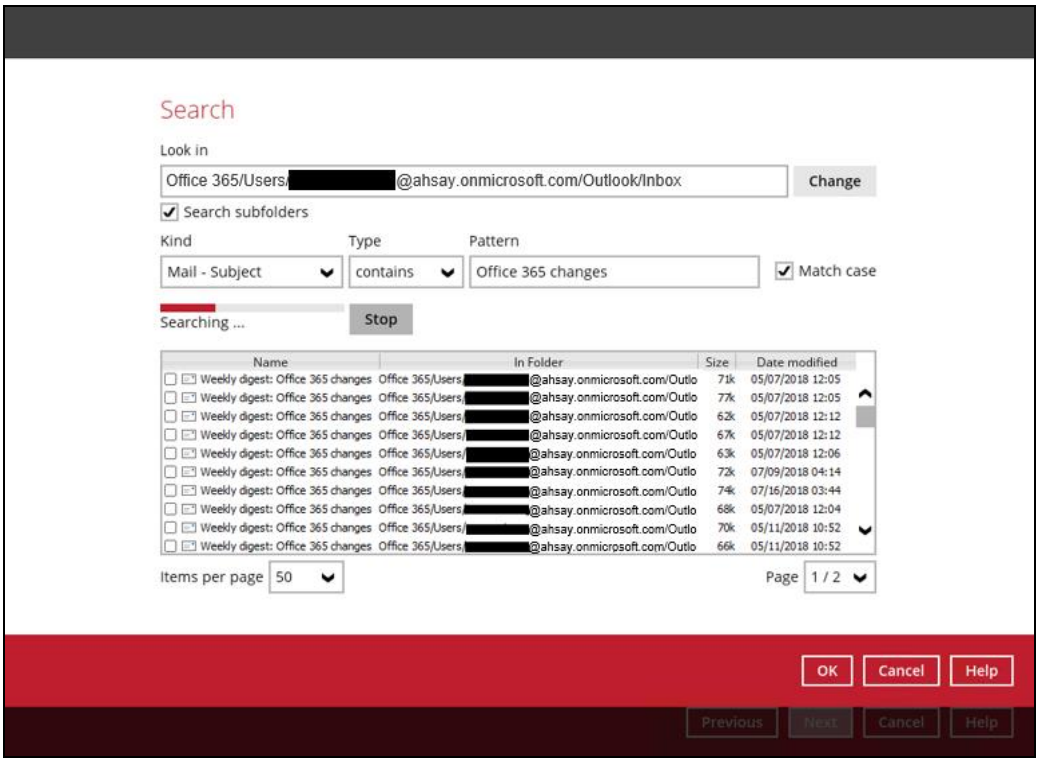
Enter a pattern you want and Tick the **Match Case** checkbox if you want to accurately search for a specific file.

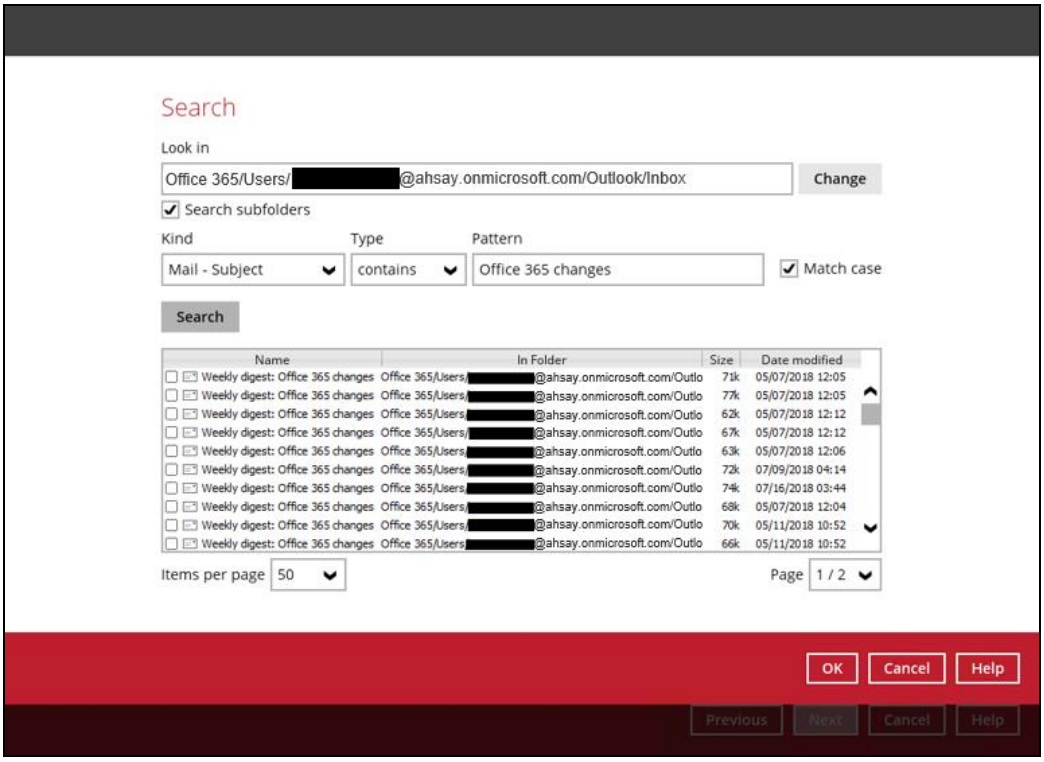




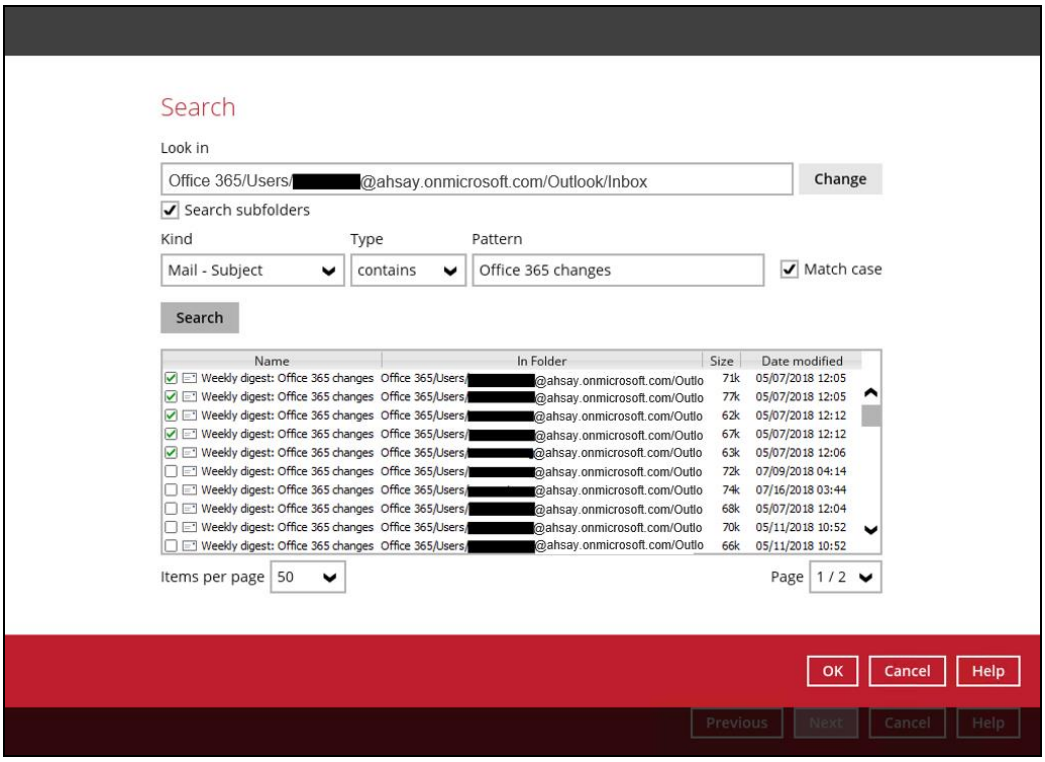
Click the Search button and the result will be displayed.


Search
Look in
Office 365/Users
Change
Search subfolders
Kind
Type
Pattern
Files and Folders
contains
arch
Match case
Search
Name
In Folder
Size
Date modified
Items per page
50
Page
-
OK
Cancel
Help
Previous
Next
Cancel
Help

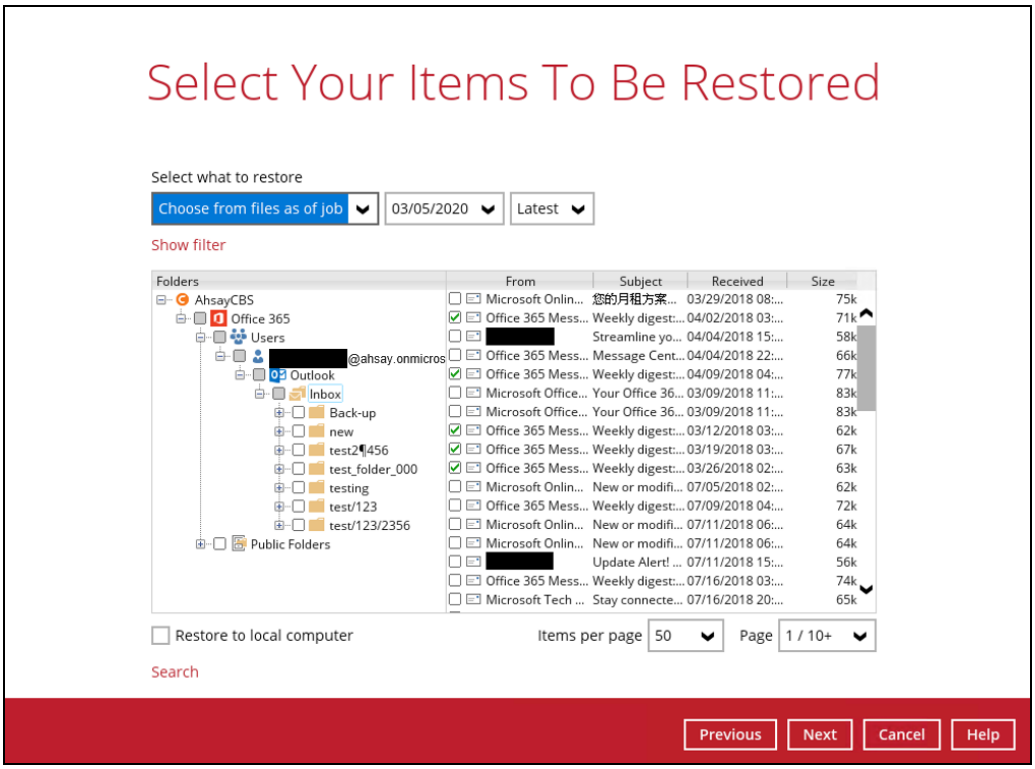

Search
Look in
Office 365/Users/[redacted]@ahsay.onmicrosoft.com/Outlook/Inbox
Change
Search subfolders
Kind
Type
Pattern
Mail - Subject
contains
Office 365 changes
Match case
Searching ...
Stop
Name
In Folder
Size
Date modified
Weekly digest: Office 365 changes Office 365/Users/[redacted]@ahsay.onmicrosoft.com/Outlo 71k 05/07/2018 12:05
Weekly digest: Office 365 changes Office 365/Users/[redacted]@ahsay.onmicrosoft.com/Outlo 77k 05/07/2018 12:05
Weekly digest: Office 365 changes Office 365/Users/[redacted]@ahsay.onmicrosoft.com/Outlo 62k 05/07/2018 12:12
Weekly digest: Office 365 changes Office 365/Users/[redacted]@ahsay.onmicrosoft.com/Outlo 67k 05/07/2018 12:12
Weekly digest: Office 365 changes Office 365/Users/[redacted]@ahsay.onmicrosoft.com/Outlo 63k 05/07/2018 12:06
Weekly digest: Office 365 changes Office 365/Users/[redacted]@ahsay.onmicrosoft.com/Outlo 72k 07/09/2018 04:14
Weekly digest: Office 365 changes Office 365/Users/[redacted]@ahsay.onmicrosoft.com/Outlo 74k 07/16/2018 03:44
Weekly digest: Office 365 changes Office 365/Users/[redacted]@ahsay.onmicrosoft.com/Outlo 68k 05/07/2018 12:04
Weekly digest: Office 365 changes Office 365/Users/[redacted]@ahsay.onmicrosoft.com/Outlo 70k 05/11/2018 10:52
Weekly digest: Office 365 changes Office 365/Users/[redacted]@ahsay.onmicrosoft.com/Outlo 66k 05/11/2018 10:52
Items per page
50
Page
1 / 2
OK
Cancel
Help
Previous
Next
Cancel
Help



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



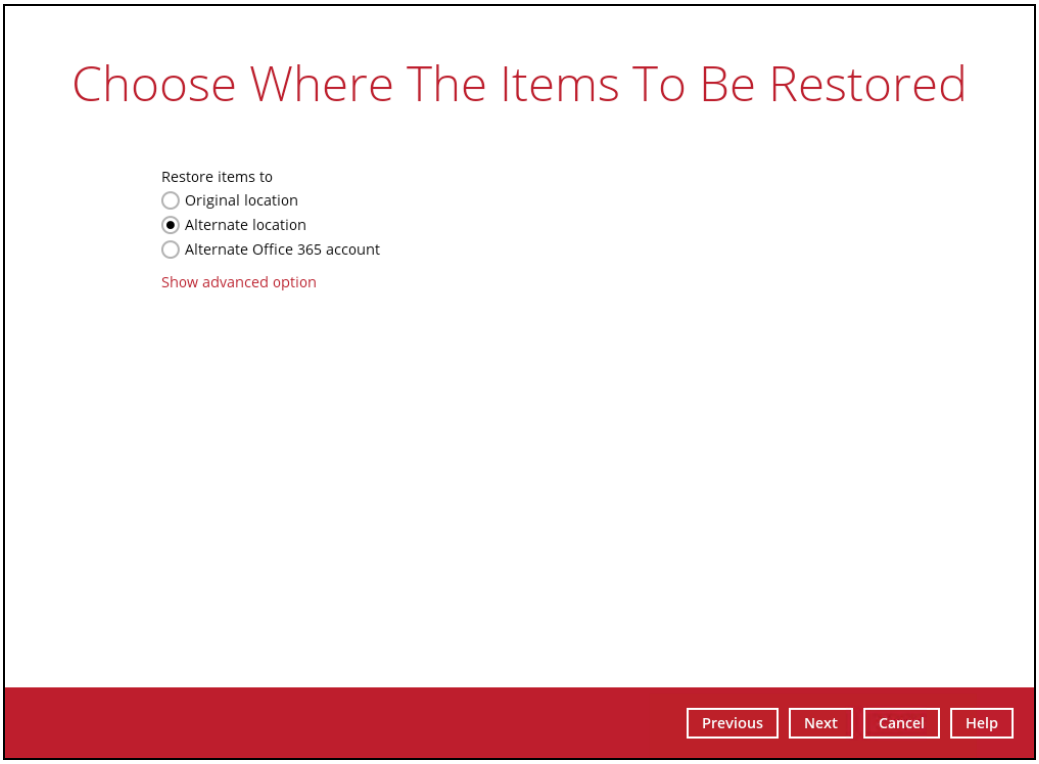
The selected files will reflect on the Restore main screen. Click the Next button to proceed.

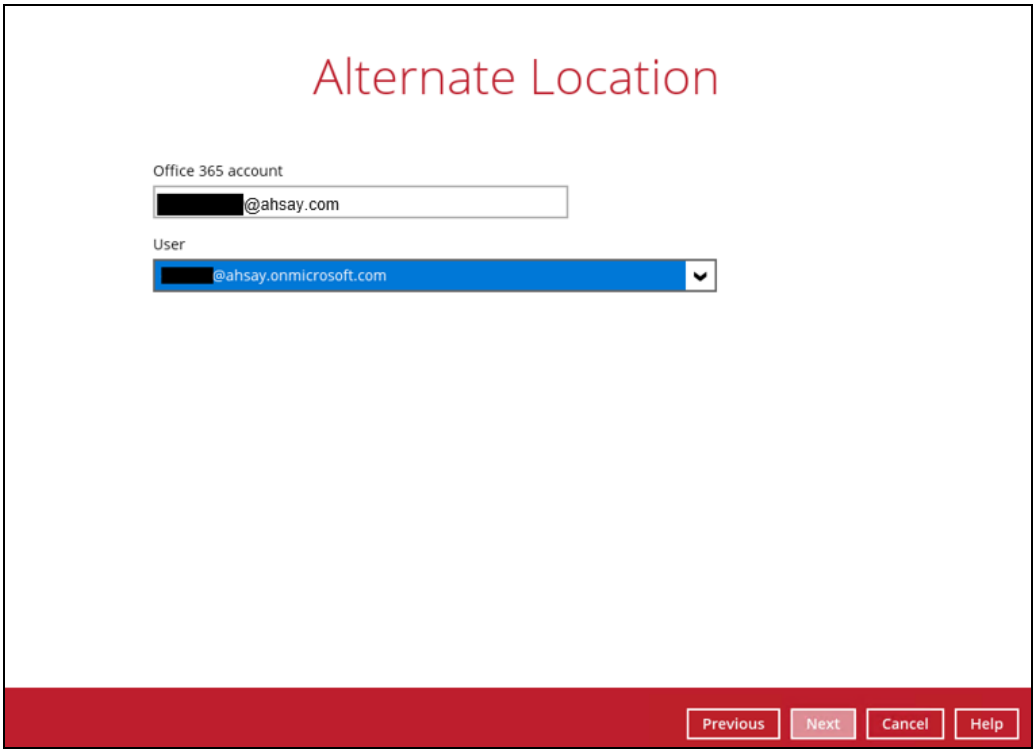


Select which location the items will be restored. Choose from the following options:

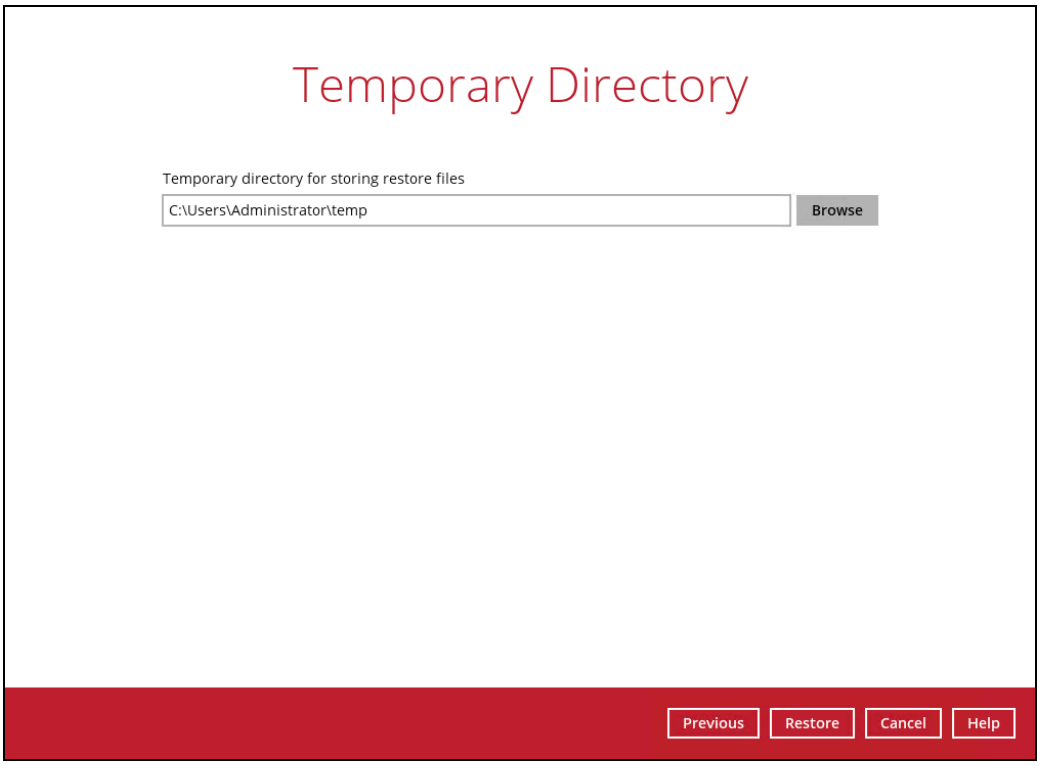
- Local machine – this option is located on the Restore main screen, lower left part.
- Original location
- Alternate location
- Alternate Office 365 account

Click the Next button to proceed.

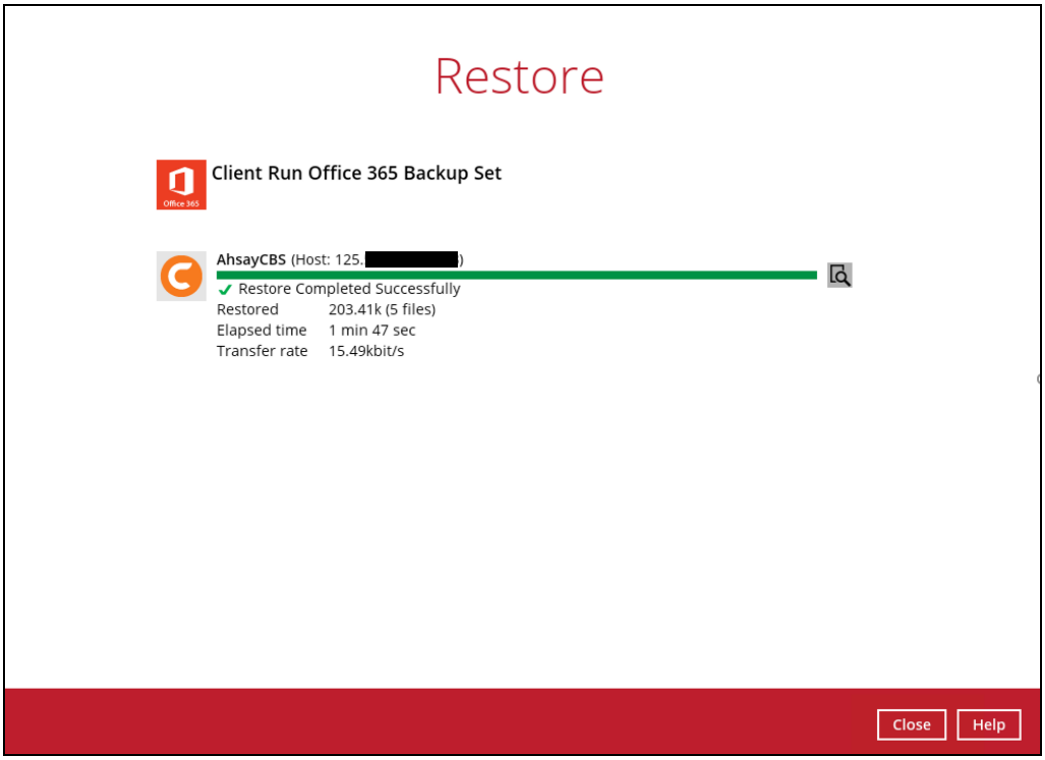

Choose Where The Items To Be Restored
Restore items to
Original location
Alternate location
Alternate Office 365 account
Show advanced option
Previous
Next
Cancel
Help


Alternate Location
Office 365 account
[redacted]@ahsay.com
User
[redacted]@ahsay.onmicrosoft.com
Previous
Next
Cancel
Help

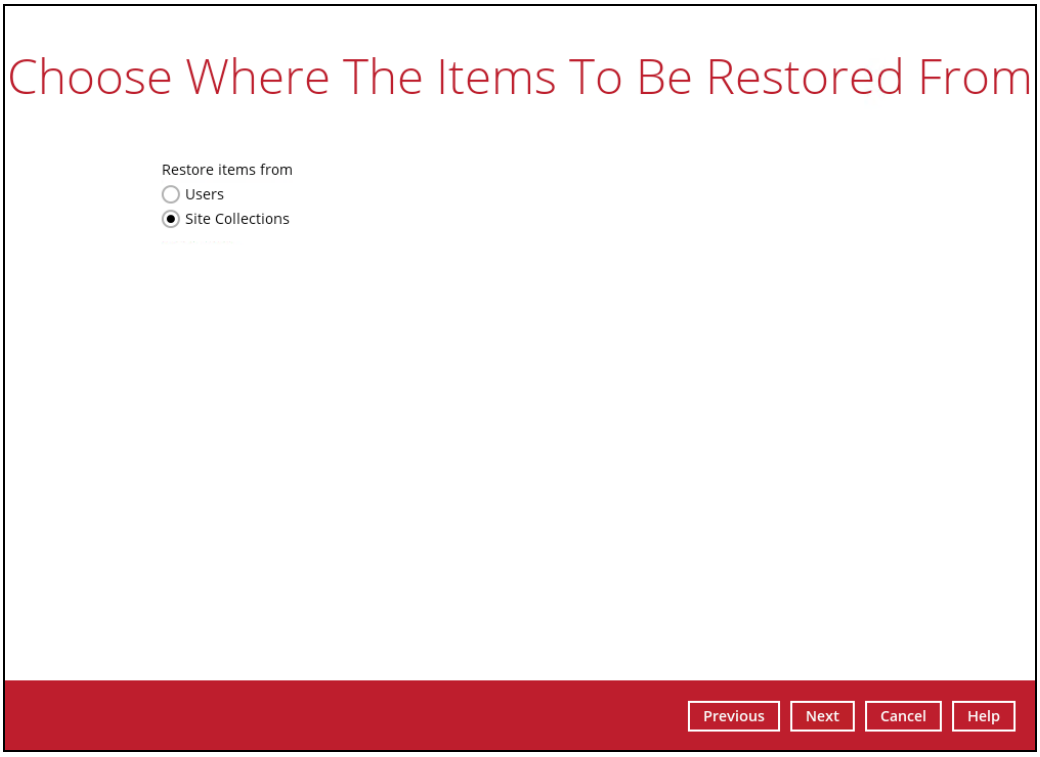
Input the temporary directory or click the Browse button to browse for the path. Click the Restore button to start.



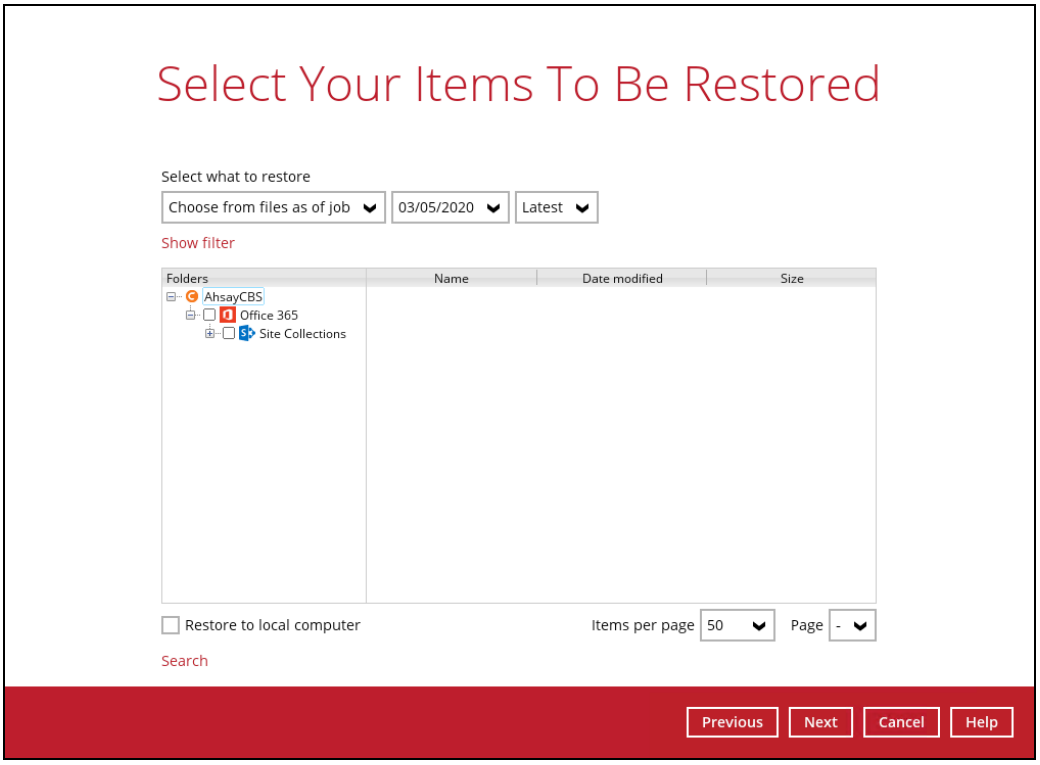
If restore is completed, the status of the activity should be, Restore Completed Successfully.



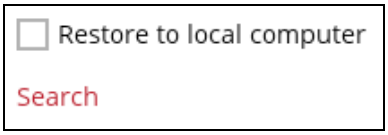
7.2.2. From Site Collections



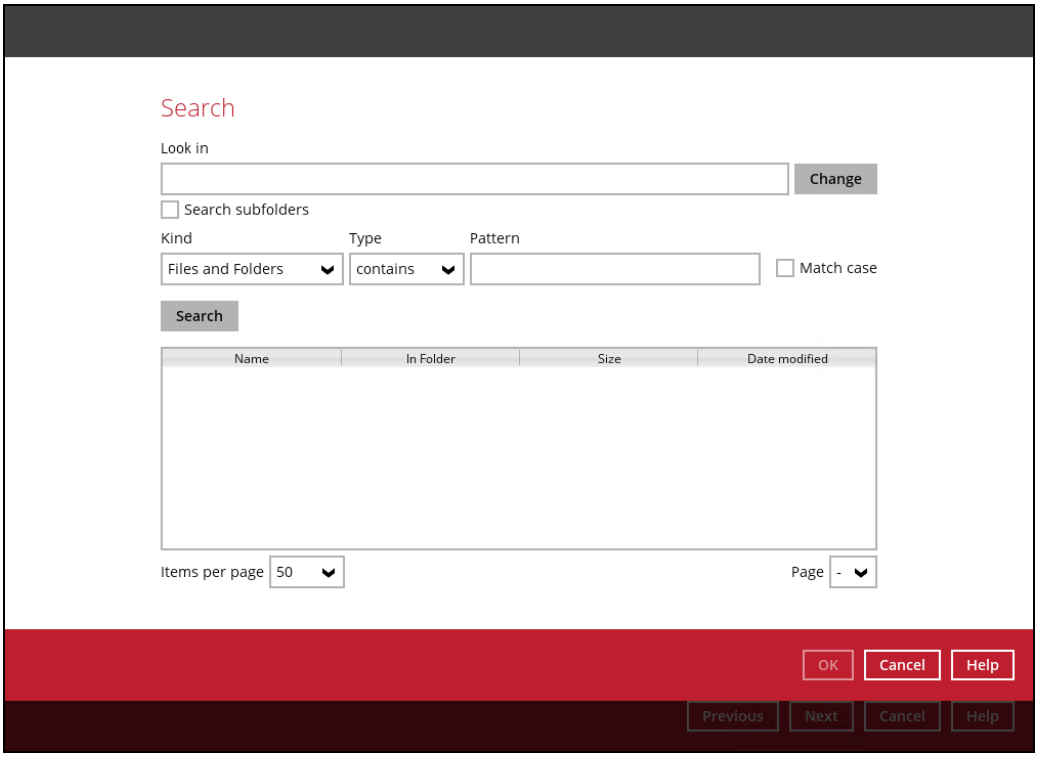
Select the item(s) you would like to restore. You can also choose to restore backed-up file from a specific backup job of your choice using the Select what to restore drop-down menu at the top. Click Next to proceed.

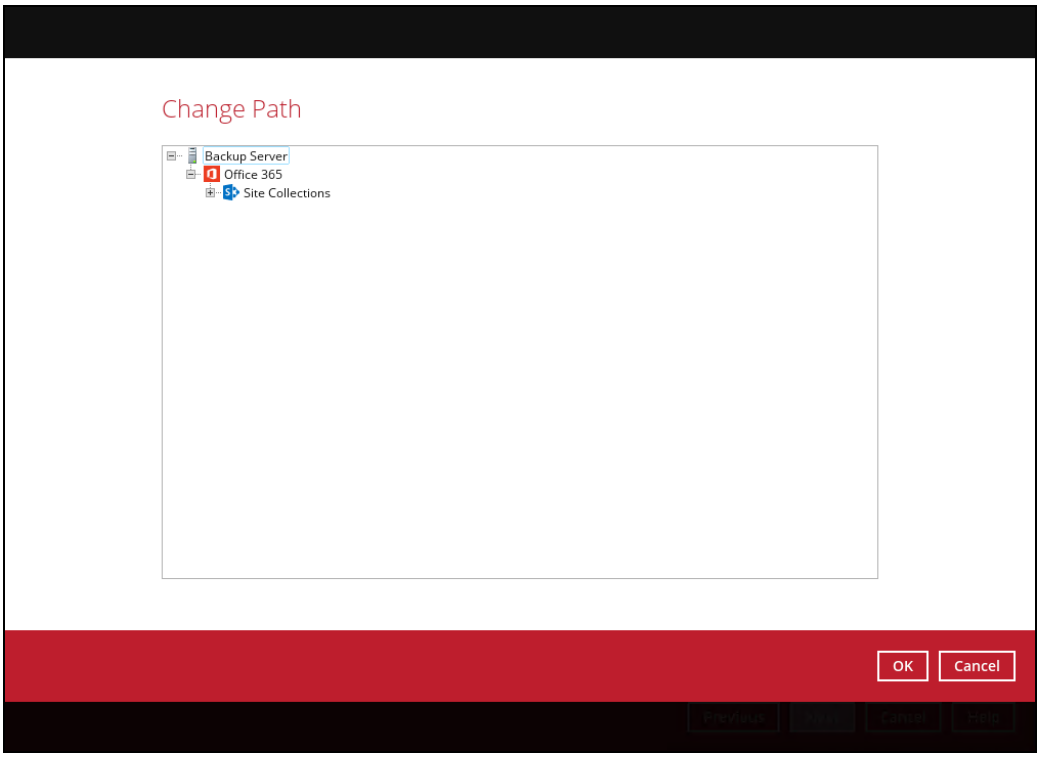


Click the Search located below the Restore to local computer checkbox.

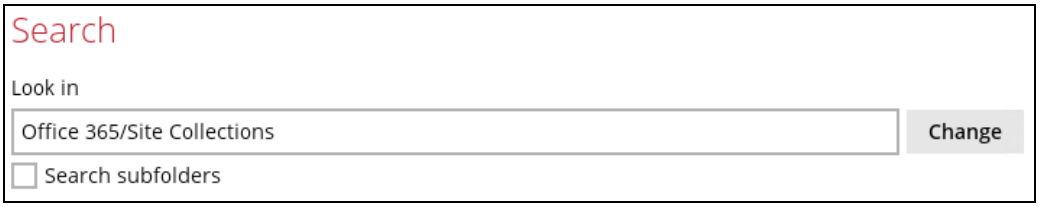


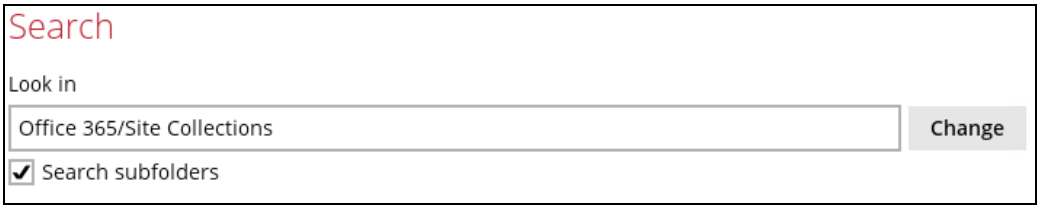
Change the path if you want to restore items from other location. Click the Change button then click OK to proceed.





