

Ahsay Cloud Backup Suite v8

Run on Server (Agentless) Office 365 Backup & Restore Guide

Ahsay Systems Corporation Limited

19 April 2021

Copyright Notice

© 2021 Ahsay Systems Corporation Limited. All rights reserved.

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

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

Trademarks

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

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

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

Dropbox is a registered trademark of Dropbox Inc.

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

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

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

MariaDB is a registered trademark of MariaDB Corporation AB.

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

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

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

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

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

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

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

Ubuntu is a registered trademark of Canonical Ltd.

ShadowProtect is a registered trademark of StorageCraft Technology Corporation.

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

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

Disclaimer

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

Revision History

Date	Descriptions	Type of modification
6 October 2020	Added Appendix H	New
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. 2.9 and 2.10; Added Ch. 2.15; Modified Limitations in Ch. 2.16	Modifications
29 January 2021	Updated screenshots in Chapters 2, 7 and Appendix F	Modifications
19 April 2021	Updated Ch. 5; Added sub-chapters for the detailed process diagrams in Ch. 5.1, 5.2, 5.2.1, 5.2.2 and 5.3	New / Modifications

Table of Contents

1	Overview.....	1
1.1	What is this software?	1
1.2	System Architecture	1
1.3	Why should I use AhsayCBS Run on Server (Agentless) solution to back up my Office 365 data?.....	2
1.4	About This Document.....	7
2	Preparing for Backup and Restore.....	9
2.1	Internet / Network Connection	9
2.2	Supported Browsers.....	9
2.3	Login Credentials to Office 365	9
2.4	Valid AhsayOBM/AhsayACB User Account.....	9
2.5	Ahsay License Requirements.....	9
2.6	Add-on Module Requirements.....	9
2.7	Backup Quota Requirement	11
2.8	Office 365 License Requirements	11
2.9	Office 365 Permission Requirements for AhsayOBM	13
2.9.1	Assigning Global Admin Role to Accounts	14
2.9.2	Granting Term Store Administrator Role	16
2.9.3	Granting Permission to Discovery Management Group.....	17
2.9.4	Granting Permission to Accounts for Creating Backup Set	19
2.9.5	Granting Permission to restore all share link types to alternate location in Office 365.....	22
2.10	Office 365 Permission Requirements for AhsayACB	25
2.10.1	Assigning Global Admin Role to Accounts	26
2.10.2	Granting Permission to Discovery Management Group.....	28
2.10.3	Granting Permission to Accounts for Creating Backup Set	30
2.11	Data Synchronization Check (DSC) Setup	33
2.12	SharePoint Requirement	34
2.12.1	SharePoint Set Backup for AhsayOBM.....	34
2.12.2	SharePoint Personal Site Backup for AhsayACB.....	34
2.13	Authentication	35
2.14	Supported Services.....	39
2.15	Maximum Supported File Size	46
2.15.1	AhsayOBM	46
2.15.2	AhsayACB	46
2.16	Limitations.....	47
2.16.1	AhsayOBM	47
2.16.2	AhsayACB	52
2.16.3	AhsayCBS Run on Server (Agentless).....	54

2.17	Best Practices and Recommendations.....	55
3	Login to AhsayCBS User Web Console.....	61
3.1	Login to AhsayCBS with no 2FA	61
3.2	Login to AhsayCBS with 2FA using Twilio.....	63
3.3	Login to AhsayCBS with 2FA using Mobile Authentication	65
4	Creating an Office 365 Backup Set.....	68
4.1	Modern Authentication	68
4.2	Hybrid Authentication	84
5	Overview of Office 365 Backup Process.....	102
5.1	Periodic Data Integrity Check (PDIC) Process	103
5.2	Backup Set Index Handling Process	105
5.2.1	Start Backup Job	105
5.2.2	Completed Backup Job.....	106
5.3	Data Validation Check Process.....	107
6	Running Backup Job.....	108
7	Restoring Office 365 Backup Set	111
7.1	Restore Backup with AhsayCBS User Web Console.....	111
7.1.1	From Users.....	112
7.1.2	From Site Collections.....	118
8	Running a Data Integrity Check.....	129
9	Performing a Space Freeing Up	131
10	Deleting Backup Data	133
11	Contact Ahsay.....	135
11.1	Technical Assistance	135
11.2	Documentation.....	135
Appendix.....		136
Appendix A:	Example Scenarios for Office 365 License Requirement and Usage.....	136
Appendix B:	Example for backup of large numbers of Office 365 users	141
Appendix C:	Setting Multi-Factor Authentication (MFA) in Microsoft 365 Admin Center.....	144
Appendix D:	Example Scenario for Backup Set Maintenance.....	157
Appendix E:	Example Scenario for Data Synchronization Check (DSC) with sample backup reports	158
Appendix F:	Steps on How to view Item count and Storage used in Microsoft 365 Admin Center.....	163
Appendix G:	Migrating Authentication of Office 365 Backup Set	168
AhsayOBM User	168

AhsayACB User	183
Appendix H: Steps on How to Change the Office 365 Authentication	193

1 Overview

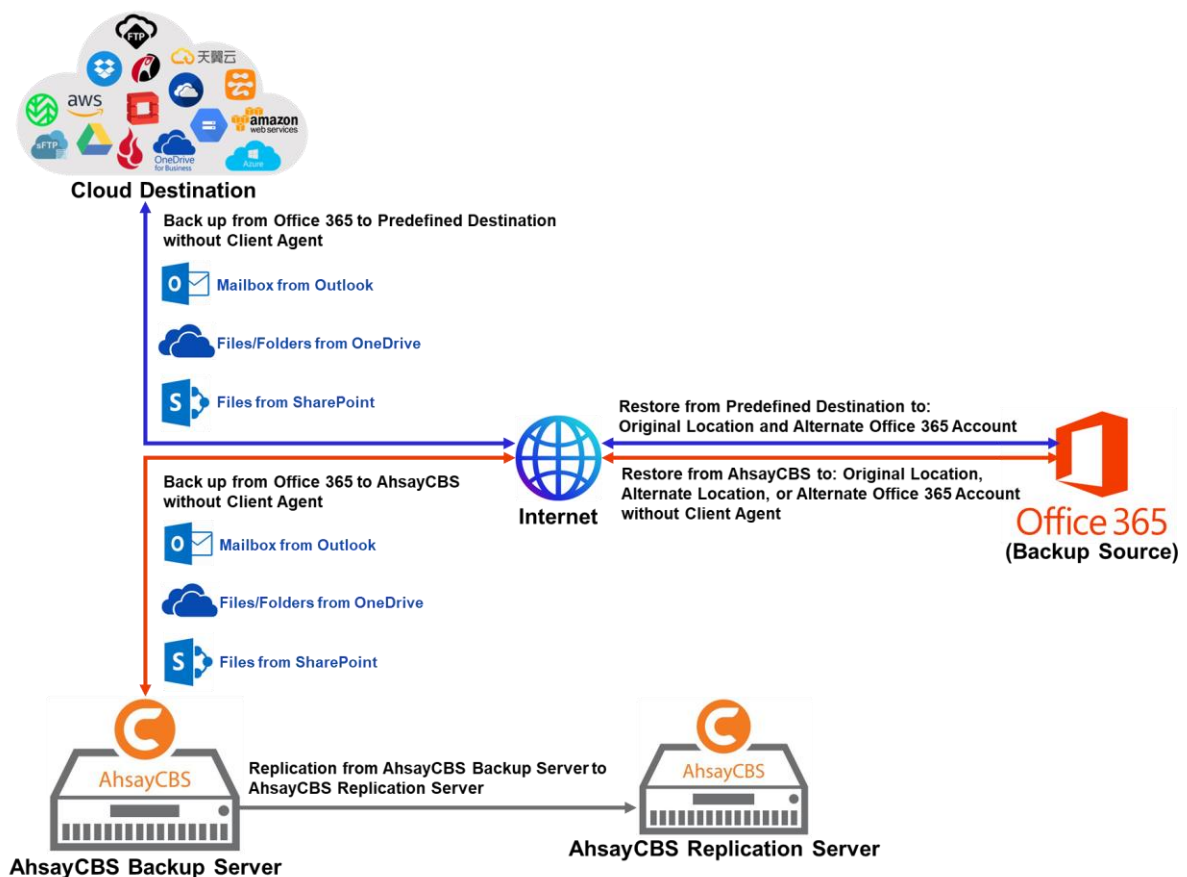
1.1 What is this software?

Ahsay Cloud Backup Suite v8 allows you to back up your Office 365 data on the cloud without the need to deploy a backup agent. You can access the AhsayCBS server environment easily on a web-based management console. This is a user interface that allows you to login remotely to a backup server to manage and monitor your backups.

1.2 System Architecture

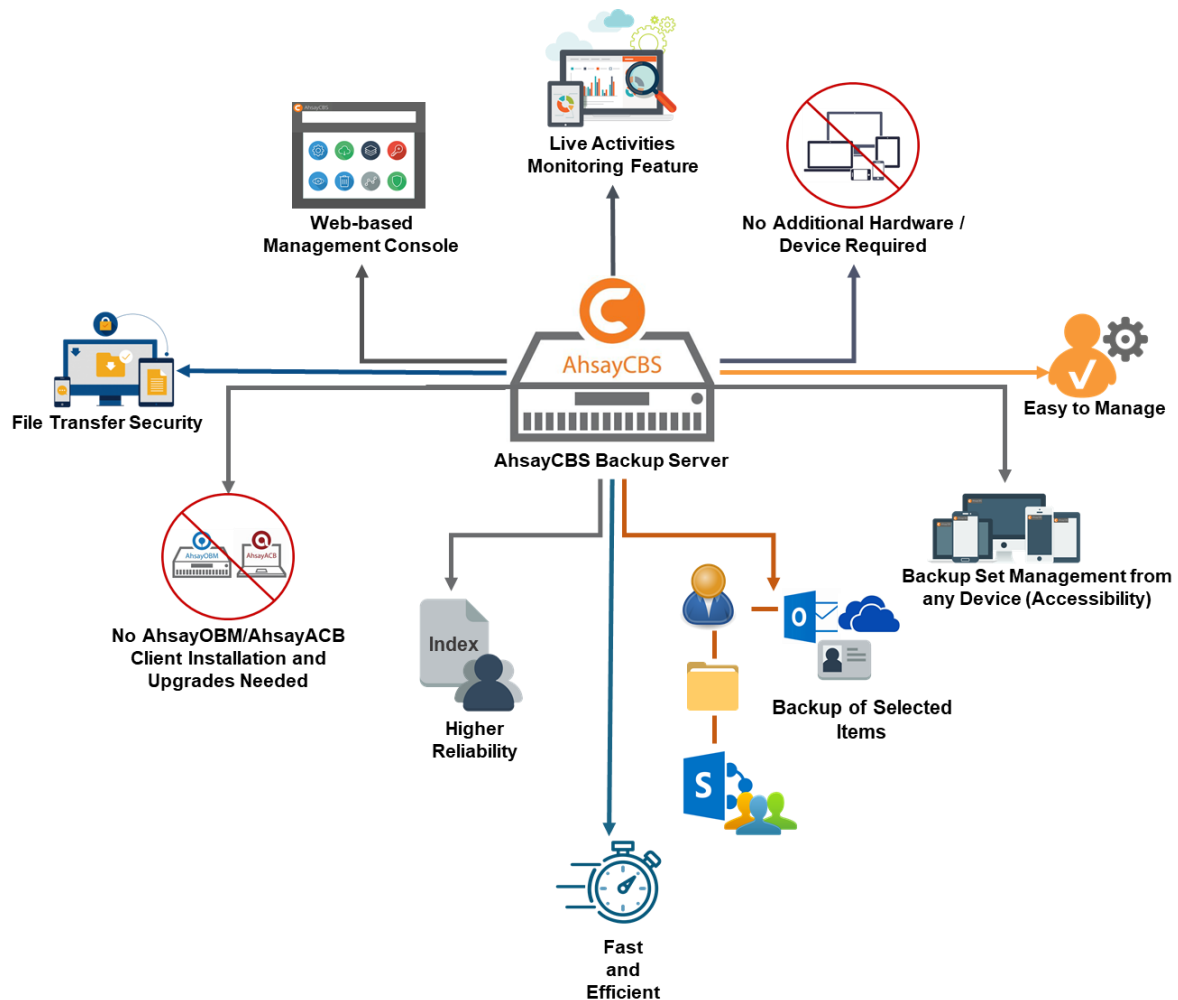
For agentless backup and restore, the AhsayCBS backup server connects to the Office 365 directly through the Internet without the need to deploy additional backup agents on the customers site.

Below is the System architecture diagram illustrating the major elements involved in the backup and restore process using Ahsay Agentless (Run on Server) backup configuration.



1.3 Why should I use AhsayCBS Run on Server (Agentless) solution to back up my Office 365 data?

We are committed to bringing you a comprehensive Run on Server (Agentless) Office 365 backup and recovery solution. Below are some key areas that we can help to make your backup experience a better one.



Web-based Management Console

Our enriched features on the centralized user web console offers you a one-stop location for monitoring and managing your backup and restore, whether you are a system administrator or a backup user. Below is an overview of what you can do with it.

- Create backup set
- Restore backup
- Configure user settings
- Configure backup settings
- View and download backup and restore reports.

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 of each incremental backup can be completed within hours.

Live Activities Monitoring Feature

The AhsayCBS User Web Console has a live activity monitoring feature which is used to keep track of the backup and restore job(s). The following operations can be performed using this feature:

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

NOTE

There is an update interval of around five (5) seconds for both backup and restore activities.

No Additional Hardware / Device Required

As the Run on Server (agentless) backup set utilizes the resources of the AhsayCBS backup server, there is no need to provision additional physical or virtual machine to run the backup/restore which means the cost of each backup set is much lower than for an agent-based Office 365 backup set.

Easy to Manage

The AhsayCBS User Web Console offers you an easy-to-manage user interface. This will help you save time and it reduces the overall cost of support.

Backup Set Management from any Device (Accessibility)

Backup/restore operation(s), backup set settings configuration, and backup/restore process monitoring can be done from any device as long as a web browser and internet connection are present in the device.

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.

Fast and Efficient

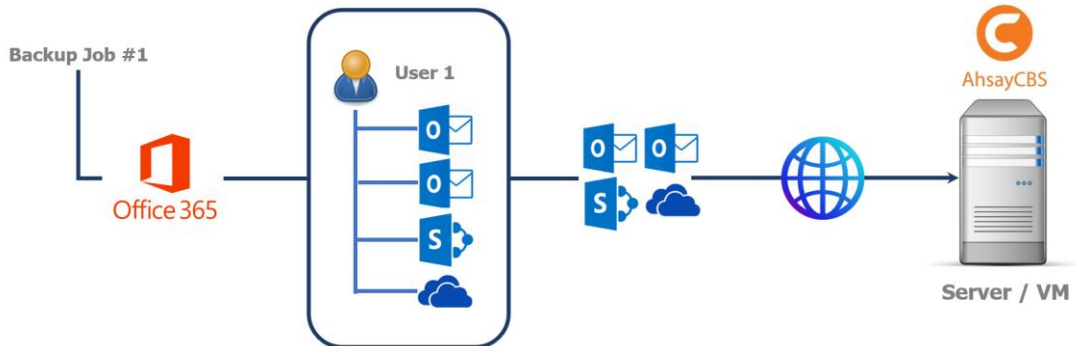
We understand that backup could be a time and resources consuming process, which is why AhsayCBS is designed with advanced technologies to make backup a fast and efficient process.

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.

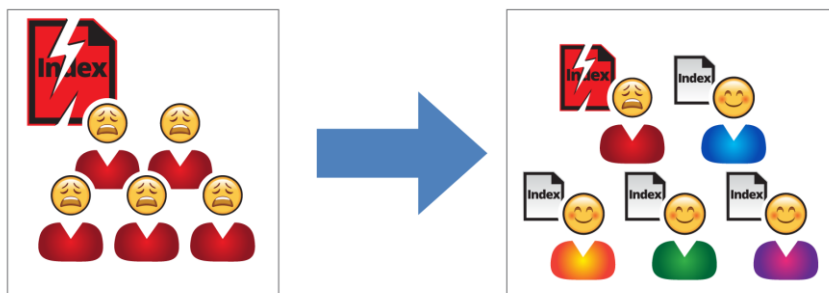
The default setting for Office 365 backup sets supports a total of 4 threads per backup job.

For Agentless Option:



Higher Reliability

The implementation of one index file per user can significantly improve the overall resilience of backup and restore from index related issues.



For example, if a single index file becomes corrupted, it will only affect corresponding user, while other users selected for backup are unaffected.

No AhsayOBM/AhsayACB Client Installation and Upgrades Needed

AhsayOBM and AhsayACB client installation is not required in running AhsayCBS server. Also, unlike the client backup agent, upgrading when a newer version becomes available is not necessary, as long as the AhsayCBS server version is upgraded by the backup service provider.

File Transfer Security

The AhsayCBS comes with a secure file transfer method using the https protocol that guarantees the highest level of security measure in safeguarding the movement of files from the backup source (Office 365) to the backup destination (AhsayCBS server).