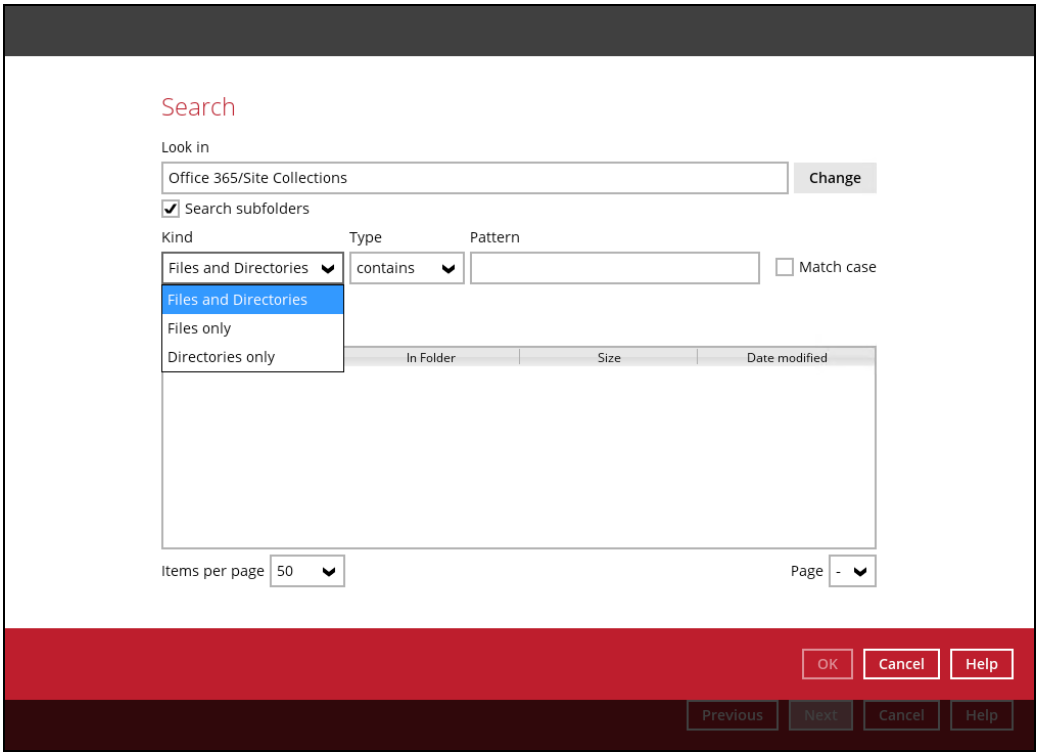
Tick the Search subfolders checkbox check if you want to include available subfolders upon searching.





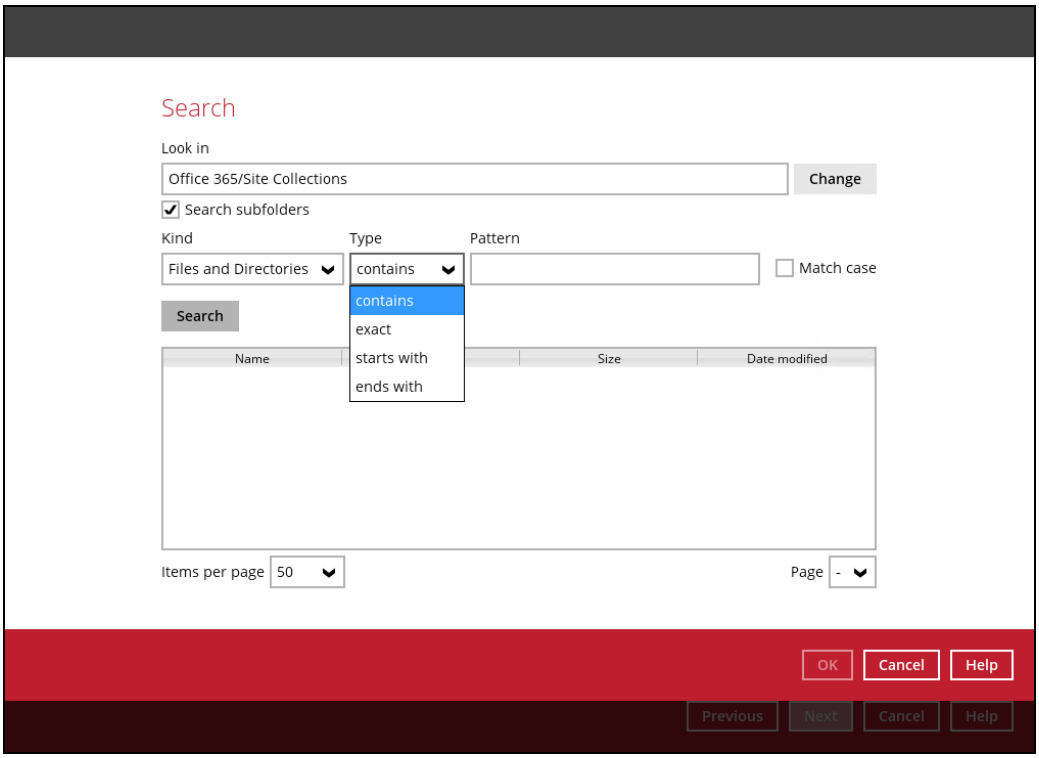
Select from the following kind of files you want to search.

- Files and Directories
- Files Only
- Directories Only

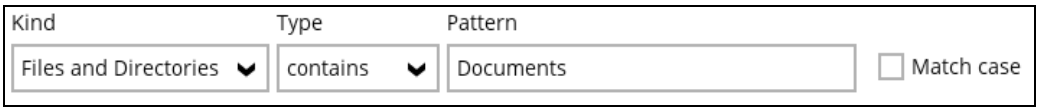


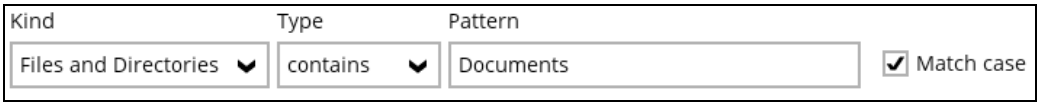
Select from the following type of filtering you want to search.

- Contains
- Exact
- Starts With
- Ends With

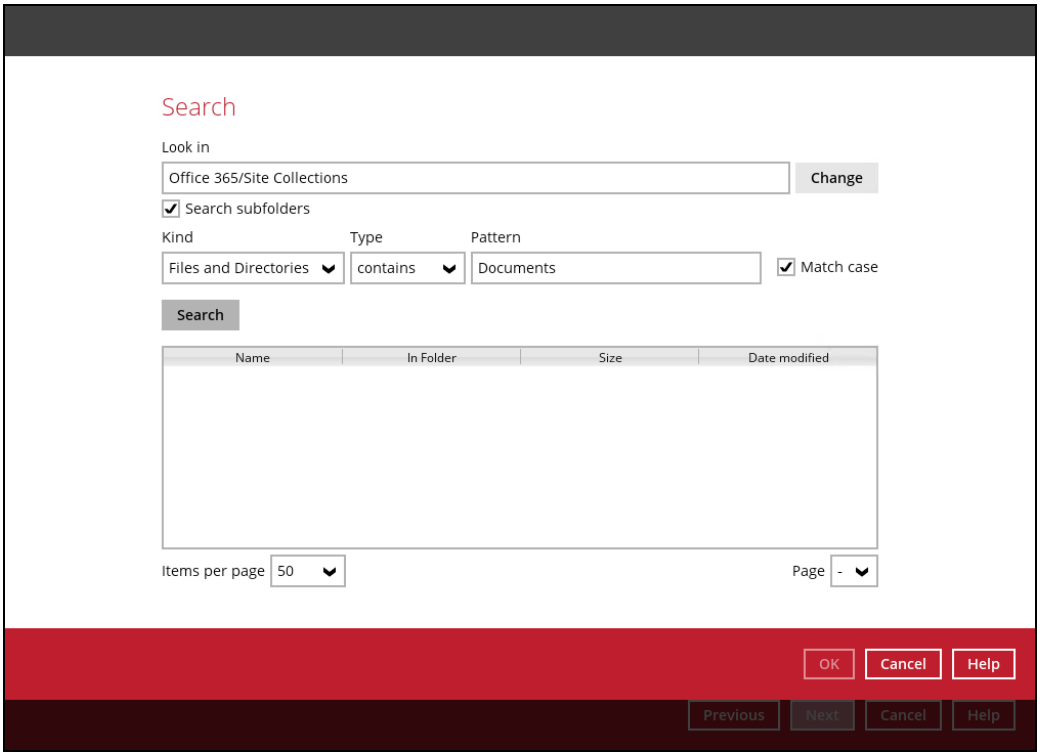


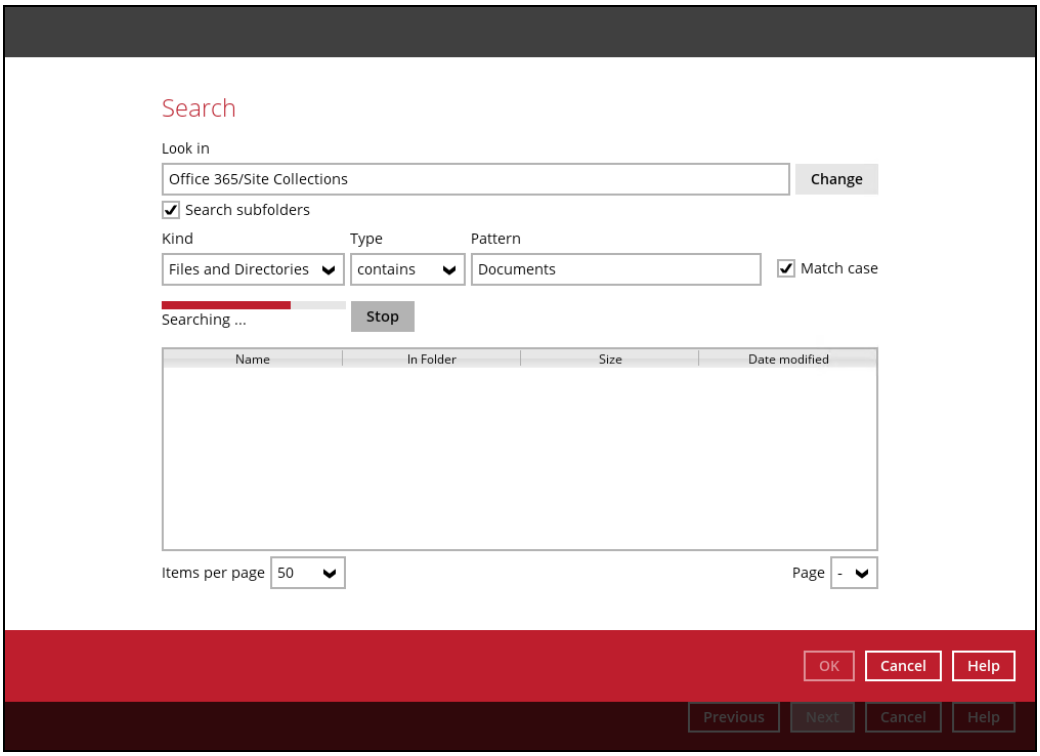
Enter a pattern you want and Tick the Match Case checkbox if you want to accurately search for a specific file.

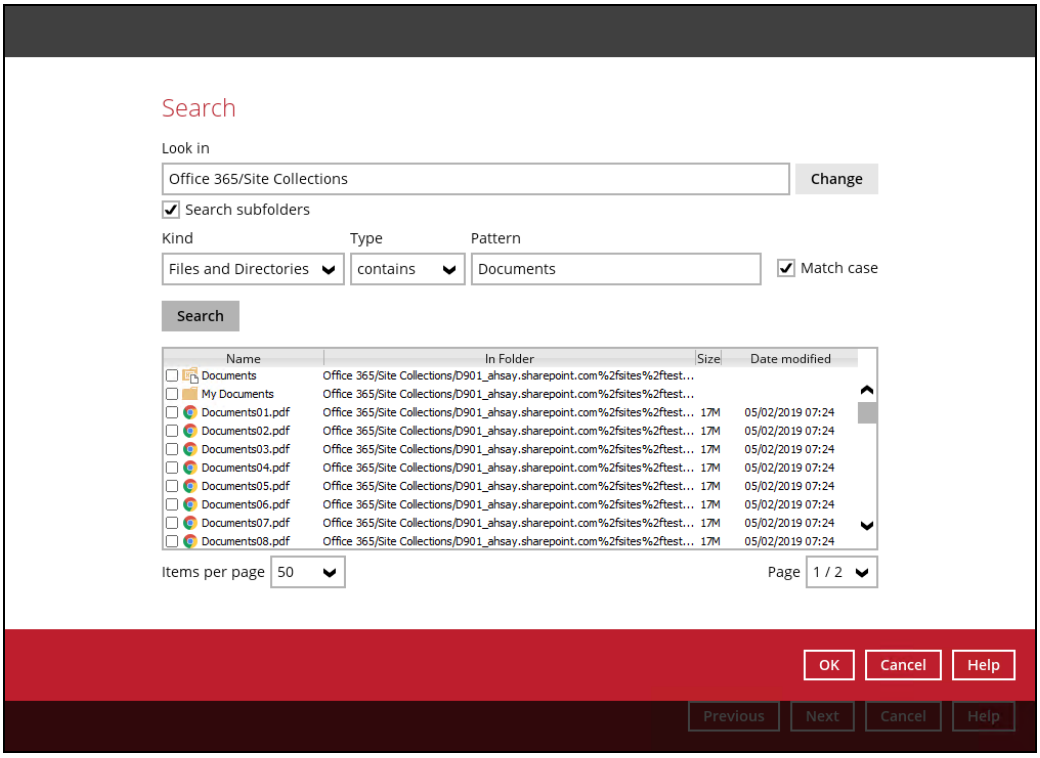




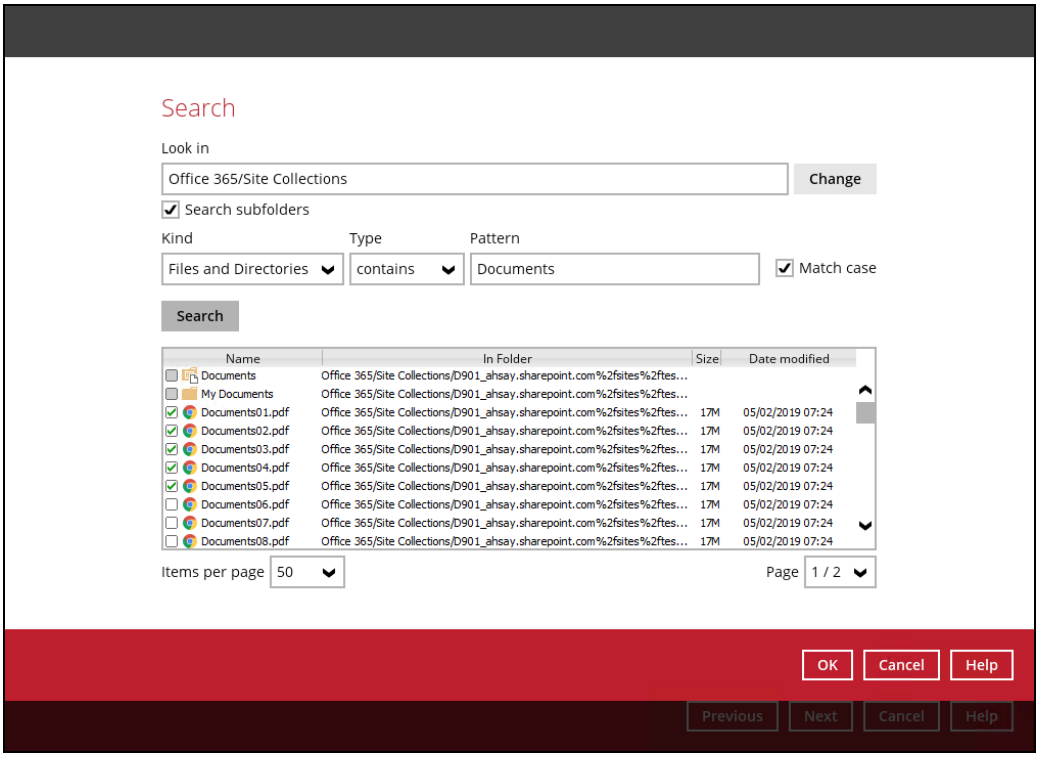
Click the Search button and the result will be displayed.



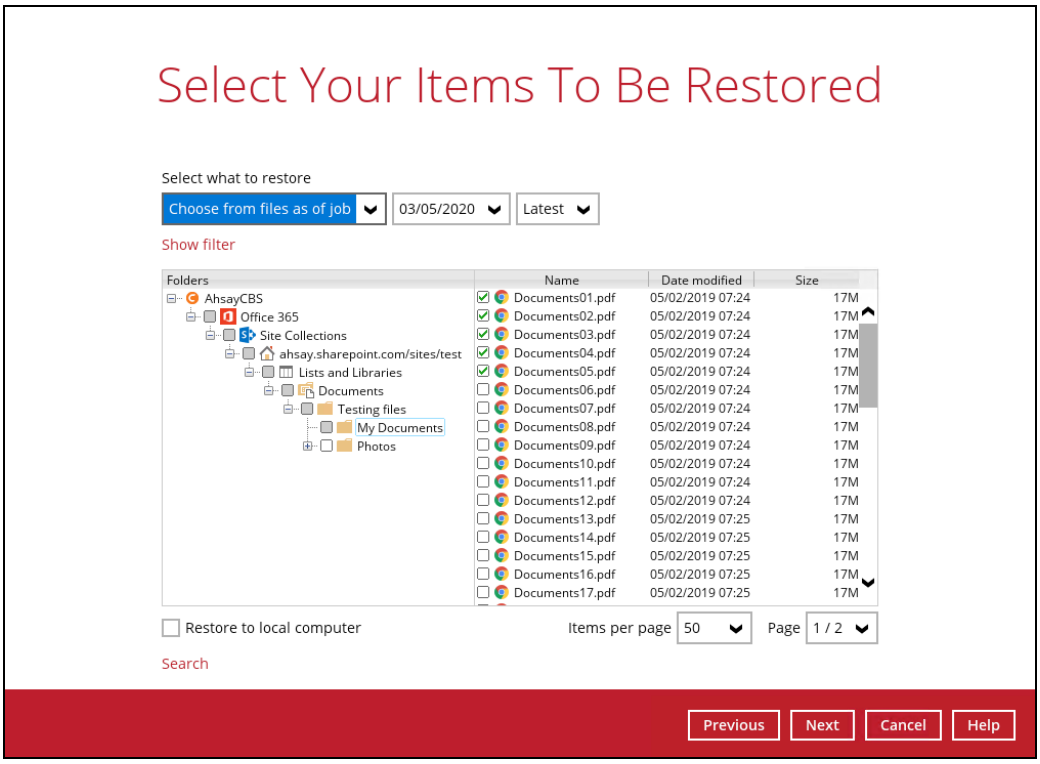




Choose files by ticking each checkbox that you wanted to restore and click the OK button.



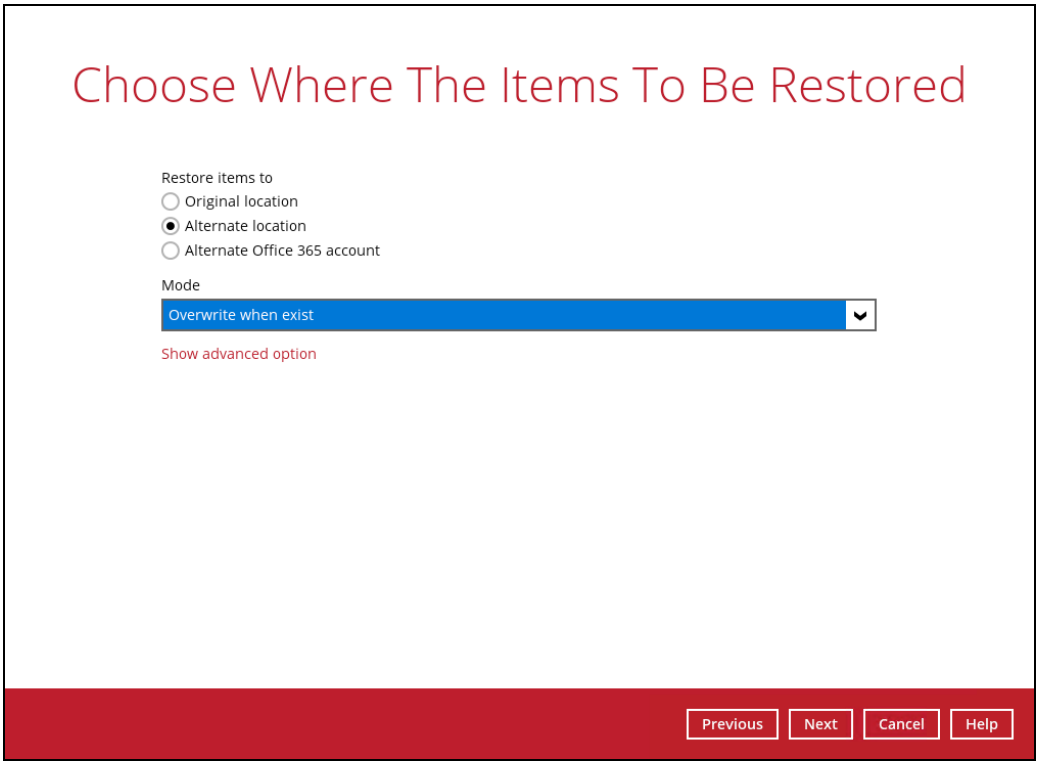
The selected files will reflect on the Restore main screen. Click the Next button to proceed.

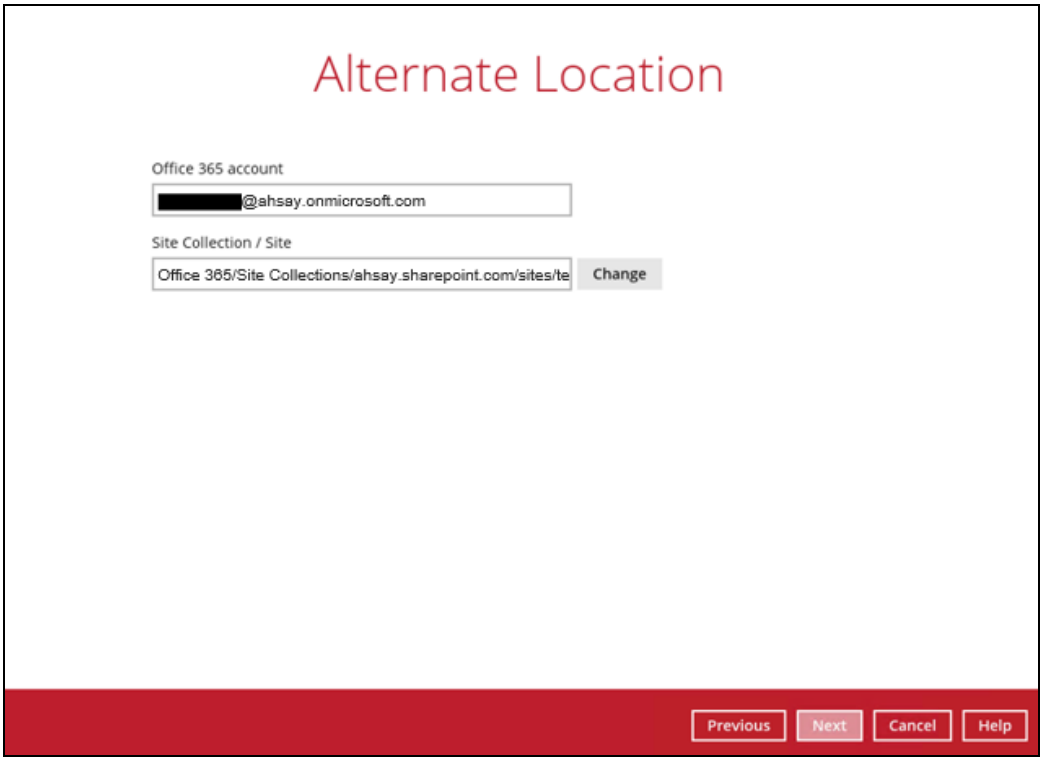


Select which location the items will be restored. Choose from the following options:

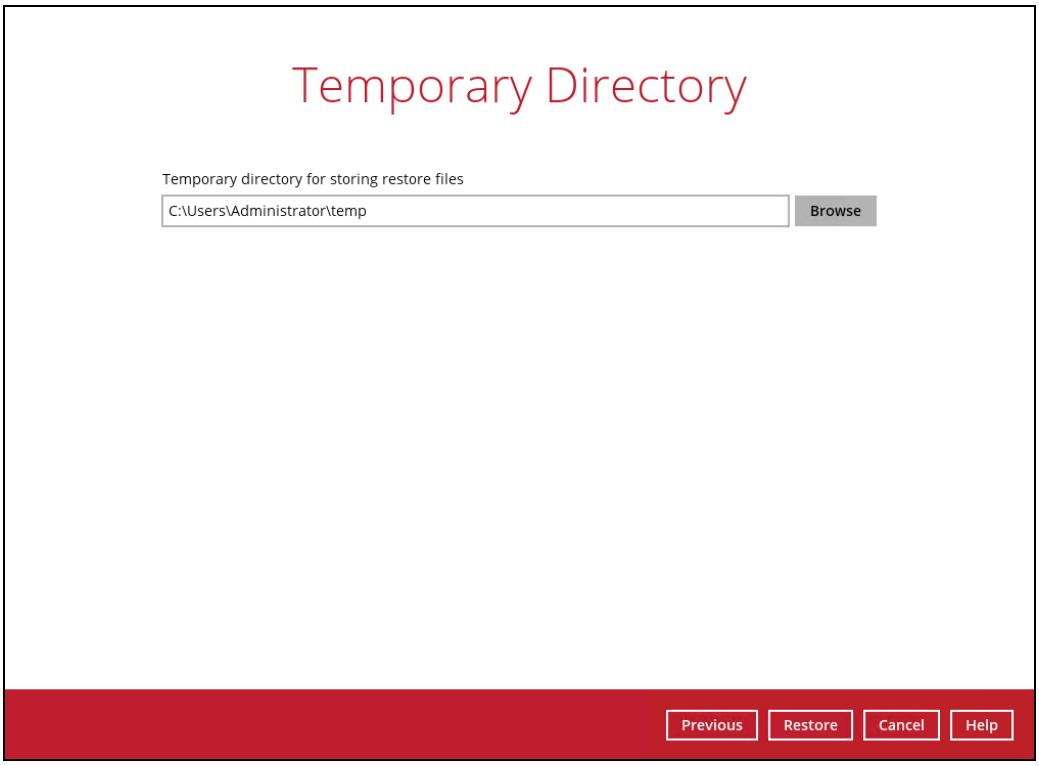
- Local machine – this option is located on the Restore main screen, lower left part.
- Original location
- Alternate location
- Alternate Office 365 account

Click the Next button to proceed.

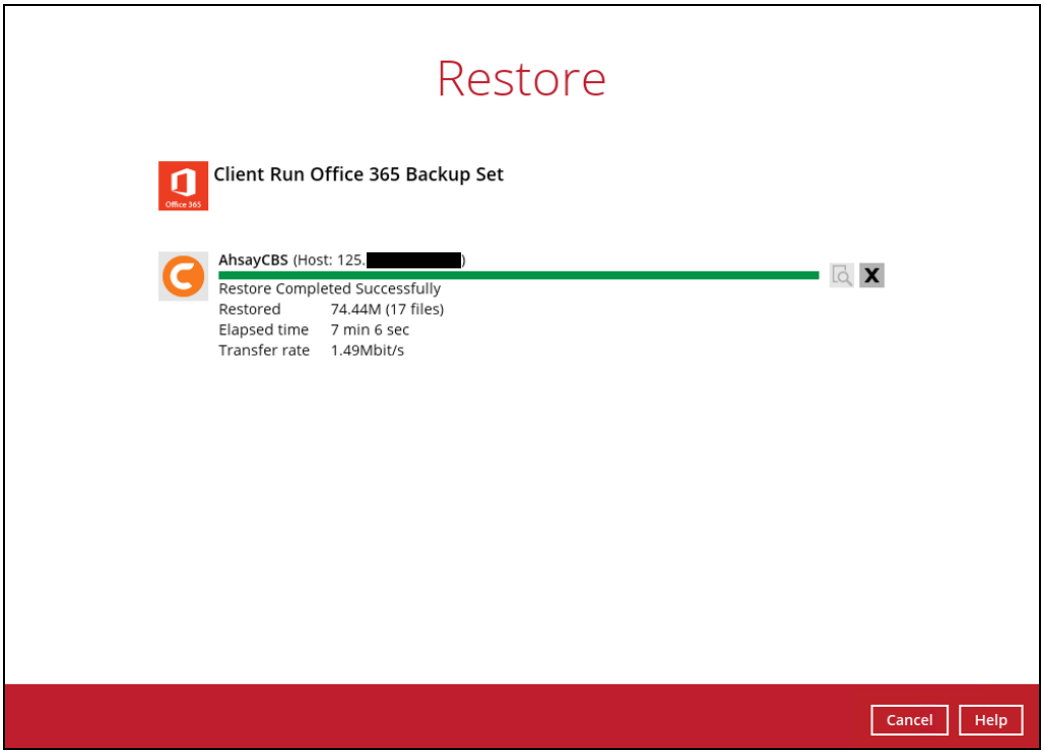

Choose Where The Items To Be Restored
Restore items to
Original location
Alternate location
Alternate Office 365 account
Mode
Overwrite when exist
Show advanced option
Previous
Next
Cancel
Help


Alternate Location
Office 365 account
[redacted]@ahsay.onmicrosoft.com
Site Collection / Site
Office 365/Site Collections/ahsay.sharepoint.com/sites/te
Change
Previous
Next
Cancel
Help

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 Partner Portal:
https://www.ahsay.com/partners/

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

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

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
	user02@company-office365.com
Backup Set B	user01@company-office365.com
Backup Set C	user02@company-office365.com

Example No. 3: To back up three (3) 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
	user02@company-office365.com
	user03@company-office365.com
Backup Set B	user01@company-office365.com
	user02@company-office365.com
Backup Set C	user03@company-office365.com

Scenario No. 2: Backing up SharePoint Sites under Site collections in multiple backup sets.

The required Office 365 license is only one.

Example No. 1: To back up one (1) SharePoint site under Site Collection, only one Office 365 license is needed.

Backup Set Name	SharePoint Site
Backup Set A	companyoffice365.sharepoint.com/user01
Backup Set B	companyoffice365.sharepoint.com/user01
Backup Set C	companyoffice365.sharepoint.com/user01

Example No. 2: To back up one (1) or two (2) SharePoint sites under Site Collection, only one Office 365 license is needed.

Backup Set Name	SharePoint Site
Backup Set A	companyoffice365.sharepoint.com/user01
	companyoffice365.sharepoint.com/user02
Backup Set B	companyoffice365.sharepoint.com/user01
Backup Set C	companyoffice365.sharepoint.com/user01
	companyoffice365.sharepoint.com/user02

Example No. 3: To back up three (3) or more SharePoint sites under Site Collection, only one Office 365 license is needed.

Backup Set Name	SharePoint Site
Backup Set A	companyoffice365.sharepoint.com/user01
	companyoffice365.sharepoint.com/user02
	companyoffice365.sharepoint.com/user03
Backup Set B	companyoffice365.sharepoint.com/user01
Backup Set C	companyoffice365.sharepoint.com/user01
	companyoffice365.sharepoint.com/user02
	companyoffice365.sharepoint.com/user03

Scenario No. 3: 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.

<table>
<tr><th>Backup Set Name</th><th>Files and/or Folders</th></tr>
<tr><td>Backup Set A</td><td>Folder01
microsoftword01.docx
powerpointpresentation01.pptx
spreadsheet01.xls
notepad01.txt
picture01.jpg
picture02.jpg</td></tr>
<tr><td rowspan="3">Backup Set B</td><td>Folder01
microsoftword01.docx
powerpointpresentation01.pptx
spreadsheet01.xls
notepad01.txt
picture01.jpg
picture02.jpg</td></tr>
<tr><td>Folder02</td></tr>
<tr><td>Folder03</td></tr>
<tr><td rowspan="3">Backup Set C</td><td>Folder01
microsoftword01.docx
powerpointpresentation01.pptx
spreadsheet01.xls
notepad01.txt
picture01.jpg
picture02.jpg</td></tr>
<tr><td>Folder02</td></tr>
<tr><td>Folder03
microsoftword02.docx
powerpointpresentation02.pptx
spreadsheet02.xls
notepad02txt
picture05.jpg
picture06.jpg</td></tr>
</table>

Scenario No. 4: Backing up Office 365 User Accounts, files and/or folders under Public Folder, and SharePoint sites under Site Collections 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 three (3) Office 365 user account, files and/or folders under Public Folder, and SharePoint sites under Site Collections on multiple backup sets, three (3) 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	user01@company-office365.com
	user02@company-office365.com
	companyoffice365.sharepoint.com/user01
	companyoffice365.sharepoint.com/user02
Backup Set C	user01@company-office365.com
	user02@company-office365.com
	Folder01 ○ microsoftword01.docx ○ powerpointpresentation01.pptx ○ spreadsheet01.xls ○ notepad01.txt ○ picture01.jpg ○ picture02.jpg
Backup Set D	user01@company-office365.com
	user02@company-office365.com
	user03@company-office365.com
	Folder01 ○ microsoftword01.docx ○ powerpointpresentation01.pptx ○ spreadsheet01.xls ○ notepad01.txt ○ picture01.jpg ○ picture02.jpg
	companyoffice365.sharepoint.com/user01
	companyoffice365.sharepoint.com/user02

Scenario No. 5: Backing up Office 365 User Accounts and Share Mailbox Accounts.

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

Example No. 1: To back up three (3) Office 365 user account and three (3) Shared mailbox accounts, six (6) Office 365 licenses are needed.

Backup Set Name	Office 365 User Account and Shared Mailbox Accounts
Backup Set A	user01@company-office365.com
	user02@company-office365.com
	user03@company-office365.com
	sharedmailbox01@test-office365.com
	sharedmailbox02@test-office365.com
	sharedmailbox03@test-office365.com

Appendix B: Example for backup of large numbers of Office 365 users

Example: 10,000 Office 365 users needed to be backup. Since the maximum number of Office 365 users per backup set is 2,000, there are 2 options available. There are further options, but this will involve a large number of backup sets and maintenance of these backup sets will be practical.

- Option 1 - 5 Backup Sets, each has 2,000 Office 365 Users
- Option 2 - 10 Backup Sets, each has 1,000 Office 365 Users

Option 1 – 5 Backup Sets, each has 2,000 Office 365 Users

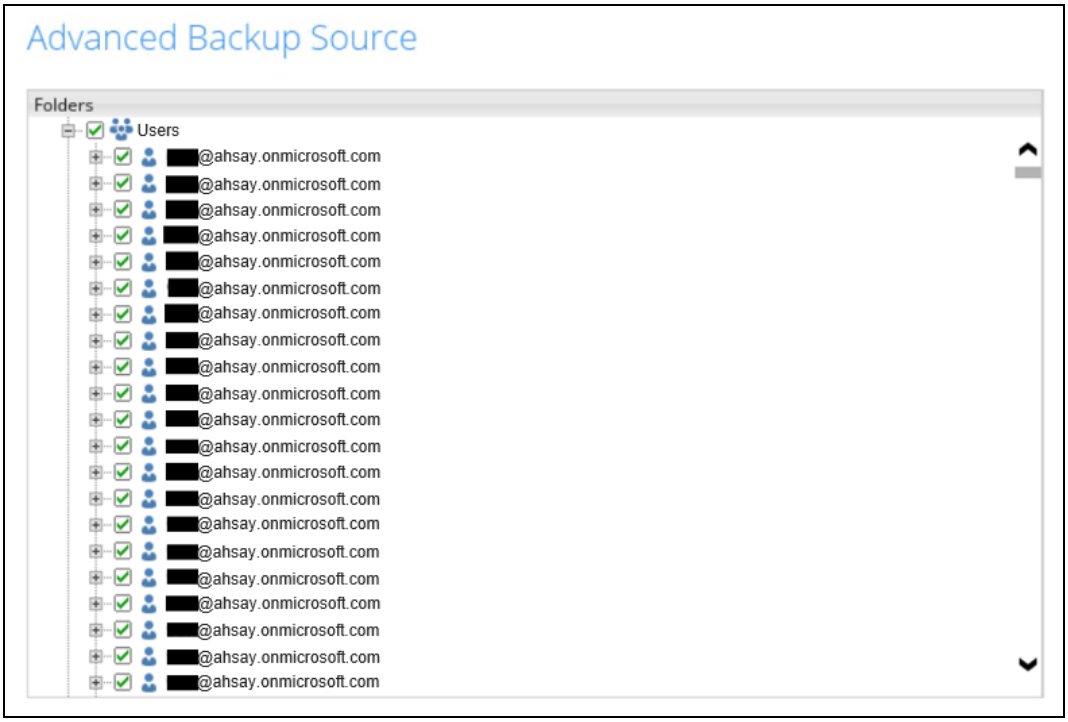
Backup Set Name	User Number
Backup -Set-1	No.1 – 2000
Backup -Set-2	No.2001 – 4000
Backup -Set-3	No. 4001 – 6000
Backup -Set-4	No. 6001 – 8000
Backup -Set-5	No. 8001 – 10000

Option 2 – 10 Backup Sets, each has 1,000 Office 365 Users

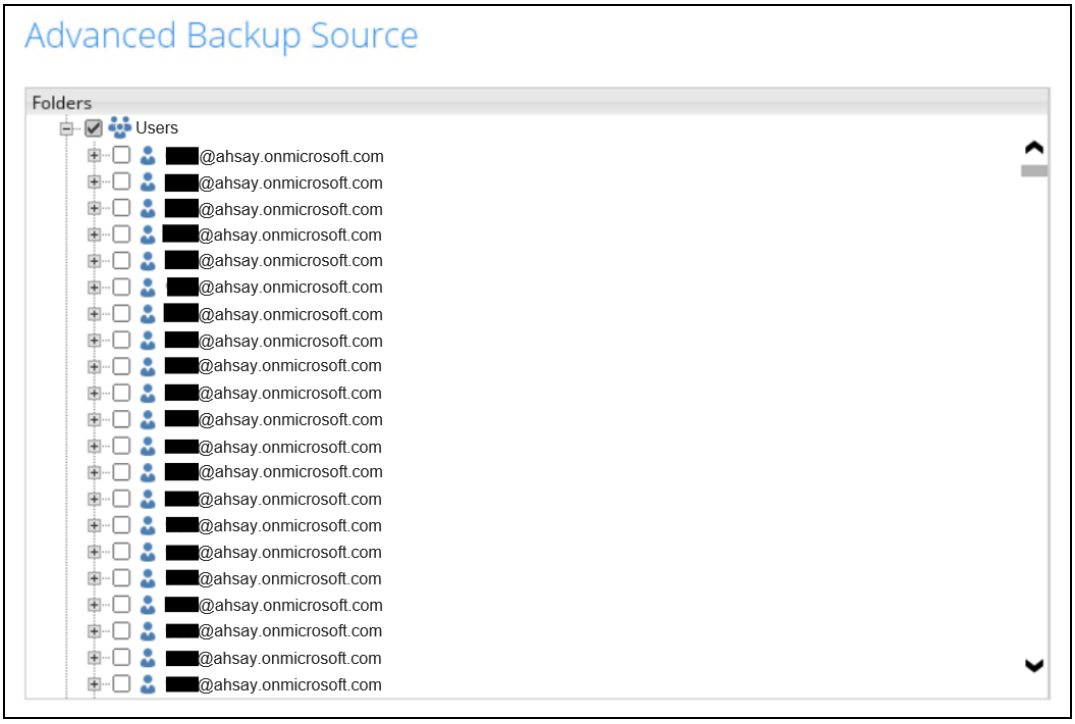
Backup Set Name	User Number
Backup -Set-1	No.1 – 1000
Backup -Set-2	No.1001 – 2000
Backup -Set-3	No. 2001 – 3000
Backup -Set-4	No. 3001 – 4000
Backup -Set-5	No. 4001 – 5000
Backup -Set-6	No. 5001 – 6000
Backup -Set-7	No. 6001 – 7000
Backup -Set-8	No. 7001 – 8000
Backup -Set-9	No. 8001 – 9000
Backup -Set-10	No. 9001 – 10000

If Option 2 was selected, for the last backup set, Backup -Set-10, follow the instructions on how to select the Office 365 users. Doing these steps will ensure that additional Office 365 users will be automatically included in the backup set.

1. On the backup source, tick the checkbox for the root selection. This will select all the Office 365 users.



2. Deselect the first 9000 Office 365 users.



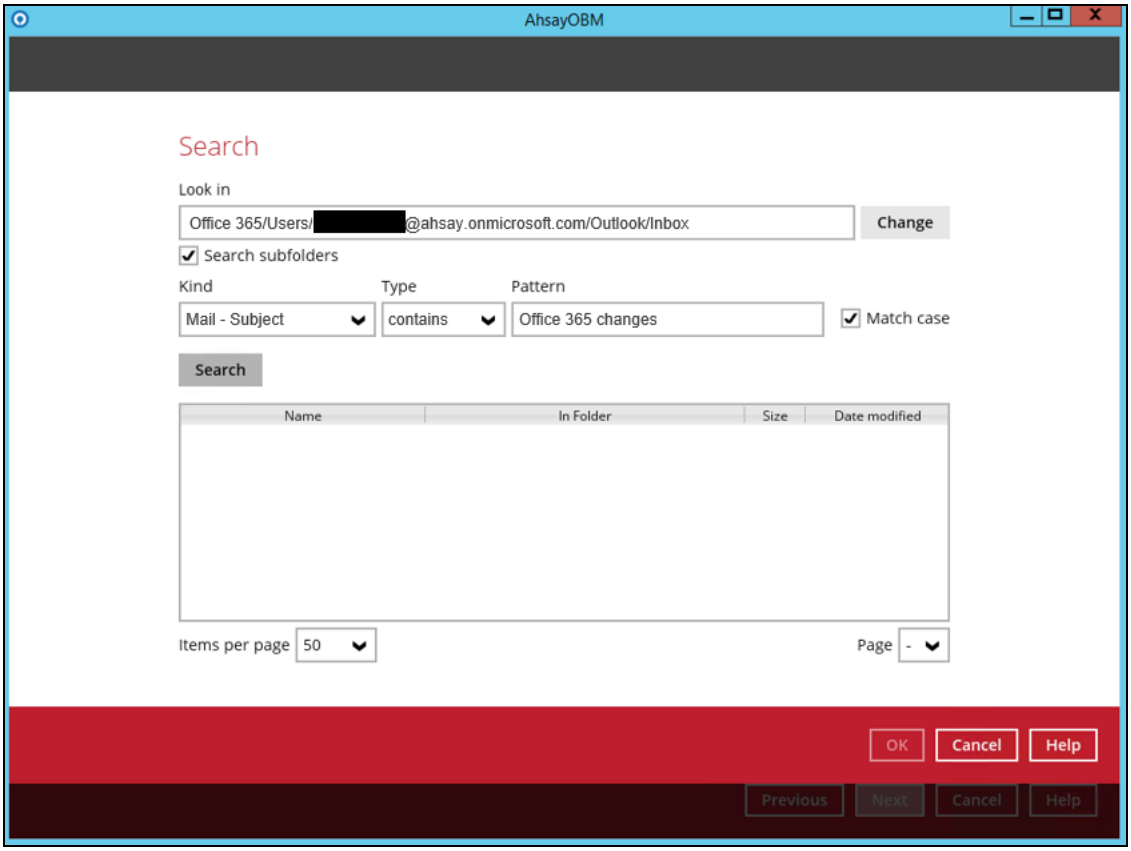
Appendix C: Example Scenarios for Restore Filter using AhsayOBM

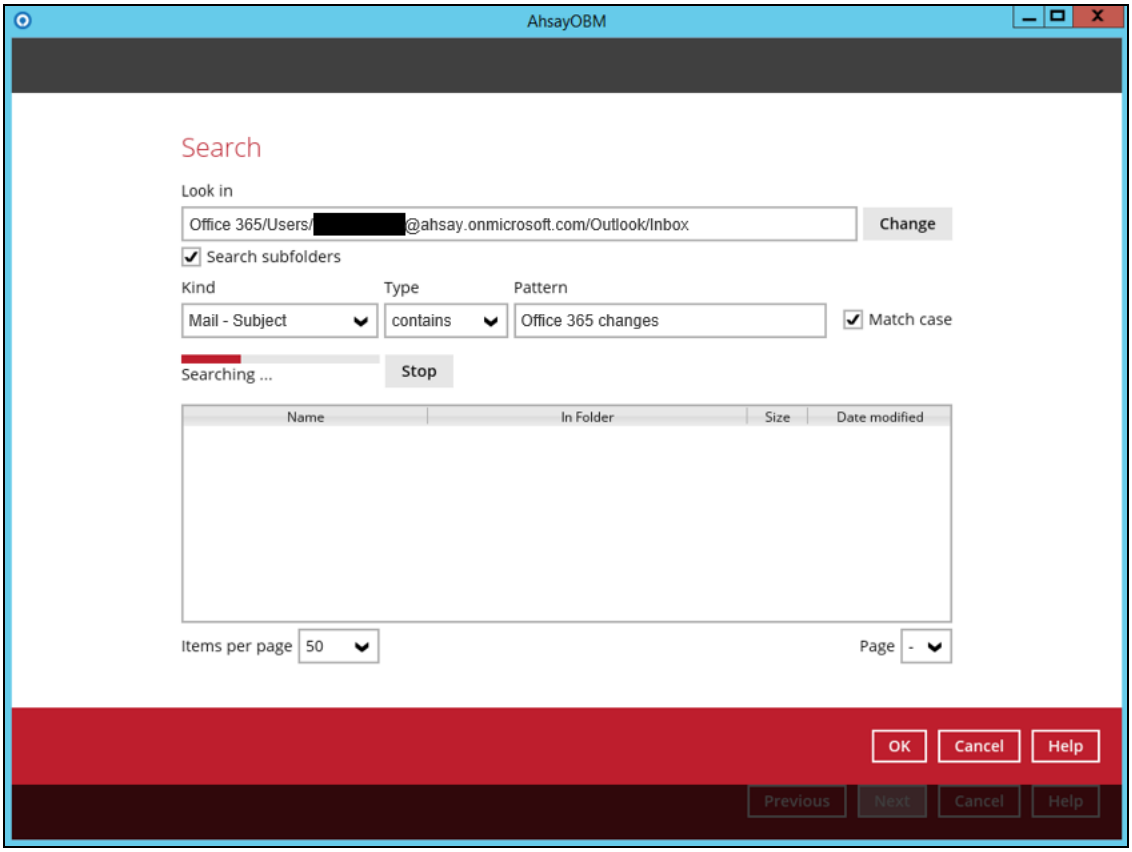
Scenarios No. 1: Items from Users

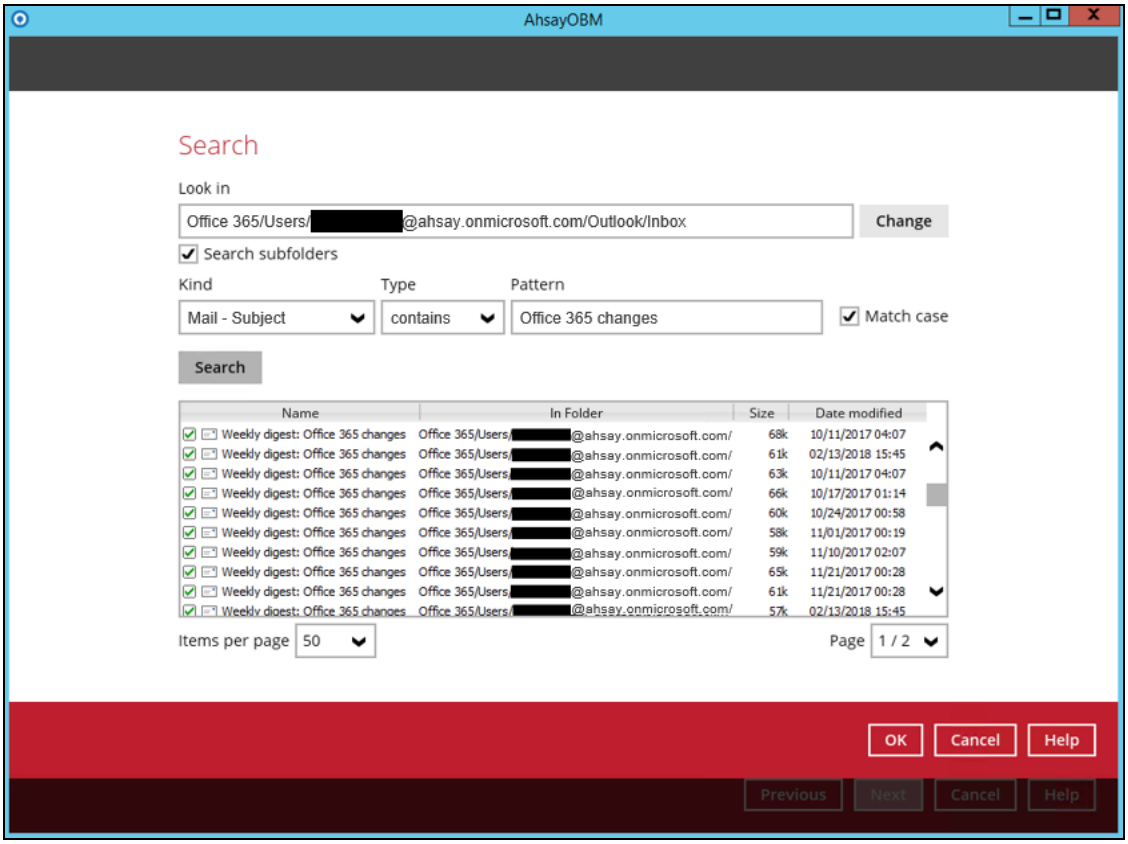
Example No. 1: Restore filter setting from an Office 365 user account's outlook inbox

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 AhsayOBM.




AhsayOBM
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


AhsayOBM
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
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.

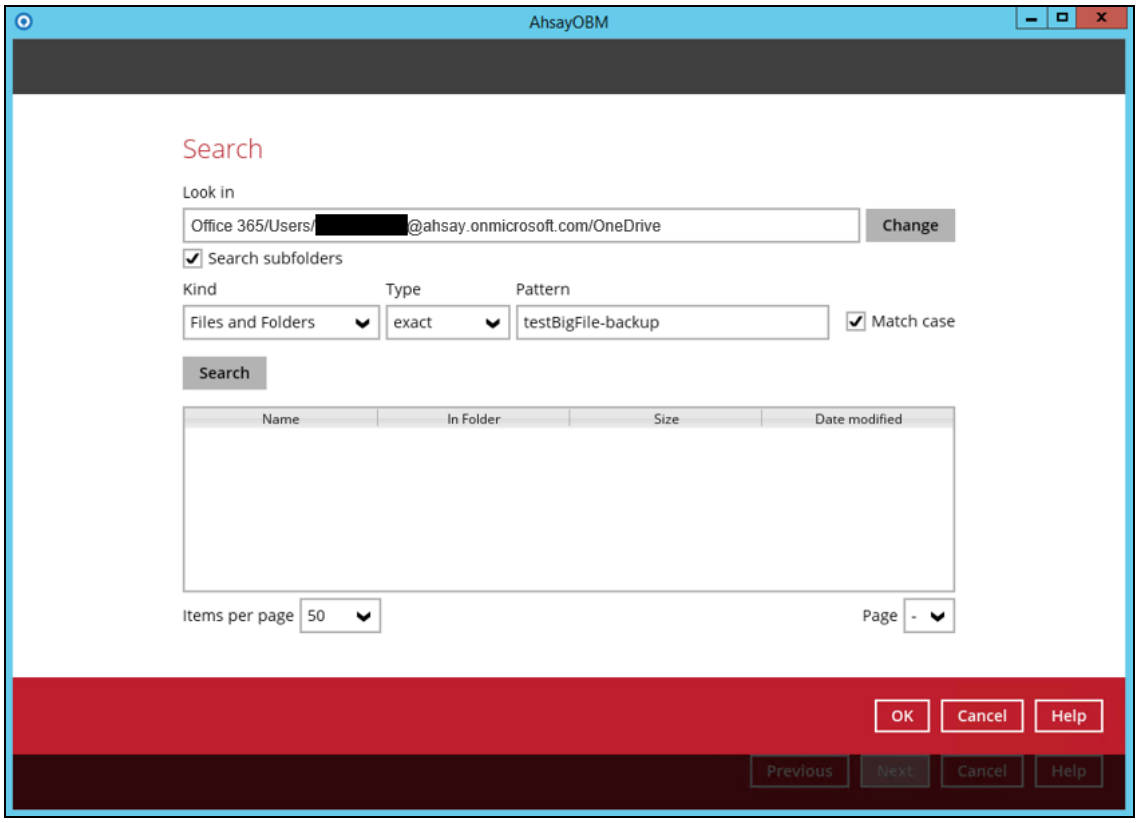
As you can see on the screen shot above, the result panel contains the Name of the mail, Directory of the mails which are indicated In-Folder column, Size of each mails, and Date Modified.

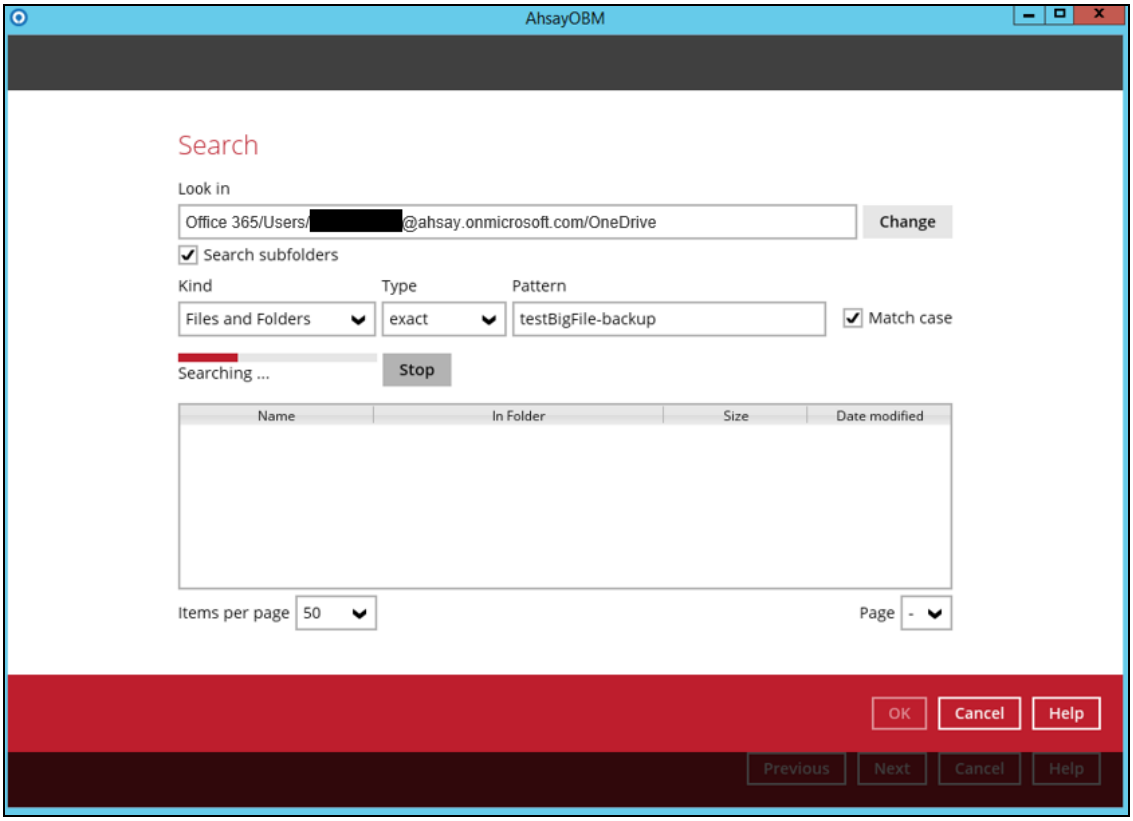
The restore filter setting includes the Search subfolder and Match case set to true. This means that the filter will include all available subfolders in the Outlook Inbox upon searching. And it will strictly search only the specified pattern and case which is the 'Office 365 changes'.

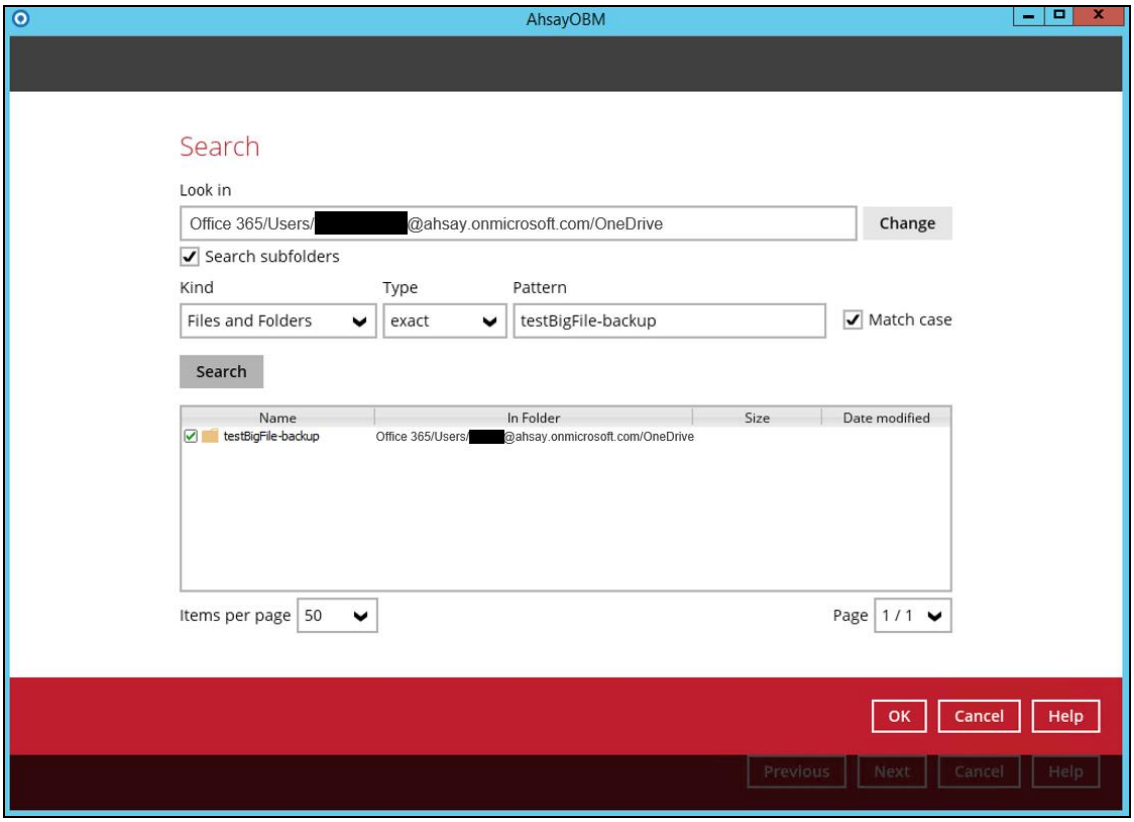
Example No. 2: Restore filter setting from an Office 365 user account's OneDrive

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

Follow the step-by-step procedure indicated on Restore Filter with AhsayOBM




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


AhsayOBM
Search
Look in
Office 365/Users/[redacted]@ahsay.onmicrosoft.com/OneDrive
Change
Search subfolders
Kind
Type
Pattern
Files and Folders
exact
testBigFile-backup
Match case
Search
Name
In Folder
Size
Date modified
testBigFile-backup
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 'testBigFile-backup' with match case set to true will be included upon performing search.

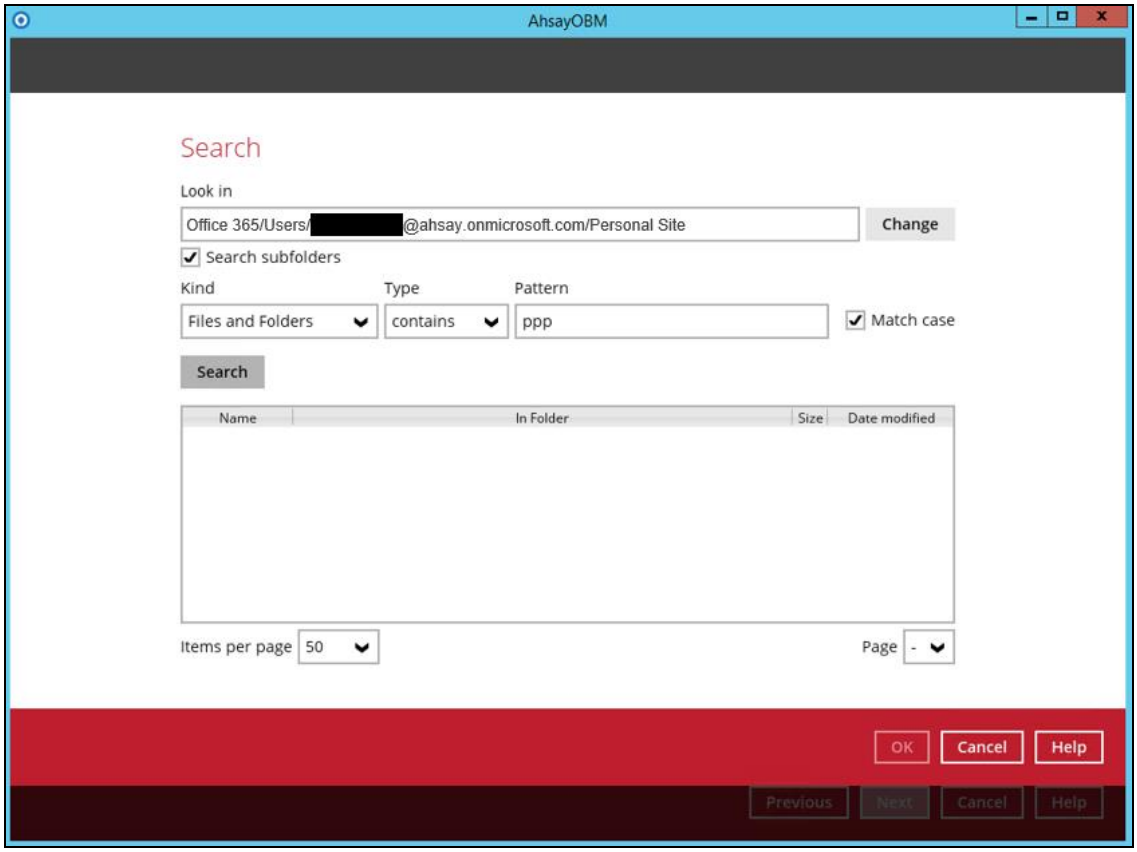
As you can see on the screen shot above, the result panel contains the Name of the mail, Directory of the mails which are indicated In-Folder column, Size of each mails, and Date Modified.

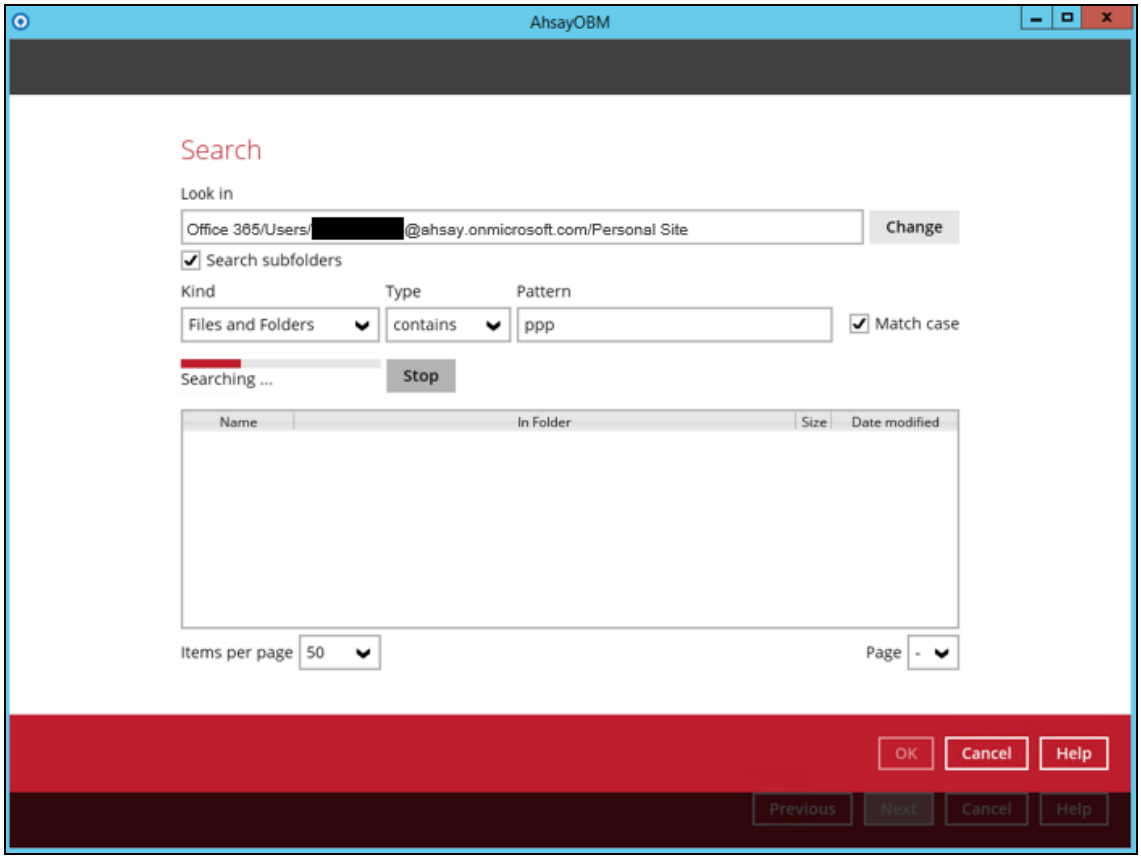
The restore filter setting includes the Search subfolder and Match case set to true. This means that the filter will include all available subfolders in OneDrive upon searching. And it will strictly search only the specified pattern and case which is the 'testBigFile-backup'.

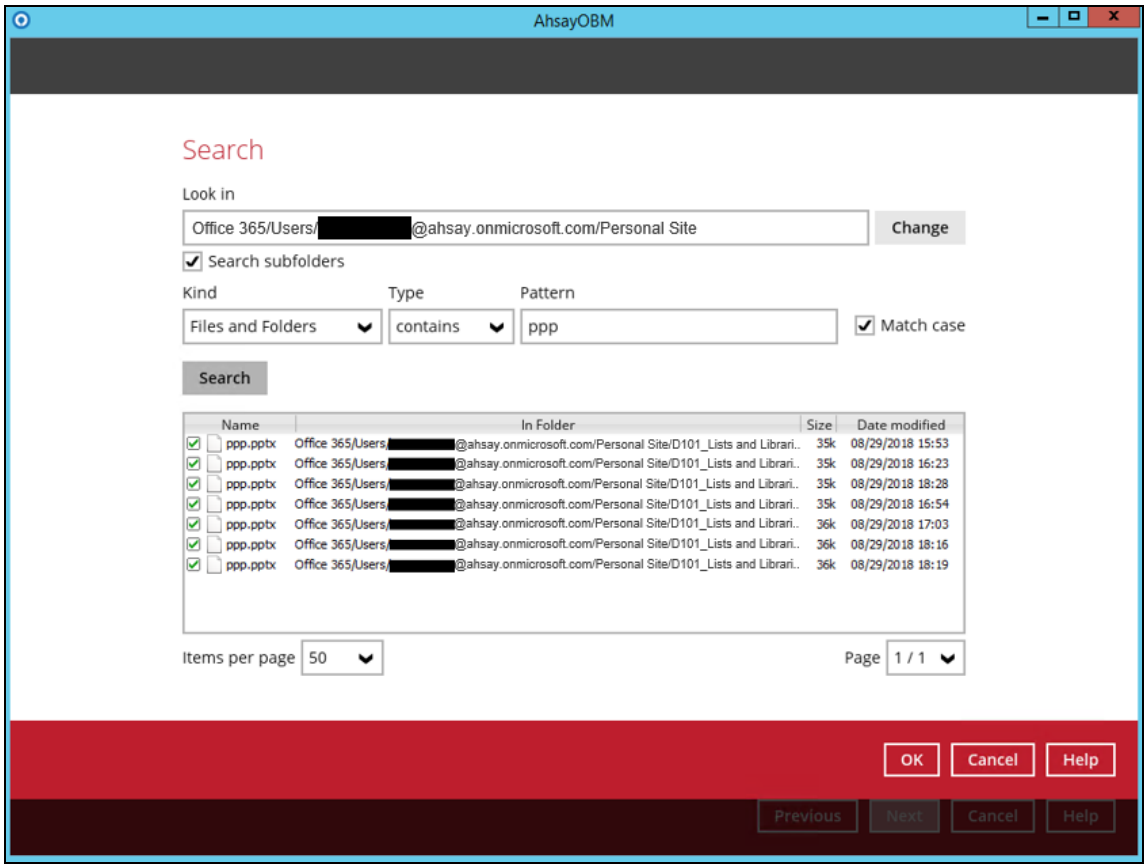
Example No. 3: Restore filter setting from an Office 365 user account's personal site

Location:	Office 365/Users/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 AhsayOBM




AhsayOBM
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


AhsayOBM
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/D101_Lists and Librari.. 35k 08/29/2018 15:53
ppp.pptx Office 365/Users/[redacted]@ahsay.onmicrosoft.com/Personal Site/D101_Lists and Librari.. 35k 08/29/2018 16:23
ppp.pptx Office 365/Users/[redacted]@ahsay.onmicrosoft.com/Personal Site/D101_Lists and Librari.. 35k 08/29/2018 18:28
ppp.pptx Office 365/Users/[redacted]@ahsay.onmicrosoft.com/Personal Site/D101_Lists and Librari.. 35k 08/29/2018 16:54
ppp.pptx Office 365/Users/[redacted]@ahsay.onmicrosoft.com/Personal Site/D101_Lists and Librari.. 36k 08/29/2018 17:03
ppp.pptx Office 365/Users/[redacted]@ahsay.onmicrosoft.com/Personal Site/D101_Lists and Librari.. 36k 08/29/2018 18:16
ppp.pptx Office 365/Users/[redacted]@ahsay.onmicrosoft.com/Personal Site/D101_Lists and Librari.. 36k 08/29/2018 18:19
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.

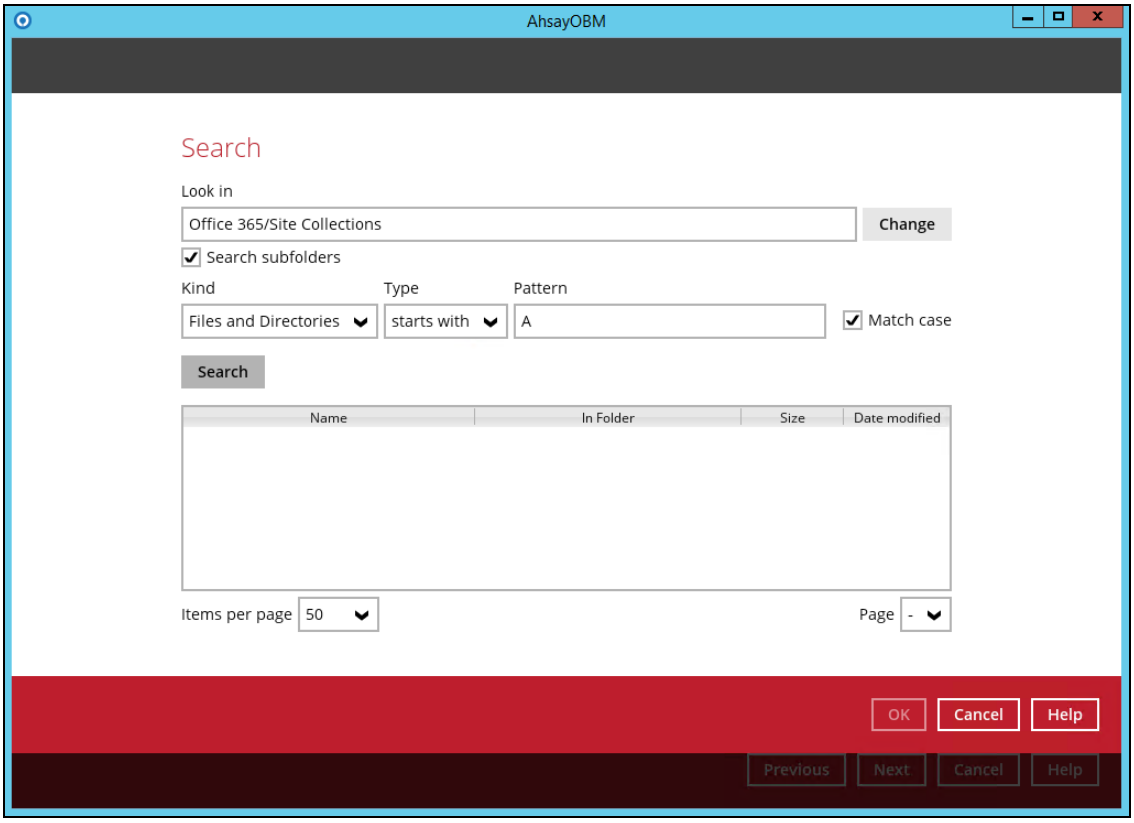
The restore filter setting includes the Search subfolder and Match case set to true. This means that the filter will include all available subfolders in Personal Site upon searching. And it will strictly search only the specified pattern and case which starts with ‘ppp’.