High Level of Security

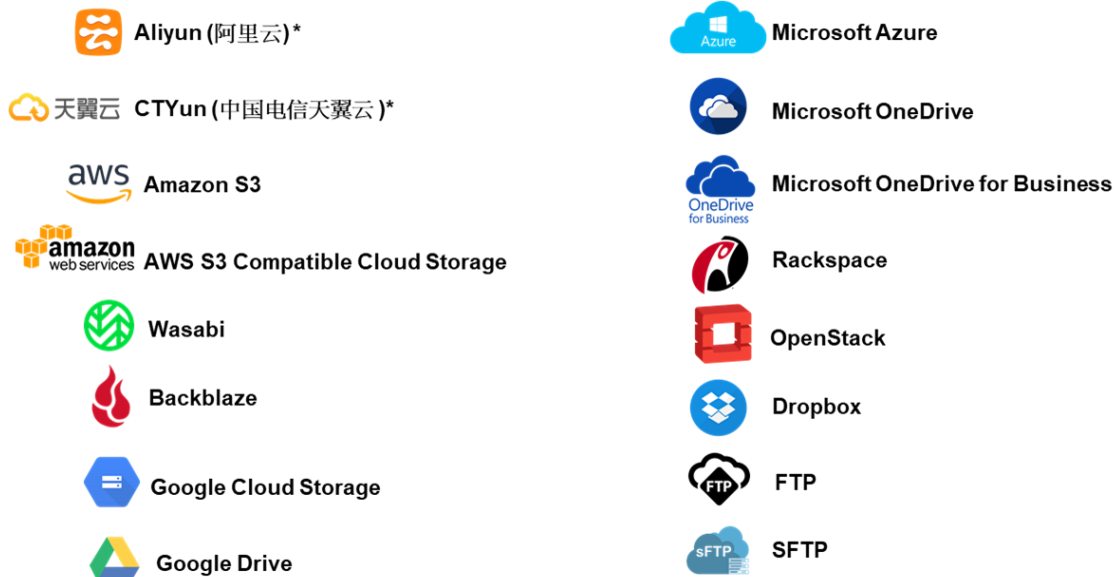
We understand your Office 365 users may contain sensitive information that requires to be protected, that is why your backup data will be encrypted with the highest level of security measure.

- **Un-hackable Encryption Key** – to provide the best protection to your backup data, the encryption feature which by default will encrypt the backup data locally with AES 256-bit truly randomized encryption key.



Cloud Destinations Backup

By default, the AhsayCBS is set as the storage destination in creating an Office 365 backup set. However, you have the option of selecting another storage destination as provided by your backup service provider. Below is a list of supported cloud destinations:



NOTE

For more details, please contact your backup service provider.

Compliance

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

Less Resources Needed

Backup client agent could interfere with the processing power of core applications of the machines that it is installed on. Run on Server Office 365 backup job is performed on the backup server, which does not consume resources on client computer during a backup job.

Run on Server

A Run on Server Office 365 backup set provides you with an agentless backup solution. Manual schedules are performed directly by the AhsayCBS backup server; you do not need to install a backup agent on your personal computer in order to back up your data on cloud storages.

Run on Server backup and restore can be managed on a computer or device running on Windows/MacOS/Linux /iOS/Android as long as the device is able to support a web browser and has an internet connection.

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

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

	Run on Server Office 365 Backup Set	Run on Client Office 365 Backup Set
General Settings	✓	✓
Backup Source	✓	✓
Backup Schedule	✓	✓
Destination	AhsayCBS or Predefined Destinations only	AhsayCBS, Predefined Destinations, Standard and Local
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	AhsayCBS User Web Console only	AhsayOBM / AhsayACB
To Run a Restore	AhsayCBS User Web Console only	AhsayOBM / AhsayACB / AhsayOBR

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

	Run on Server Office 365 Backup Set	Run on Client Office 365 Backup Set
Data Integrity Check	✓	✓
Space Freeing Up	✓	✓
Delete Backup Data	✓	✓
Decrypt Backup Data	✗	✓

NOTE

For more details on the Run on Client backup option, please refer to the following guides:

[AhsayOBM v8 User Guide - Office365 Backup & Restore for Windows](#)

[AhsayOBM v8 User Guide - Office365 Backup & Restore for Mac](#)

[AhsayACB v8 User Guide - Office365 Backup & Restore for Windows](#)

[AhsayACB v8 User Guide - Office365 Backup & Restore for Mac](#)

1.4 About This Document

What is the purpose of this document?

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

The document can be divided into six (6) main parts.

Part 1: Preparing for Office 365 Backup & Restore

Requirements

Requirements for Office 365 backup set

Best Practices and Recommendations

Items recommended to pay attention to before backup and restore

Part 2: Performing an Office 365 Backup

Logging in to AhsayCBS User Web Console

Log in to AhsayCBS User Web Console

Creating a Backup Set

Create a backup set using AhsayCBS User Web Console

Running a Backup Set

Run a backup set using AhsayCBS User Web Console

Part 3: Restoring an Office 365 Backup

Restoring a Backup Set using AhsayCBS User Web Console

Restore a backup using AhsayCBS User Web Console

Part 4: Running a Data Integrity Check

Running a Data Integrity Check using AhsayCBS User Web Console

Run a data integrity check using AhsayCBS User Web Console

Part 5: Performing a Space Freeing Up

Performing a Space Freeing Up using AhsayCBS User Web Console

Perform a space free up using AhsayCBS User Web Console

Part 6: Deleting Backup Data

Deleting a Backup Data using AhsayCBS User Web Console

Delete a backup data using AhsayCBS User Web Console

What should I expect from this document?

After reading through this documentation, you can expect to have sufficient knowledge to perform various tasks on the AhsayCBS server, as well as to carry out an end-to-end backup and restore process, and to be instructed about the other actions that can be performed through the User Web Console (i.e. Data Integrity Check, Space Freeing Up and Delete Backup Data).

Who should read this document?

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

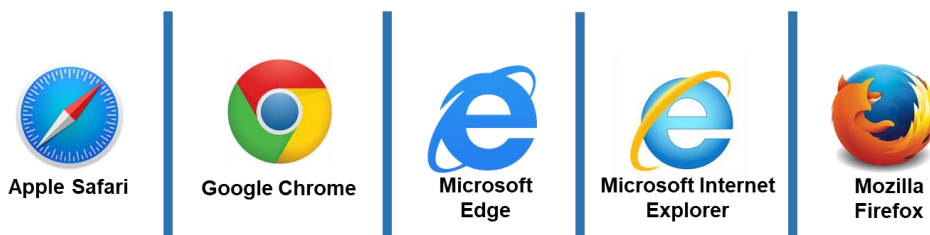
2 Preparing for Backup and Restore

2.1 Internet / Network Connection

In order to access the AhsayCBS Backup Server through the Web-based Management Console, you need to have internet connection and LAN access.

2.2 Supported Browsers

The AhsayCBS User Web Console runs with all major browsers. Please make sure that you are using the latest version and enable pop-ups on your preferred web browsers.



2.3 Login Credentials to Office 365

To allow access to Office 365 (backup source) in performing a backup, make sure to have the correct login credentials to Office 365.

2.4 Valid AhsayOBM/AhsayACB User Account

A valid AhsayOBM/AhsayACB user account is required before you can access the AhsayCBS User Web Console. Please contact your system administrator for more details.

2.5 Ahsay License Requirements

• Licenses

Licenses are calculated on a per device basis for AhsayOBM and AhsayACB.

For Agentless, to be able to backup users using AhsayCBS User Web Console, one AhsayOBM or AhsayACB license is required.

Please contact your backup service provider for more details.

2.6 Add-on Module Requirements

• Office 365 Add-on Module

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

Please contact your backup service provider for more details. Below are the sample screenshots of an AhsayOBM and AhsayACB user with an add-on module of Office 365 with licenses.

AhsayOBM User with five (5) licenses

User Profile | **General** | **Backup Client Settings** | **Contact** | **User Group** | **Authentication** | **Mobile Backup**

Backup Set
Settings
Report
Statistics
Effective Policy

Settings of the client backup agent for this user.

Backup Client

☒ AhsayOBM User ☐ AhsayACB User

Add-on Modules

<input type="checkbox"/> Microsoft Exchange Server	<input type="checkbox"/> Microsoft SQL Server
<input type="checkbox"/> MySQL Database Server	<input type="checkbox"/> Oracle Database Server
<input type="checkbox"/> Lotus Domino	<input type="checkbox"/> Lotus Notes
<input type="checkbox"/> Windows System Backup	<input type="checkbox"/> Windows System State Backup
<input type="checkbox"/> VMware <input type="text" value="Guest VM"/> <input type="text" value="0"/>	<input type="checkbox"/> Hyper-V <input type="text" value="Guest VM"/> <input type="text" value="0"/>
<input type="checkbox"/> Microsoft Exchange Mailbox <input type="text" value="0"/>	<input type="checkbox"/> ShadowProtect System Backup
<input type="checkbox"/> NAS - QNAP	<input type="checkbox"/> NAS - Synology
<input checked="" type="checkbox"/> Mobile (max. 10)	<input checked="" type="checkbox"/> Continuous Data Protection
<input type="checkbox"/> Volume Shadow Copy	<input checked="" type="checkbox"/> In-File Delta
<input type="checkbox"/> OpenDirect / Granular Restore <input type="text" value="0"/>	<input checked="" type="checkbox"/> Office 365 Backup <input type="text" value="5"/>
<input type="checkbox"/> MariaDB Database Server	

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, it would be counted as 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 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](#).

AhsayACB User with two (2) licenses

The screenshot shows the 'Backup Client Settings' tab for a user. The 'Backup Client' section has 'AhsayACB User' selected. The 'Add-on Modules' section shows the following settings:

Module	Status
Windows System Backup	<input type="checkbox"/>
Mobile (max. 10)	<input checked="" type="checkbox"/>
Volume Shadow Copy	<input type="checkbox"/>
OpenDirect / Granular Restore	<input type="checkbox"/>
Lotus Notes	<input type="checkbox"/>
Continuous Data Protection	<input type="checkbox"/>
In-File Delta	<input checked="" type="checkbox"/>
Office 365 Backup	<input checked="" type="checkbox"/> 2

NOTE

Please be reminded that a maximum of two (2) modules are allowed for Office 365 Backup on AhsayACB. If you wish to back up more than two Office 365 users, consider using AhsayOBM instead. Please contact your backup service provider for more details.

2.7 Backup Quota Requirement

Make sure that your AhsayACB or 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 F: Steps on How to view Item count and Storage used in Microsoft 365 Admin Center](#)

2.8 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 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 to 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 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.

2.9 Office 365 Permission Requirements for AhsayOBM

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

- **Global Admin Role**

Starting with AhsayCBS 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. 2.9.1](#).

- **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. 2.9.2](#).

- 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. 2.9.3](#).

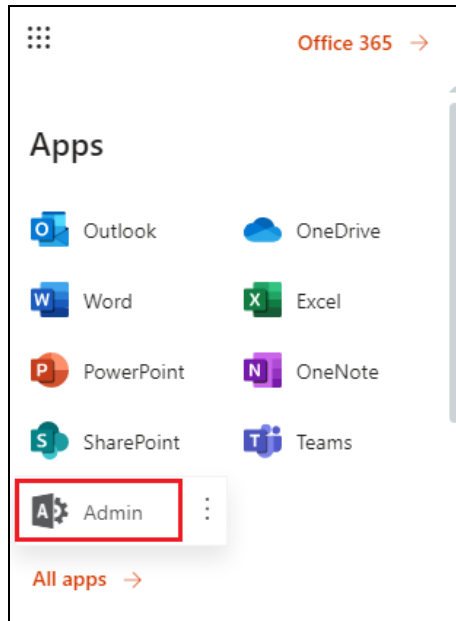
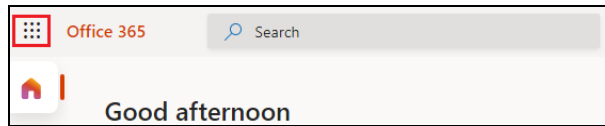
- ◉ ApplicationImpersonation
- ◉ Legal Hold
- ◉ Mailbox Import Export
- ◉ Mailbox Search
- ◉ Public Folders

Otherwise, proceed to grant all necessary permissions to the Office user account as shown in the following chapters [2.9.1](#), [2.9.2](#), [2.9.3](#), [2.9.4](#), and [2.9.5](#).

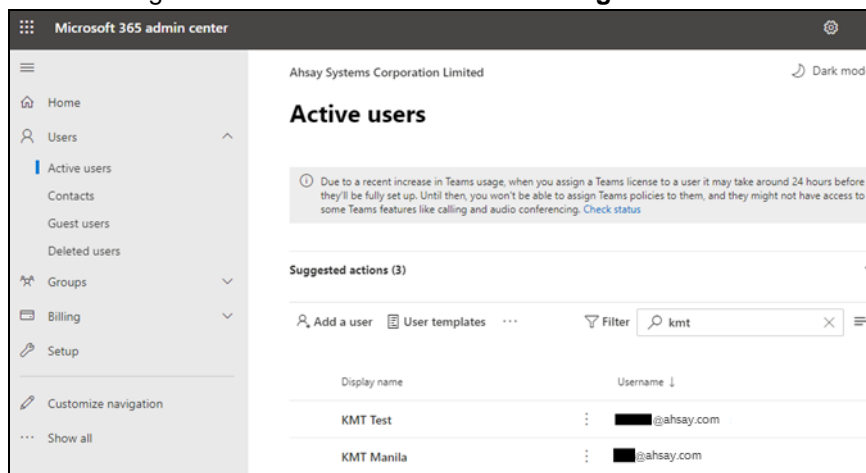
2.9.1 Assigning Global Admin Role to Accounts

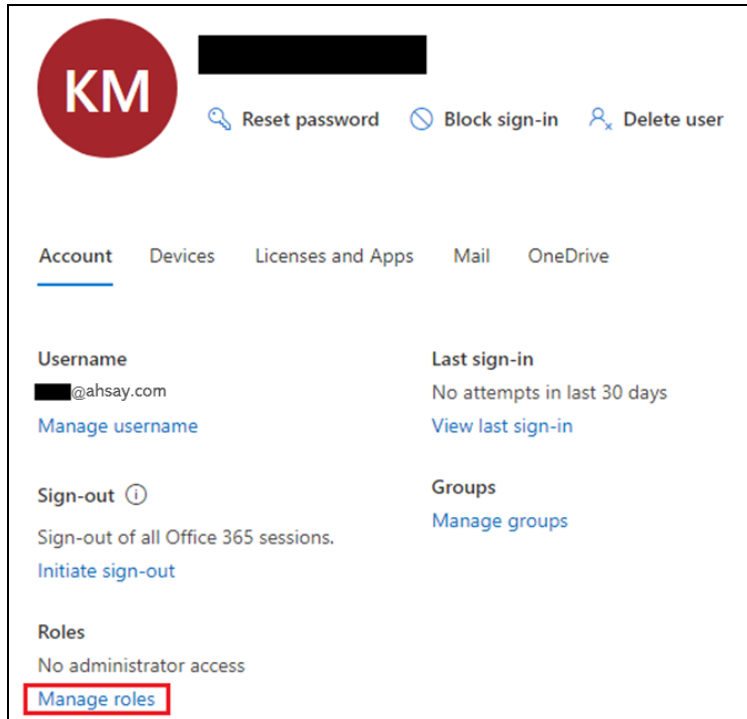
To assign the Global Admin role to accounts, follow the steps below:

- 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 and select **Manage roles**.





KM [Redacted Name]

[Reset password](#) [Block sign-in](#) [Delete user](#)

[Account](#) [Devices](#) [Licenses and Apps](#) [Mail](#) [OneDrive](#)

Username
[Redacted]@ahsay.com
[Manage username](#)

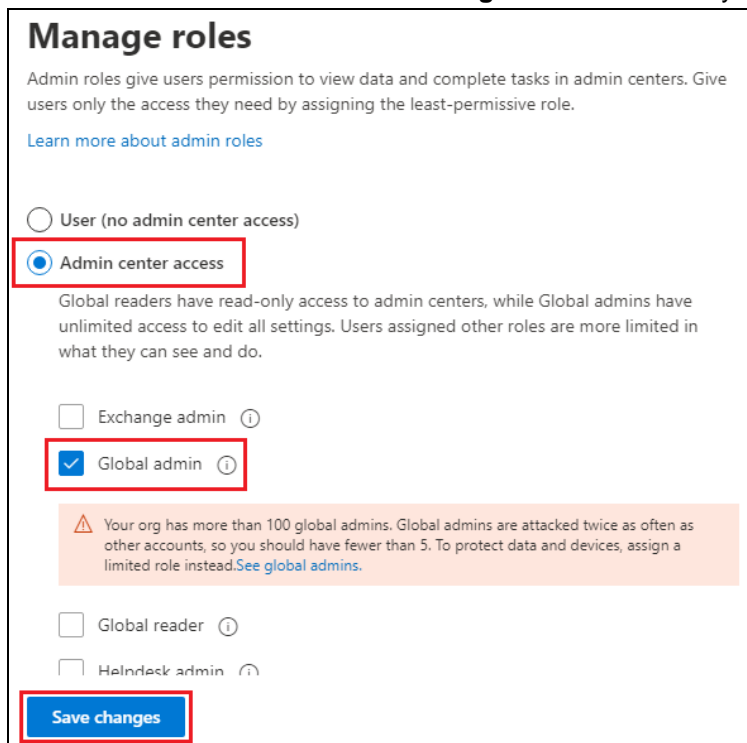
Last sign-in
No attempts in last 30 days
[View last sign-in](#)

Sign-out ⓘ
Sign-out of all Office 365 sessions.
[Initiate sign-out](#)

Groups
[Manage groups](#)

Roles
No administrator access
[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.



Manage roles

Admin roles give users permission to view data and complete tasks in admin centers. Give users only the access they need by assigning the least-permissive role.

[Learn more about admin roles](#)

☐ User (no admin center access)

☒ **Admin center access**

Global readers have read-only access to admin centers, while Global admins have unlimited access to edit all settings. Users assigned other roles are more limited in what they can see and do.

☐ Exchange admin ⓘ

☒ **Global admin** ⓘ

⚠ Your org has more than 100 global admins. Global admins are attacked twice as often as other accounts, so you should have fewer than 5. To protect data and devices, assign a limited role instead. [See global admins.](#)

☐ Global reader ⓘ

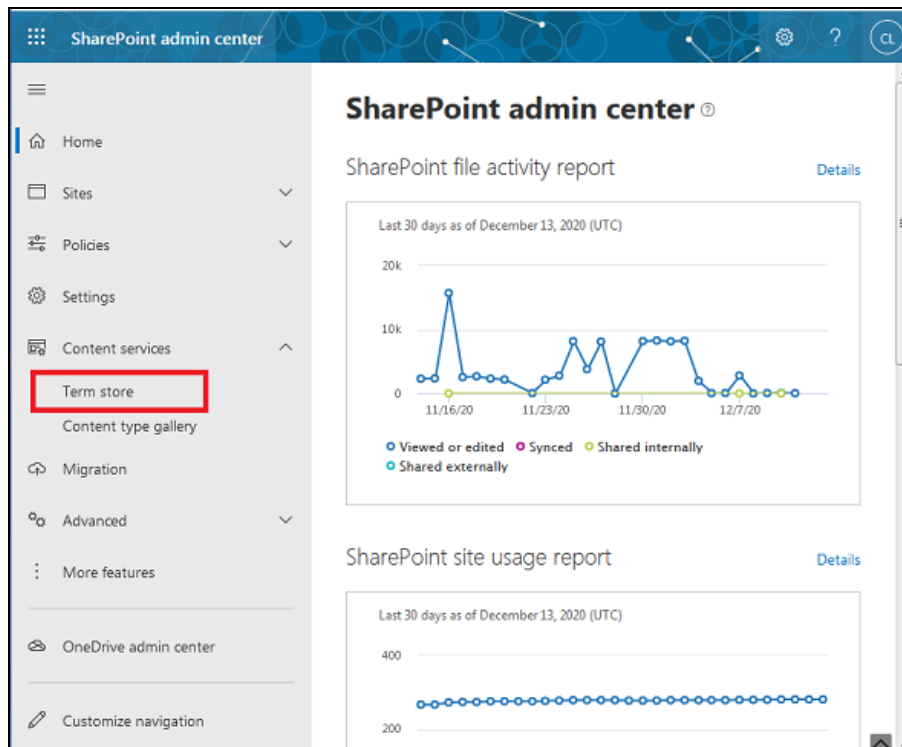
☐ Helndesk admin ⓘ

[Save changes](#)

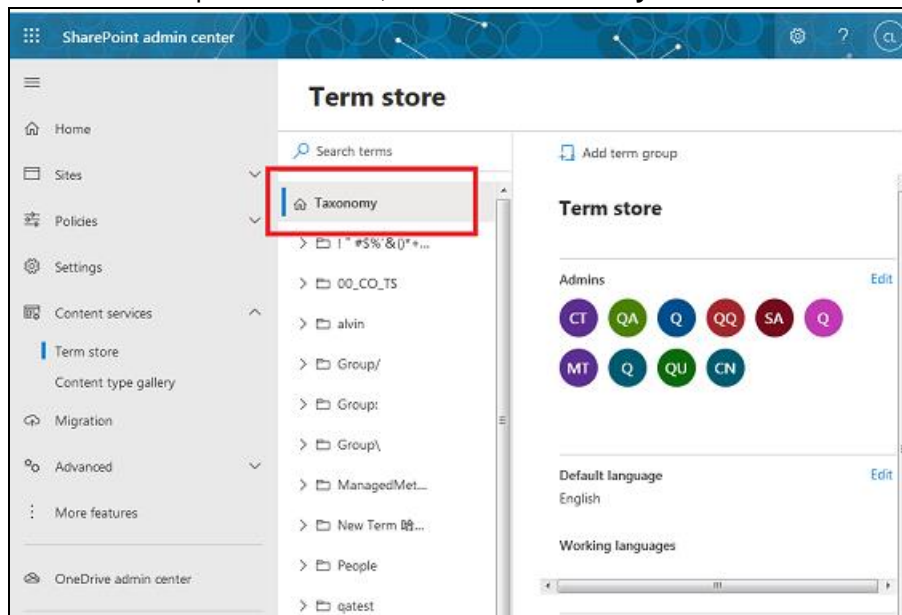
2.9.2 Granting Term Store Administrator Role

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

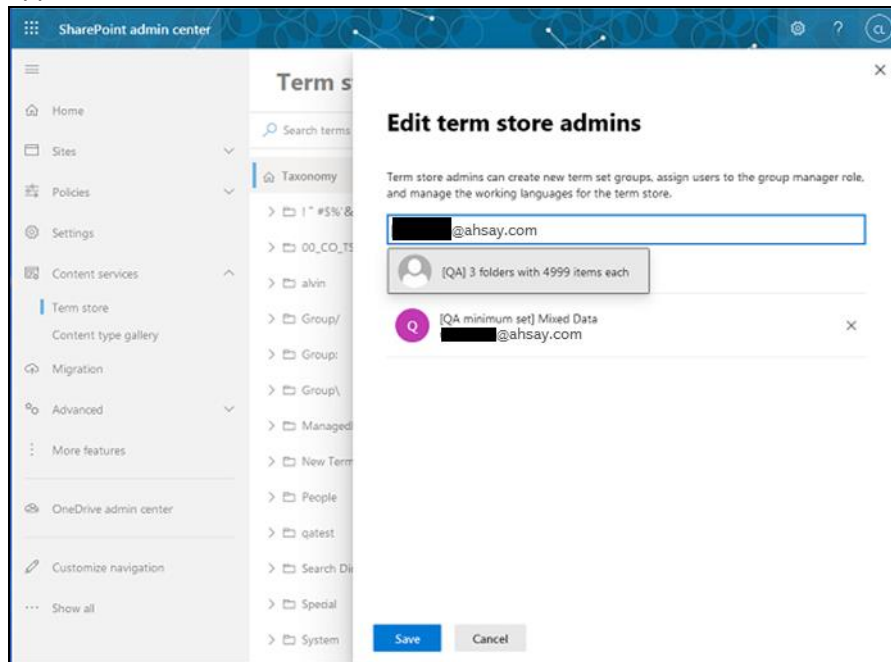
- i. In the SharePoint admin center, under **Content services**, click **Term store**.



- 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.

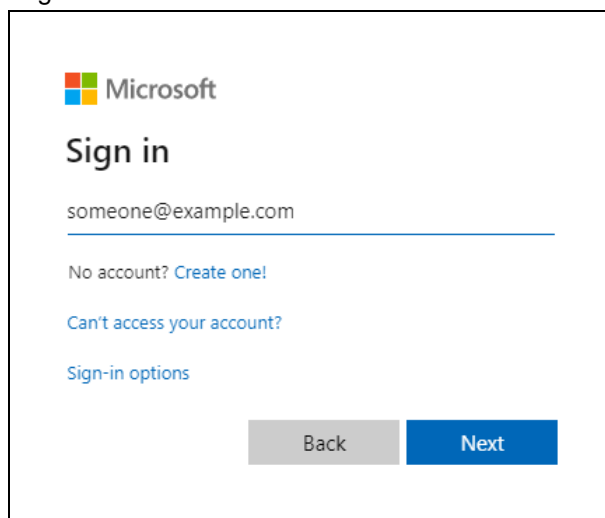


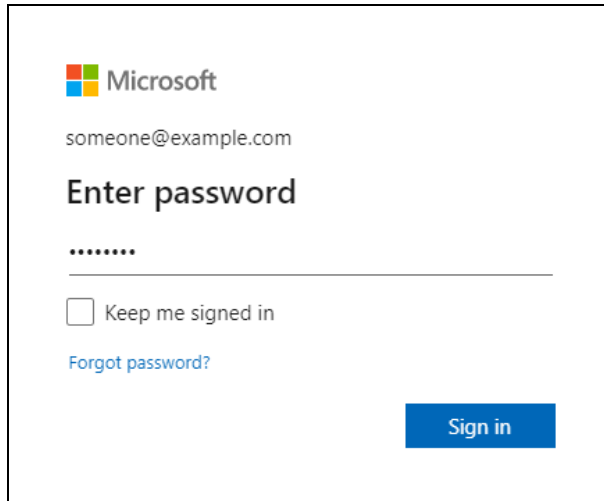
- iv. Enter the names or email addresses of the Office 365 user who you want to add as term store admins. Select **Save**.

2.9.3 Granting Permission to Discovery Management Group

This permission allows users added under the **Members** section of the **Discovery Management** group (refer to [Ch. 2.9.4](#) 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.





Microsoft

someone@example.com

Enter password

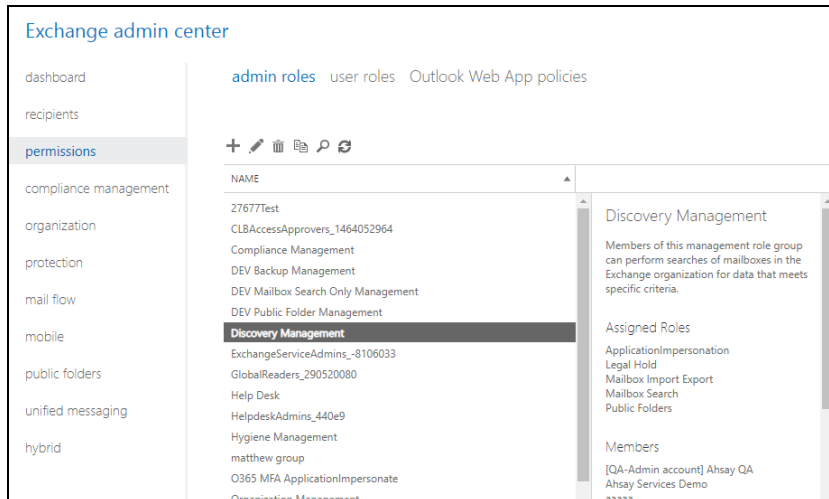
.....

☐ Keep me signed in

[Forgot password?](#)

Sign in

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



Exchange admin center

dashboard admin roles user roles Outlook Web App policies

recipients

permissions

compliance management

organization

protection

mail flow

mobile

public folders

unified messaging

hybrid

+ [edit] [delete] [refresh] [help]

NAME
27677Test
CLBAccessApprovers_1464052964
Compliance Management
DEV Backup Management
DEV Mailbox Search Only Management
DEV Public Folder Management
Discovery Management
ExchangeServiceAdmins_-8106033
GlobalReaders_290520080
Help Desk
HelpdeskAdmins_440e9
Hygiene Management
matthew group
O365 MFA ApplicationImpersonate
Organization Management

Discovery Management

Members of this management role group can perform searches of mailboxes in the Exchange organization for data that meets specific criteria.

Assigned Roles

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

Members

- [QA-Admin account] Ahsay QA
- Ahsay Services Demo
- aaaaa

- iv. Click the **+** icon under the **Roles** section. These are the following roles:
- ApplicationImpersonation
 - Legal Hold
 - Mailbox Import Export
 - Mailbox Search
 - Public Folders

Discovery Management

*Name:
Discovery Management

Description:
Members of this management role group can perform searches of mailboxes in the Exchange organization for data that meets specific criteria.

Write scope:
Default

Roles:
+ -

NAME
ApplicationImpersonation
Legal Hold
Mailbox Import Export
Mailbox Search
Public Folders

Members:
+ -

NAME	DISPLAY NAME
ahsay.qa	[QA-Admin account] Ah...

Save Cancel

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

2.9.4 Granting Permission to Accounts for Creating Backup Set

- Open <https://outlook.office365.com/ecp>
- Log in to the **Office 365** as an account administrator.

Microsoft

Sign in

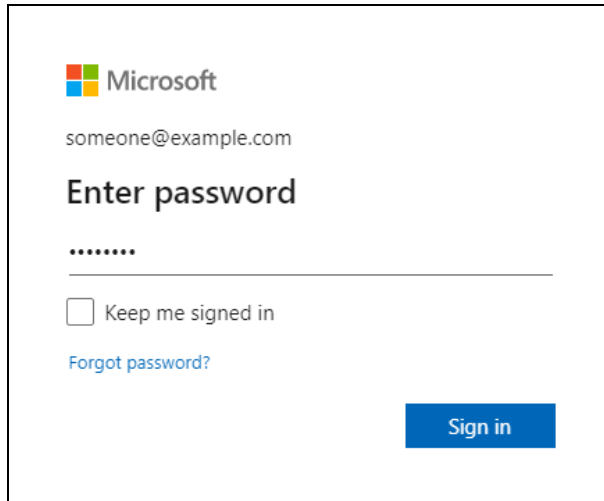
someone@example.com

No account? [Create one!](#)

[Can't access your account?](#)

[Sign-in options](#)

Back Next



Microsoft

someone@example.com

Enter password

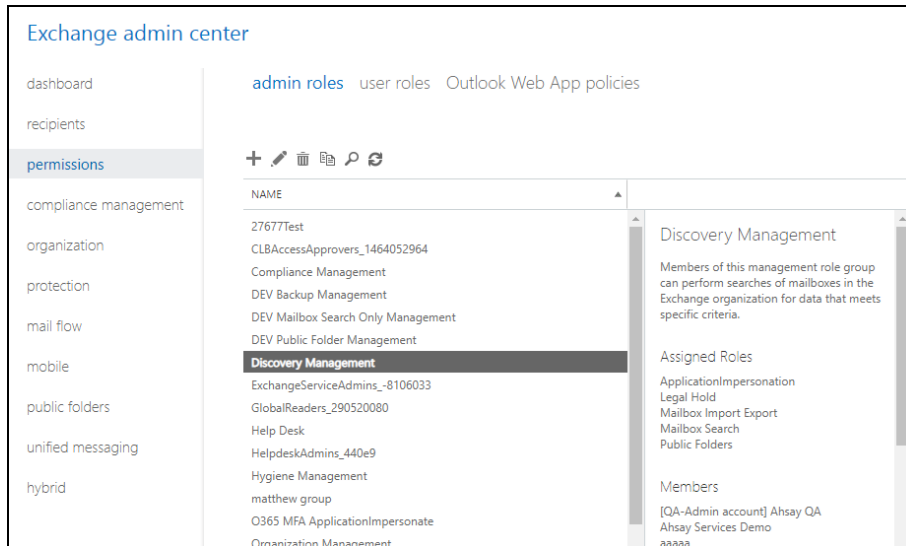
.....

☐ Keep me signed in

[Forgot password?](#)

Sign in

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



Exchange admin center

dashboard recipients **permissions** compliance management organization protection mail flow mobile public folders unified messaging hybrid

admin roles user roles Outlook Web App policies

+ ✎ 🗑️ 📄 🔍 ↺

NAME	
27677Test	
CLBAccessApprovers_1464052964	
Compliance Management	
DEV Backup Management	
DEV Mailbox Search Only Management	
DEV Public Folder Management	
Discovery Management	
ExchangeServiceAdmins_-8106033	
GlobalReaders_290520080	
Help Desk	
HelpdeskAdmins_440e9	
Hygiene Management	
matthew group	
O365 MFA ApplicationImpersonate	
Organization Management	

Discovery Management

Members of this management role group can perform searches of mailboxes in the Exchange organization for data that meets specific criteria.

Assigned Roles

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

Members

- [QA-Admin account] Ahsay QA
- Ahsay Services Demo
- aaaaa

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

Discovery Management

*Name:

Description:
 Members of this management role group can perform searches of mailboxes in the Exchange organization for data that meets specific criteria.

Write scope:

Roles:
 + -

NAME
ApplicationImpersonation
Legal Hold
Mailbox Import Export
Mailbox Search
Public Folders

Members:
 + -

NAME	DISPLAY NAME
exchange-administrator-02	[QA single 15GB file in On...
ahsay.qa	[QA-Admin account] Ahs...
[REDACTED]	[QA-Auto] [REDACTED]
user01	[QA-DataType] user01
qa.test.admin	[QA] qatest admin

Save Cancel

- 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.

NAME	DISPLAY NAME
performance-10000mails-user0006	[QA] File100000
performance-10000mails-user0007	[QA] 10000mails-user0007
performance-10000mails-user0008	[QA] 10000mails-user0008
performance-3MBAttachment-user0001	[QA] 3MBAttachment-user0001
performance-3MBAttachment-user0002	[QA] 3MBAttachment-user0002
performance-3MBAttachment-user0003	[QA] 3MBAttachment-user0003
performance-3MBAttachment-user0004	[QA] 3MBAttachment-user0004
performance-3MBAttachment-user0005	[QA] 3MBAttachment-user0005
performance-3MBAttachment-user0006	[QA] 3MBAttachment-user0006
performance-3MBAttachment-user0007	[QA] 3MBAttachment-user0007
performance-3MBAttachment-user0008	[QA] 20095files

1 selected of 500 total

add ->

OK Cancel

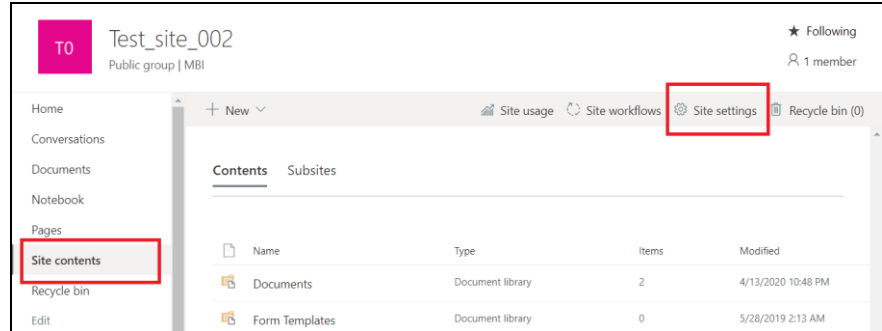
- vi. Click **Save** to confirm and exit the setting.