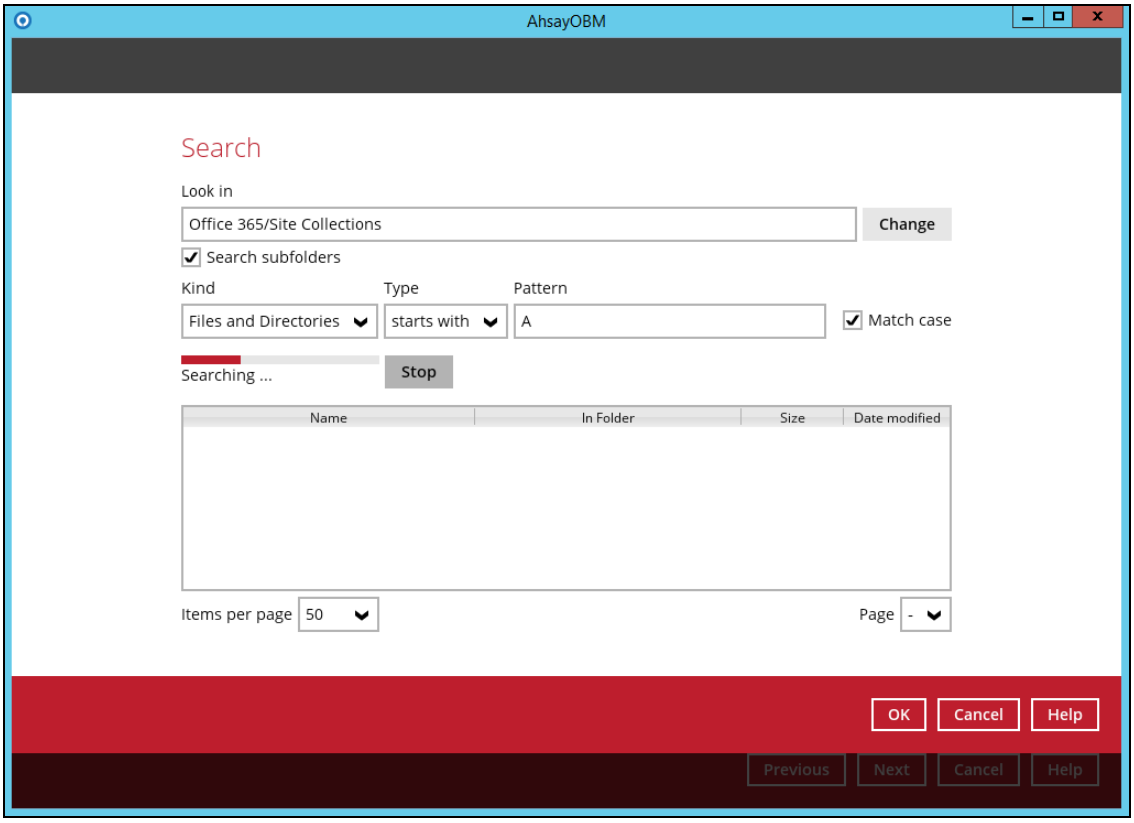
Scenarios No. 2: Items from Site Collections

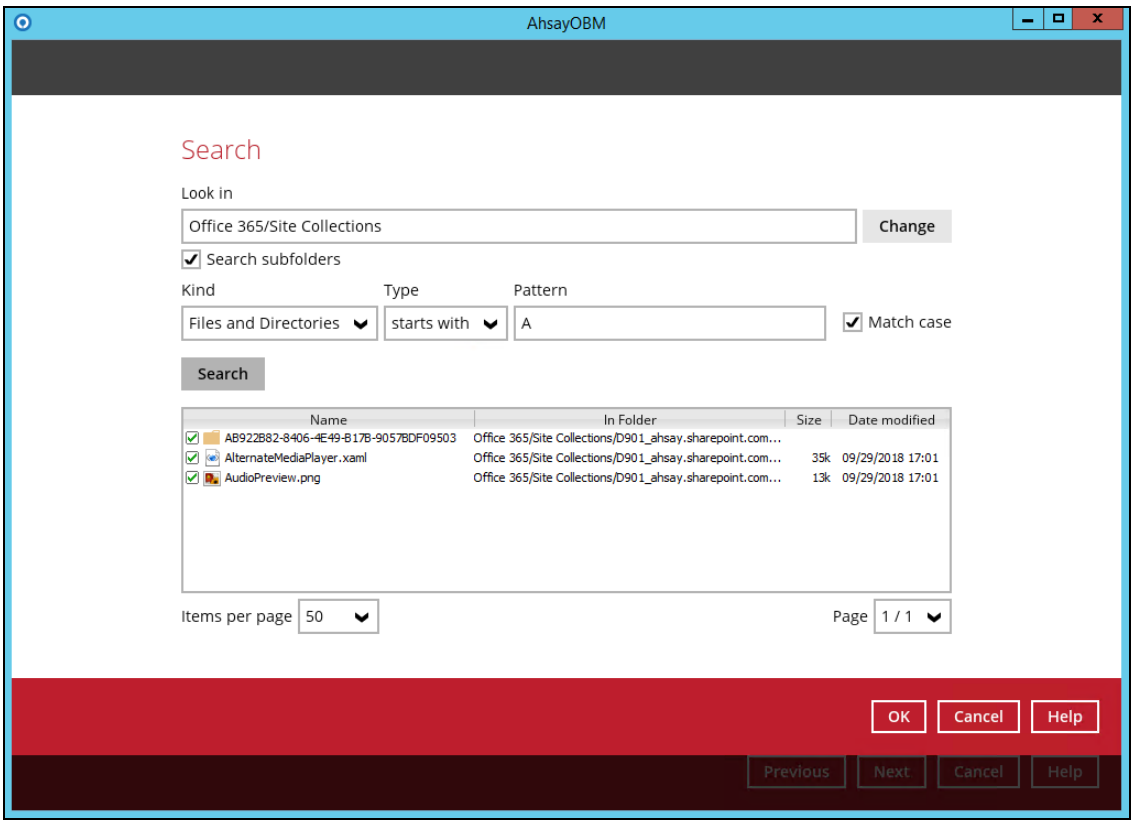
Example No. 1: Restore filter setting from Site Collections

Location:	Office 365/Site Collections
Search subfolders:	True
Kind:	Files and Directories
Type:	Starts With
Pattern:	A
Match Case:	True

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




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


AhsayOBM
Search
Look in
Office 365/Site Collections
Change
Search subfolders
Kind
Type
Pattern
Files and Directories
starts with
A
Match case
Search
Name
In Folder
Size
Date modified
AB922B82-8406-4E49-B17B-9057BDF09503
Office 365/Site Collections/D901_ahsay.sharepoint.com...
AlternateMediaPlayer.xaml
Office 365/Site Collections/D901_ahsay.sharepoint.com...
35k
09/29/2018 17:01
AudioPreview.png
Office 365/Site Collections/D901_ahsay.sharepoint.com...
13k
09/29/2018 17:01
Items per page
50
Page
1 / 1
OK
Cancel
Help
Previous
Next
Cancel
Help

Explanation:

All SharePoint sites under Office 365/Site Collections that has the pattern that starts with 'A' with match case set to true will be included upon performing search.

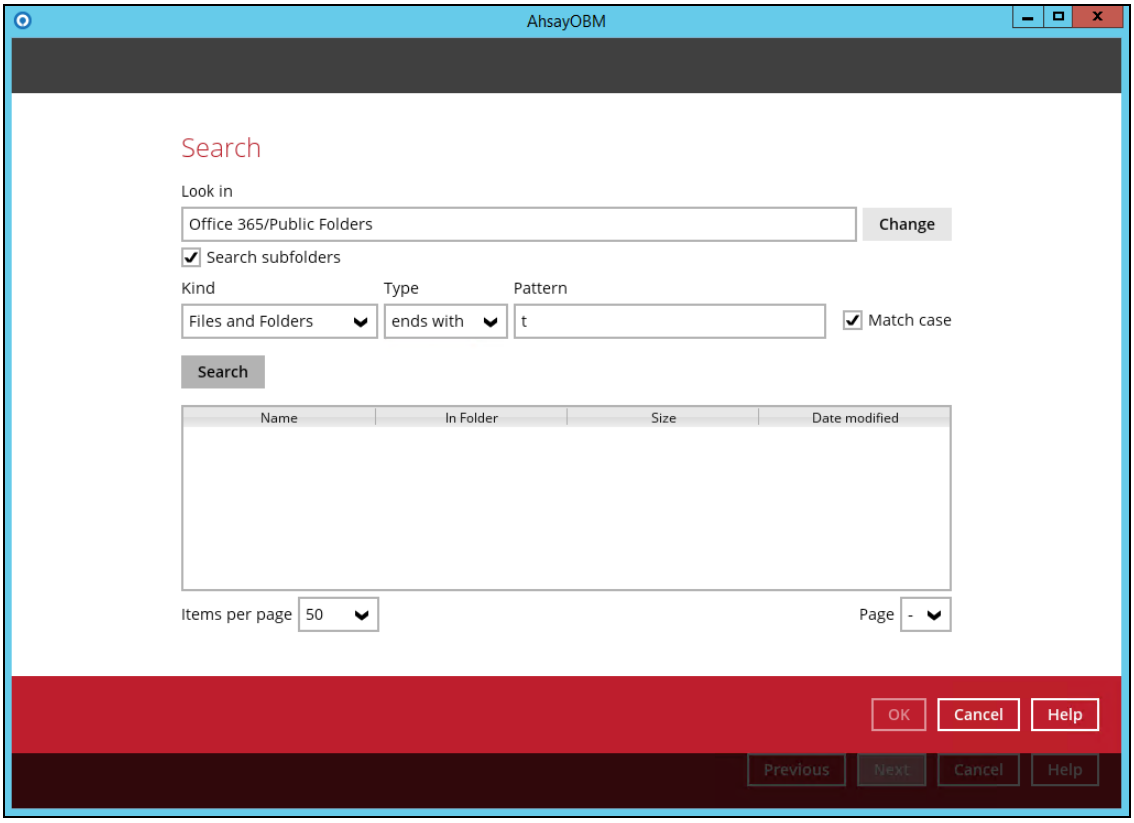
As you can see on the screen shot above, the result panel contains the Name of the mail, Directory of the mails which are indicated In-Folder column, Size of each mails, and Date Modified.

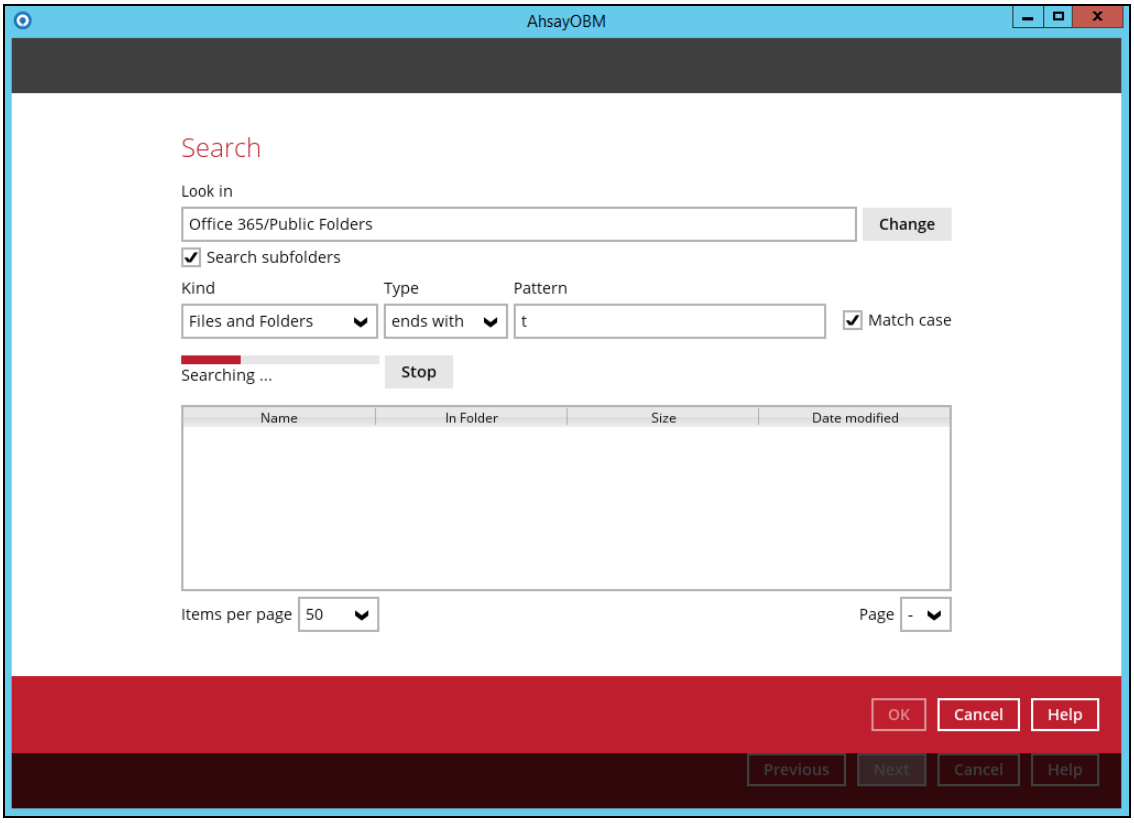
The restore filter setting includes the Search subfolder and Match case set to true. This means that the filter will include all available subfolders in Site Collections upon searching. And it will strictly search only the specified pattern and case which starts with 'A'.

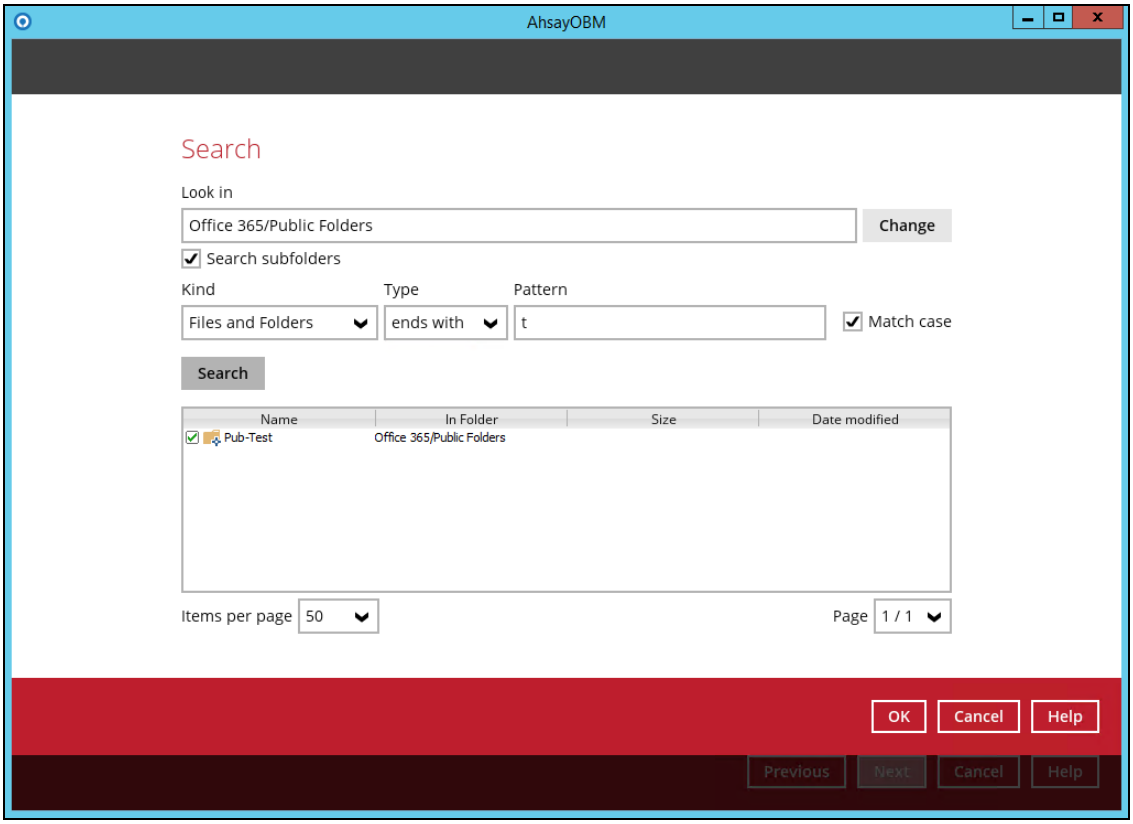
Example No. 2: Restore filter setting from Public Folders

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

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




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


AhsayOBM
Search
Look in
Office 365/Public Folders
Change
Search subfolders
Kind
Type
Pattern
Files and Folders
ends with
t
Match case
Search
Name
In Folder
Size
Date modified
Pub-Test
Office 365/Public Folders
Items per page
50
Page
1 / 1
OK
Cancel
Help
Previous
Next
Cancel
Help

Explanation:

All files and folders under Office 365/Public Folders that has the pattern that ends with ‘t’ 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.

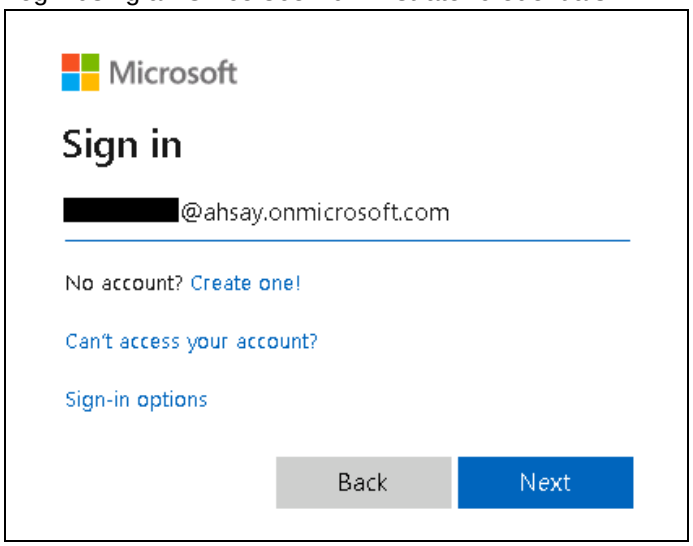
The restore filter setting includes the Search subfolder and Match case set to true. This means that the filter will include all available subfolders in Public Folder upon searching. And it will strictly search only the specified pattern and case which ends with ‘t’.

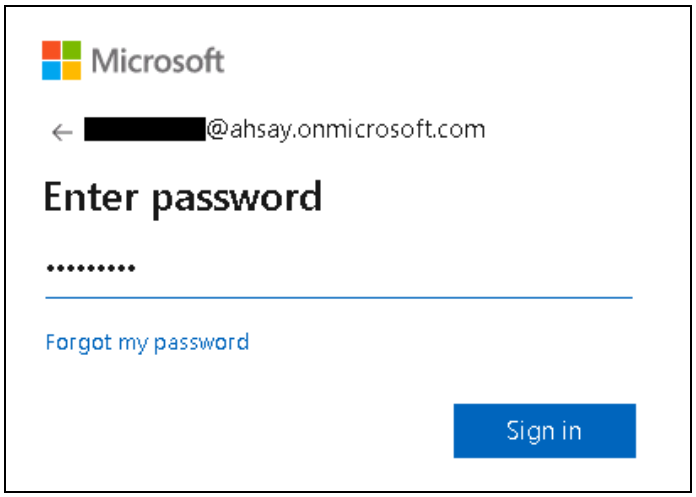
Appendix D: Setting Multi-Factor Authentication (MFA) in Microsoft 365 Admin Center

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.

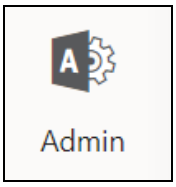
To enable MFA to any Office 365 user accounts, follow the steps below:

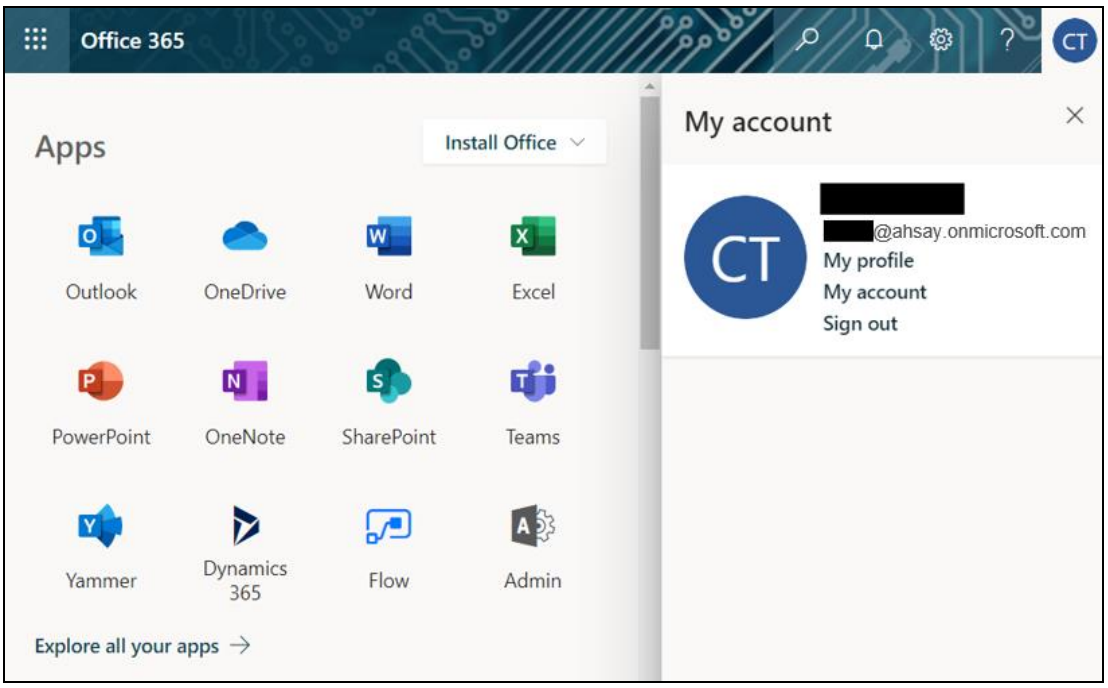
1. Login using an Office 365 Administrator credentials.



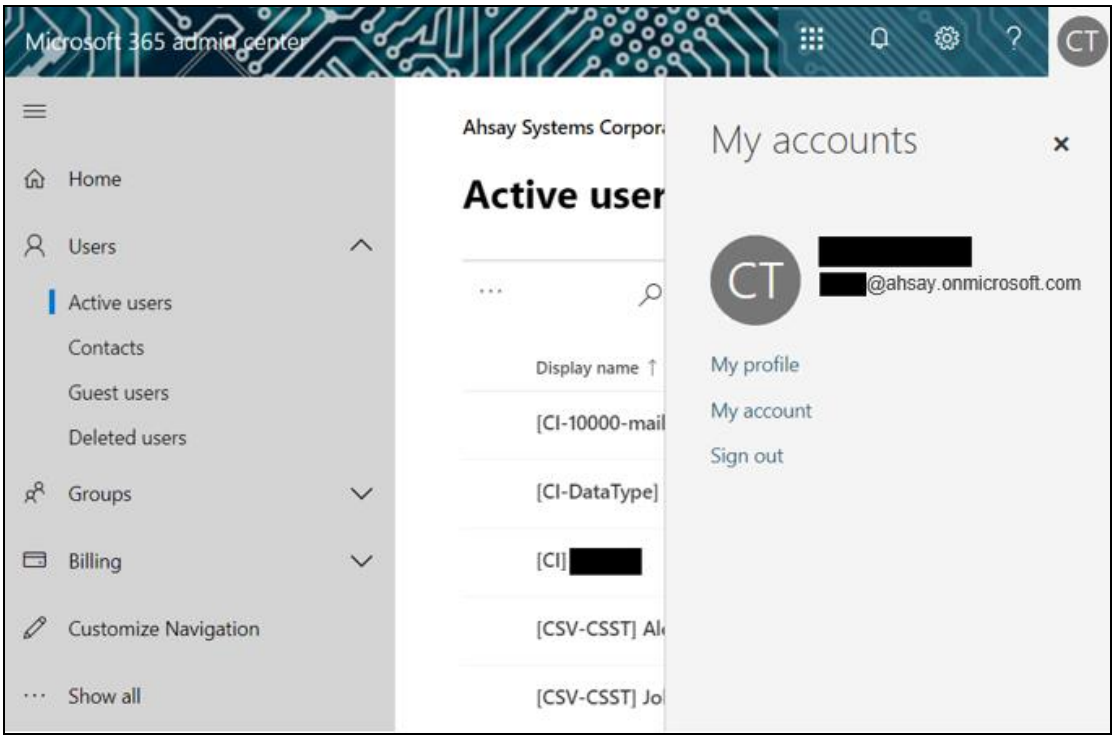


2. Click the **Admin Center** icon.



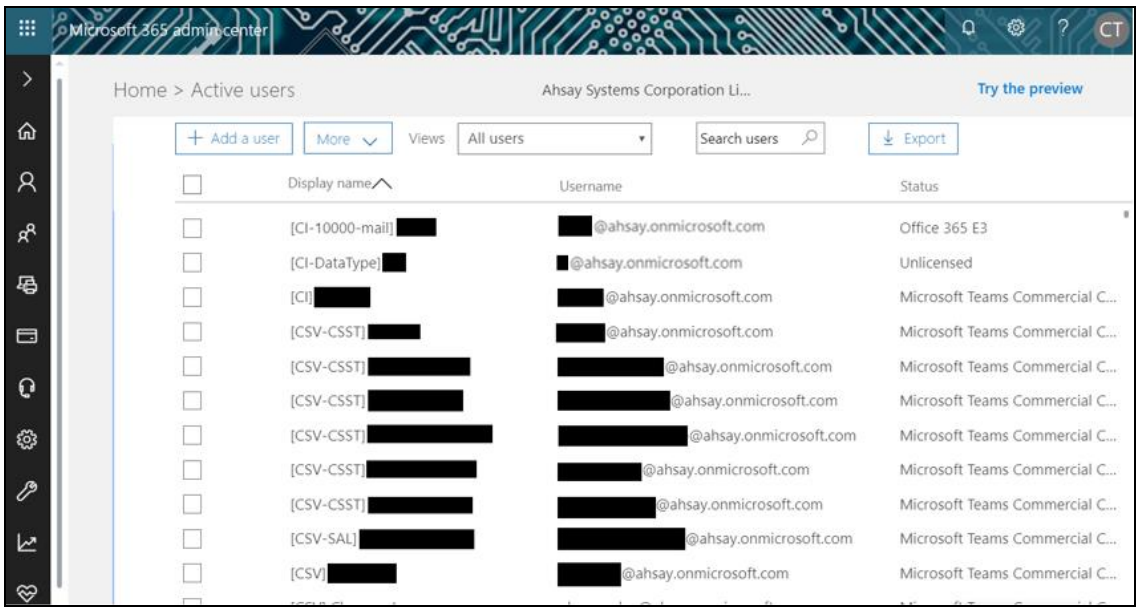


3. Go to **Users** and select the **Active users** from the list.

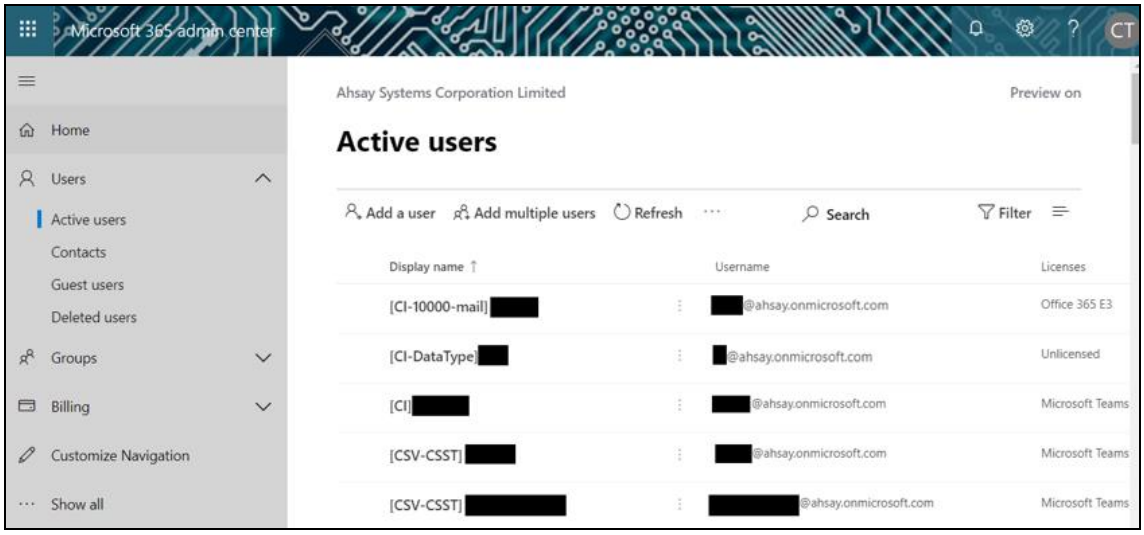


4. There are two (2) modes of viewing the Active users.

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

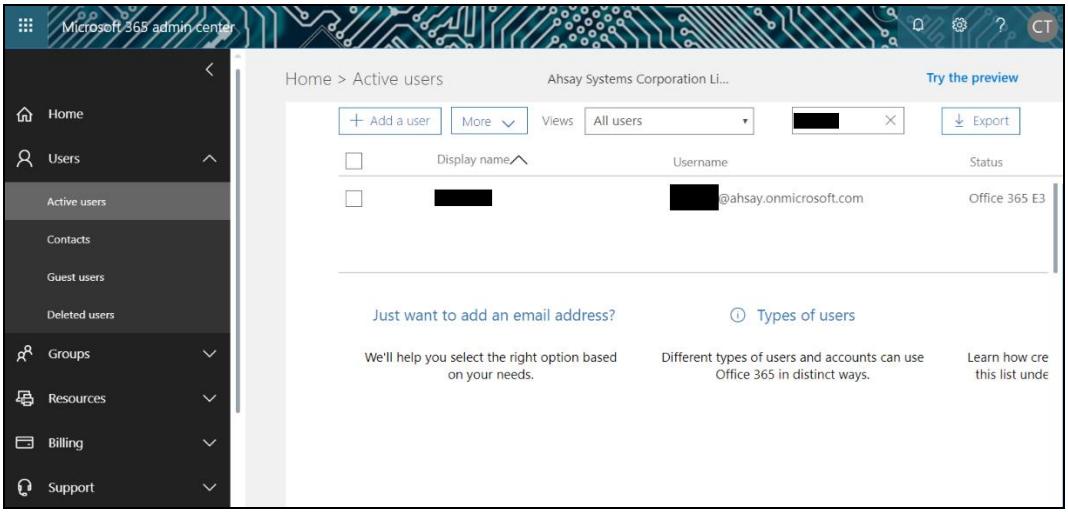


   Preview Mode – This is a new feature in the Office 365 Admin Center that offers simplification to manage your Microsoft 365 and Office 365 services. It also has all the capabilities of the classic mode.

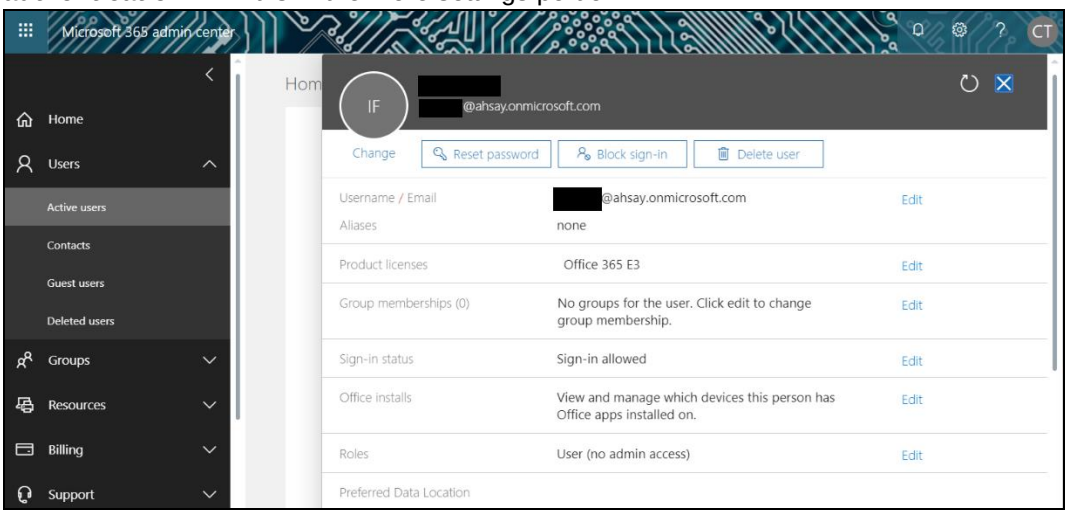


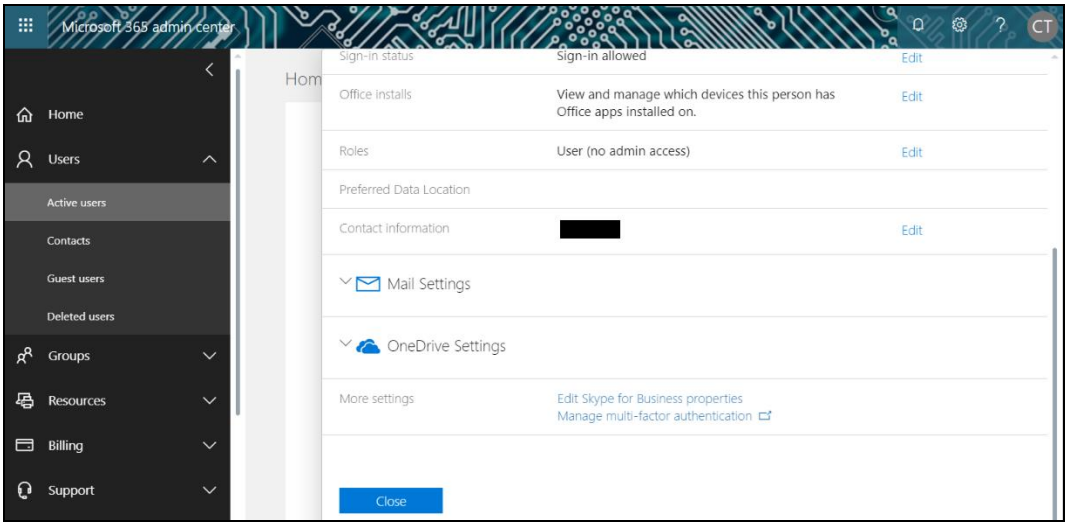
5. To go to the Multifactor Authentication screen, below are the steps for classic and preview mode.
   For the Classic Mode:

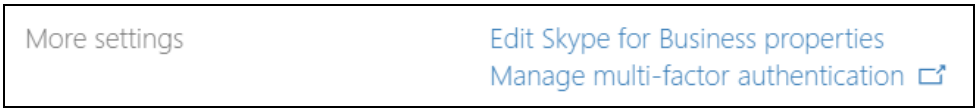
   - Search and select an Office 365 user account. The user's information will be displayed.



- 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.



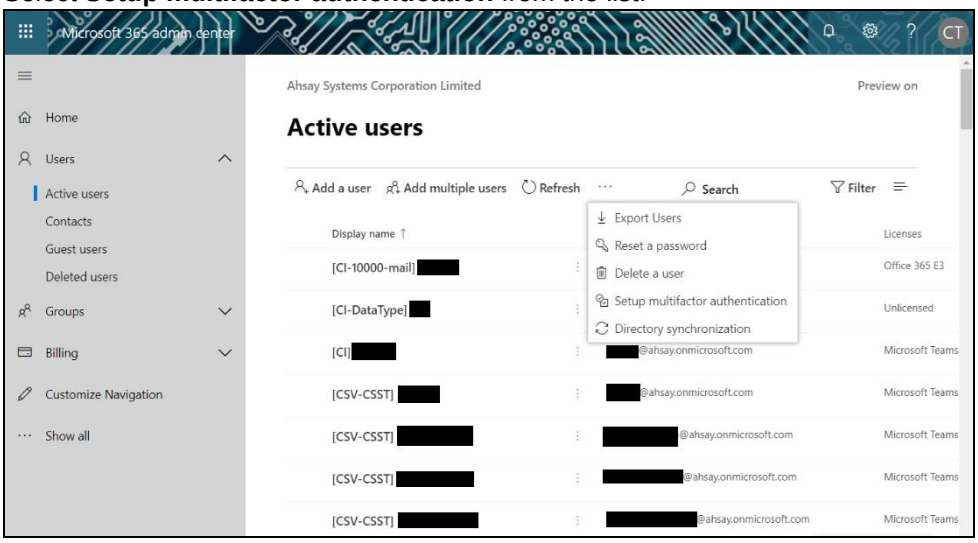




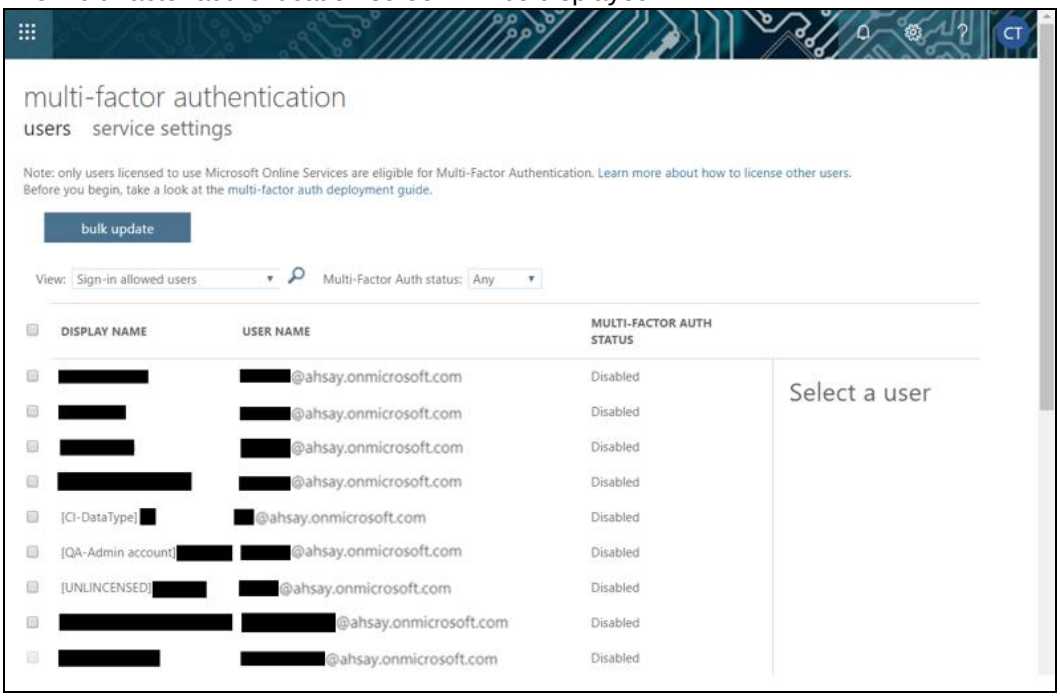
For the Preview Mode:

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

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

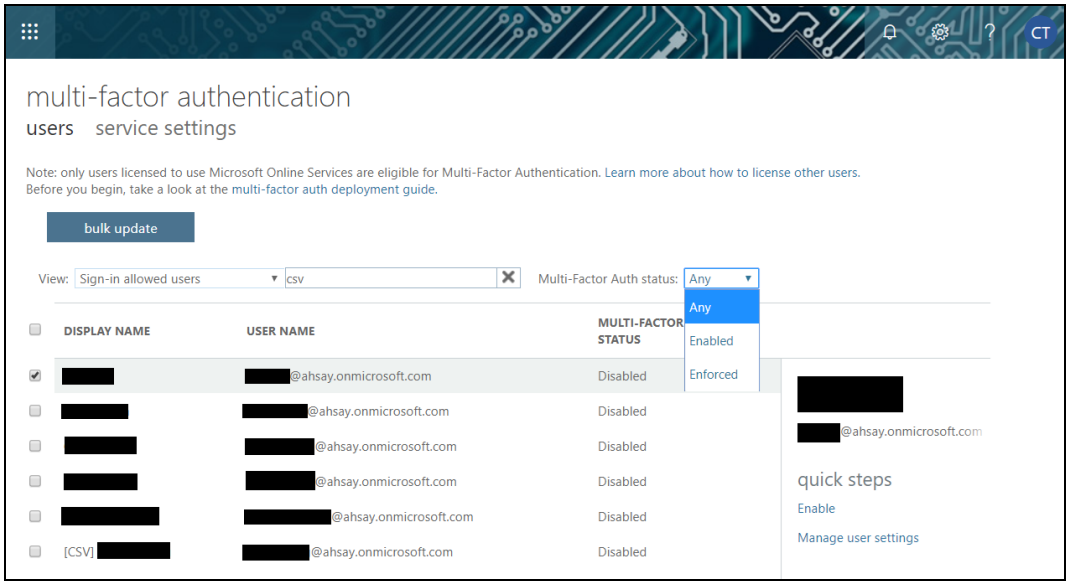


6. The multi-factor authentication screen will be displayed.



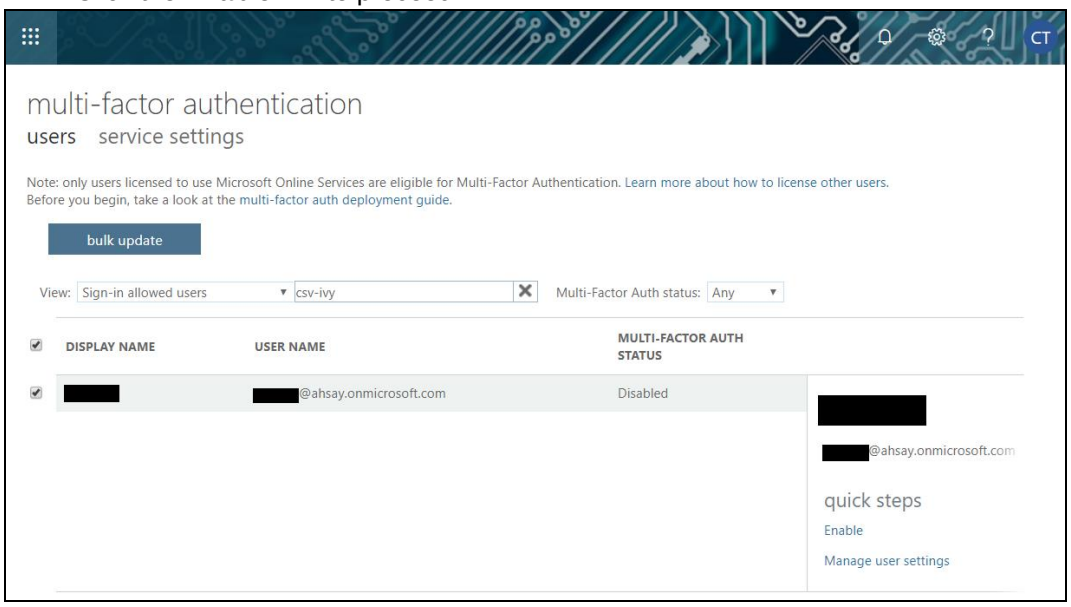
Note: The two (2) modes will go to the same screen.

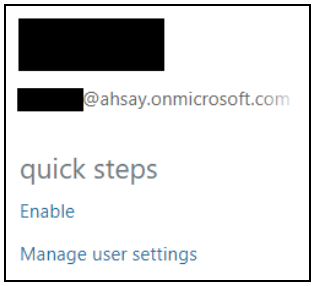
7. You can search and select one or more Office 365 user accounts. There is also a drop-down list available for multi-factor authentication status namely, **Disabled, Enabled**, and **Enforced**.



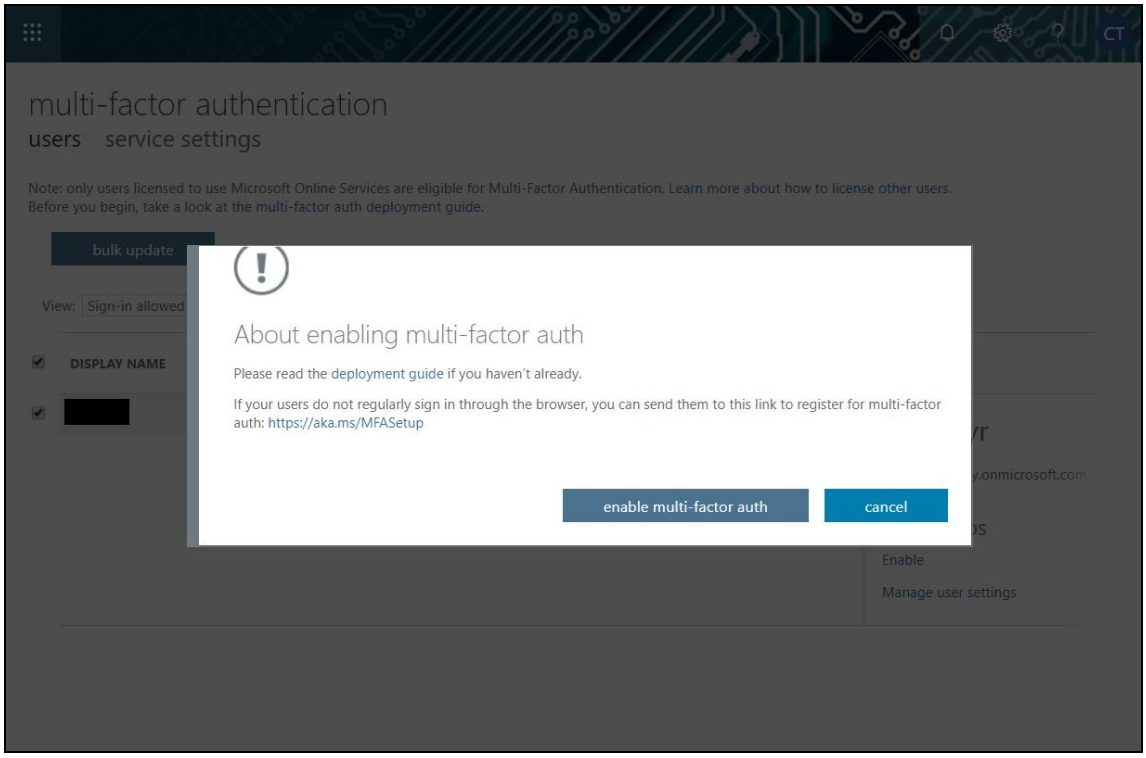
- Disabled – This status refers to the users who are not yet enrolled in the MFA. This is the default status.
- Enabled – This status refers to the users who are enrolled in the MFA, but changes have not yet taken effect.
- Enforced – This status refers to the users who are enrolled in the MFA has completed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

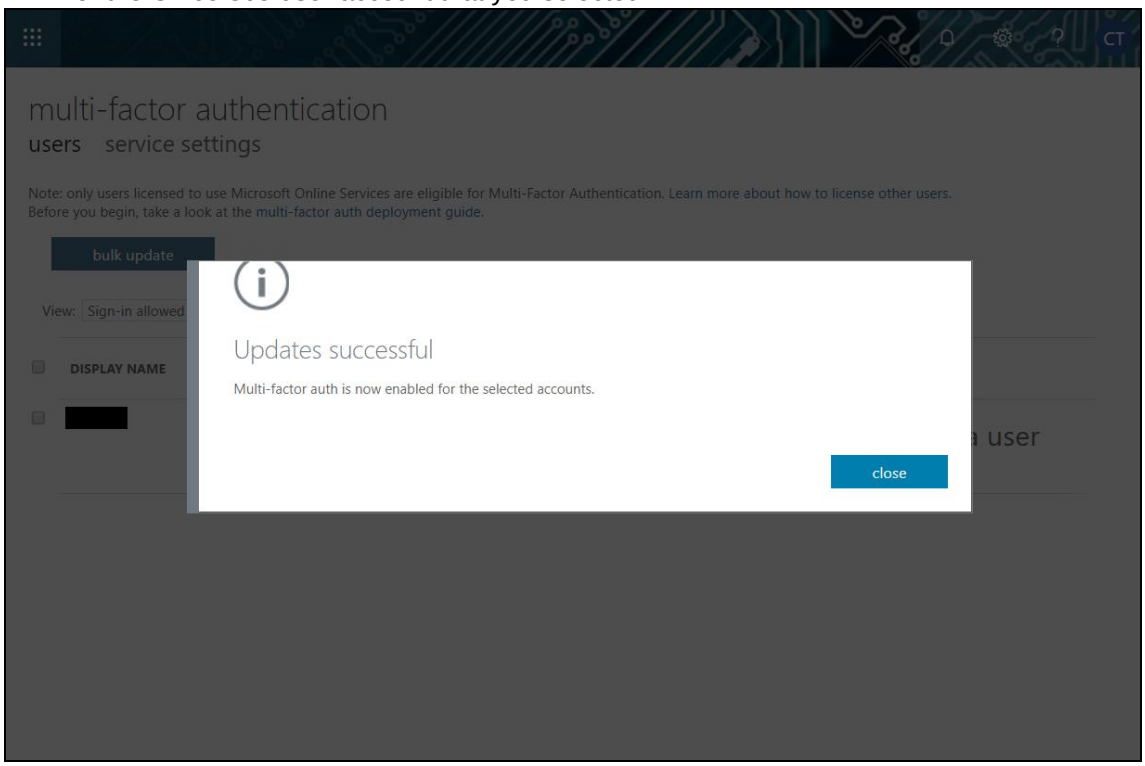




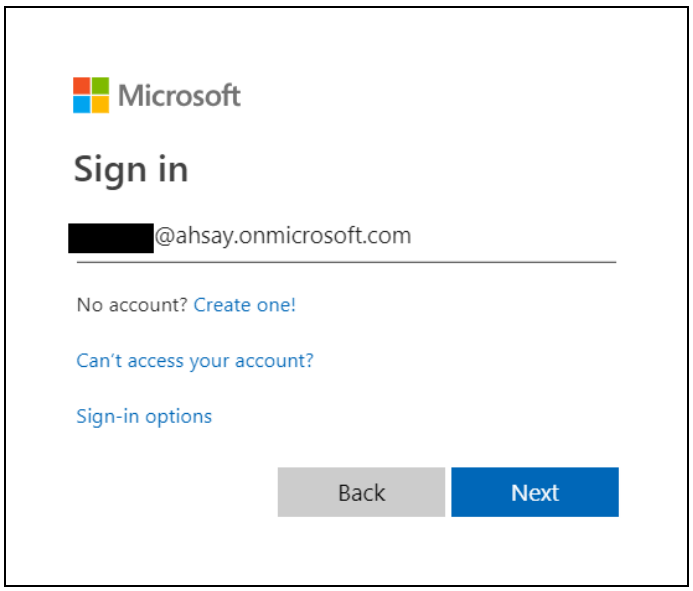
9. A warning message will be displayed. Click the **enable multi-factor auth** button to proceed. Otherwise, click the **cancel** button to abort.

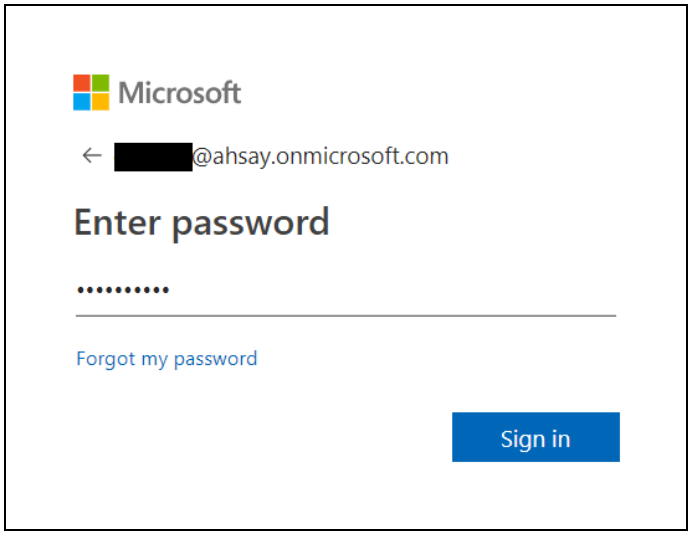


10. If you select enable multi-factor auth, the screen below shows the successful enabling of MFA for the Office 365 user account that you selected.

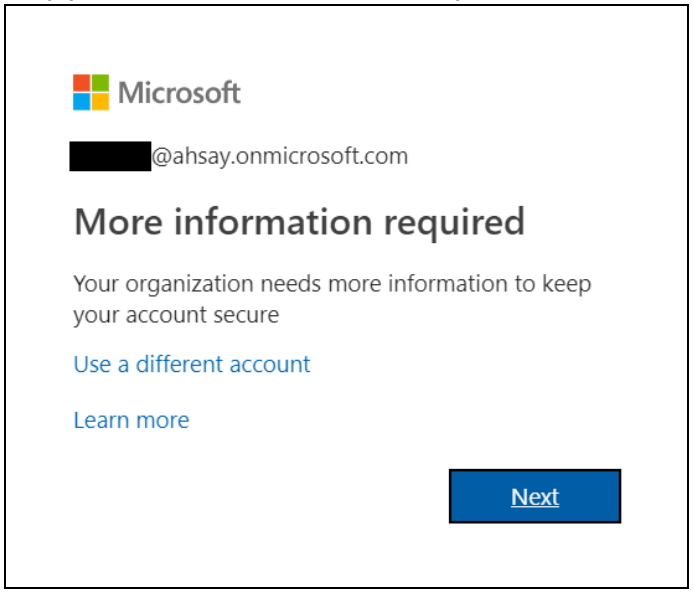


11. To finish the setup for the MFA, login using the MFA enabled Office 365 user account.

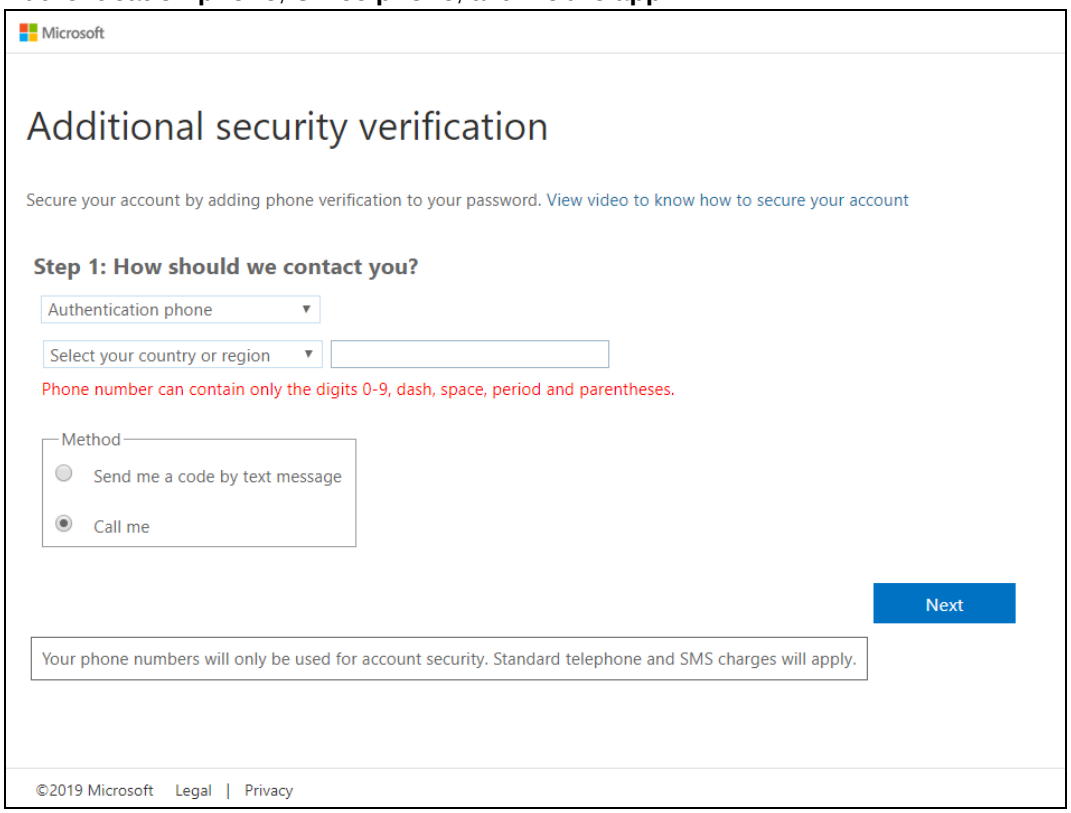




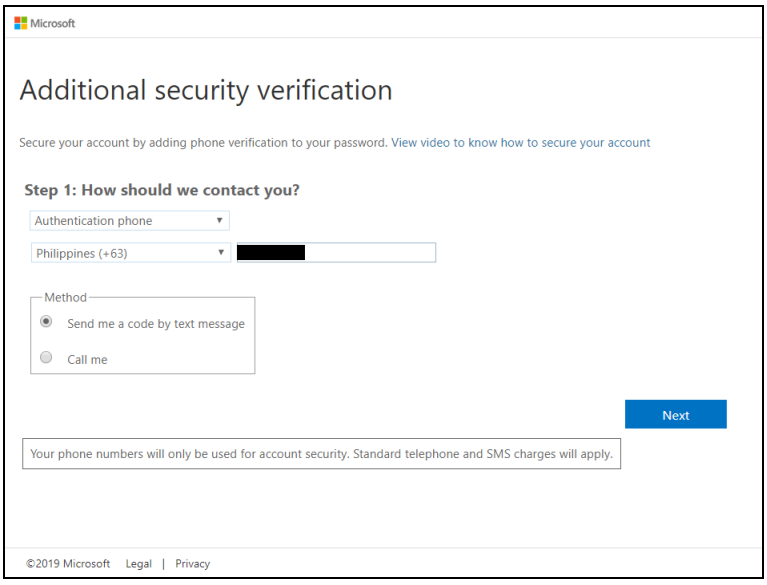
12. Upon logging in, there will be a message that will require you to provide more information to keep your account safe. Click **Next** to proceed.



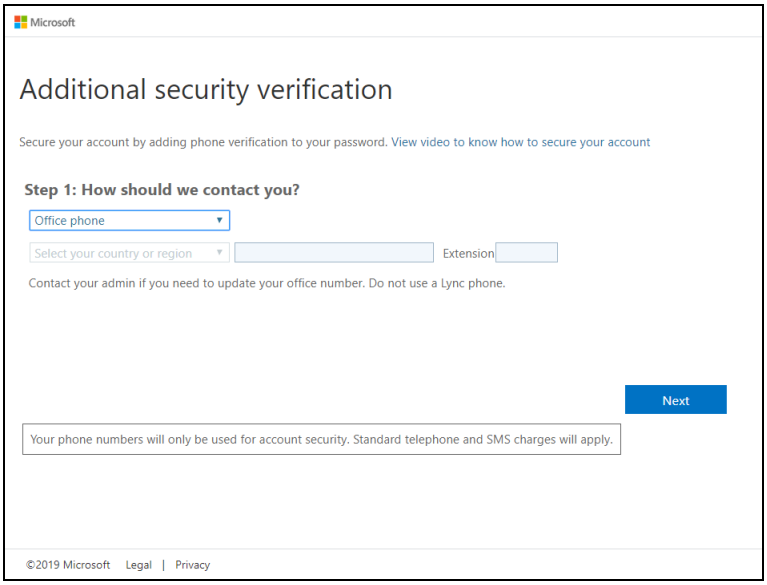
13. The **Additional security verification** screen will be displayed. Select one (1) option you want for the security of your account. You can choose from the three (3) options, **Authentication phone**, **Office phone**, and **Mobile app**.



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

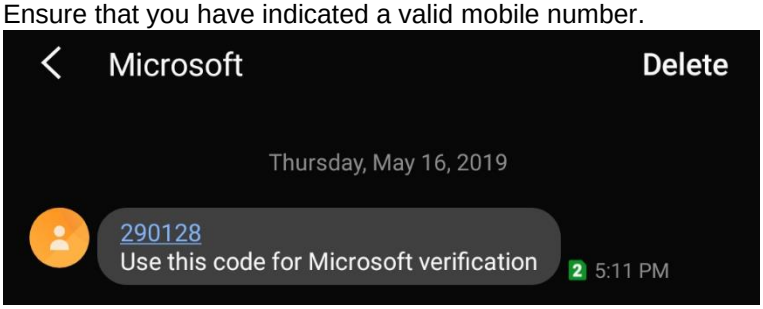


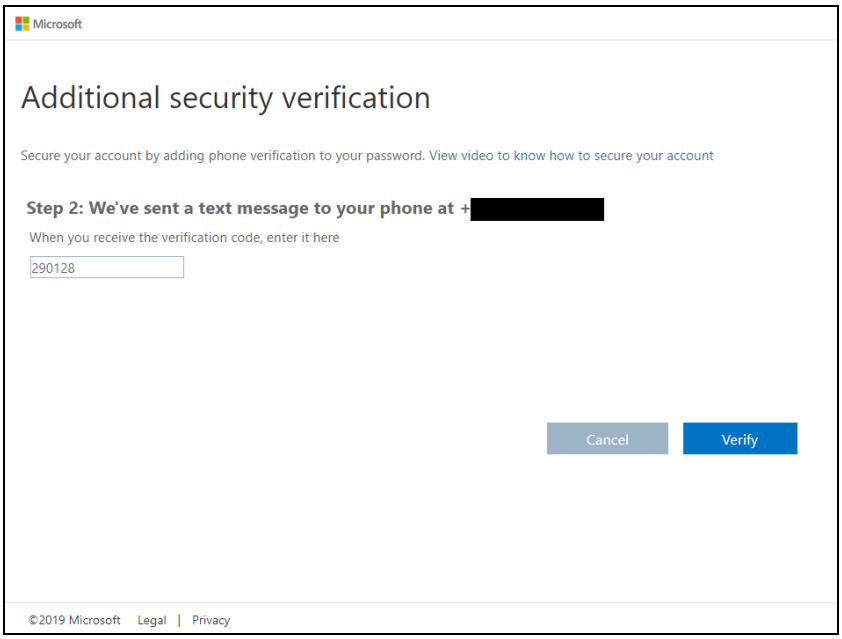
- Office phone – This option is disabled. Please ask your administrator if you need to update your office phone number.

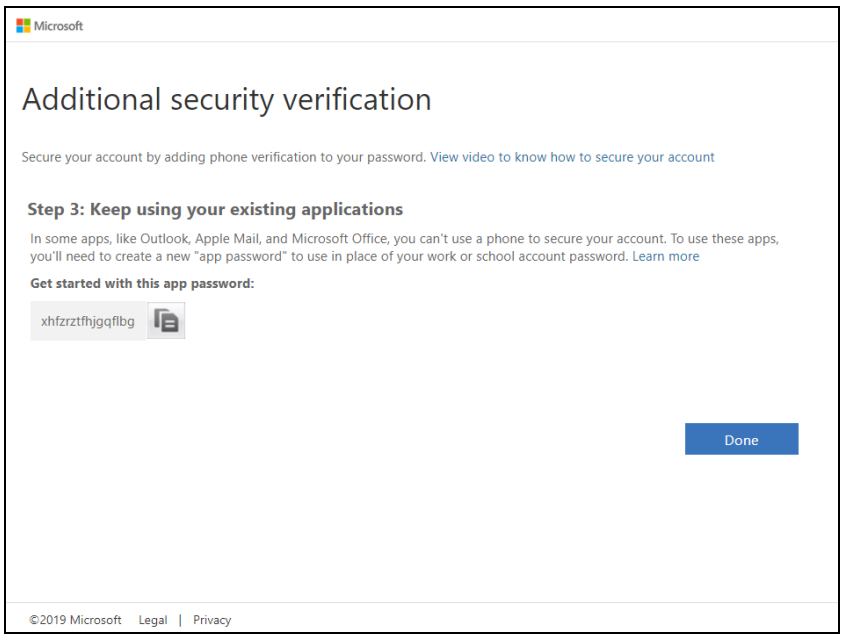


- Mobile app
  - Select which option you like upon using the mobile app
    - Receive notifications for verification
    - Use verification code

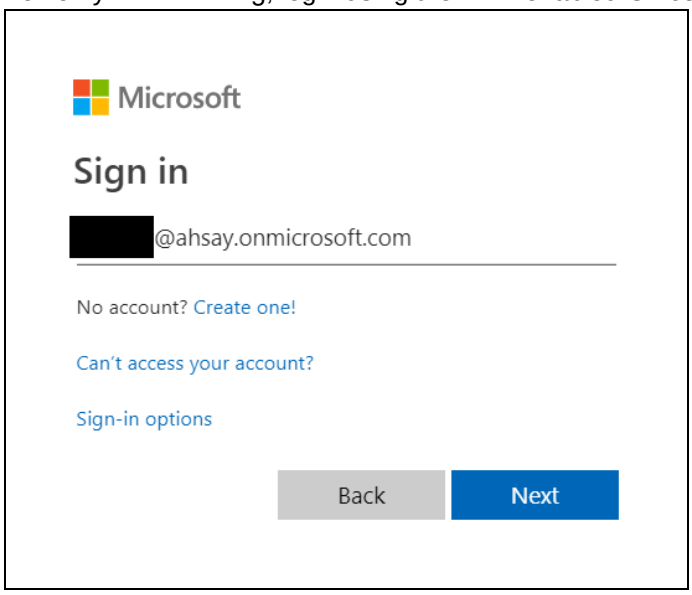
14. If you have selected the first option which is the **Authentication phone** with a method of **Send me a code by text,** you will receive a text message containing the verification code. Ensure that you have indicated a valid mobile number.



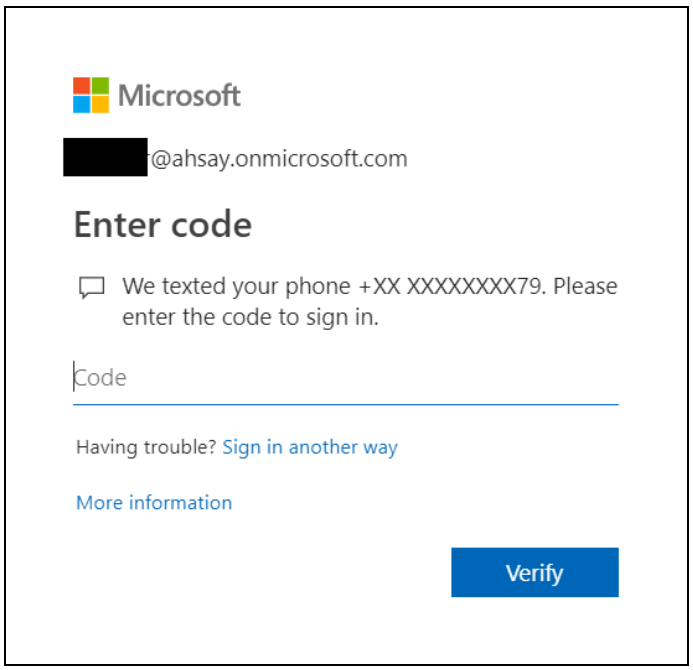


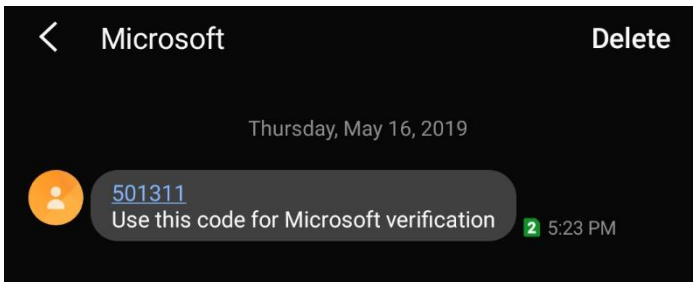


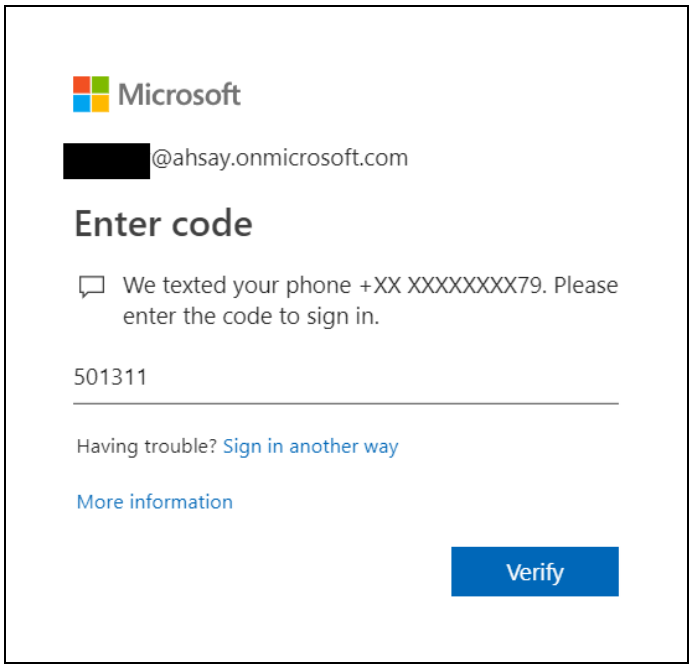
15. To verify if it's working, login using the MFA enabled Office 365 user account.



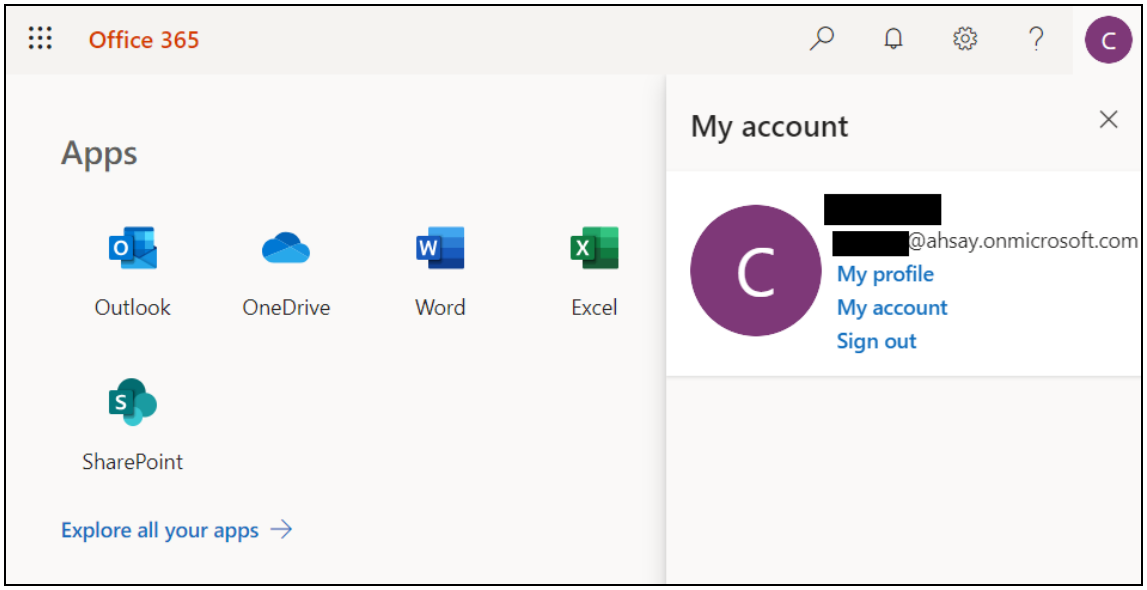
16. Upon logging in, there will be a message that will require you to provide the code that have been sent to your personal mobile number. Click **Verify** to proceed.