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

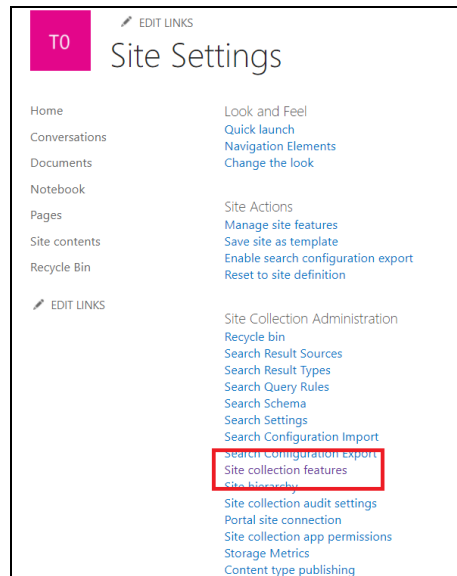
To successfully restore all share link types to alternate location of the same organization in Office 365, follow the settings below:

- Allowing anonymous users to access application pages

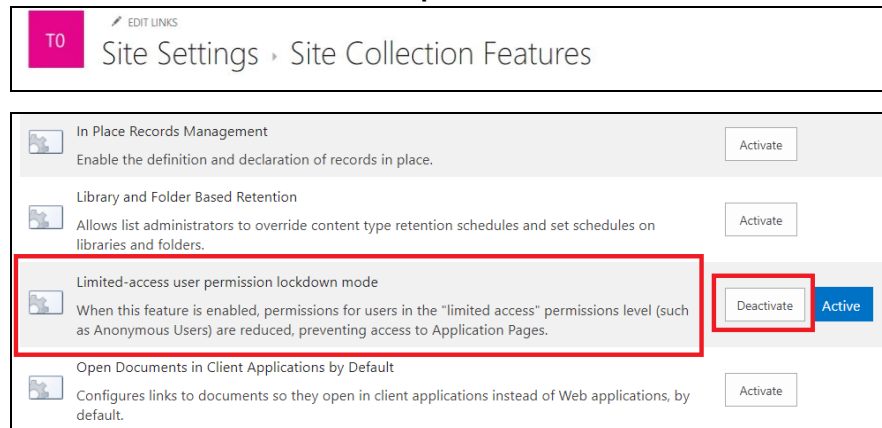
- i. Go to the alternate Site > in the left pane, select **Site Contents > Site Settings**



- ii. Go to **Site Collection features**

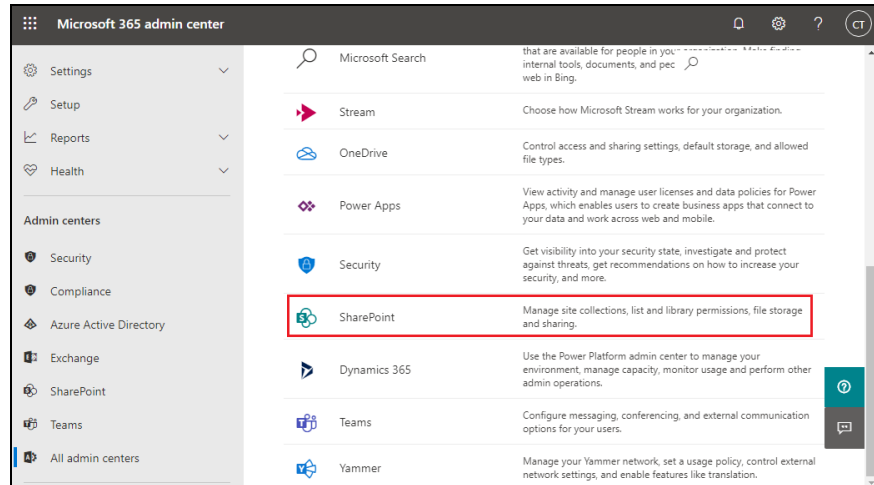


- iii. Deactivate “**Limited-Access user permission lockdown mode**” feature

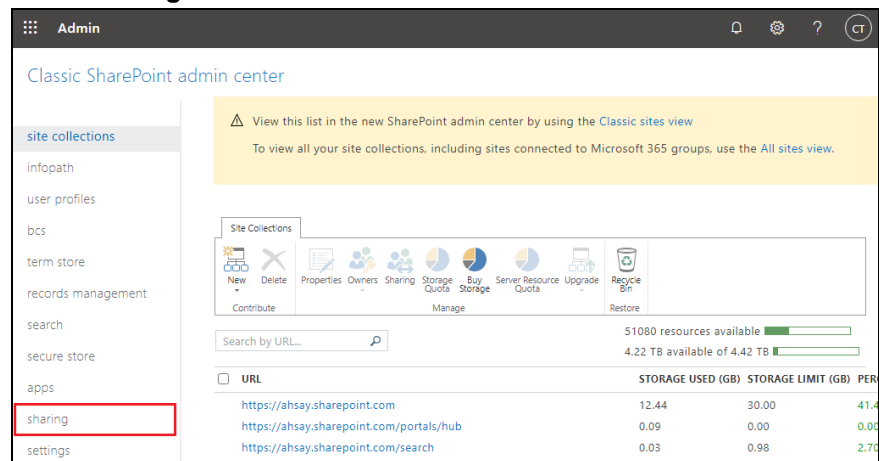


⦿ Allowing sharing to external users

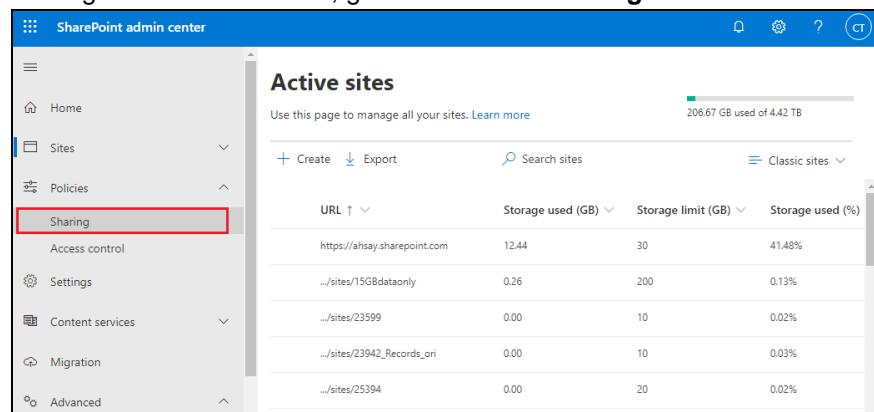
- i. Go to your **Microsoft 365 Admin Center > All admin centers >** in the right pane select **SharePoint**



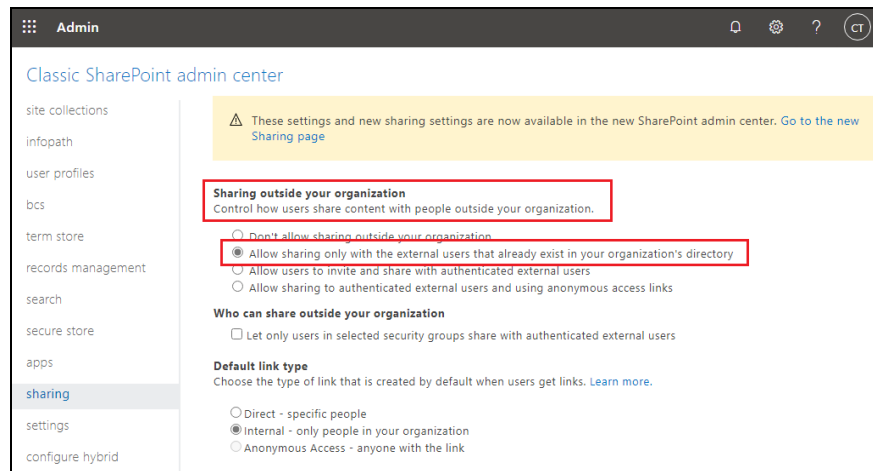
- ii. Go to **Sharing**



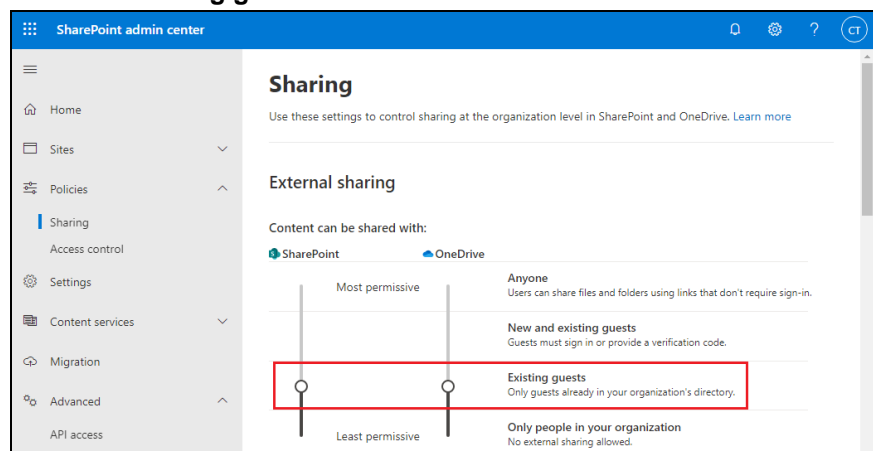
If using **Classic sites view**, go to **Policies > Sharing**.



- 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**.



2.10 Office 365 Permission Requirements for AhsayACB

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

- **Global Admin Role**

Starting with AhsayCBS 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. 2.10.1](#).

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

The **Discovery Management** security group must be assigned the following roles. To assign the role, please refer to [Ch. 2.10.2](#).

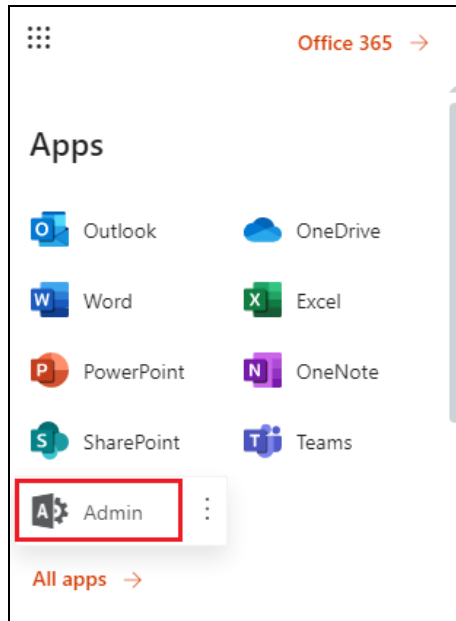
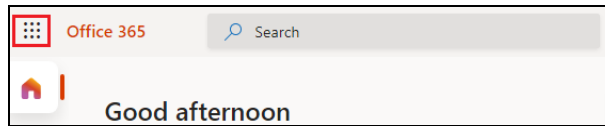
- Mailbox Search
- Public Folders

Otherwise, proceed to grant all necessary permissions to the Office user account as shown in the following chapters [2.10.1](#), [2.10.2](#) and [2.10.13](#).

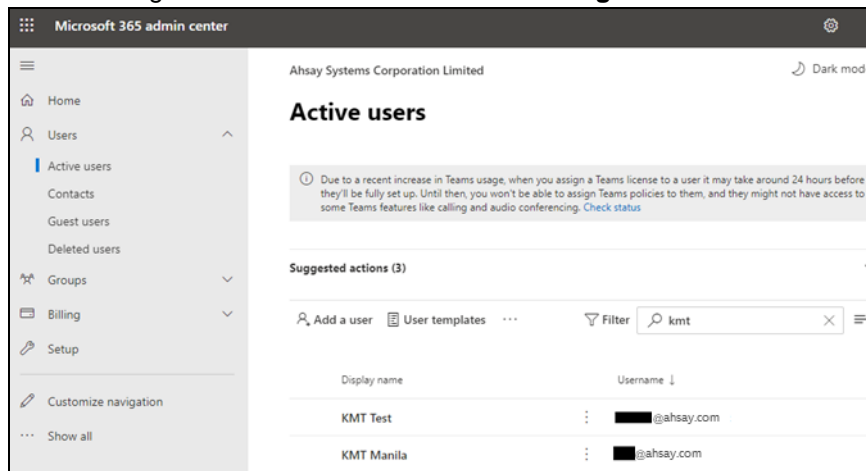
2.10.1 Assigning Global Admin Role to Accounts

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 and select **Manage roles**.



[Reset password](#)
[Block sign-in](#)
[Delete user](#)

[Account](#)
[Devices](#)
[Licenses and Apps](#)
[Mail](#)
[OneDrive](#)

Username
@ahsay.com
[Manage username](#)

Last sign-in
 No attempts in last 30 days
[View last sign-in](#)

Sign-out ⓘ
 Sign-out of all Office 365 sessions.
[Initiate sign-out](#)

Groups
[Manage groups](#)

Roles
 No administrator access
[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.

Manage roles

Admin roles give users permission to view data and complete tasks in admin centers. Give users only the access they need by assigning the least-permissive role.

[Learn more about admin roles](#)

☐ User (no admin center access)

☒ **Admin center access**

Global readers have read-only access to admin centers, while Global admins have unlimited access to edit all settings. Users assigned other roles are more limited in what they can see and do.

☐ Exchange admin ⓘ

☒ **Global admin** ⓘ

Your org has more than 100 global admins. Global admins are attacked twice as often as other accounts, so you should have fewer than 5. To protect data and devices, assign a limited role instead. [See global admins.](#)

☐ Global reader ⓘ

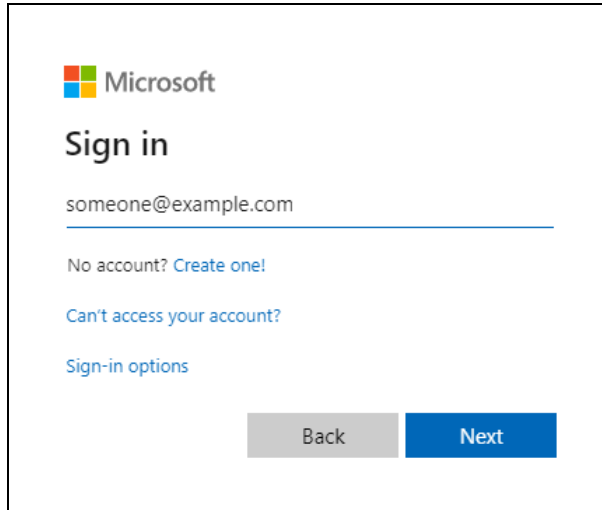
☐ Helndesk admin ⓘ

[Save changes](#)

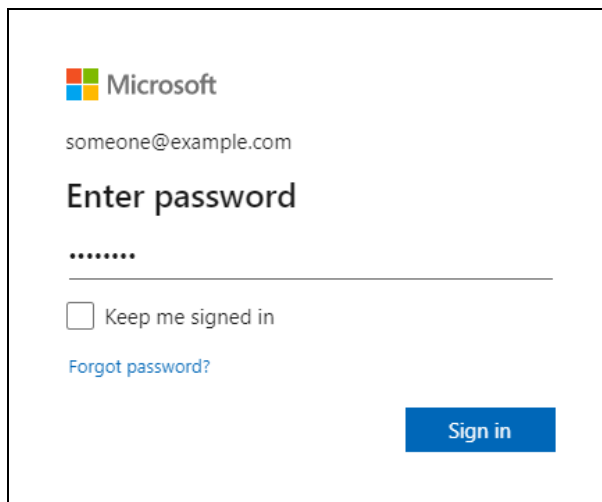
2.10.2 Granting Permission to Discovery Management Group

This permission allows users added under the **Members** section of the **Discovery Management** group (refer to [Ch. 2.10.3](#) for setup) to back up and/or restore user item(s) not only for their own account, but also the accounts of other users in the same **Members** section.

- i. Open <https://outlook.office365.com/ecp>
- ii. Log in to the **Office 365** as an account administrator.

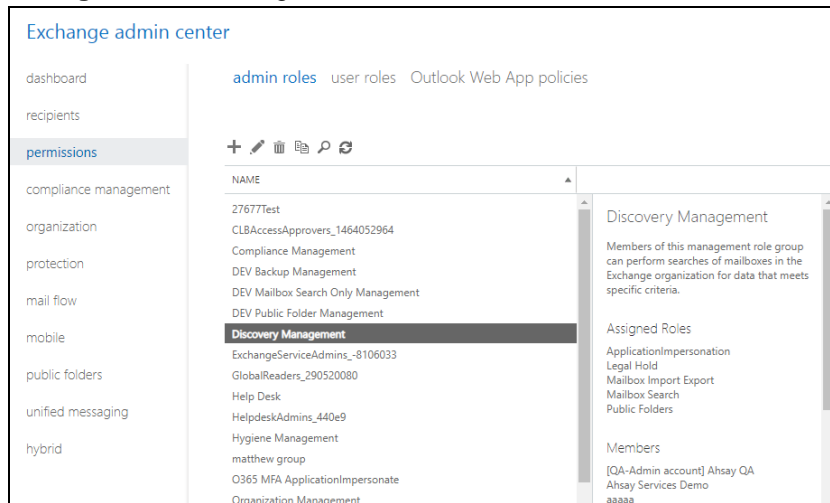


The image shows the Microsoft sign-in page. At the top is the Microsoft logo. Below it is the text "Sign in". There is a text input field containing "someone@example.com". Below the input field are three links: "No account? Create one!", "Can't access your account?", and "Sign-in options". At the bottom are two buttons: "Back" (grey) and "Next" (blue).



The image shows the Microsoft "Enter password" screen. At the top is the Microsoft logo. Below it is the text "Enter password". There is a text input field with masked characters ".....". Below the input field is a checkbox labeled "Keep me signed in". Below the checkbox is a link "Forgot password?". At the bottom right is a blue button labeled "Sign in".