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.

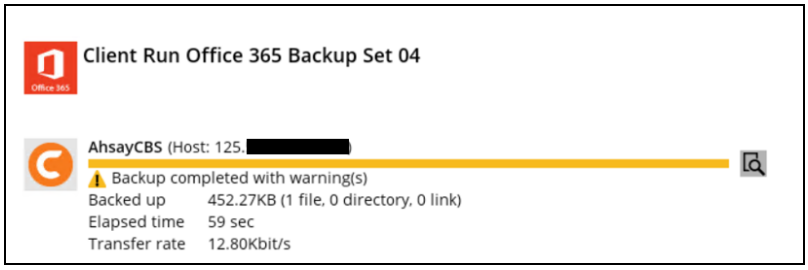


Appendix E: Example Scenario for Backup Set Maintenance

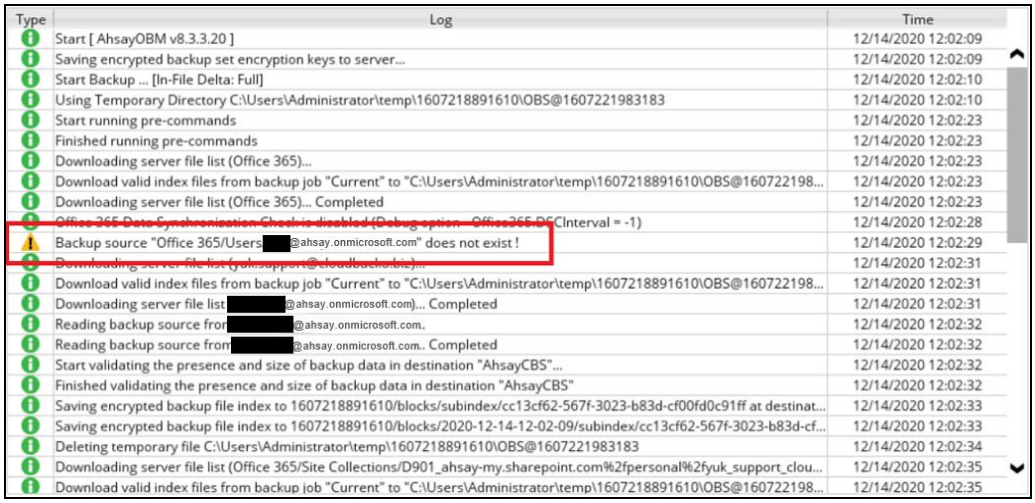
Scenario: Office 365 user account does not exist warning message

This is the sample warning message if the user does not exist. If a user is removed from the domain and the Admin did not manually unselected the user from the backup source, then during backup job there will be a warning that the user does not exist. The warning will appear on the backup log.

Backup job is completed with warning(s). Check the backup log for the warning message.



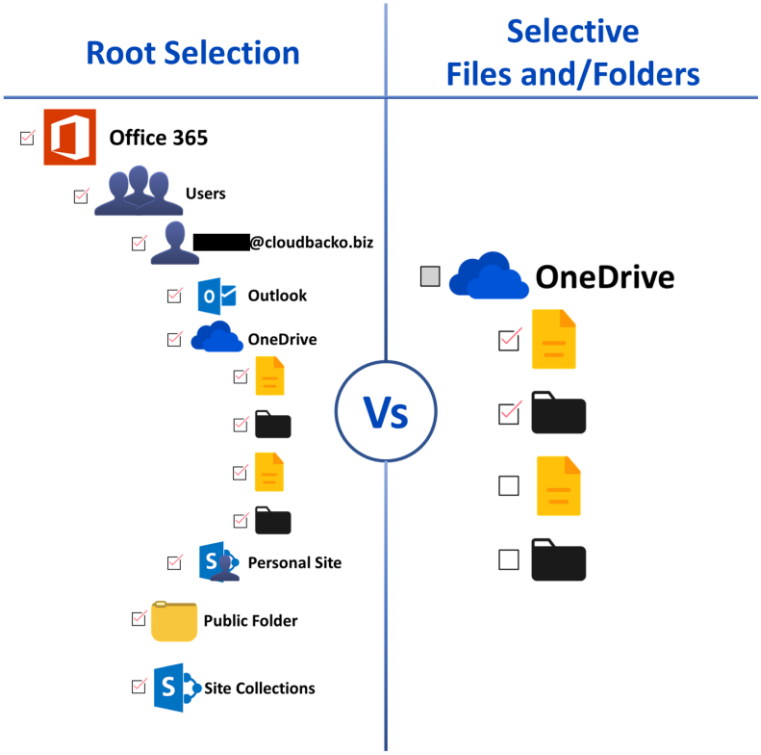
Backup log contains a warning message.



Type	Log	Time
	Start [AhsayOBM v8.3.3.20]	12/14/2020 12:02:09
	Saving encrypted backup set encryption keys to server...	12/14/2020 12:02:09
	Start Backup ... [In-File Delta: Full]	12/14/2020 12:02:10
	Using Temporary Directory C:\Users\Administrator\temp\1607218891610\OBS@1607221983183	12/14/2020 12:02:10
	Start running pre-commands	12/14/2020 12:02:23
	Finished running pre-commands	12/14/2020 12:02:23
	Downloading server file list (Office 365)...	12/14/2020 12:02:23
	Download valid index files from backup job "Current" to "C:\Users\Administrator\temp\1607218891610\OBS@160722198...	12/14/2020 12:02:23
	Downloading server file list (Office 365)... Completed	12/14/2020 12:02:23
	Office 365 Data Synchronization Check is disabled (Debug option - Office365DSCInterval = -1)	12/14/2020 12:02:28
	Backup source "Office 365/Users[redacted]@ahsay.onmicrosoft.com" does not exist !	12/14/2020 12:02:29
	[redacted]	12/14/2020 12:02:31
	Download valid index files from backup job "Current" to "C:\Users\Administrator\temp\1607218891610\OBS@160722198...	12/14/2020 12:02:31
	Downloading server file list [redacted]@ahsay.onmicrosoft.com)... Completed	12/14/2020 12:02:31
	Reading backup source fro[redacted]@ahsay.onmicrosoft.com.	12/14/2020 12:02:32
	Reading backup source fro[redacted]@ahsay.onmicrosoft.com.. Completed	12/14/2020 12:02:32
	Start validating the presence and size of backup data in destination "AhsayCBS"...	12/14/2020 12:02:32
	Finished validating the presence and size of backup data in destination "AhsayCBS"	12/14/2020 12:02:32
	Saving encrypted backup file index to 1607218891610/blocks/subindex/cc13cf62-567f-3023-b83d-cf00fd0c91ff at destinat...	12/14/2020 12:02:33
	Saving encrypted backup file index to 1607218891610/blocks/2020-12-14-12-02-09/subindex/cc13cf62-567f-3023-b83d-cf...	12/14/2020 12:02:33
	Deleting temporary file C:\Users\Administrator\temp\1607218891610\OBS@1607221983183	12/14/2020 12:02:34
	Downloading server file list (Office 365/Site Collections/D901_ahsay-my.sharepoint.com%2fpersonal%2fyuk_support_clou...	12/14/2020 12:02:35
	Download valid index files from backup job "Current" to "C:\Users\Administrator\temp\1607218891610\OBS@160722198...	12/14/2020 12:02:35

Appendix F: Example Scenario for Data Synchronization Check (DSC) with sample backup logs

Selection of root folder vs Selective files and/folders

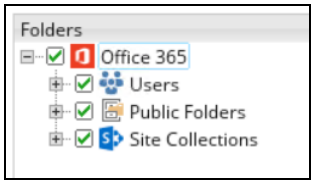


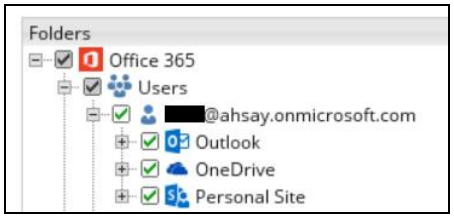
Root Selection

Selecting the root folder automatically selects all the files and/or folders under all Office 365 user accounts including the Public Folder and Site Collections. 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.





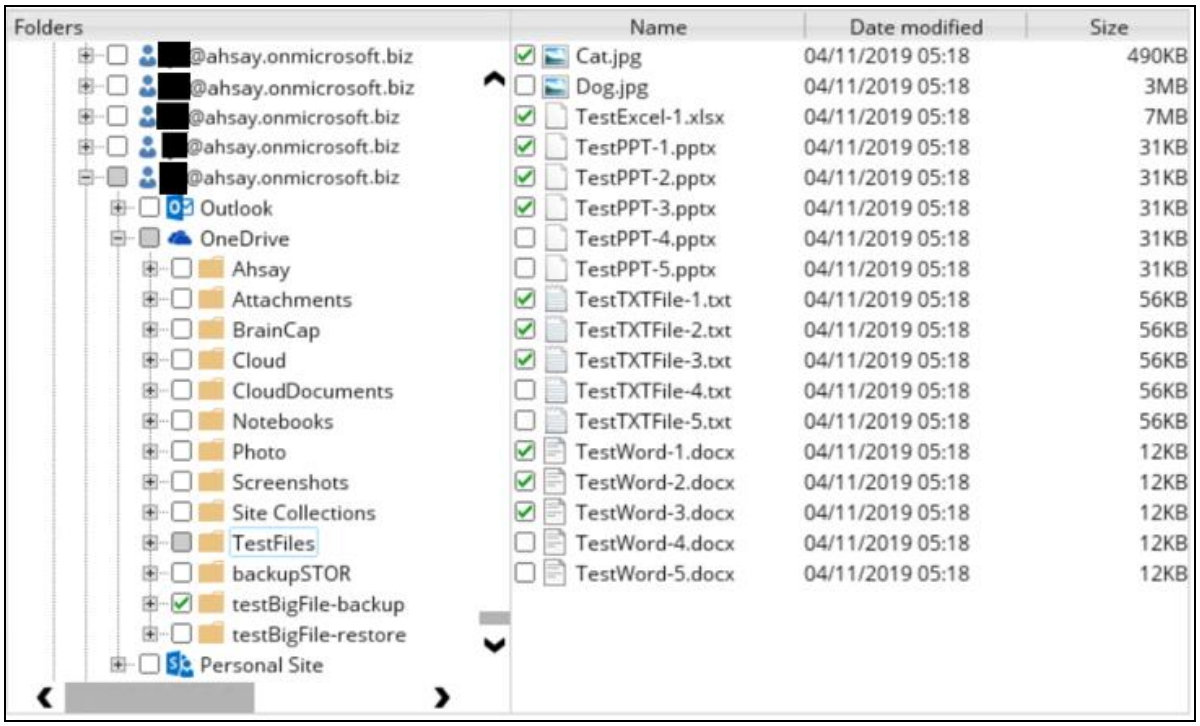
Selective Files and/or Folders

When the root folder is not selected, and the files and/or folders are selected individually. If the files and/or folders are subsequently un-selected from the backup source. The backup job will not pick up the changes of the de-selected files and/or folders, they will not be moved the retention area but remain in the data area. In the long run this could result in a build-up of data in the backup destinations(s).

On the comparison image above, the “OneDrive” checkbox is greyed out because there is 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).

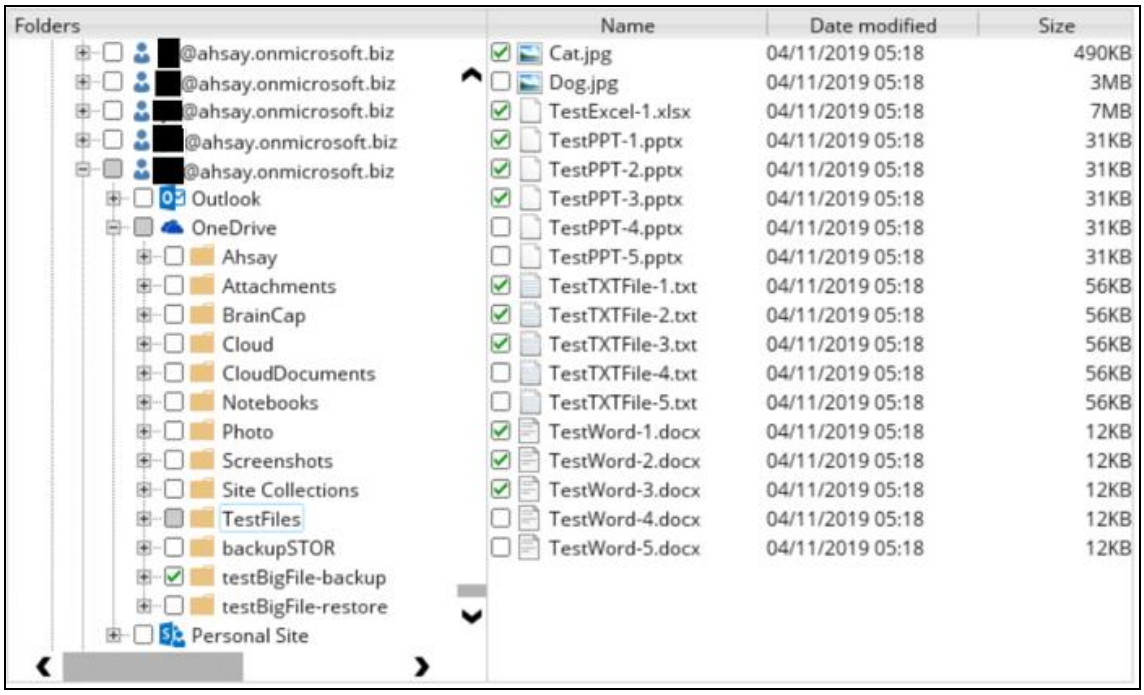
Below is the sample screenshot of the backup source with selective files and/or folders.



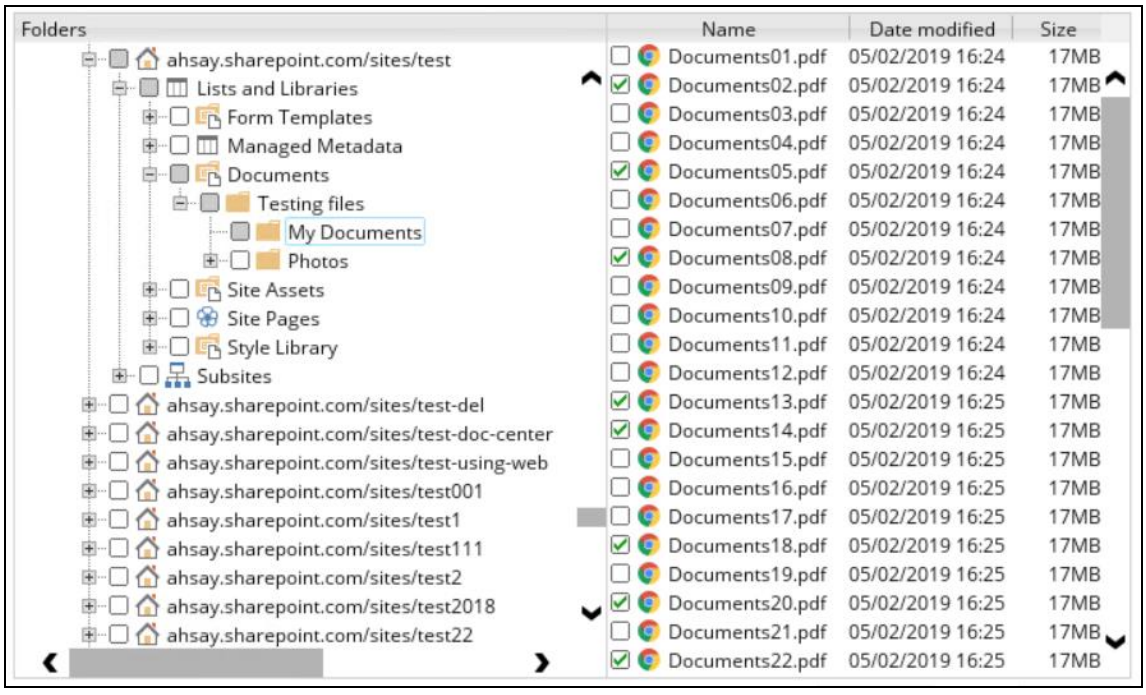
Only selected files and/or folders are selected in OneDrive. Also, the Office 365 user account is greyed out as this indicates that not all items are selected.

NOTE: Selective Files and/or Folders only applies to files and/or folders under Outlook, OneDrive, Personal Site, Public Folders, and Site Collections. This is **NOT** applicable for User Level.

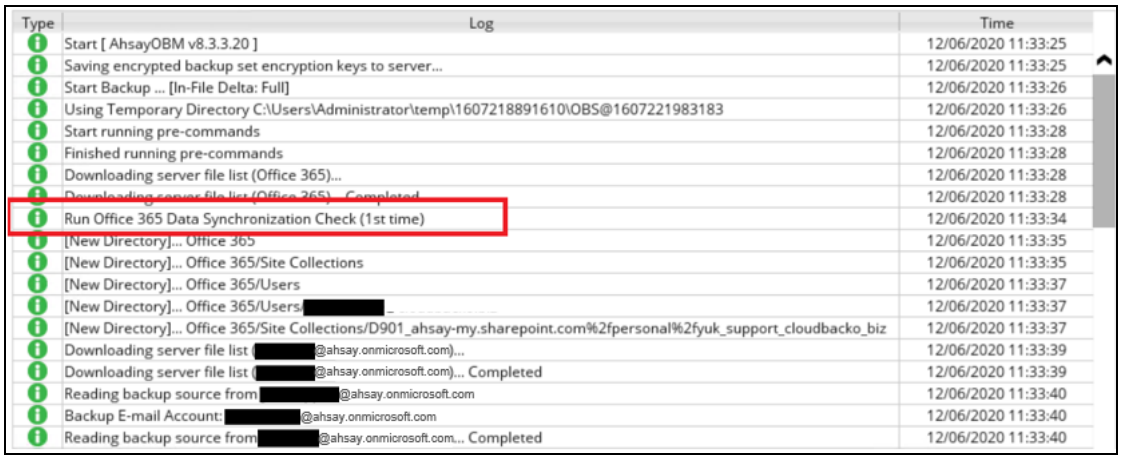
This is an example of selective files and/folders from OneDrive.



This is an example of selective files and/folders from Site Collections.

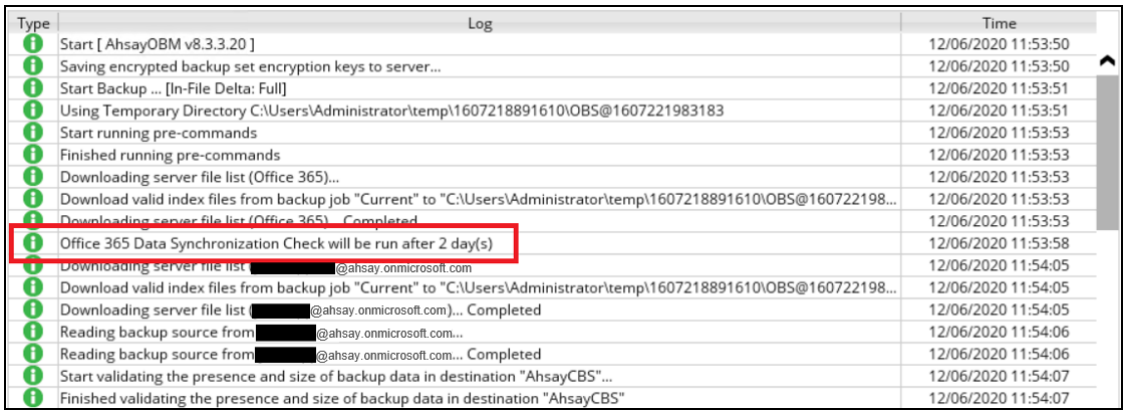


On the sample backup log, it shows that data synchronization check is enabled and runs for the first time.



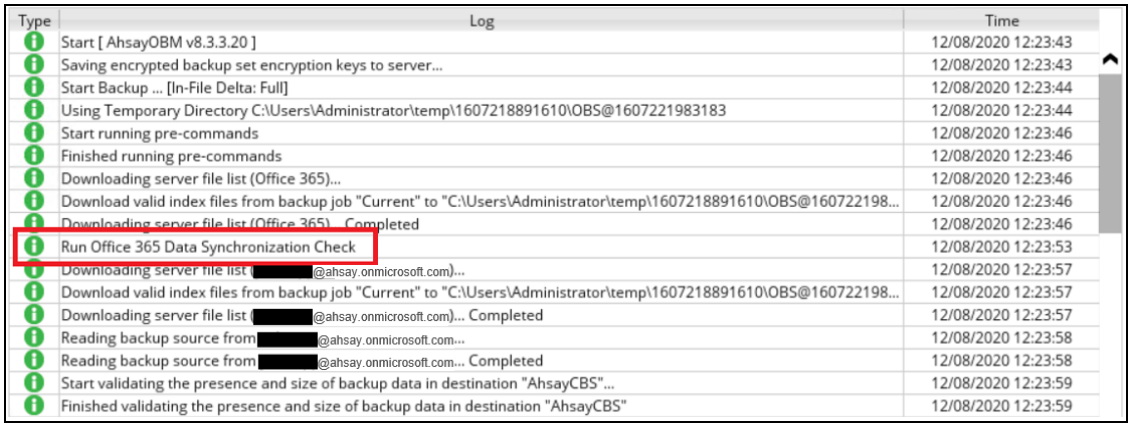
Type	Log	Time
	Start [AhsayOBM v8.3.3.20]	12/06/2020 11:33:25
	Saving encrypted backup set encryption keys to server...	12/06/2020 11:33:25
	Start Backup ... [In-File Delta: Full]	12/06/2020 11:33:26
	Using Temporary Directory C:\Users\Administrator\temp\1607218891610\OBS@1607221983183	12/06/2020 11:33:26
	Start running pre-commands	12/06/2020 11:33:28
	Finished running pre-commands	12/06/2020 11:33:28
	Downloading server file list (Office 365)...	12/06/2020 11:33:28
	Downloading server file list (Office 365)... Completed	12/06/2020 11:33:28
	Run Office 365 Data Synchronization Check (1st time)	12/06/2020 11:33:34
	[New Directory]... Office 365	12/06/2020 11:33:35
	[New Directory]... Office 365/Site Collections	12/06/2020 11:33:35
	[New Directory]... Office 365/Users	12/06/2020 11:33:37
	[New Directory]... Office 365/Users/[redacted]	12/06/2020 11:33:37
	[New Directory]... Office 365/Site Collections/D901_ahsay-my.sharepoint.com%2fpersonal%2fyuk_support_cloudbacko_biz	12/06/2020 11:33:37
	Downloading server file list ([redacted]@ahsay.onmicrosoft.com)...	12/06/2020 11:33:39
	Downloading server file list ([redacted]@ahsay.onmicrosoft.com)... Completed	12/06/2020 11:33:39
	Reading backup source from [redacted]@ahsay.onmicrosoft.com	12/06/2020 11:33:40
	Backup E-mail Account: [redacted]@ahsay.onmicrosoft.com	12/06/2020 11:33:40
	Reading backup source from [redacted]@ahsay.onmicrosoft.com... Completed	12/06/2020 11:33:40

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.



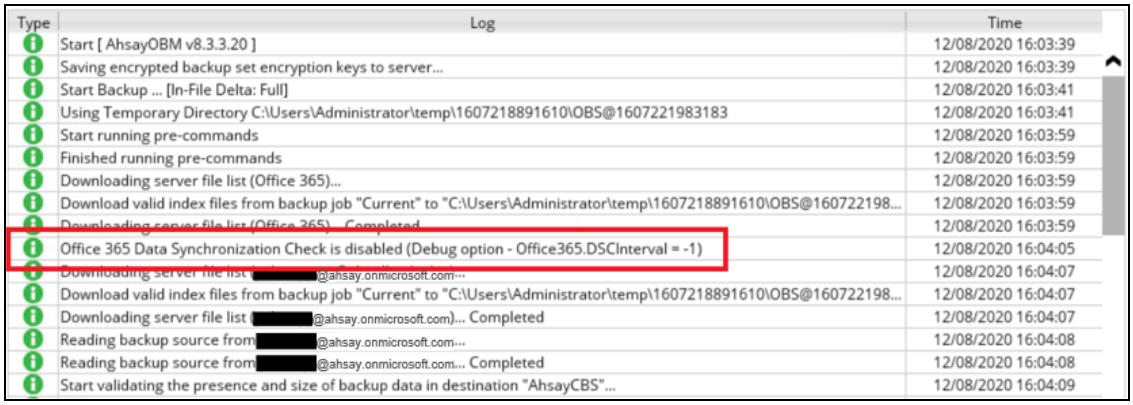
Type	Log	Time
	Start [AhsayOBM v8.3.3.20]	12/06/2020 11:53:50
	Saving encrypted backup set encryption keys to server...	12/06/2020 11:53:50
	Start Backup ... [In-File Delta: Full]	12/06/2020 11:53:51
	Using Temporary Directory C:\Users\Administrator\temp\1607218891610\OBS@1607221983183	12/06/2020 11:53:51
	Start running pre-commands	12/06/2020 11:53:53
	Finished running pre-commands	12/06/2020 11:53:53
	Downloading server file list (Office 365)...	12/06/2020 11:53:53
	Download valid index files from backup job "Current" to "C:\Users\Administrator\temp\1607218891610\OBS@160722198...	12/06/2020 11:53:53
	Downloading server file list (Office 365)... Completed	12/06/2020 11:53:53
	Office 365 Data Synchronization Check will be run after 2 day(s)	12/06/2020 11:53:58
	Downloading server file list ([redacted]@ahsay.onmicrosoft.com	12/06/2020 11:54:05
	Download valid index files from backup job "Current" to "C:\Users\Administrator\temp\1607218891610\OBS@160722198...	12/06/2020 11:54:05
	Downloading server file list ([redacted]@ahsay.onmicrosoft.com)... Completed	12/06/2020 11:54:05
	Reading backup source from [redacted]@ahsay.onmicrosoft.com...	12/06/2020 11:54:06
	Reading backup source from [redacted]@ahsay.onmicrosoft.com... Completed	12/06/2020 11:54:06
	Start validating the presence and size of backup data in destination "AhsayCBS"...	12/06/2020 11:54:07
	Finished validating the presence and size of backup data in destination "AhsayCBS"	12/06/2020 11:54:07

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



Type	Log	Time
	Start [AhsayOBM v8.3.3.20]	12/08/2020 12:23:43
	Saving encrypted backup set encryption keys to server...	12/08/2020 12:23:43
	Start Backup ... [In-File Delta: Full]	12/08/2020 12:23:44
	Using Temporary Directory C:\Users\Administrator\temp\1607218891610\OBS@1607221983183	12/08/2020 12:23:44
	Start running pre-commands	12/08/2020 12:23:46
	Finished running pre-commands	12/08/2020 12:23:46
	Downloading server file list (Office 365)...	12/08/2020 12:23:46
	Download valid index files from backup job "Current" to "C:\Users\Administrator\temp\1607218891610\OBS@160722198...	12/08/2020 12:23:46
	Downloading server file list (Office 365)... Completed	12/08/2020 12:23:46
	Run Office 365 Data Synchronization Check	12/08/2020 12:23:53
	Downloading server file list ([redacted]@ahsay.onmicrosoft.com)...	12/08/2020 12:23:57
	Download valid index files from backup job "Current" to "C:\Users\Administrator\temp\1607218891610\OBS@160722198...	12/08/2020 12:23:57
	Downloading server file list ([redacted]@ahsay.onmicrosoft.com)... Completed	12/08/2020 12:23:57
	Reading backup source from [redacted]@ahsay.onmicrosoft.com...	12/08/2020 12:23:58
	Reading backup source from [redacted]@ahsay.onmicrosoft.com... Completed	12/08/2020 12:23:58
	Start validating the presence and size of backup data in destination "AhsayCBS"...	12/08/2020 12:23:59
	Finished validating the presence and size of backup data in destination "AhsayCBS"	12/08/2020 12:23:59

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



Type	Log	Time
ⓘ	Start [AhsayOBM v8.3.3.20]	12/08/2020 16:03:39
ⓘ	Saving encrypted backup set encryption keys to server...	12/08/2020 16:03:39
ⓘ	Start Backup ... [In-File Delta: Full]	12/08/2020 16:03:41
ⓘ	Using Temporary Directory C:\Users\Administrator\temp\1607218891610\OBS@1607221983183	12/08/2020 16:03:41
ⓘ	Start running pre-commands	12/08/2020 16:03:59
ⓘ	Finished running pre-commands	12/08/2020 16:03:59
ⓘ	Downloading server file list (Office 365)...	12/08/2020 16:03:59
ⓘ	Download valid index files from backup job "Current" to "C:\Users\Administrator\temp\1607218891610\OBS@160722198...	12/08/2020 16:03:59
ⓘ	Downloading server file list (Office 365)... Completed	12/08/2020 16:03:59
ⓘ	Office 365 Data Synchronization Check is disabled (Debug option - Office365.DSCInterval = -1)	12/08/2020 16:04:05
ⓘ	Downloading server file list [redacted]@ahsay.onmicrosoft.com...	12/08/2020 16:04:07
ⓘ	Download valid index files from backup job "Current" to "C:\Users\Administrator\temp\1607218891610\OBS@160722198...	12/08/2020 16:04:07
ⓘ	Downloading server file list [redacted]@ahsay.onmicrosoft.com)... Completed	12/08/2020 16:04:07
ⓘ	Reading backup source from [redacted]@ahsay.onmicrosoft.com...	12/08/2020 16:04:08
ⓘ	Reading backup source from [redacted]@ahsay.onmicrosoft.com... Completed	12/08/2020 16:04:08
ⓘ	Start validating the presence and size of backup data in destination "AhsayCBS"...	12/08/2020 16:04:09

Appendix G: Setting the Data Synchronization Check (DSC)

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

Assumption: AhsayOBM Installation path is **C:\Program Files\AhsayOBM**

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

1. Make sure there are no active backup or restore job running.
2. Close AhsayOBM UI.
3. Stop the Ahsay Online Backup Manager services
4. Go to C:\Program Files\AhsayOBM\ folder.
5. Open **cb.opt** file using a text editor such as Notepad or Notepad++.
6. Add this line, *Office365.DSCInterval=-1*

   A value of **-1** indicates data synchronization check is disabled.
7. Start the Ahsay Online Backup Manager services

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

1. Go to C:\Program Files\AhsayOBM\ folder.
2. Open **cb.opt** file using a text editor such as Notepad or Notepad++.
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/restore job running.
2. Close AhsayOBM UI.
3. Stop the Ahsay Online Backup Manager services
4. Go to C:\Program Files\AhsayOBM\ folder.
5. Open **cb.opt** file using a text editor such as Notepad or Notepad++.
6. Change the interval number.

   For example:

   Current interval: *Office365.DSCInterval=60*

   Updated interval: *Office365.DSCInterval=10*

   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.
7. Start the Ahsay Online Backup Manager services

Appendix H: Steps on How to Increase the Number of Concurrent Backup Threads

Assumption: AhsayOBM Installation path is **C:\Program Files\AhsayOBM**

To increase the number of concurrent backup threads, follow the instructions below:

1. Make sure there are no active backup or restore job running.
2. Close AhsayOBM UI.
3. Stop the Ahsay Online Backup Manager services
4. Go to C:\Program Files\AhsayOBM\ folder.
5. Open **afc.opt** file using a text editor such as Notepad or Notepad++.
6. Add this parameter,

   obx.core.backup.file.BackupResourceManager.maxConcurrentSubCmd=xx

   A *xx* value indicates the number of threads. Minimum thread is 1.

   NOTE

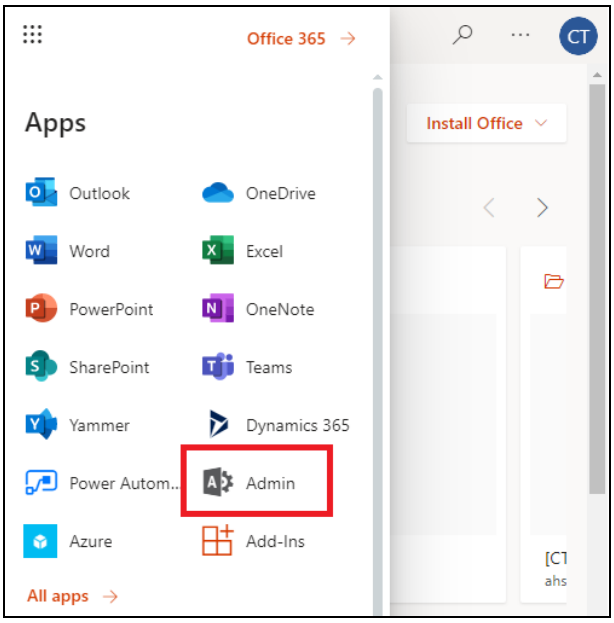
   Increasing the number of concurrent backup threads does not guarantee that the overall backup speed will be faster since there will be an increased chance of throttling by Microsoft Office 365.

7. Start the Ahsay Online Backup Manager services.

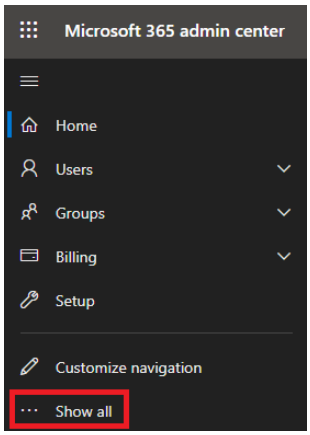
Appendix I: Steps on How to view Item count and Storage used in Microsoft 365 Admin Center

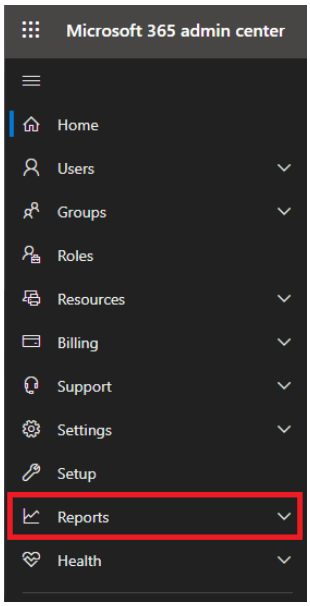
To view the item count and storage size of Office 365 user account based on the usage for Exchange (Outlook), OneDrive, and SharePoint, follow the instructions below:

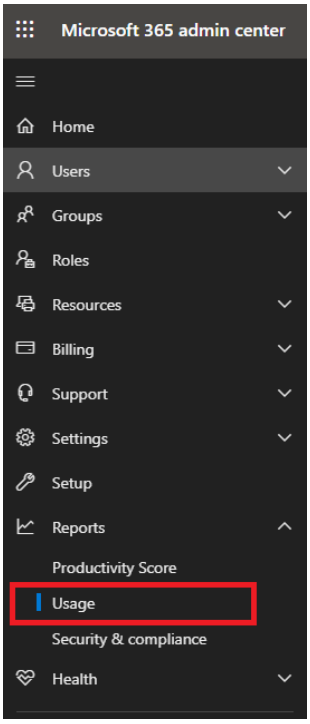
1. Login to the Office 365 (https://login.microsoft.com).
2. Go to Microsoft 365 admin center.



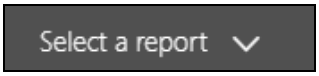
3. On the Microsoft 365 admin center, click **Show all** then click the dropdown arrow for the **Reports** and select **Usage**.

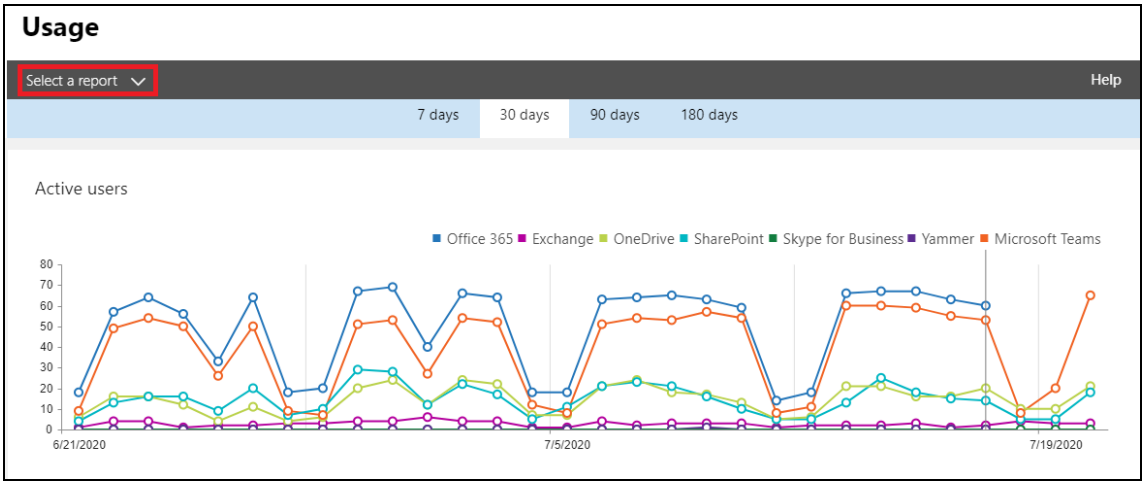


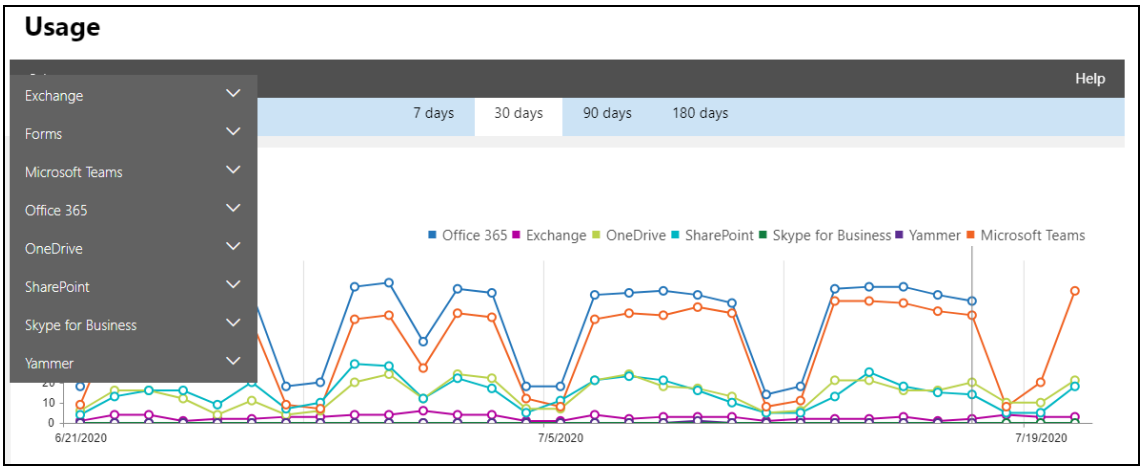




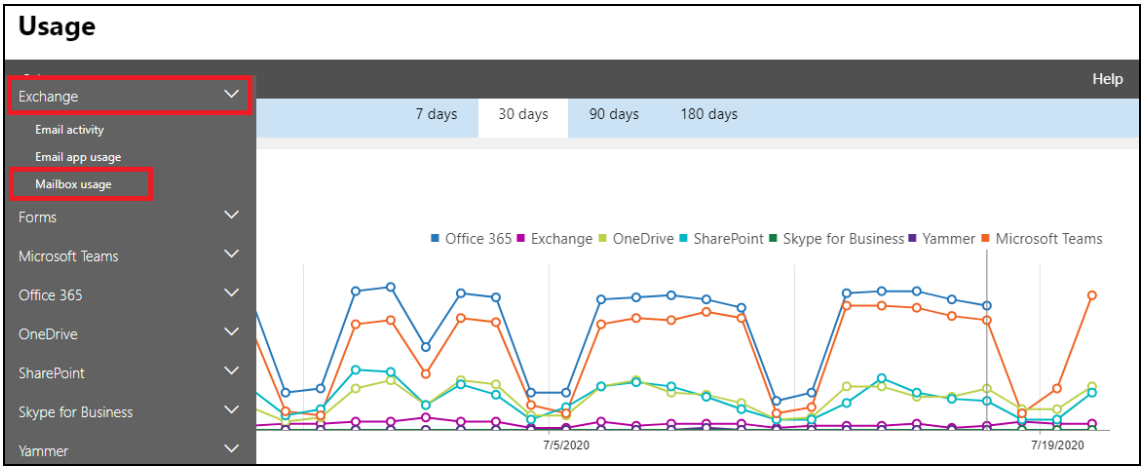
4. On the Usage screen, select a report you want to view.

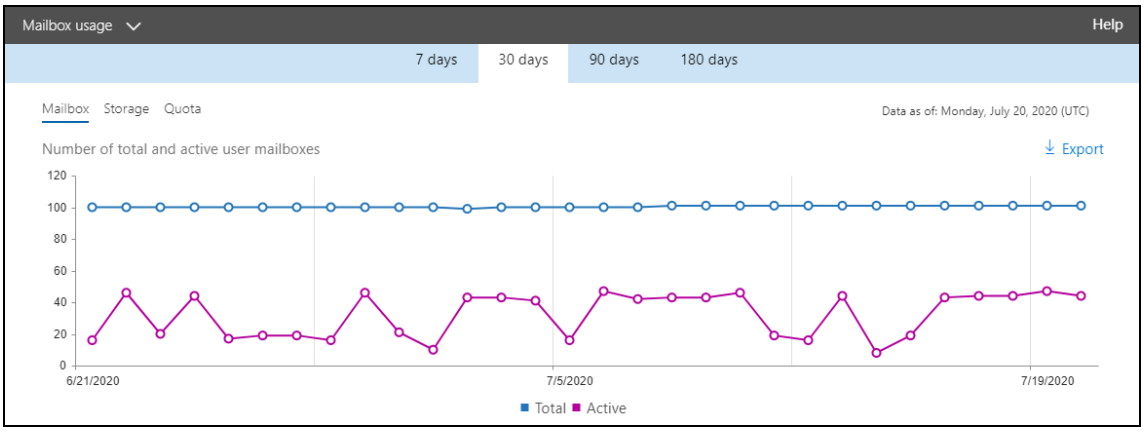






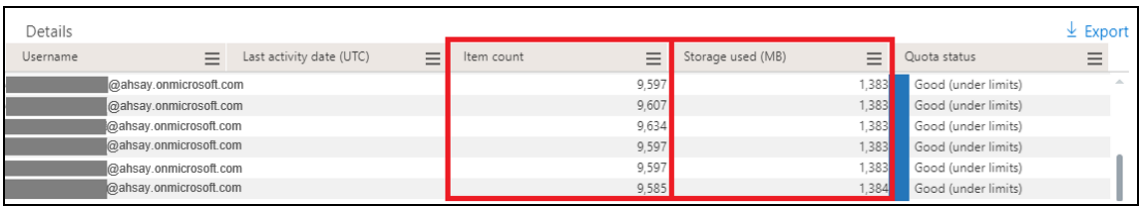
5. For **Exchange**, go to **Mailbox usage**.



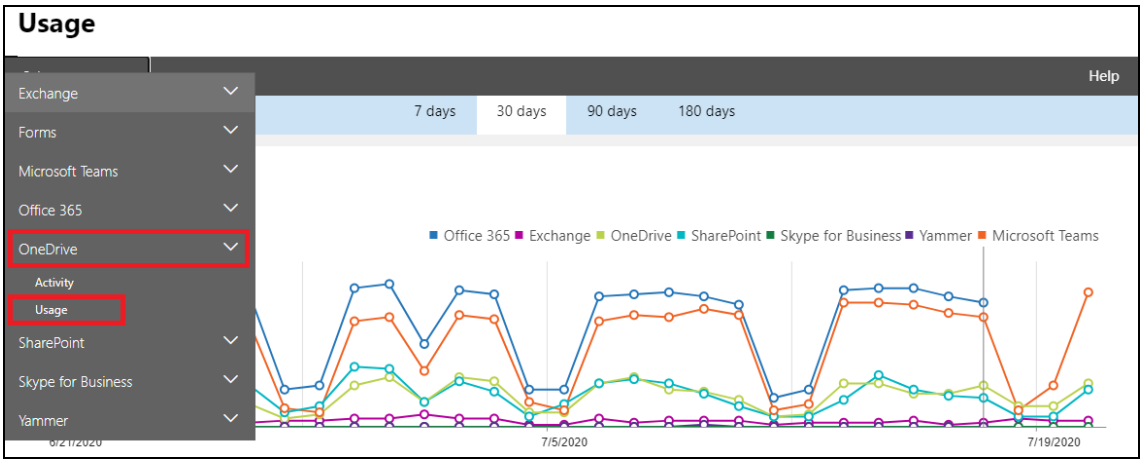


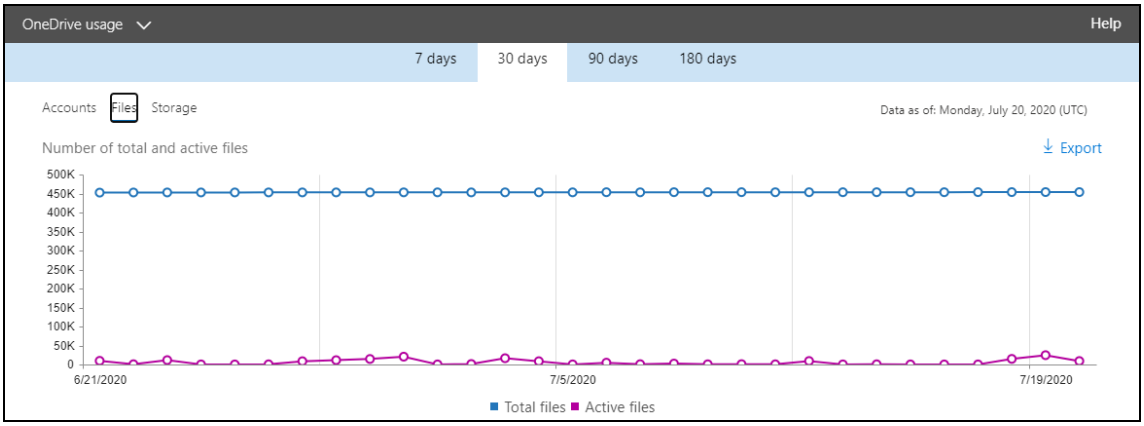
Highlighted columns are, Item count and Storage used (MB).

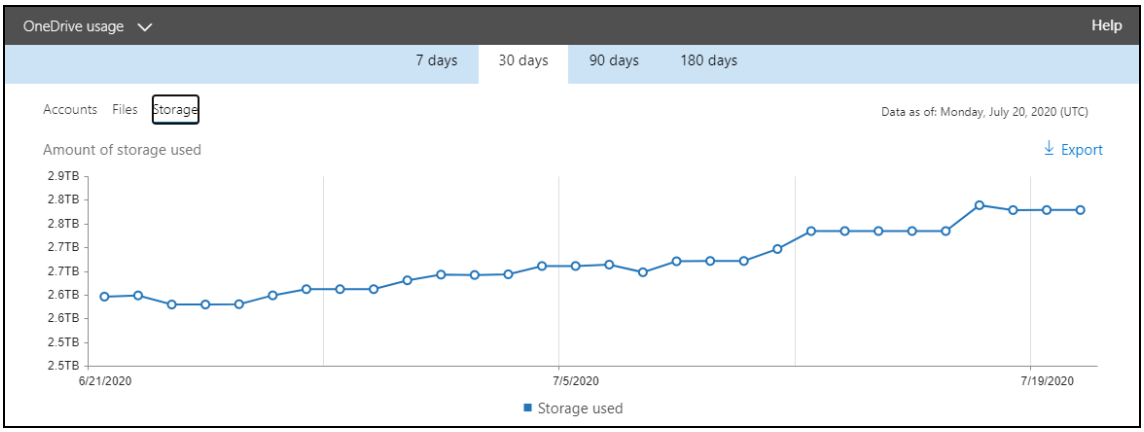
- **Item count** – number of mailbox items in Outlook per Office 365 user account
- **Storage used (MB)** – storage used in MB size per Office 365 user account



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



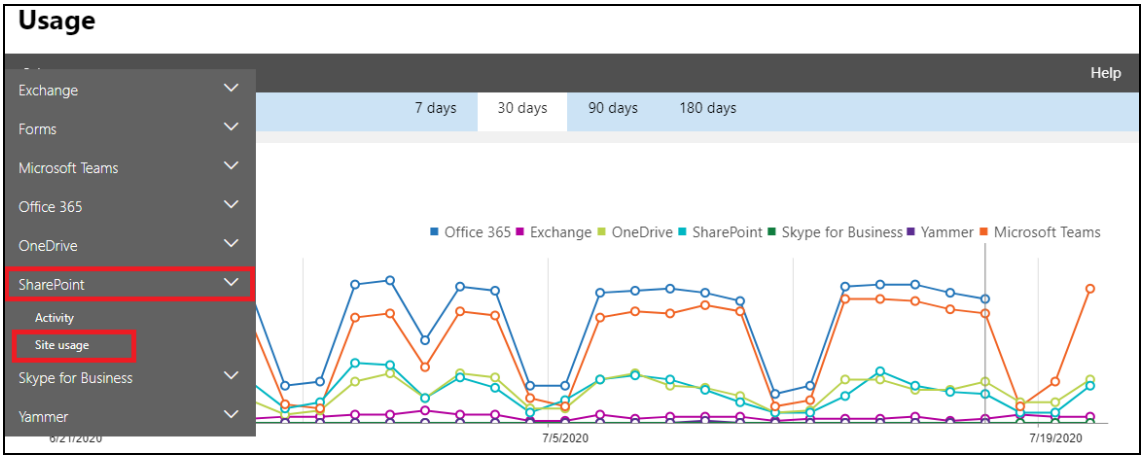


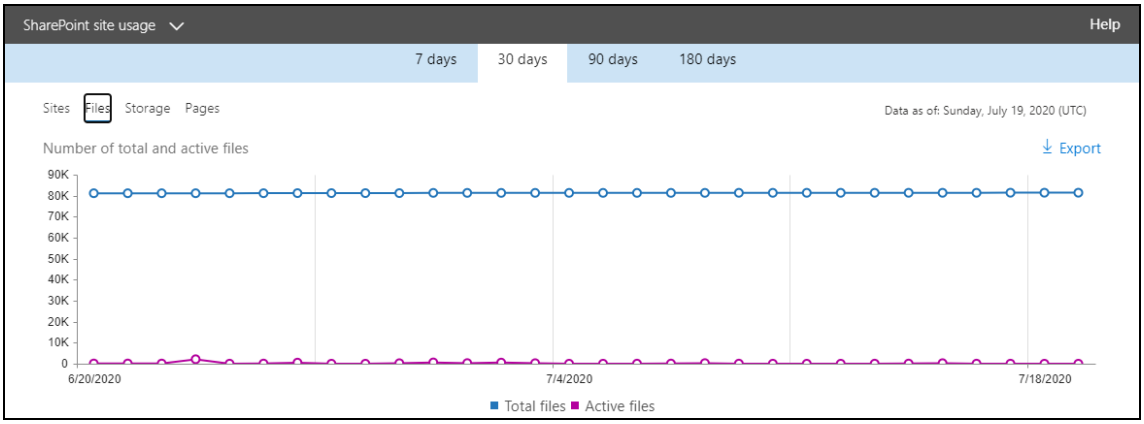


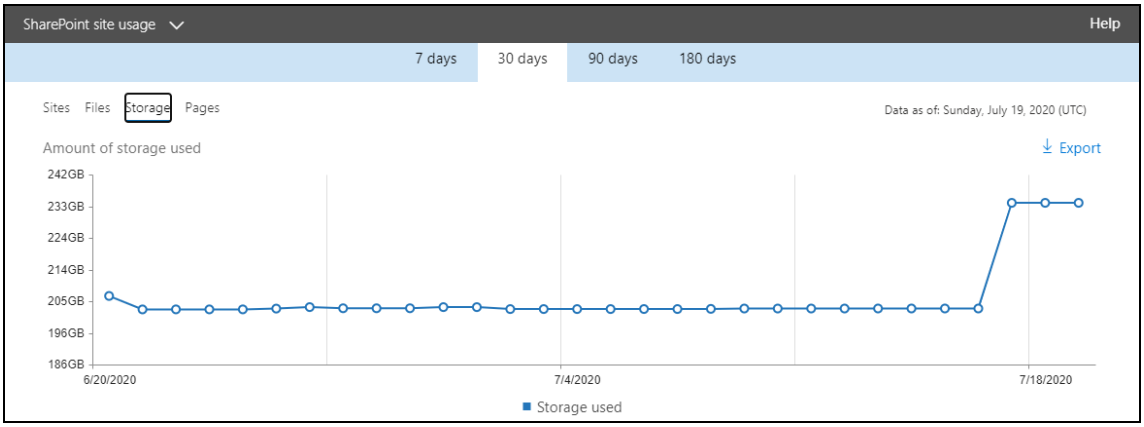
Highlighted columns are, Files and Storage used (MB).

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

7. For **SharePoint**, go to **Site usage.**

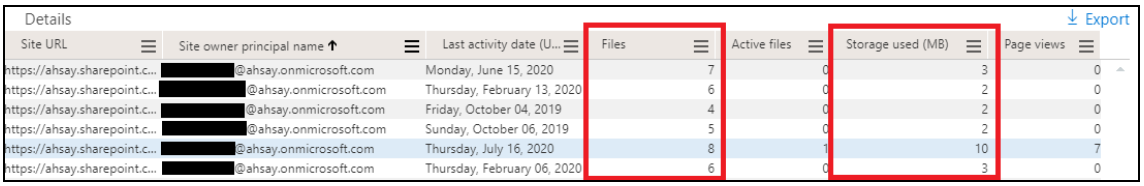






Highlighted columns are, Files and Storage used (MB).

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



Appendix J: Migrating Authentication of Office 365 Backup Set

Starting with AhsayOBM v8.3.6.0 or above, existing backup sets are suggested to 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.

Existing Office 365 backup sets may have been created using an ordinary Office 365 account or an Office 365 account with the Global Admin role. The following are the required Office 365 account that must be used to authorize the migration of authentication of the existing Office 365 backup set:

- When migrating to Hybrid Authentication, any type of Office 365 account may be used to authorize the migration of authentication.
- When migrating to Modern Authentication, if the existing Office 365 backup set was created using an ordinary Office 365 account, an Office 365 account with a Global Admin role 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
  - using an ordinary Office 365 account
  - using an Office 365 account with Global Admin role

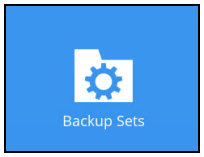
NOTE

Due to the current limitation with Microsoft API, Modern Authentication is currently not suitable for backup sets with Personal Sites and/or SharePoint Sites selected. As a temporary workaround for Office 365 backup sets which require backup of Personal Sites and/or SharePoint Sites selected 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.

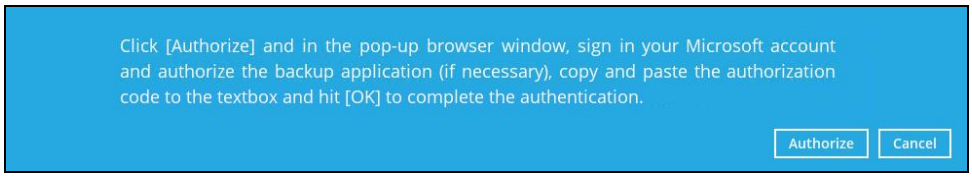
2. In the AhsayOBM main interface, click **Backup Sets**.



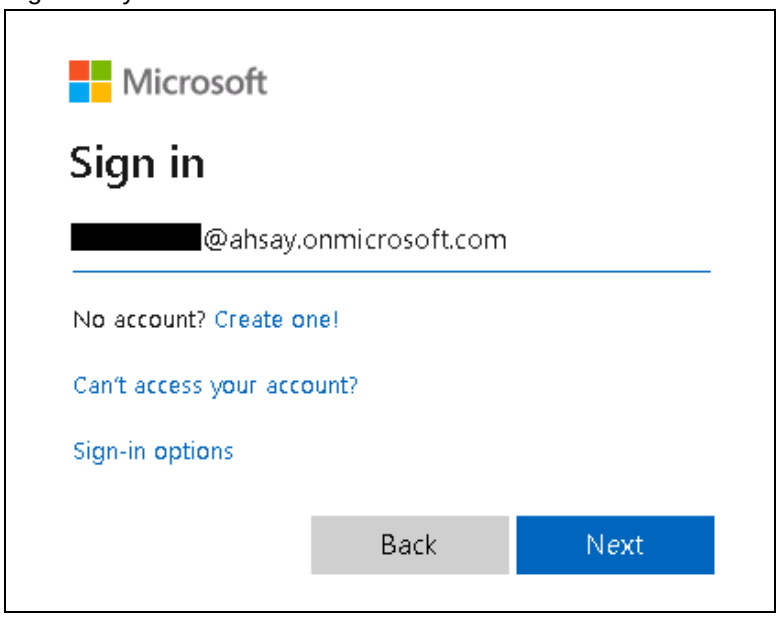
3. Select the backup set that you want to migrate to Hybrid Authentication.

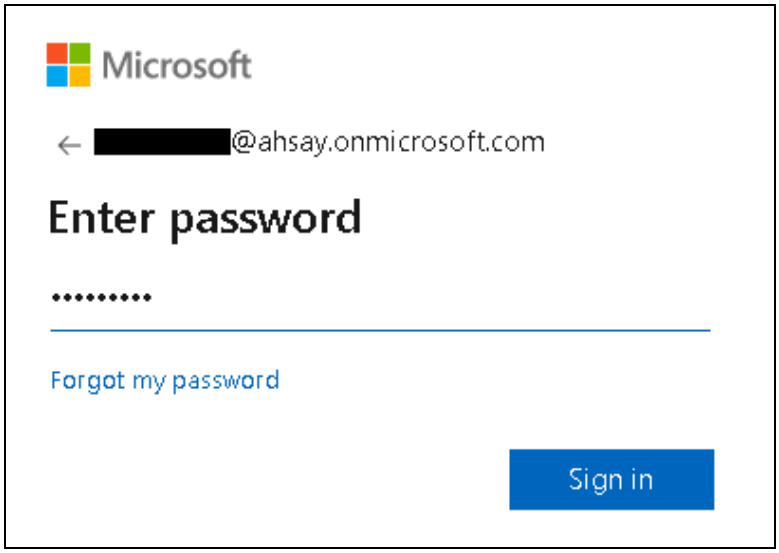
4. Click **Continue**.

5. Click **Authorize**.

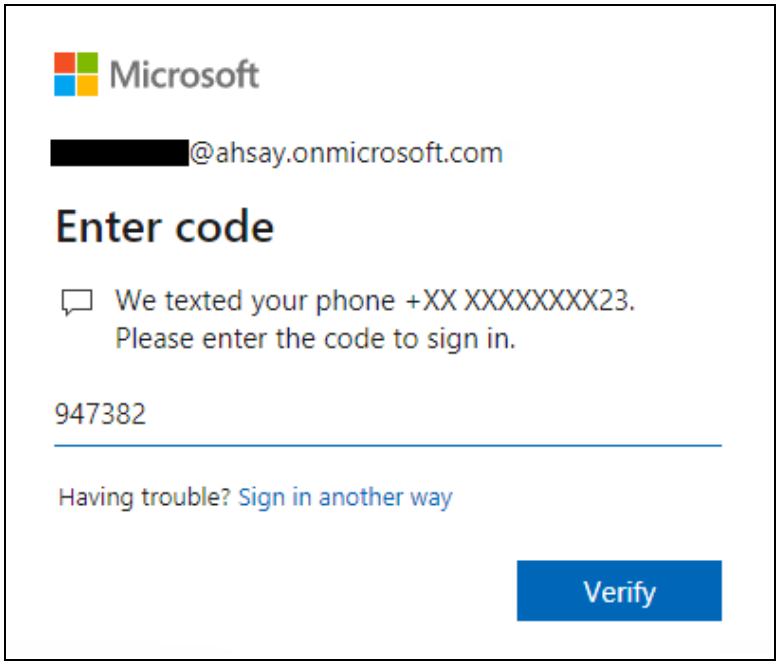


6. Sign in to your account.





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

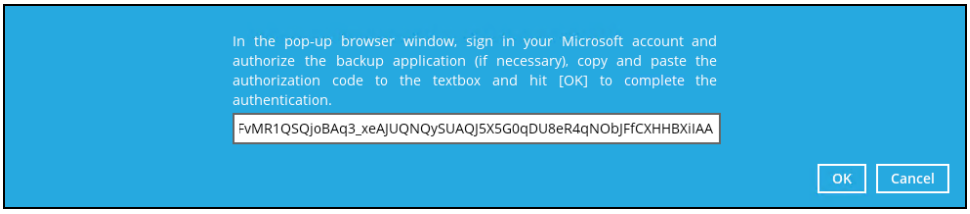


NOTE

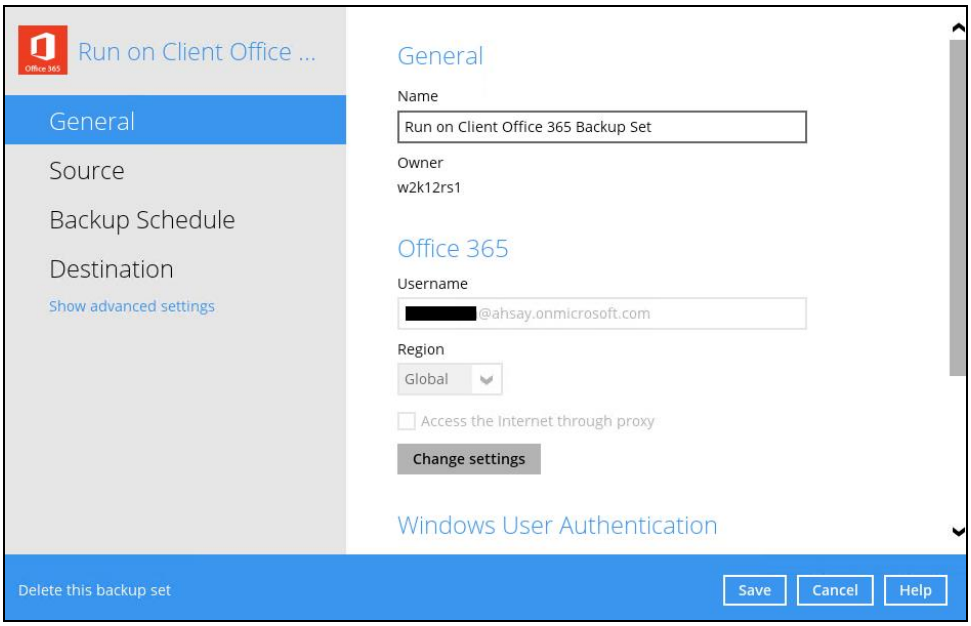
The verification code will only be required if the MFA status of an Office 365 account is enforced.

8. Copy the authorization code.

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



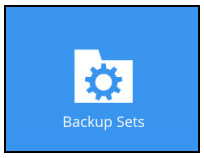
10. Click **Save** to finish the migration.



To migrate a backup set from **Basic Authentication to Modern Authentication using an ordinary Office 365 account**, follow the instructions below:

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

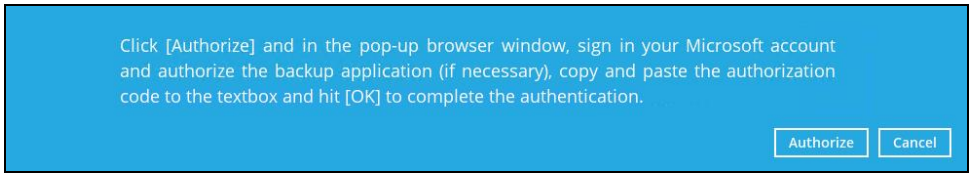
2. In the AhsayOBM main interface, click **Backup Sets**.



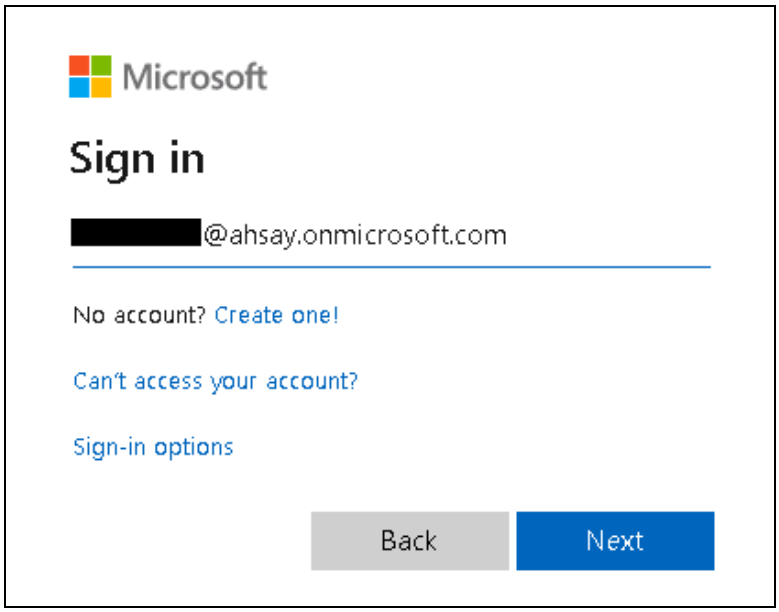
3. Select the backup set that will be migrated.

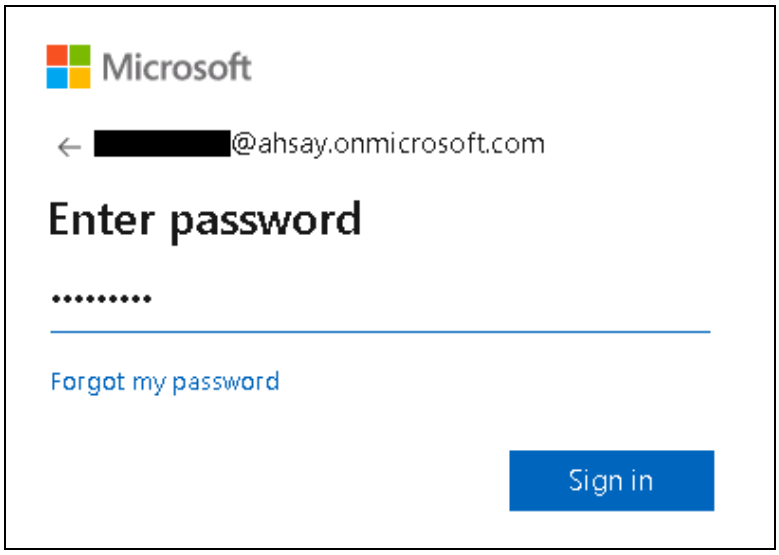
4. Click **Continue**.

5. Click **Authorize**.

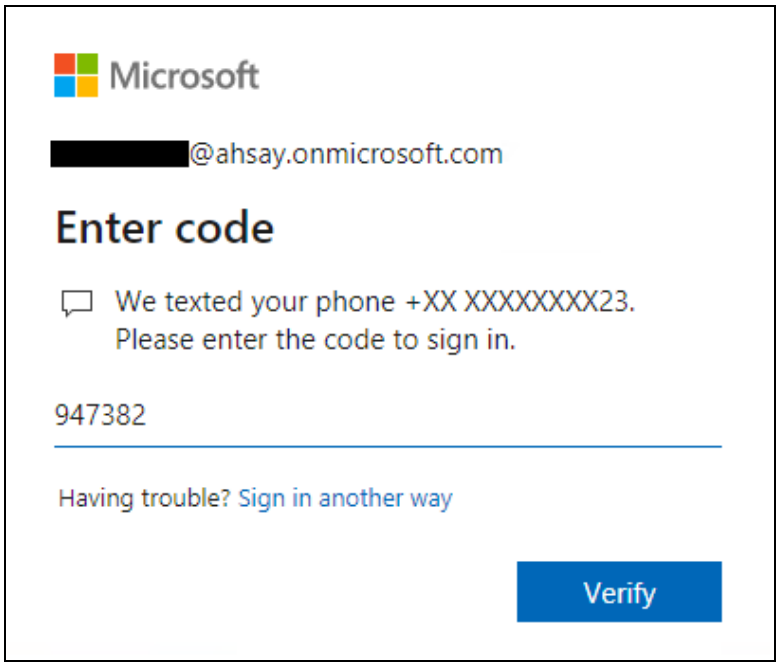


6. Ask your administrator to sign in using an Office 365 account with Global Admin role in order to migrate the backup set.





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

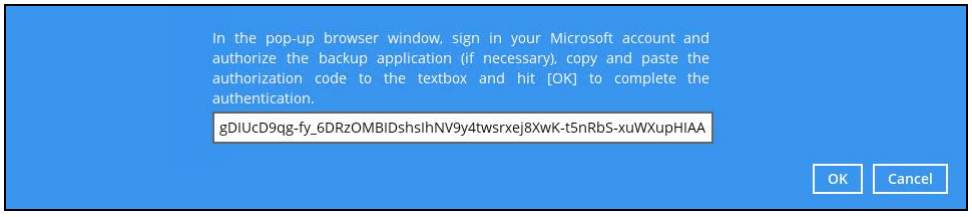


NOTE

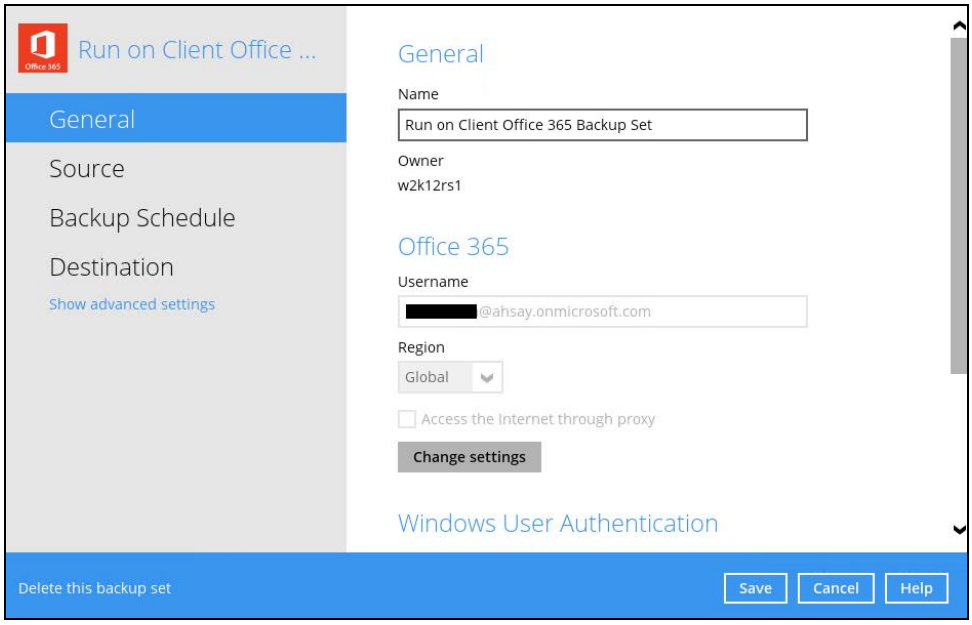
The verification code will only be required if the MFA status of an Office 365 account is enforced.