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



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

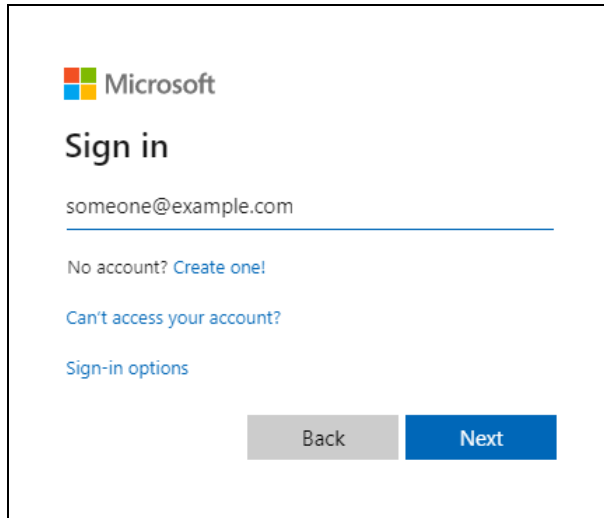
- Mailbox Search
- Public Folders

The screenshot shows the 'Discovery Management' configuration window. The 'Name' field is 'Discovery Management'. The 'Description' field contains the text: 'Members of this management role group can perform searches of mailboxes in the Exchange organization for data that meets specific criteria.' The 'Write scope' is set to 'Default'. The 'Roles' section is expanded, showing 'Mailbox Search' and 'Public Folders' roles. The 'Members' section shows a list of users, including 'ahsay.qa'.

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

2.10.3 Granting Permission to Accounts for Creating Backup Set

- i. Open <https://outlook.office365.com/ecp>
- ii. Log in to the **Office 365** as an account administrator.



Microsoft

Sign in

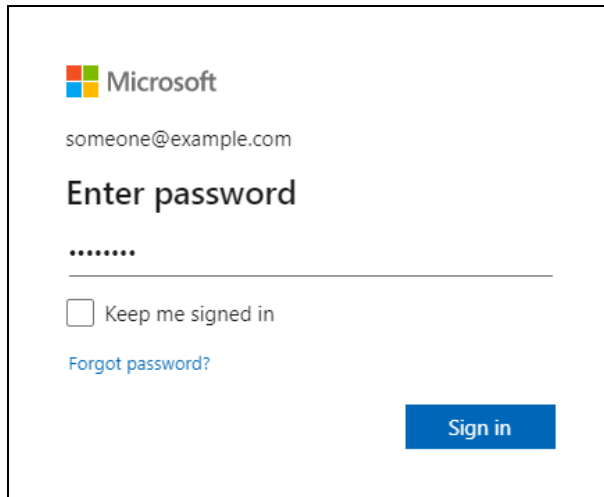
someone@example.com

No account? [Create one!](#)

[Can't access your account?](#)

[Sign-in options](#)

[Back](#) [Next](#)



Microsoft

someone@example.com

Enter password

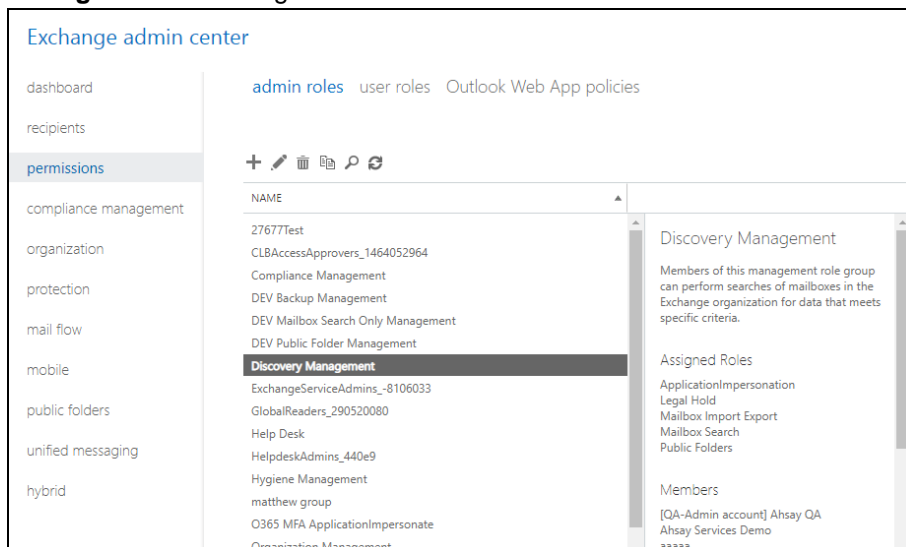
.....

☐ Keep me signed in

[Forgot password?](#)

[Sign in](#)

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



Exchange admin center

dashboard recipients **permissions** compliance management organization protection mail flow mobile public folders unified messaging hybrid

admin roles user roles Outlook Web App policies

+ ✎ 🗑️ 🔍 ↺

NAME
27677Test
CLBAccessApprovers_1464052964
Compliance Management
DEV Backup Management
DEV Mailbox Search Only Management
DEV Public Folder Management
Discovery Management
ExchangeServiceAdmins_-8106033
GlobalReaders_290520080
Help Desk
HelpdeskAdmins_440e9
Hygiene Management
matthew group
O365 MFA ApplicationImpersonate
Organization Management

Discovery Management

Members of this management role group can perform searches of mailboxes in the Exchange organization for data that meets specific criteria.

Assigned Roles

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

Members

- [QA-Admin account] Ahsay QA
- Ahsay Services Demo
- aaaaa

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

Discovery Management

*Name:

Description:

Members of this management role group can perform searches of mailboxes in the Exchange organization for data that meets specific criteria.

Write scope:

Roles:

NAME

Mailbox Search

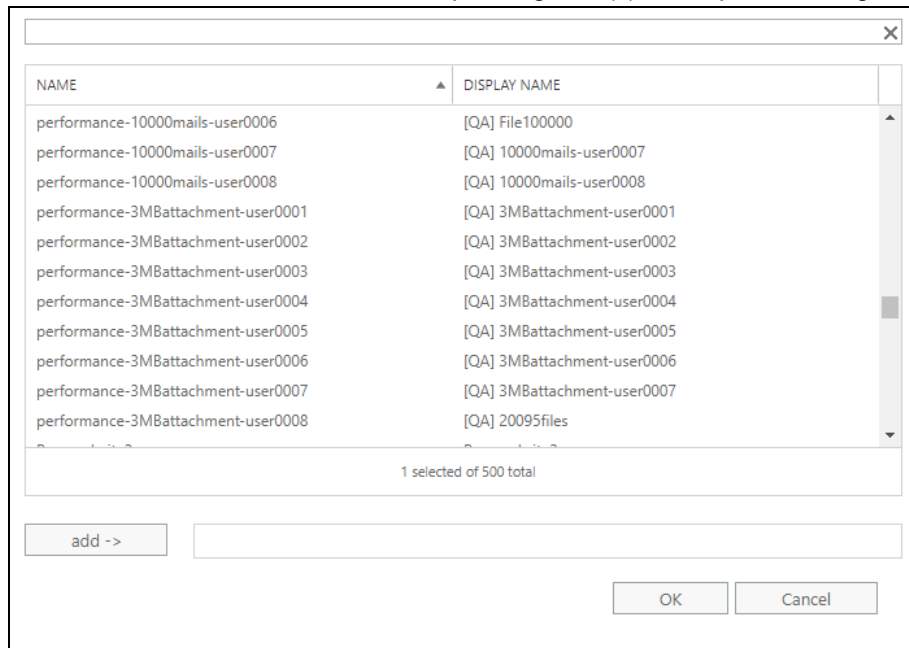
Public Folders

Members:

Save

Cancel

- 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.

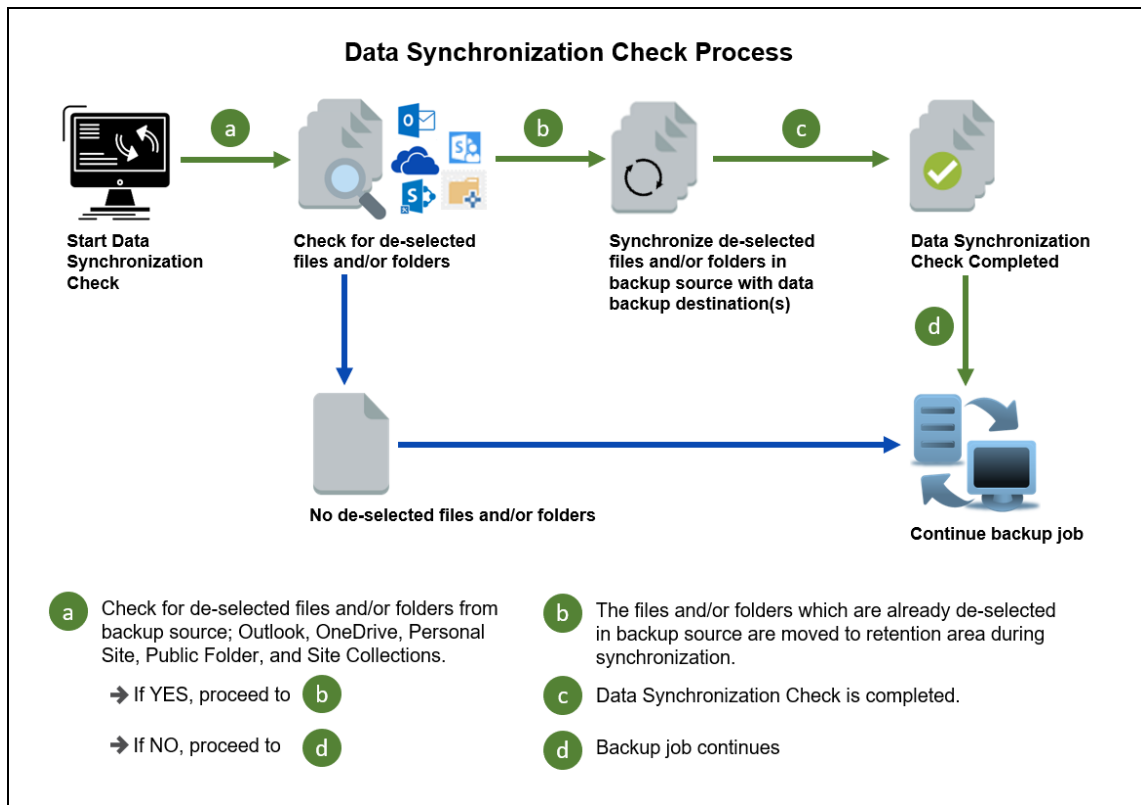
2.11 Data Synchronization Check (DSC) Setup

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 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 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	<p>Since data synchronization check is enabled, it will only run on the set interval. For example, the default number of interval is 60 days.</p> <p>The backup time for the data synchronization job which is trigger every 60 days by default 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).</p>	<p>As data synchronization check is disabled, the backup time will be not be affected.</p>
Storage	<p>Management of storage quota will be more efficient as it will detect items that are de-selected and move it to retention and will be removed after it exceeds the retention policy freeing up the storage quota.</p>	<p>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).</p>



2.12 SharePoint Requirement

2.12.1 SharePoint Set Backup for AhsayOBM

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.

2.12.2 SharePoint Personal Site Backup for AhsayACB

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

2.13 Authentication

To comply with Microsoft's product roadmap for Office 365, from AhsayCBS 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 AhsayCBS v8.3.6.0 can be migrated to Hybrid Authentication or Modern Authentication. However, once the authentication process is completed, the authentication can never be reverted back to Basic Authentication. For more information on how to migrate to Hybrid Authentication or Modern Authentication please refer to [Appendix G: Migrating Authentication of Office 365 Backup Set](#). After the upgrade to AhsayCBS 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.
- 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 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.**

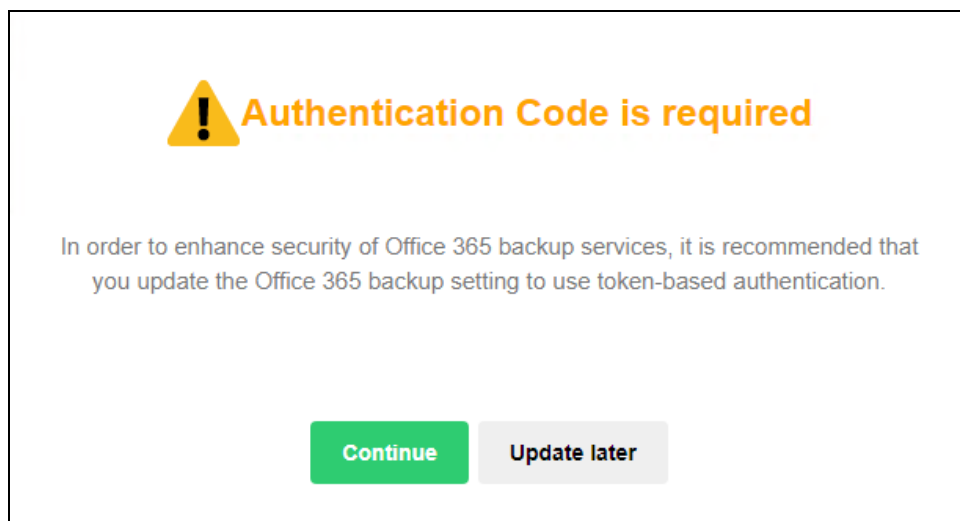
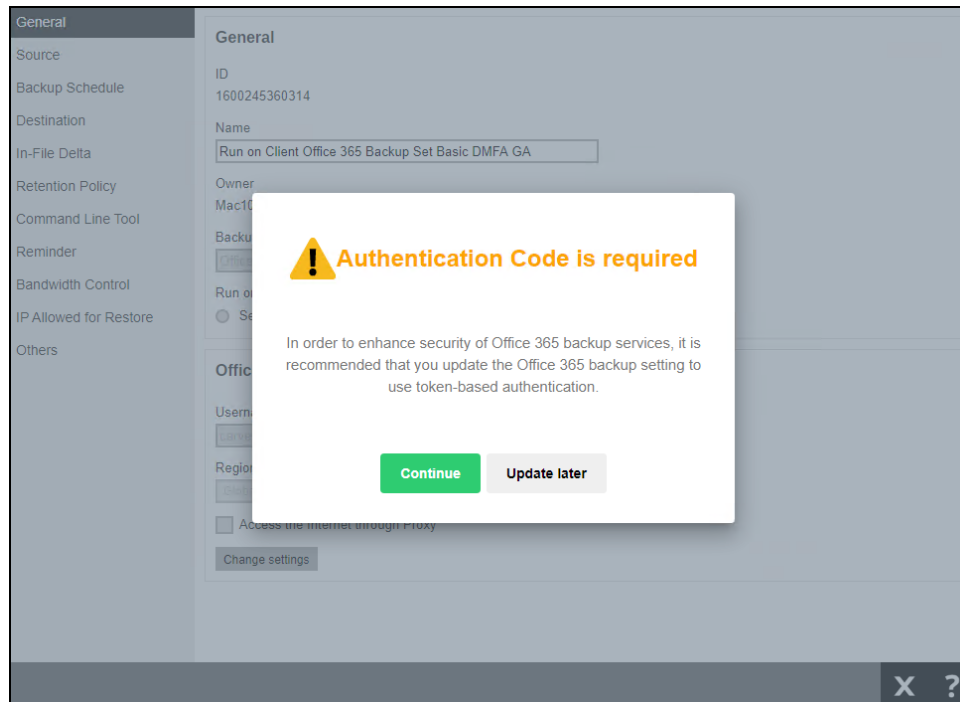
NOTE

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.**

The screenshot shows the 'General' settings page for a backup set. On the left is a sidebar with a list of settings: General (selected), Source, Backup Schedule, Destination, In-File Delta, Retention Policy, Bandwidth Control, and Others. The main content area is titled 'General' and contains the following fields:

- ID: 1600163242929
- Name: Run on Server Office 365 Backup Set Basic to Modern DMFA
- Owner: -
- Backup set type: Office 365 Backup
- Run on: ☒ Server ☐ Client

Below these fields is a section titled 'Office 365' with the following fields:

- Username: [redacted]@ahsay.onmicrosoft.com
- Region: Global (dropdown menu)
- ☐ Access the Internet through Proxy
- Change settings button

At the bottom right of the window, there are 'X' and '?' icons.

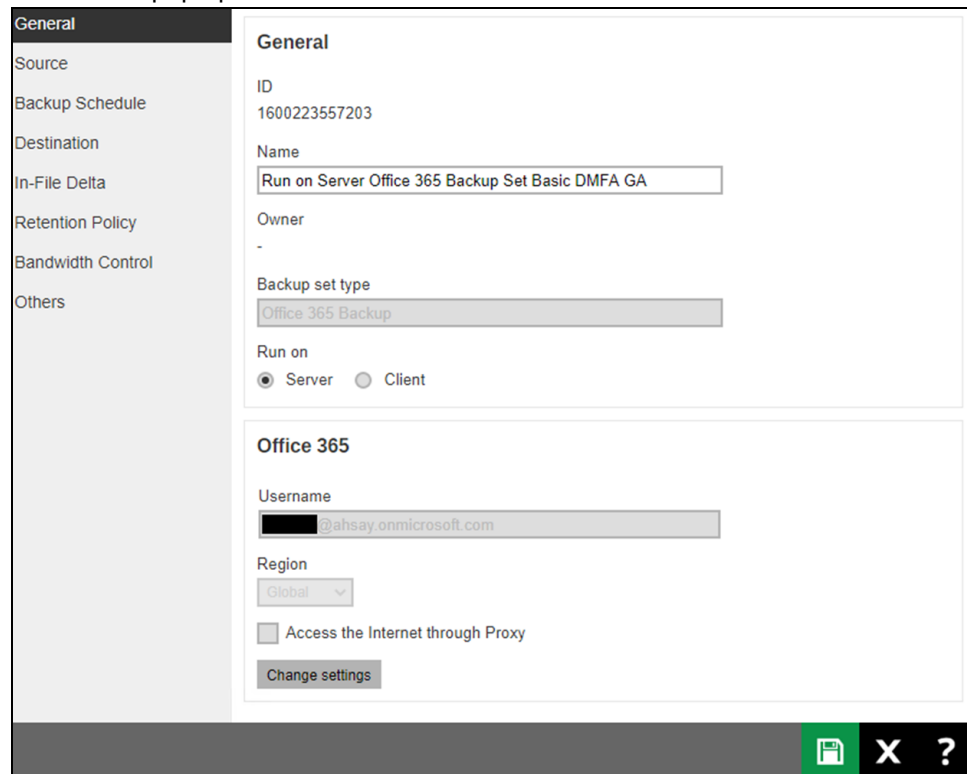
In the Office 365 credentials page, the region is Global and the Username exists but has no Account password, then the backup set is using Modern Authentication.

The screenshot shows the 'Office 365' credentials page. It contains the following fields:

- Username: [redacted]@ahsay.onmicrosoft.com
- Account password: [empty text box]
- App password: (Required if Multi-Factor Authentication is enforced) [empty text box]
- Region: Global (dropdown menu)
- ☐ Access the Internet through Proxy

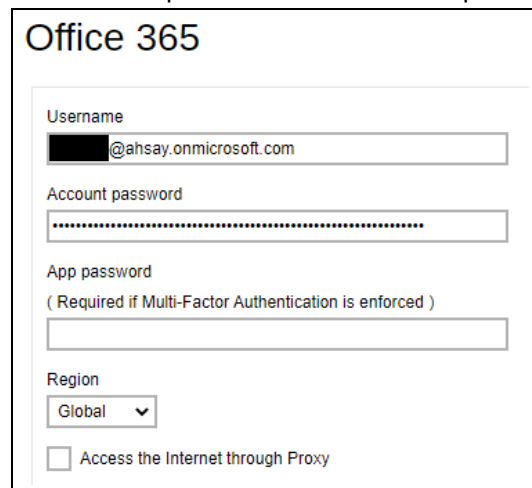
Hybrid Authentication

1. There is no pop up authentication alert.



The screenshot shows a web-based configuration interface. On the left is a sidebar with a menu: General, Source, Backup Schedule, Destination, In-File Delta, Retention Policy, Bandwidth Control, and Others. The 'General' tab is selected. The main content area is divided into two sections. The top section, titled 'General', contains fields for ID (1600223557203), Name (Run on Server Office 365 Backup Set Basic DMFA GA), Owner (-), Backup set type (Office 365 Backup), and Run on (Server selected, Client unselected). The bottom section, titled 'Office 365', contains fields for Username (redacted@ahsay.onmicrosoft.com), Region (Global), a checkbox for 'Access the Internet through Proxy' (unchecked), and a 'Change settings' button. At the bottom right of the interface are icons for save, close, and help.



















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.















The screenshot shows the 'Office 365' credentials page. It has a title 'Office 365' at the top. Below it are input fields for Username (redacted@ahsay.onmicrosoft.com), Account password (masked with dots), and App password (with a note: '(Required if Multi-Factor Authentication is enforced)'). There is also a Region dropdown menu set to 'Global' and an unchecked checkbox for 'Access the Internet through Proxy'.

2.14 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.

Office 365			
Services	Supported?	Services	Supported?
 Outlook		 Yammer	
 OneDrive		 Microsoft Stream	
 Personal Site		 Power BI	
 Site Collections		 Microsoft Power Apps	
 Microsoft Teams			

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

<div>  </div> <div>Outlook Mailbox</div>			
Item	Supported?	Item	Supported?
Archive Mailbox		Distribution Group	
Dynamic Distribution Group		Equipment Mailbox	
Office 365 Group		Public Folder	
Public Folder Mailbox		Room Mailbox	
Security Group		Shared Mailbox	
User Mailbox			
Notes			
1	For backing up Shared Mailbox on ACB, it is required to set a password to the Shared Mailbox on Office 365 portal, such that it can be logged in on ACB to create backup set		
2	For backing up Public Folder, a licensed Exchange Administrator or a licensed user with Public Folder permission is required		

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










Folder Level

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.

<div> OneDrive</div>			
Item	Supported?	Item	Supported?
Folders		Files	
Access Permissions		Albums	
Recycle Bin		Tag	

















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

<div>  </div> <div>Site Collections / Personal Site</div>			
Item	Supported?	Item	Supported?
Announcements		Assets Libraries	
Bright Banner		Calendar	
Contacts		Custom Lists	
Data Connection Libraries		Discussion Boards	
External Lists		Form Libraries	
General Settings	1	Import Spreadsheets	
Issue Tracking		Links	
Look and Feel	2	Manage Site Features	
Newsfeed		Permissions and Management	3
Picture and Libraries		Report Libraries	
Site Collection Features		Site Page	
Survey		Version History	3
Wiki / Page Libraries			
Notes			
	1	For the General Settings, only the List Name can be restored.	
	2	For the Look and Feel, only the Title can be restored.	
	3	For the Version History and Permissions and Management, the backup and restore are supported for OneDrive files and SharePoint documents (Document Library) only.	

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

SharePoint Site Level Collection			
Item	Supported?	Item	Supported?
Team Site		Team Site (Classic Experience)	
Blog		Project Site	
Developer Site		Community Site	
Document Center		eDiscovery Center	
Records Center		Business Intelligence Center	
Compliance Policy Center		Enterprise Search Center	
Community Portal		Basic Search Center	
Visio Process Repository		Enterprise Wiki	
Publishing Portal		Modern Communication Site	
Modern Team Sites			

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	
MeetingCancellation MessageType		MeetingMessageType	
MeetingRequestMessa geType		MeetingResponseMess ageType	
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	





2.15 Maximum Supported File Size

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

2.15.1 AhsayOBM

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

2.15.2 AhsayACB

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

2.16 Limitations

2.16.1 AhsayOBM

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 back up only if he/she is assigned as a site admin of that site collection. Feature setting for SharePoint Site and Personal Site.
 - 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 (e.g. 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 de-select 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 filter feature

Restore filter using AhsayCBS User Web Console is not yet supported.

• Restore to Local machine

Restore to Local Machine is not supported using AhsayCBS User Web Console. It is only available using AhsayOBM and AhsayACB.

• Restore to Alternate location

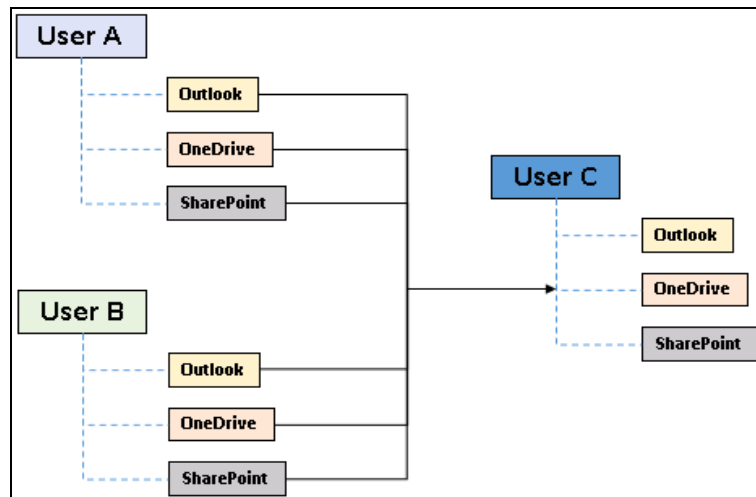
- Only administrator account or user account with administrative authority can restore backup items to an alternate location.
- If you are trying to restore item(s) from one user to an alternate location user, AhsayOBM will restore the item(s) to their respective destination folder(s) with the same name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

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

- **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.

- **Command Line Tool**

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

In the AhsayCBS Run on Server (Agentless) backup, this feature is not supported.

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.

2.16.2 AhsayACB

Ahsay Limitations

• Supports Backup up to 2 accounts

Each AhsayACB backup user account supports backup of a maximum of **TWO** Office 365 personal accounts.

Consider using AhsayOBM instead if you wish to back up for more than two Office 365 accounts. Contact your backup service provider for further details. Click here to read the [AhsayOBM v8 User Guide - Office365 Backup & Restore for Windows](#).

• Modern Authentication

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

- **OneDrive**

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

- **Outlook**

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

Microsoft Limitations

- **OneDrive**

For more detailed information on the limitations of OneDrive, please refer to this Microsoft article, [OneDrive Limits](#). These are some of the limitations that will be discussed in the OneDrive Limits article:

- File upload size which is 15GB for OneDrive
- File name and path lengths
- Thumbnails and previews
- Number of items to be synced
- Information rights management
- Differential sync
- Libraries with specific columns
- Windows specific limitations

2.16.3 AhsayCBS Run on Server (Agentless)

- **Standard and Local Destination Settings**

For the backup destination settings, only the AhsayCBS or predefined destination is supported in the AhsayCBS Run on Server (Agentless) backup.

It is not possible to assign other standard destinations such as the customers personal Google Drive, OneDrive, DropBox, Amazon S3, Azure, and other storage accounts as the backup destination for a Run on Server backup set.

- **Reminder**

The reminder feature is not supported in the AhsayCBS User Web Console. Unlike with the agent-based backup, when this feature is enabled, a backup confirmation dialog box will prompt the user to run a backup job during machine log off, restart, or shut down when AhsayOBM/AhsayACB is installed on a Windows platform.

- **IP Allowed for Restore**

This setting permits to predefine IP ranges that are allowed to perform restore as configured by the system administrator. This feature is only applicable in a Run on Client Office 365 restore operation and is not supported in a Run on Server Office 365 restore.

- **Decrypt Backup Data**

Decrypt backup data feature is used to restore raw data by using the data encryption key that was set for the backup set. This feature is only applicable in a Run on Client Office 365 Backup Set and is not supported in a Run on Server Office 365 Backup.

- **System Logs**

AhsayOBM/AhsayACB backup user account does not have access to the system logs related to the following operations through the AhsayCBS user console.

- Data Integrity Check
- Space Freeing Up

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

2.17 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 on Run on Server (Agentless).

- **Performance Recommendations**

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

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.

- **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.

- **Recommended Number of Office 365 users on a Backup Set**

To ensure that your Office 365 Run on Server backup set completes the backup job within 24 hours, it is recommended that a single Office 365 Run On Server backup set should not contain more than 2,000 users. That is assuming that only small incremental daily changes will be made on the Run on Server backup set.

- **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**

It is recommended to divide the users into multiple backup sets. A single Office 365 backup set should not contain more than 2,000 Office 365 users. That is assuming that only small incremental daily changes will be made on the Run on Client backup set.

By splitting up all the users into separate backup sets, the more backup sets, the faster the backup process can finish.

It is also a requirement that for every split backup set 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](#).

• 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, e.g. the number of new files created, the number of files which are updated/deleted, and new users may be added etc.

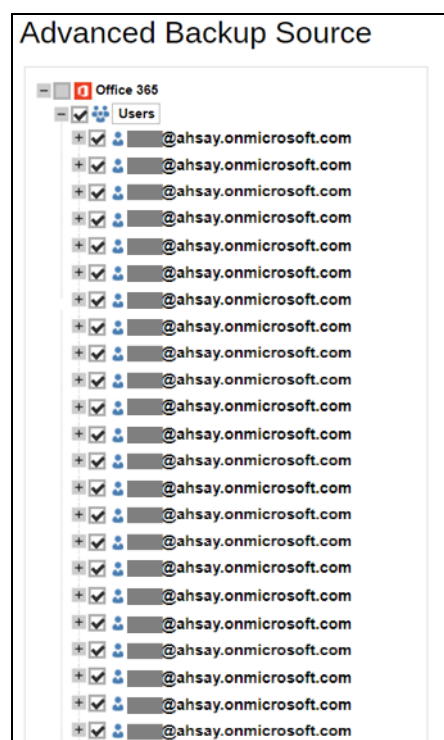
Consider the following key points to efficiently handle backup sets with periodic backup schedule.

- Hardware – to achieve optimal performance, compatible hardware requirements is a must. Ensure you have the backup machine's appropriate hardware specifications to accommodate frequency of backups,
 - so that the data is always backed up within the periodic backup interval
 - so that the backup frequency does not affect the performance of the production server
- Network – make sure to have enough network bandwidth to accommodate the volume of data within the backup interval.
- Retention Policy - also make sure to consider the retention policy settings and retention area storage management which can grow because of the changes in the backup data for each backup job.

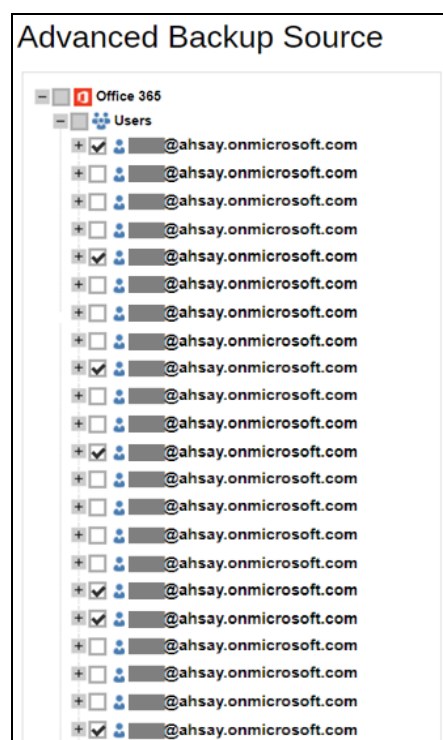
• Backup Source for AhsayOBM

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.

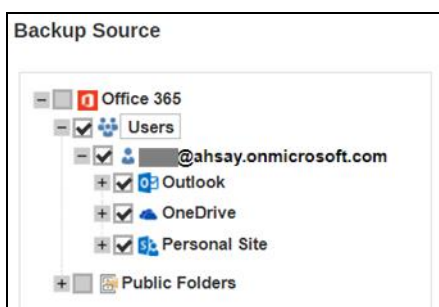
	All Office 365 users	Selective Office 365 user
Backup Set Maintenance	The Admin does not need to manage the backup set, e.g. to select or unselect user when an Office 365 user account is added or removed, the changes are automatically updated in the backup source.	<p>The Admin will have to select or unselect users manually when an Office 365 user account is added or removed, as the changes are not automatically updated in the backup source this can be very time consuming.</p> <p>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.</p> <p>For more details on the backup set maintenance, please see, Appendix D: Example Scenario for Backup Set Maintenance</p>
Office 365 License	<p>The backup user account must have additional Office 365 license modules assigned to cover any increase in 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.</p> <p>For more details on the computation on the required license, please see, Appendix A: Example Scenarios for Office 365 License Requirement and Usage</p>	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	Only selective Office 365 user accounts will be backed up.

	the initial full backup job will take longer, any subsequent incremental backup will take longer.	This will mean the initial 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.
Data Synchronization Check	As all Office 365 user accounts are selected for backup, regular data synchronization check may not be required.	<p>As only selective files and/or folders are selected for backup, data synchronization check is highly recommended to synchronize de-selected files and/or folders in the backup source with the backup destination(s).</p> <p>To know more about the Data Synchronization Check, please refer to Appendix E: Example Scenario for Data Synchronization Check (DSC) with sample backup reports</p>

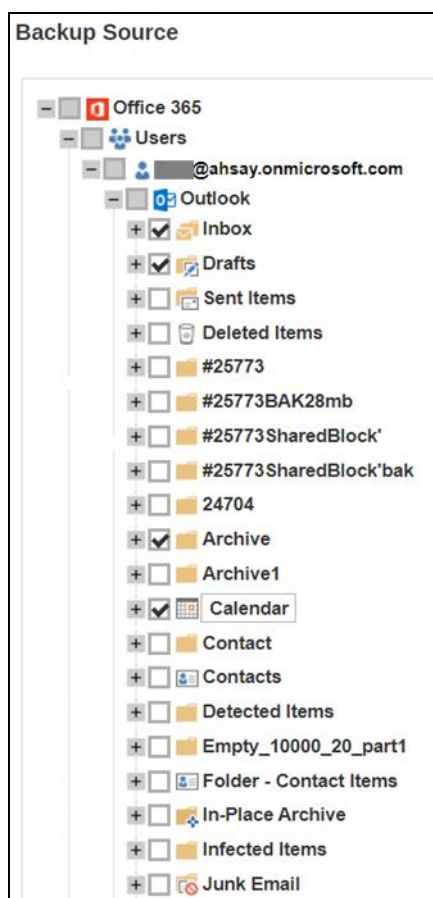
● Backup Source for AhsayACB

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

All Items



Selective Items



● All Items

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

● Selective Items

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

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

	All Items	Selective Items
User Maintenance	The Admin does not need to manage the backup set, e.g. to select or unselect items, the changes are automatically updated in the backup source	The Admin will have to select or unselect items manually as the changes are not automatically updated in the backup source.
Backup Time	All Items of the Office 365 user account will be backed	Only selective Items of the Office 365 user account will

	up. This means the initial full backup job will take longer, any subsequent incremental backup will take longer.	be backed up. This will mean the initial full backup job will be faster, any subsequent incremental backup will be faster.
Storage	As all Items of the Office 365 user account are backed up, more storage will be required.	As only selective items of the Office 365 user account will be backed up, the backup set will require relatively less storage.
Data Synchronization Check	Since an AhsayACB Office 365 backup set only handles 1 or 2 Office 365 accounts and there's no SharePoint, Data Synchronization Check may not be required to run frequently.	<p>Since an AhsayACB Office 365 backup set only handles 1 or 2 Office 365 accounts and there's no SharePoint, and if selective files and/or folders method is selected for backup, it is recommended to keep the data synchronization check enabled to be able to synchronize de-selected files and/or folders in the backup source with the backup destination(s).</p> <p>To know more about Data Synchronization Check, please refer to Appendix E: Example Scenario for Data Synchronization Check (DSC) with sample backup reports</p>