8. Copy the authorization code.

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



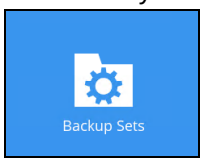
10. Click **Save** to finish the migration.



To migrate a backup set with **Basic Authentication to Modern Authentication using an Office 365 account with a Global Admin role**, follow the steps below:

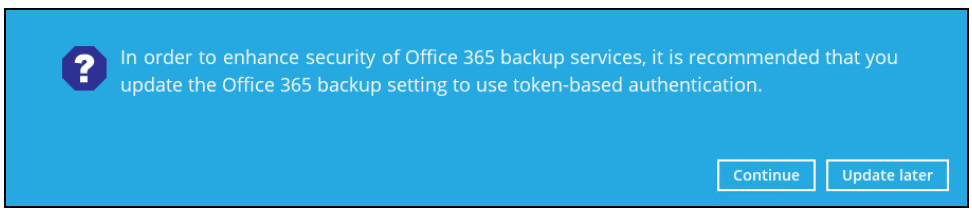
1. Logout all Office 365 account on the default browser before starting the migration of backup set.

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

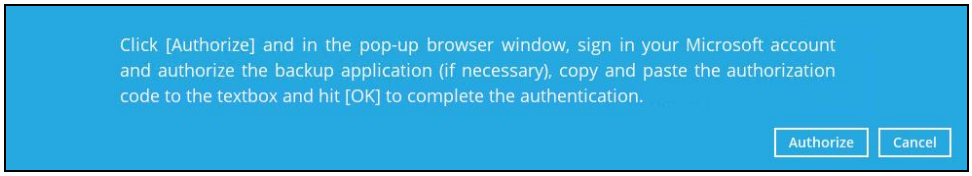


3. Select the backup set that will be migrated.

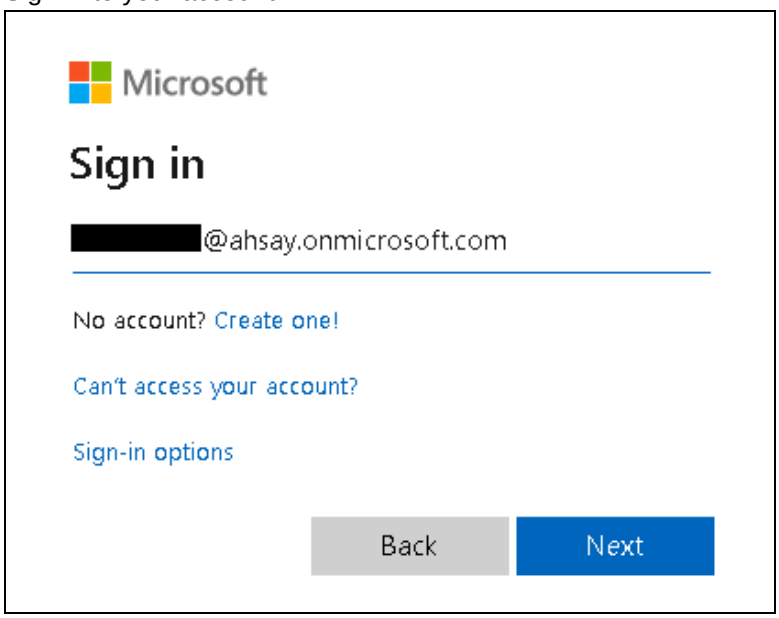
4. Click **Continue**.

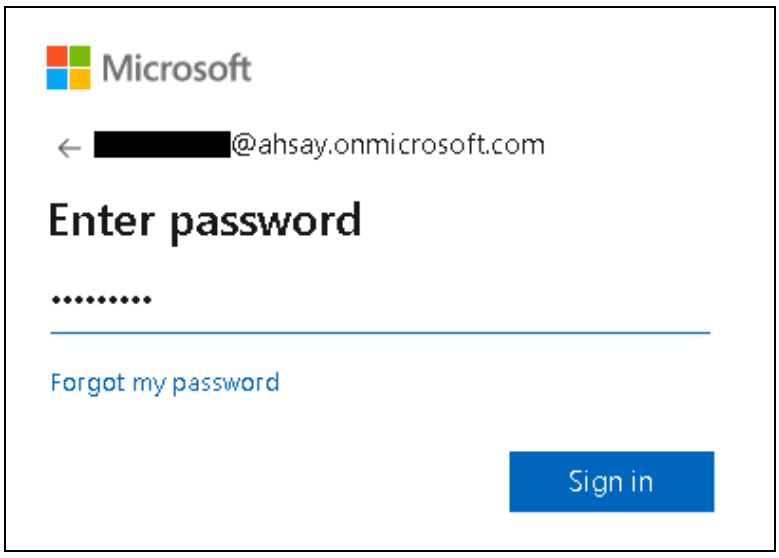


5. Click **Authorize**

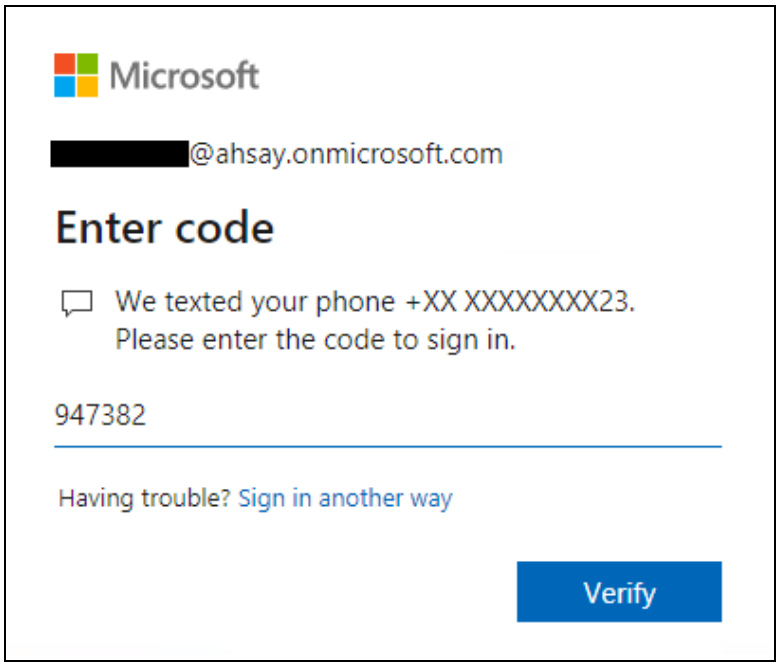


6. Sign in to your account.





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

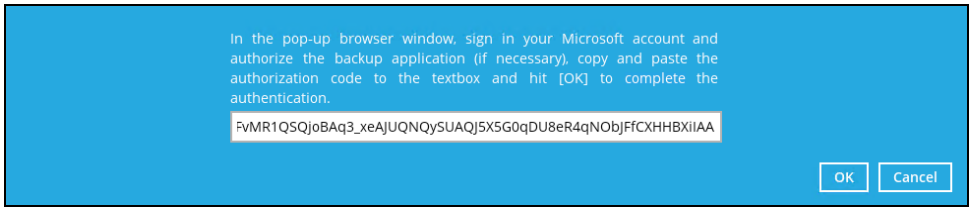


NOTE

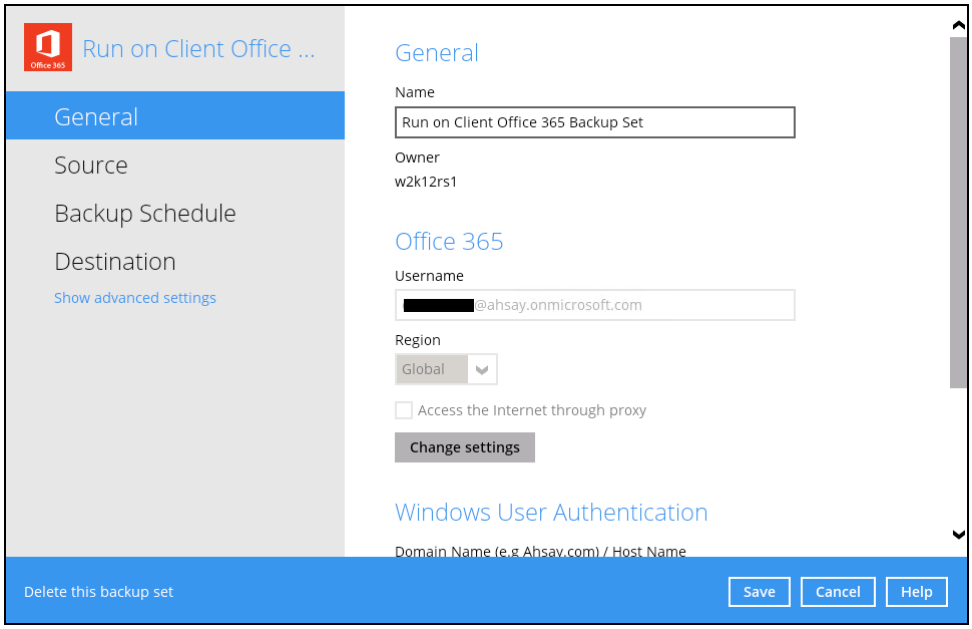
The verification code will only be required if the MFA status of an Office 365 account is enforced.

8. Copy the authorization code.

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



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



Appendix K: Steps on How to Change the Office 365 Authentication

After upgrading to AhsayOBM 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 and/or SharePoint 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 2.18.1 and 2.18.2 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.

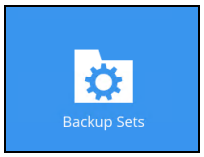
The following are the two (2) types of authentication change:

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

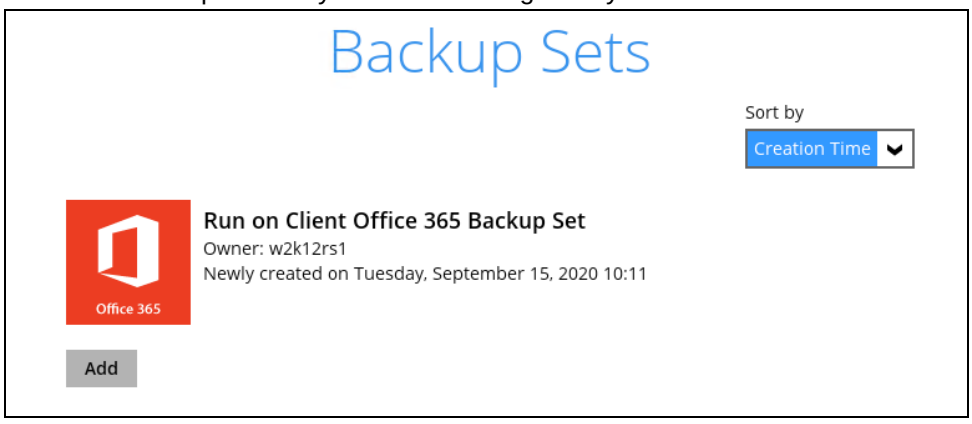
To change the authentication from **Modern Authentication to Hybrid Authentication**, follow the instructions below:

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

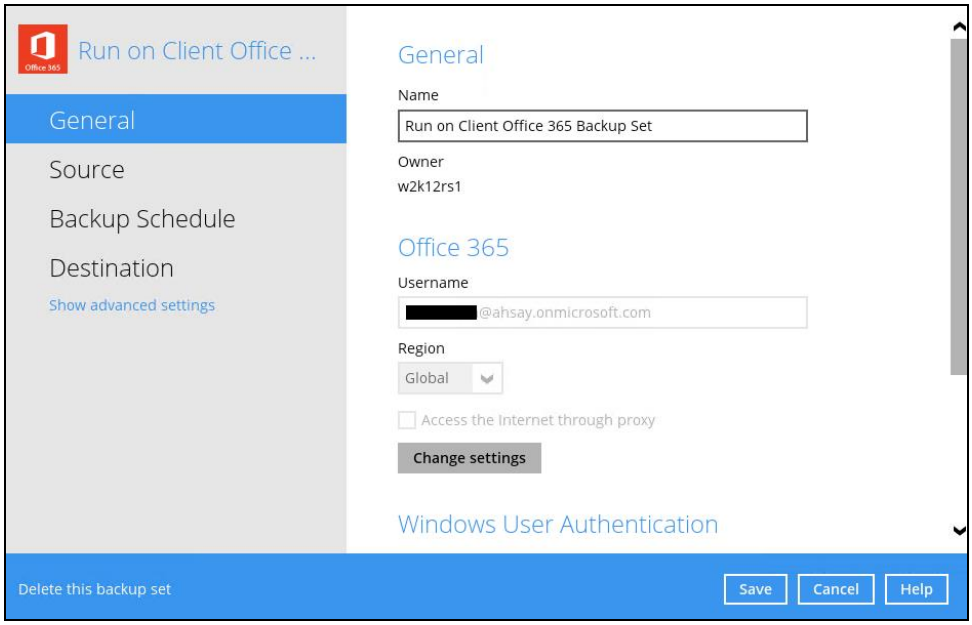
2. In the AhsayOBM main interface, click **Backup Sets**.



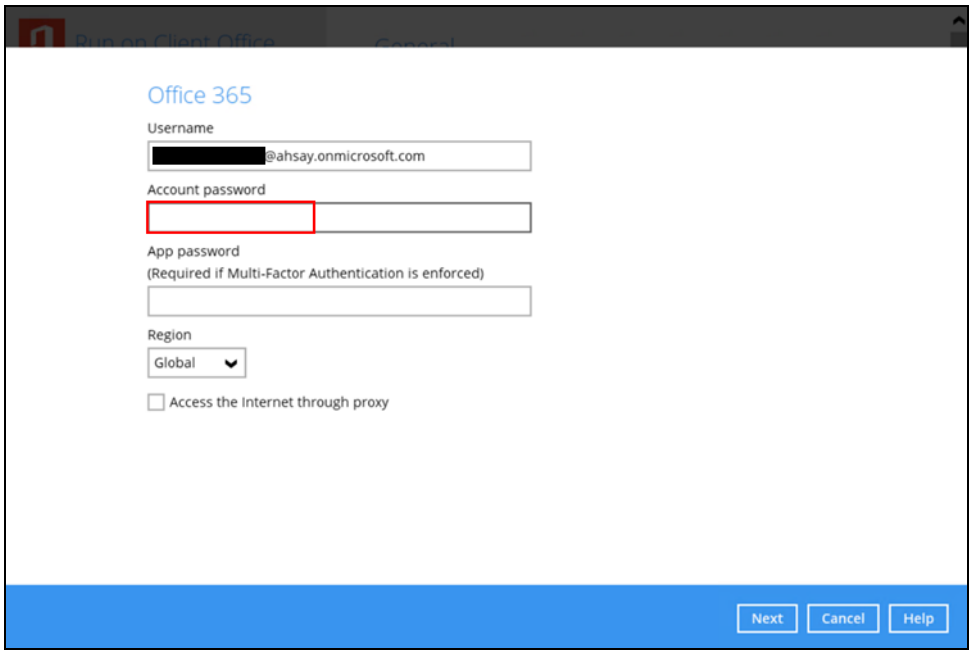
3. Select the backup set that you want to change to Hybrid Authentication.



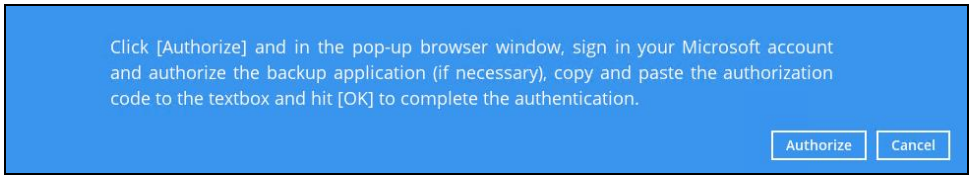
4. In the Backup Set Settings, click **Change settings** under the Office 365 screen.



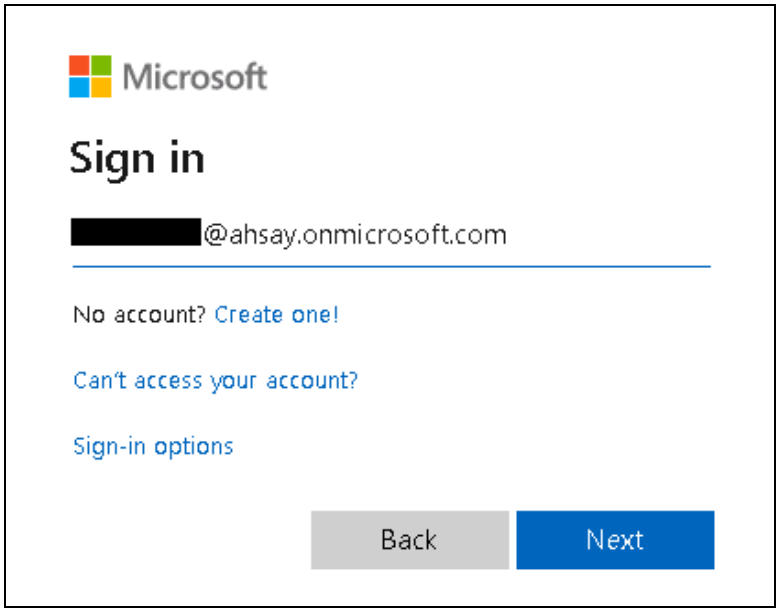
5. In the Office 365 credentials page, **input the Office 365 login account and password** then click **Next**.

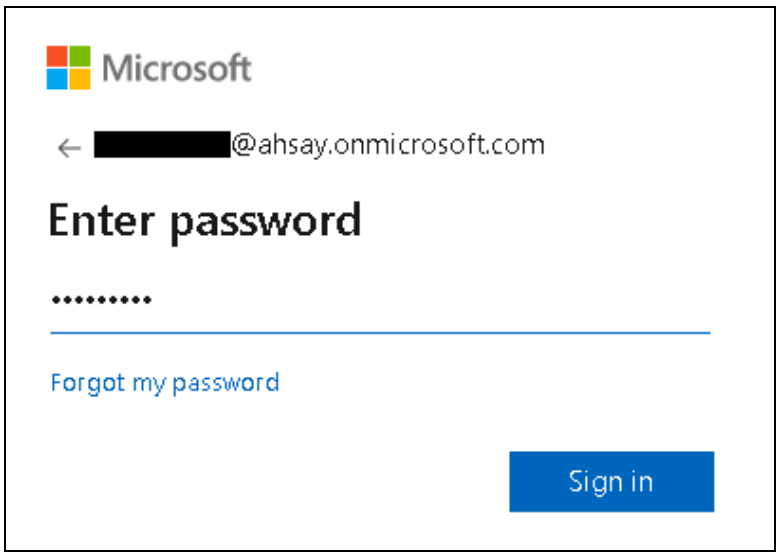


6. Click **Authorize** to start the authentication change process.

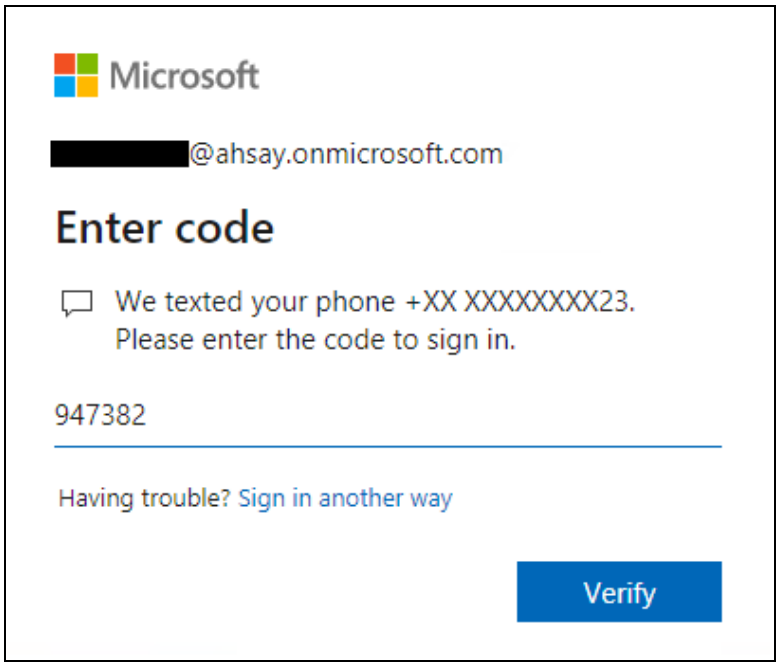


7. Sign in to your account.


Microsoft
Sign in
[redacted]@ahsay.onmicrosoft.com
No account? Create one!
Can't access your account?
Sign-in options
Back
Next


Microsoft
[redacted]@ahsay.onmicrosoft.com
Enter password
••••••••••
Forgot my password
Sign in

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

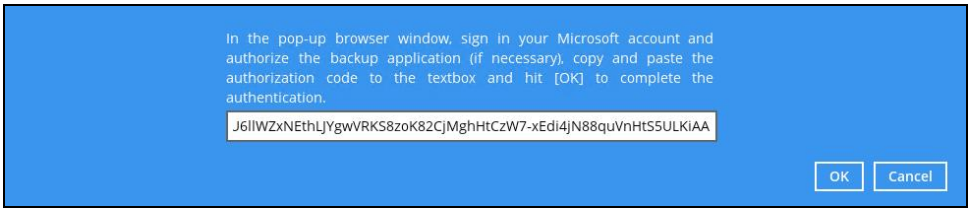


NOTE

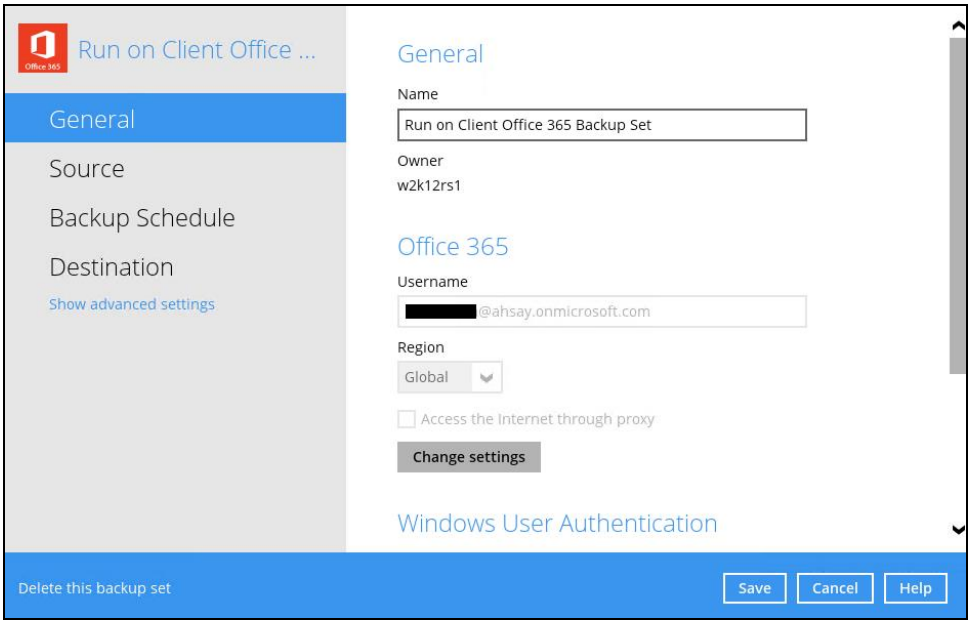
The verification code will only be required if the MFA status of an Office 365 account is enforced.

9. Copy the authorization code.

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



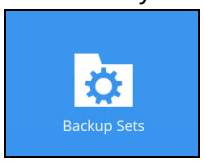
11. Click **Save** to finish the authentication change of the backup set.



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

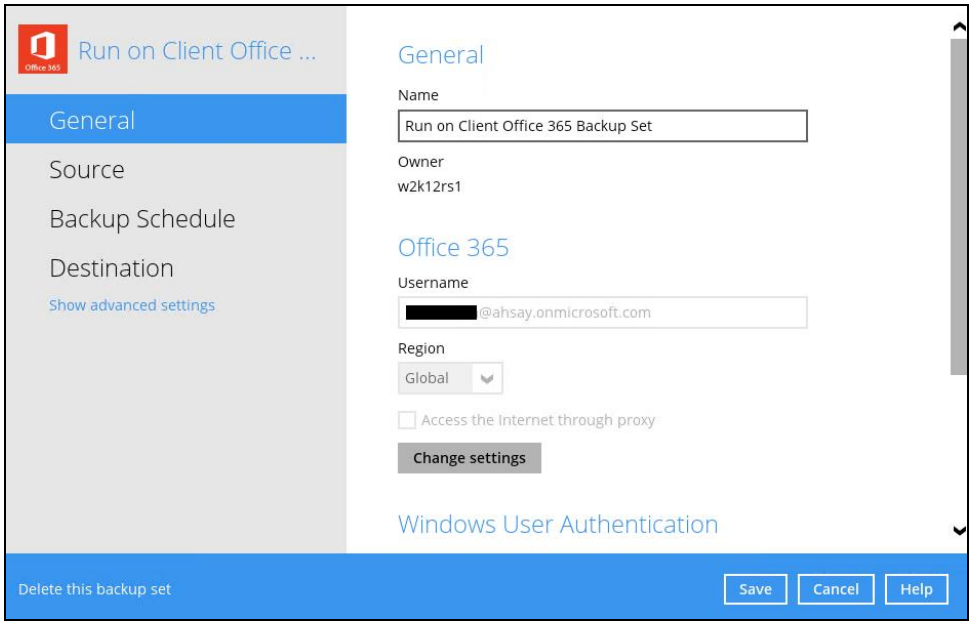
1. Logout all Office 365 account on the default browser before starting the authentication change of the backup set.

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

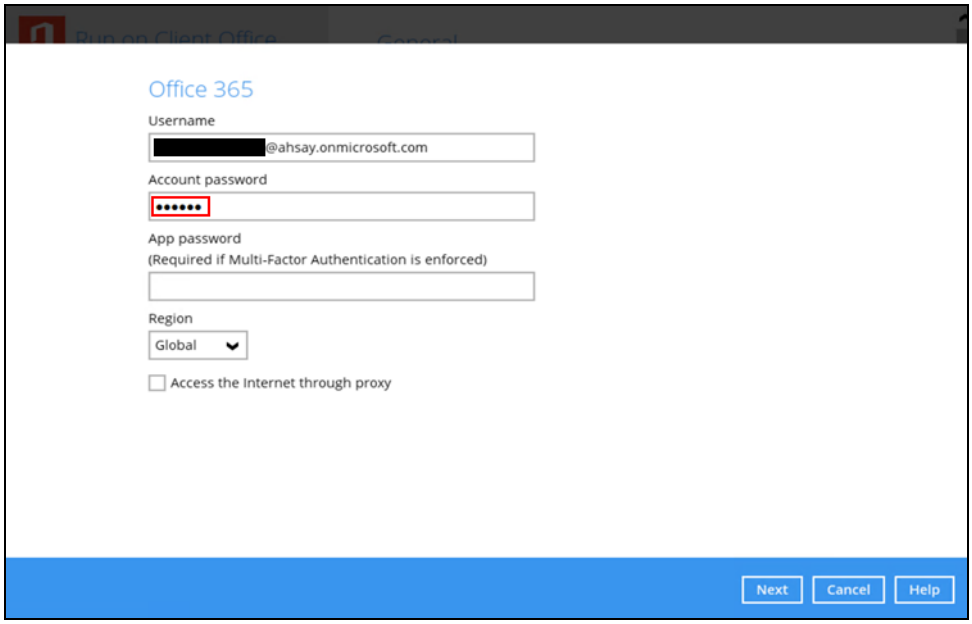


3. Select the backup set that you want to change to Modern Authentication.

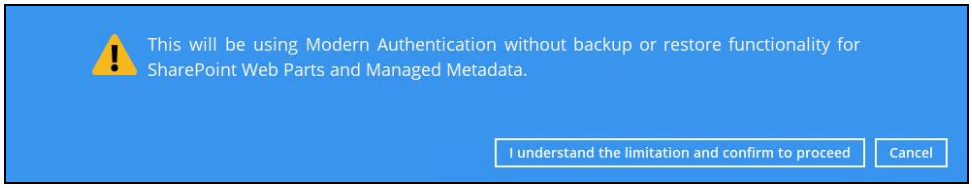
4. In the Backup Set Settings, click **Change settings** under the Office 365 screen.



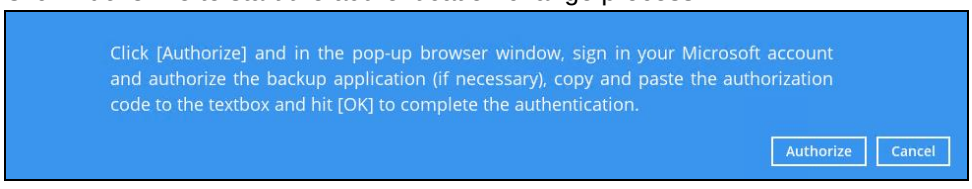
5. In the Office 365 credentials page, **remove the Account password** then click **Next**.



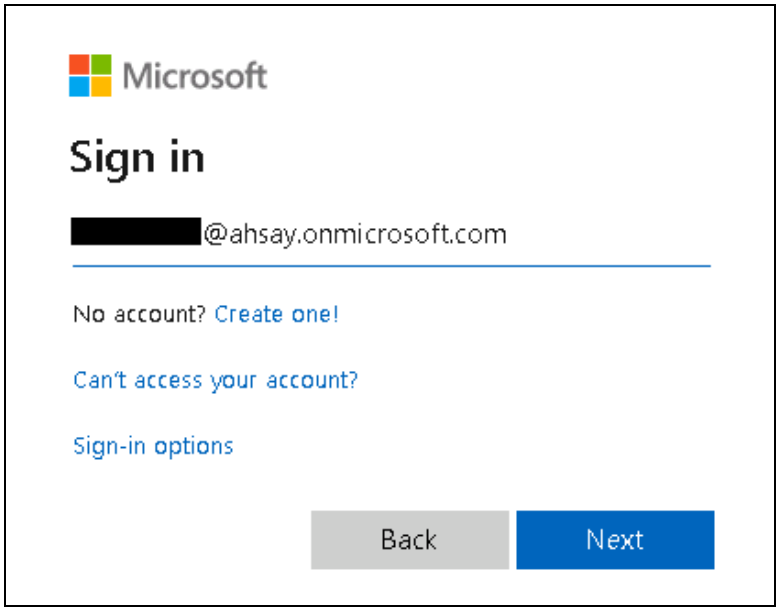
6. Click **I understand the limitation and confirm to proceed**.

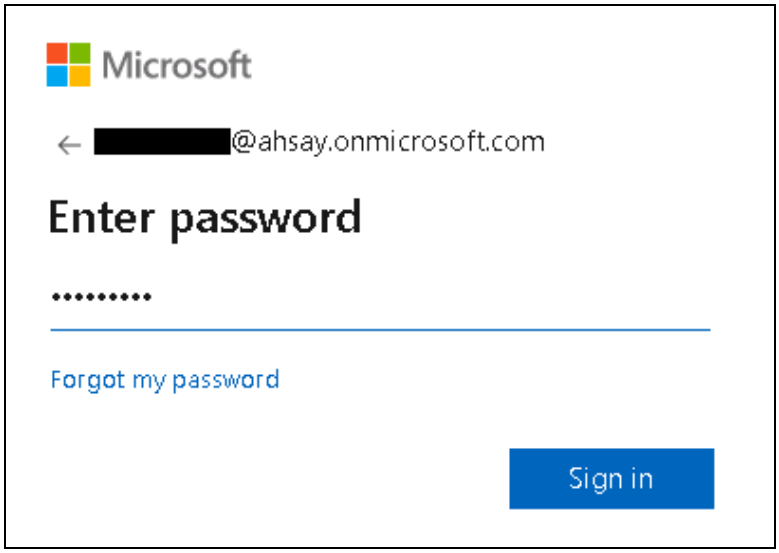


7. Click **Authorize** to start the authentication change process.

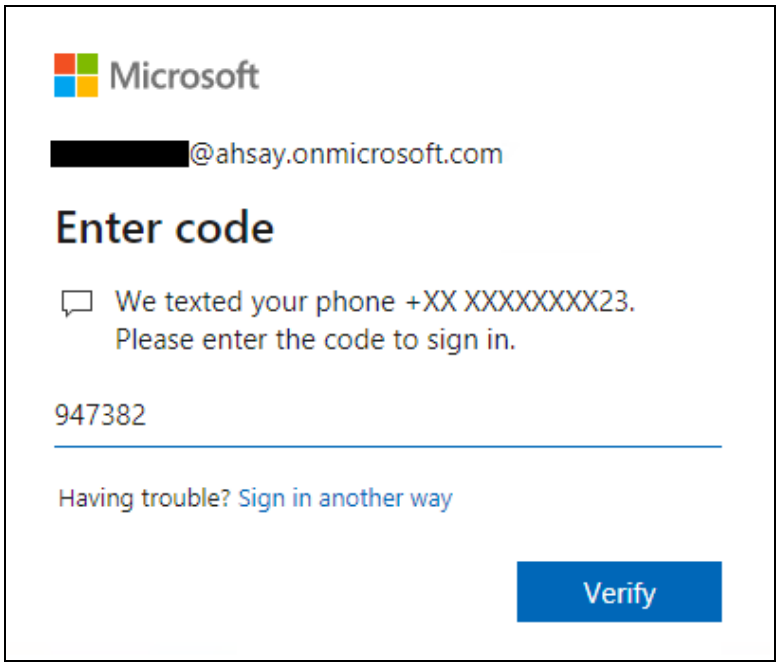


8. Sign in to your account.





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

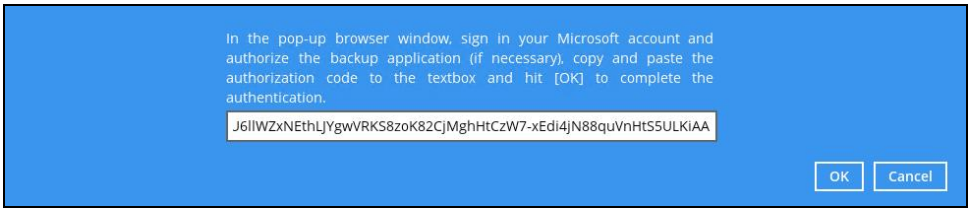
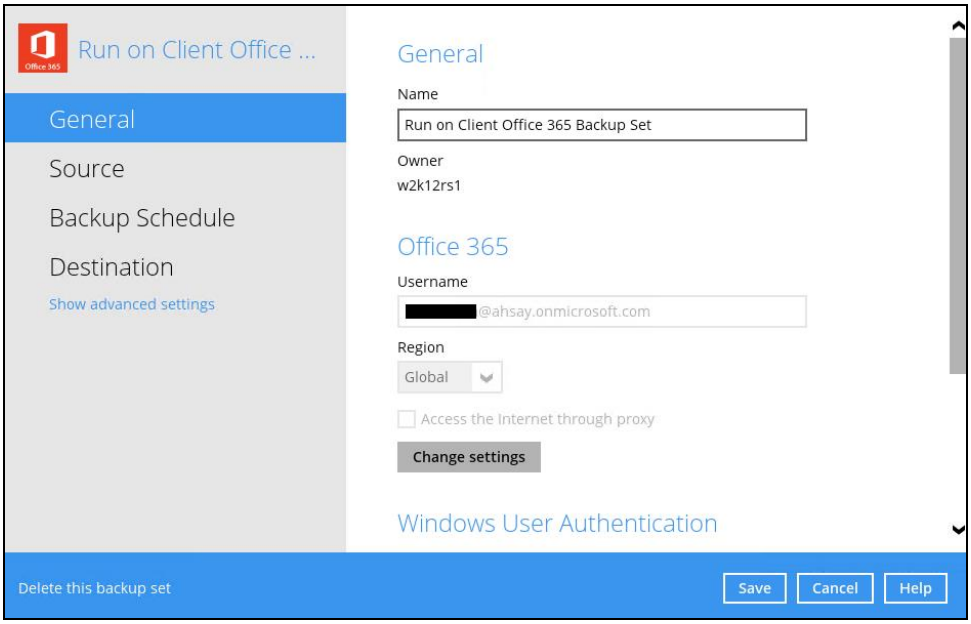


NOTE

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

10. Copy the authorization code.

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



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