3 Login to AhsayCBS User Web Console

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

- [Login with no 2FA](#)
- [Login with 2FA using Twilio](#)
- [Login with 2FA using Mobile Authentication](#)

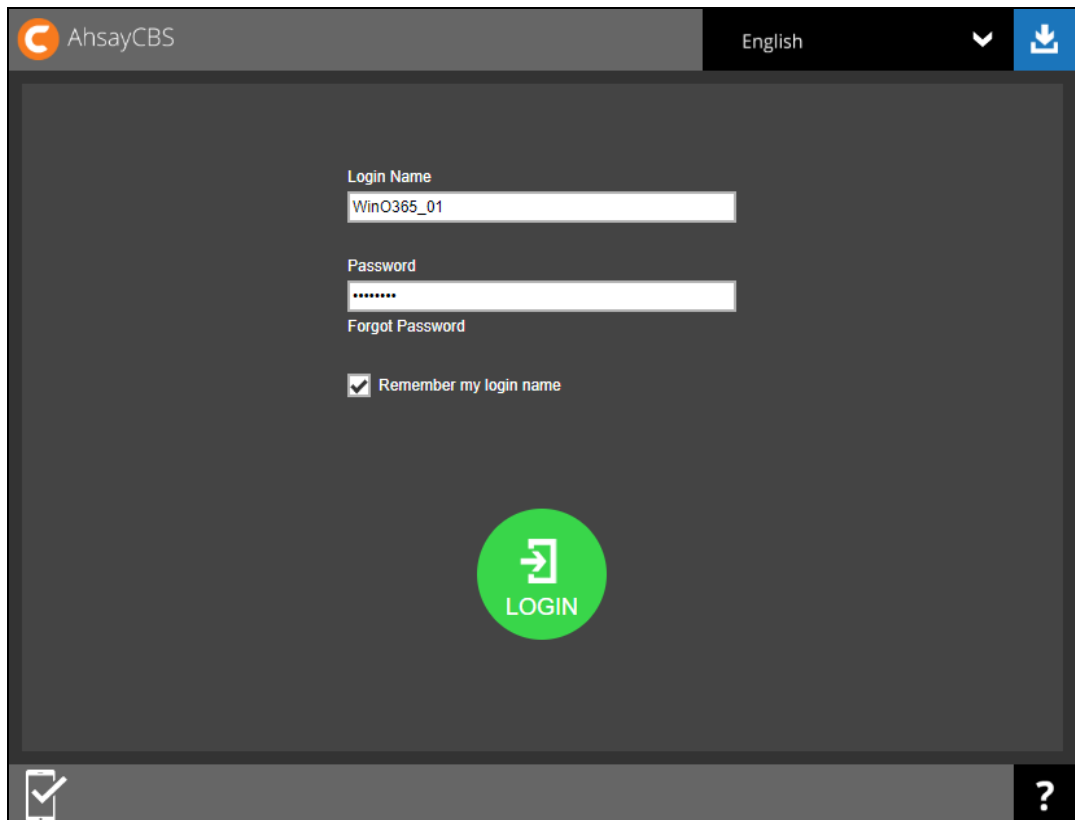
3.1 Login to AhsayCBS with no 2FA

1. Login to the AhsayCBS web console at
https://backup_server_hostname:port

NOTE

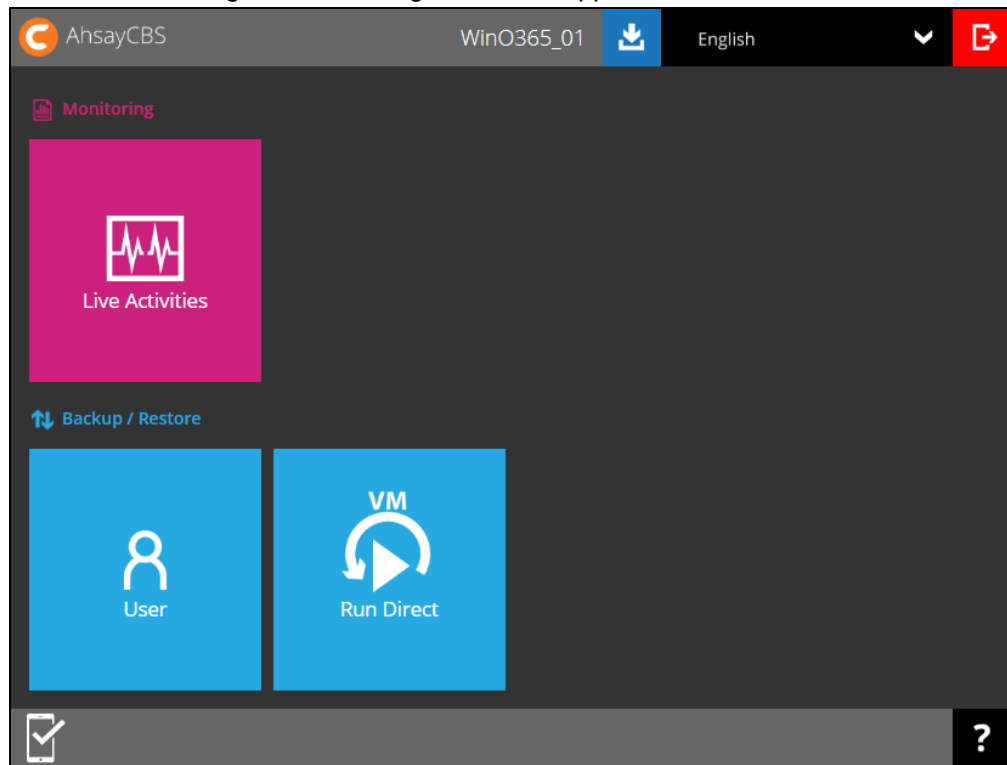
Contact your backup service provider for the URL to connect to the web console if necessary.

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



The screenshot shows the AhsayCBS login web console. At the top, there is a header bar with the AhsayCBS logo on the left, the word "English" in the center, and a download icon on the right. The main content area is dark gray and contains a login form. The form has two input fields: "Login Name" with the text "WinO365_01" and "Password" with masked characters "*****". Below the password field is a link that says "Forgot Password". Underneath the password field is a checkbox labeled "Remember my login name" which is checked. At the bottom center of the form is a large green circular button with a white right-pointing arrow and the word "LOGIN" below it. At the bottom of the page, there is a dark gray footer bar with a mobile device icon on the left and a question mark icon on the right.

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



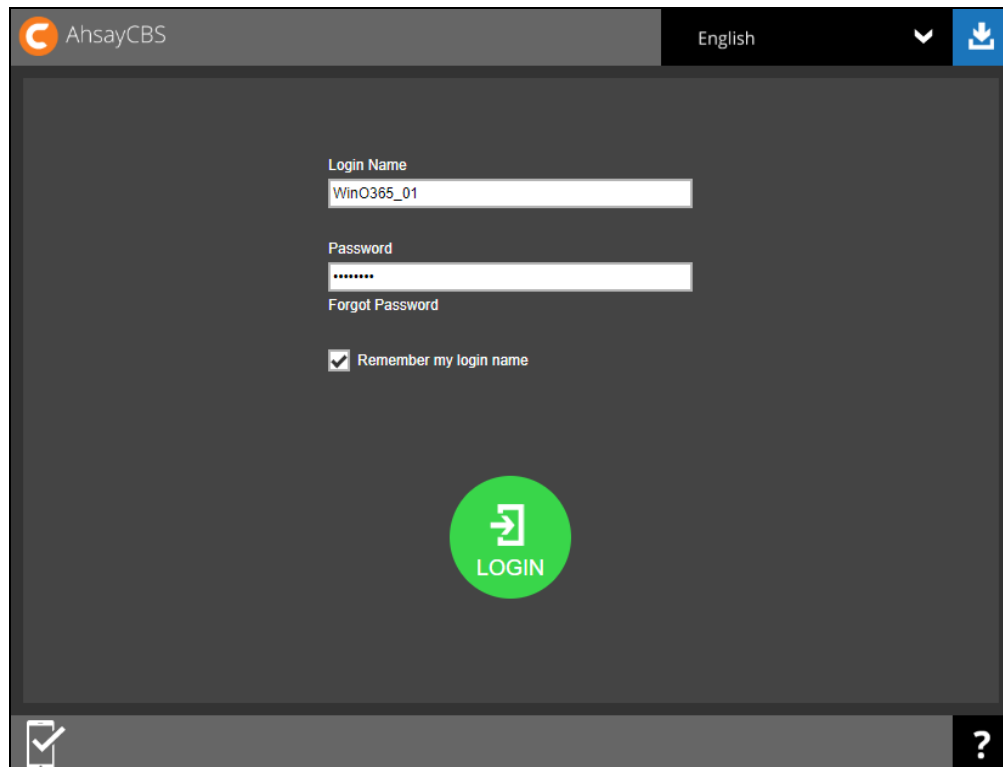
3.2 Login to AhsayCBS with 2FA using Twilio

1. Login to the AhsayCBS web console at
https://backup_server_hostname:port

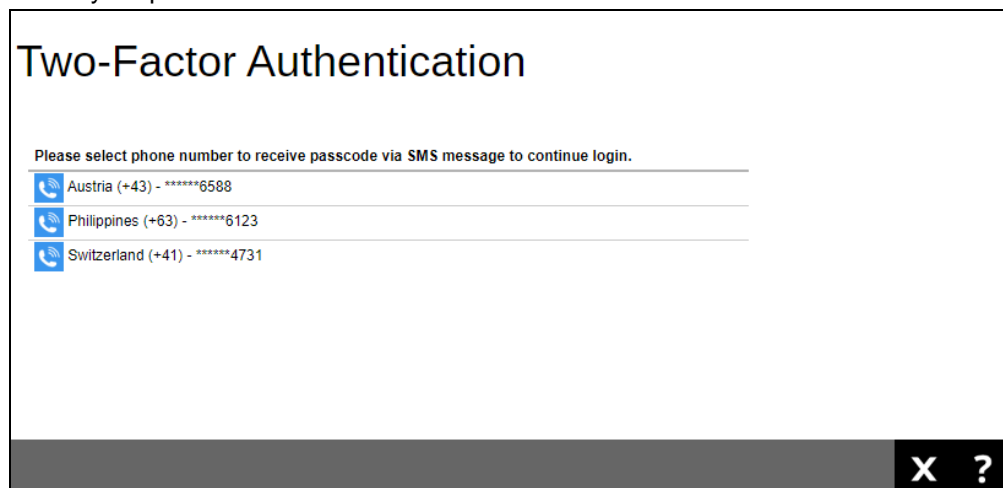
NOTE

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

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



3. Select your phone number.



4. Enter the passcode and Verify to login.

Two-Factor Authentication

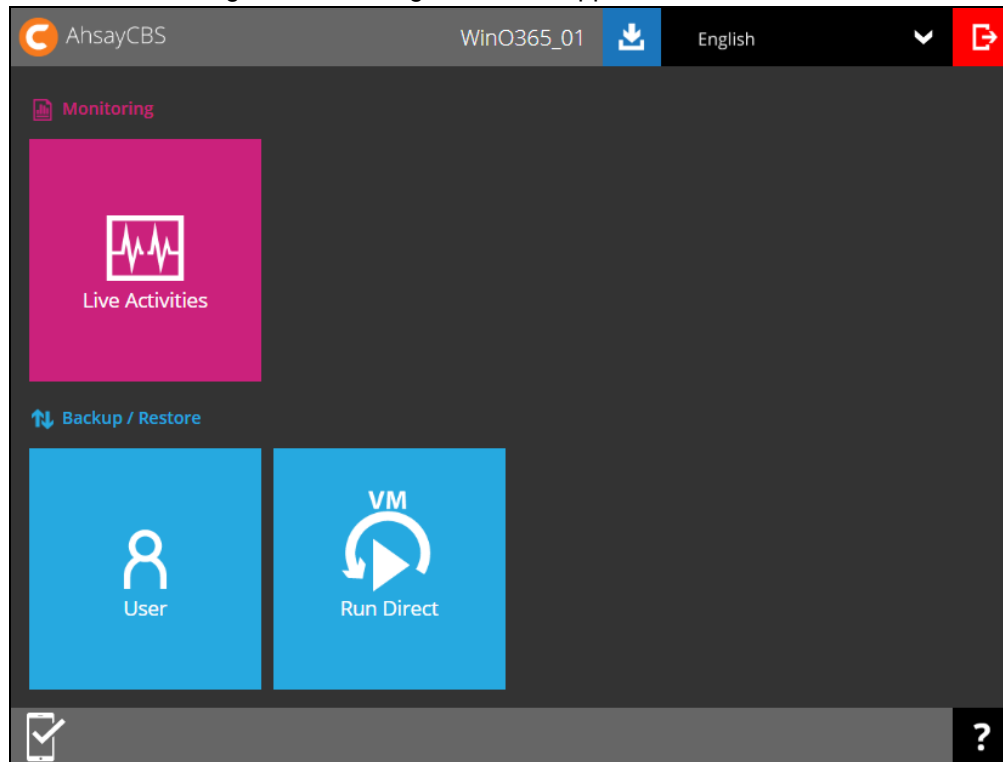
SMS message with a passcode was already sent to the phone number +63-*****6123 Please enter the passcode to continue login.

HQDW - (00:04:54)

[Resend passcode](#)

✓ ✕ ?

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



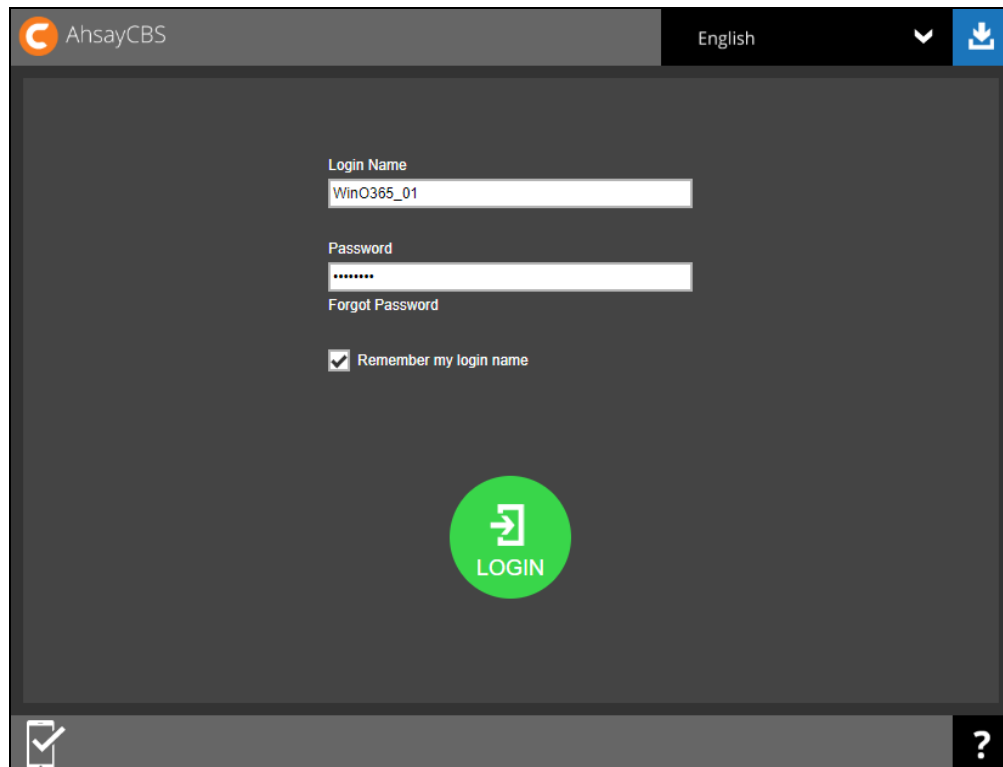
3.3 Login to AhsayCBS with 2FA using Mobile Authentication

1. Login to the AhsayCBS web console at
https://backup_server_hostname:port

NOTE

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

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



3. Click the authentication method you want to use.

Two-Factor Authentication

Please select one Two-Factor Authentication method to continue.



Approve request in Authenticator App from "Galaxy A70"




Input one-time password generated in Authenticator App from "WinO365_01"

[Unable to login/Do not have any Authenticator App\(s\)](#)

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


Two-Factor Authentication


Please approve the notification request in Authenticator App on "Galaxy A70".

 Waiting for response (00:04:57)

[Authenticate with one-time password](#)

[Unable 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 .

Two-Factor Authentication

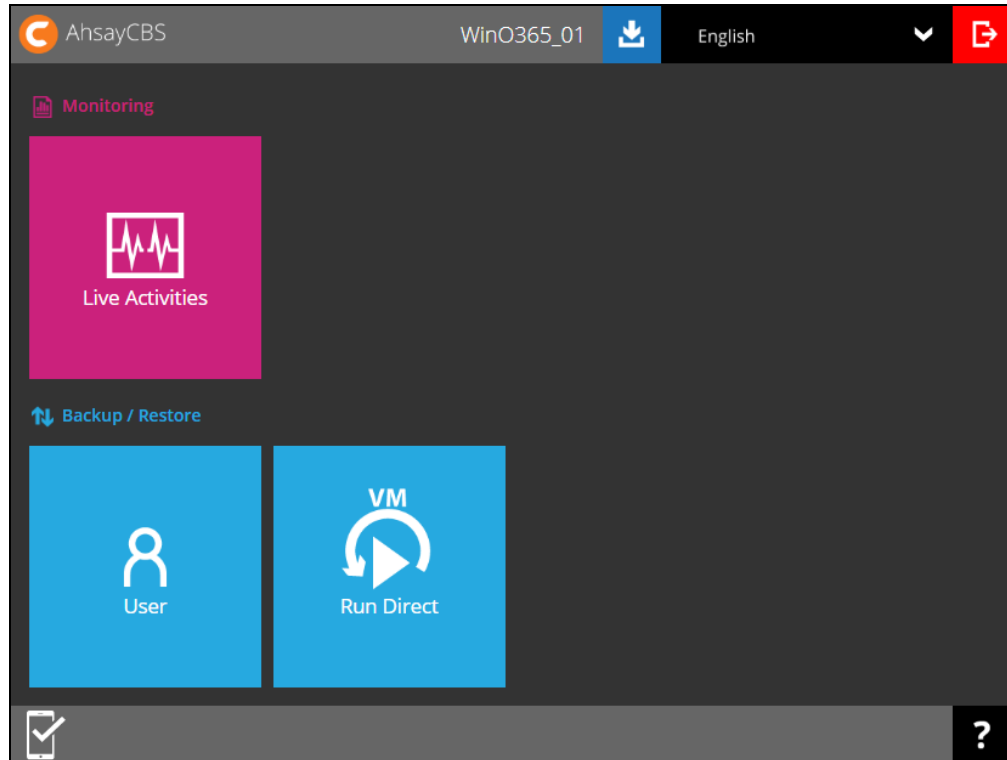
Please input the one-time password generated in Authenticator App from "WinO365_01".

(00:00:16)

[Unable to login](#)



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

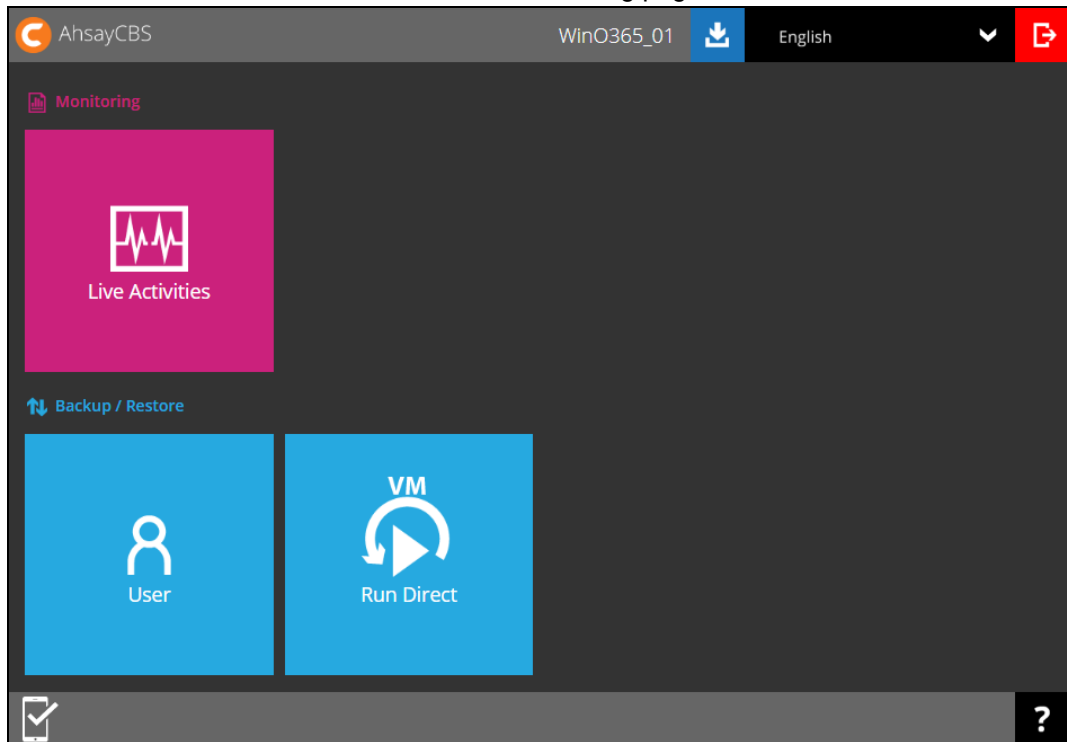


4 Creating an Office 365 Backup Set

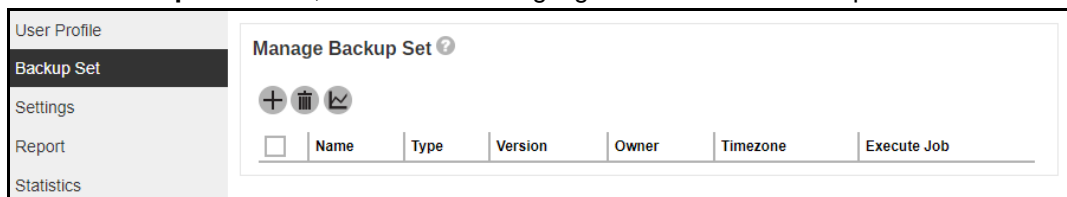
Starting with AhsayCBS v8.3.6.0, Basic Authentication will not be utilized anymore, but instead there are two types of authentication that can be used in creating a backup set namely [Modern Authentication](#) or [Hybrid Authentication](#).

4.1 Modern Authentication

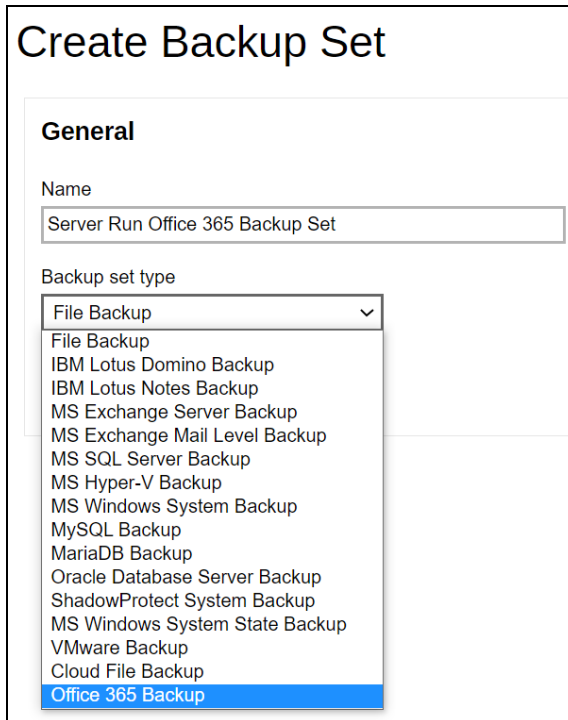
1. Log in to the User Web Console according to the instructions in [Login to AhsayCBS User Web Console](#).
2. Click the User icon on the User Web Console landing page.



3. On the **Backup Set** menu, click the + icon highlighted to create a backup set.



4. Select the type as **Office 365 Backup**, then name the backup set.



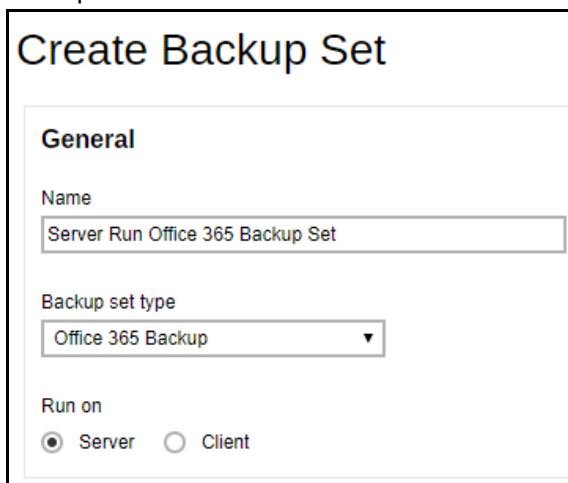
Create Backup Set

General

Name
Server Run Office 365 Backup Set

Backup set type
File Backup
IBM Lotus Domino Backup
IBM Lotus Notes Backup
MS Exchange Server Backup
MS Exchange Mail Level Backup
MS SQL Server Backup
MS Hyper-V Backup
MS Windows System Backup
MySQL Backup
MariaDB Backup
Oracle Database Server Backup
ShadowProtect System Backup
MS Windows System State Backup
VMware Backup
Cloud File Backup
Office 365 Backup

5. On the same menu under **Run on**, select **Server** to create a Run on Server (Agentless) backup set.



Create Backup Set

General

Name
Server Run Office 365 Backup Set

Backup set type
Office 365 Backup

Run on
☒ Server ☐ Client

NOTES

- If you choose to run the backup set on the AhsayCBS server, you won't be able to back up, restore or manage your backups on the AhsayOBM once the backup set is created.
- This setting **CANNOT** be altered once the backup set is created. If you wish to change the backup method later, you will have to create a new backup set and start over the configurations again.
- For backup sets created in **Run on Server** backup type, the backup destination is restricted to either AhsayCBS or a predefined destination (if setup by your backup service provider). If you wish to back up to other cloud destinations or back up to multiple destinations, the backup set should be created in **Run on Client** backup type instead.

To create a backup set using Modern Authentication, leave the **Username** and **Account password** blank and click **Test**.

Create Backup Set

General

Name

Backup set type

Run on
☒ Server ☐ Client

Office 365

Username

Account password


App password
(Required if Multi-Factor Authentication is enforced)

Region

☐ Access the Internet through Proxy

[Sign up for Office 365 Backup](#)

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



This will create Office 365 backup set using modern authentication protocol without backup functionality for SharePoint Web Parts and Metadata.

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

Click [Authorize] and in the pop-up browser window, sign in your Microsoft account and authorize the backup application (if necessary), copy and paste the authorization code to the textbox and hit [OK] to complete the authentication.

Authorize

Cancel

Sign in to your Microsoft account.



Sign in

██████████@ahsay.onmicrosoft.com

No account? [Create one!](#)

[Can't access your account?](#)

[Sign-in options](#)

Back

Next



← ██████████@ahsay.onmicrosoft.com

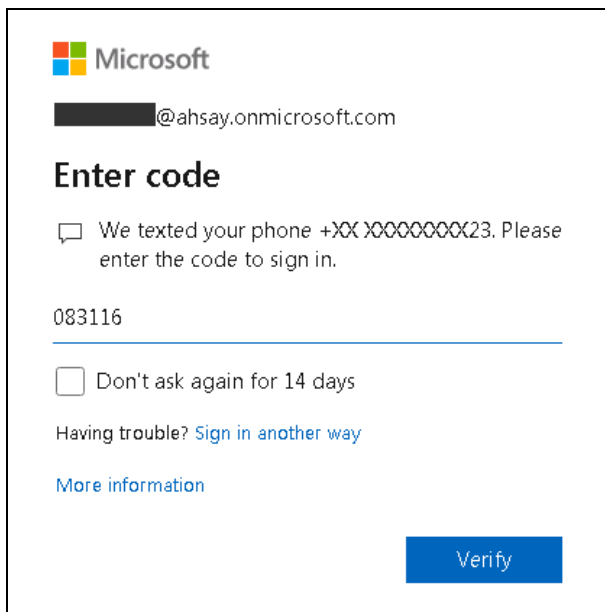
Enter password

.....

[Forgot my password](#)

Sign in

If MFA is enforced, enter the code and click Verify.

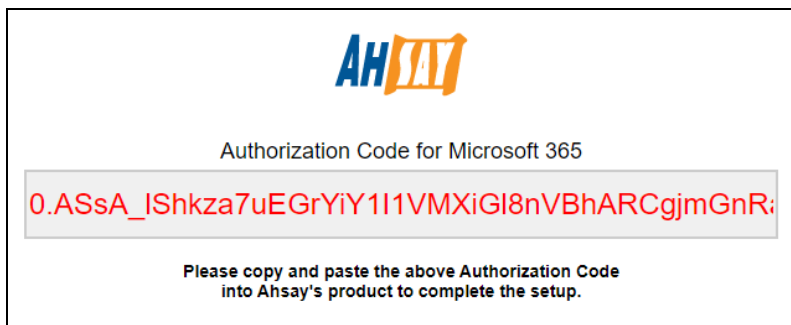


The image shows a Microsoft login interface. At the top is the Microsoft logo. Below it is a blurred email address followed by '@ahsay.onmicrosoft.com'. The heading 'Enter code' is prominent. A message states: 'We texted your phone +XX XXXXXXXX23. Please enter the code to sign in.' Below this, the code '083116' is entered into a text field. There is a checkbox for 'Don't ask again for 14 days'. Links for 'Having trouble? Sign in another way' and 'More information' are present. A blue 'Verify' button is at the bottom right.

NOTE

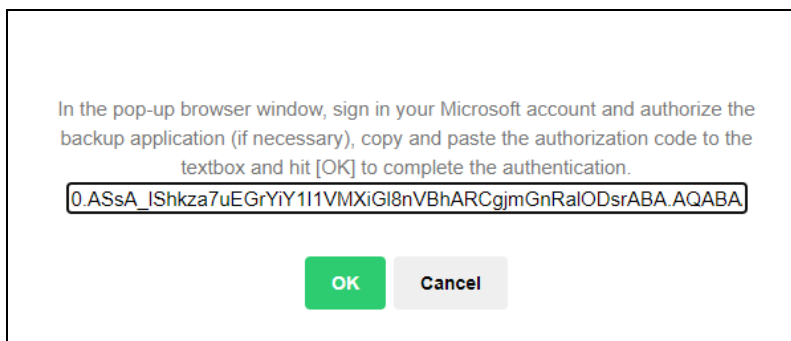
The verification code is only required if the MFA status of an Office 365 account is enforced.

Copy the authorization code.



The image shows an Ahsay interface with the Ahsay logo at the top. Below the logo, it says 'Authorization Code for Microsoft 365'. A red text box contains the authorization code: '0.ASsA_IShkza7uEGrYiY1I1VMXiGI8nVBhARCgjmGnR:'. Below the code, it says 'Please copy and paste the above Authorization Code into Ahsay's product to complete the setup.'

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



The image shows a confirmation dialog box. It contains the text: 'In the pop-up browser window, sign in your Microsoft account and authorize the backup application (if necessary), copy and paste the authorization code to the textbox and hit [OK] to complete the authentication.' Below this text is a text box containing the authorization code: '0.ASsA_IShkza7uEGrYiY1I1VMXiGI8nVBhARCgjmGnRaIODsrABA.AQABA'. At the bottom are two buttons: 'OK' (green) and 'Cancel' (grey).

Test completed successfully is displayed when the validation is successful.

Create Backup Set

General
Name

Backup set type

Run on
☒ Server ☐ Client

Office 365
Username

Account password

App password
(Required if Multi-Factor Authentication is enforced)






Region

☐ Access the Internet through Proxy
✓ Test completed successfully
[Sign up for Office 365 Backup](#)

6. Select the **Backup Source** in this menu. Select the desired Outlook, OneDrive, Personal Site, Public Folders or Site Collections for backup. Check the box will back up all, i.e. check the box of Outlook will back up the mailboxes of all the users.

Backup Source

Select the items and folders that you want to backup

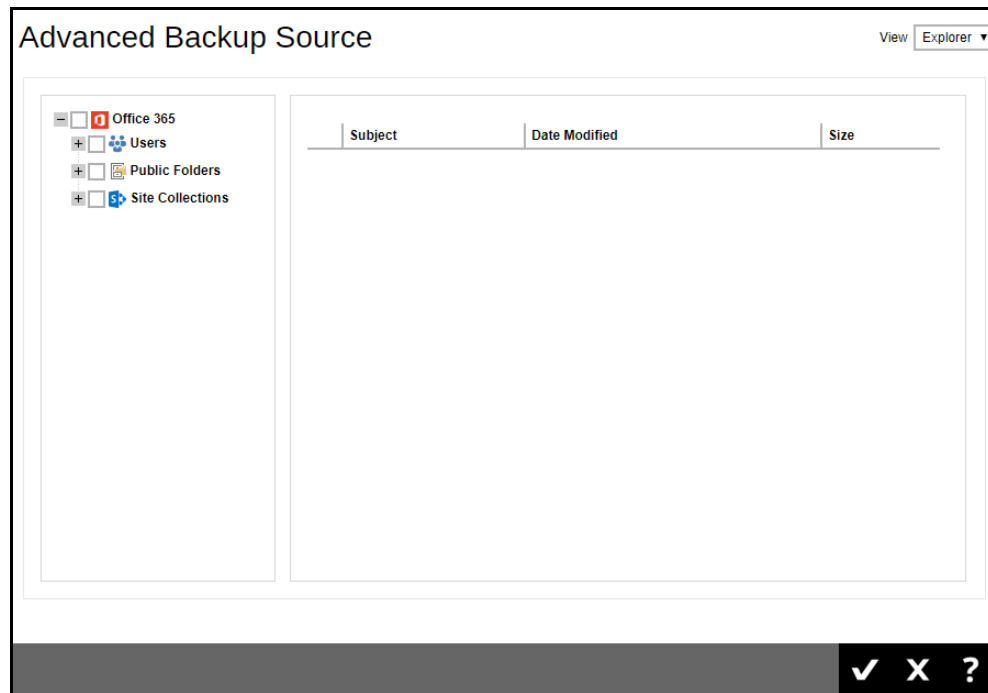
☐  Outlook
☐  OneDrive
☐  Personal Site
☐  Public Folders
☐  Site Collections

[I would like to choose the items to backup](#)

Or click **I would like to choose the items to backup** to choose the detailed items to backup.

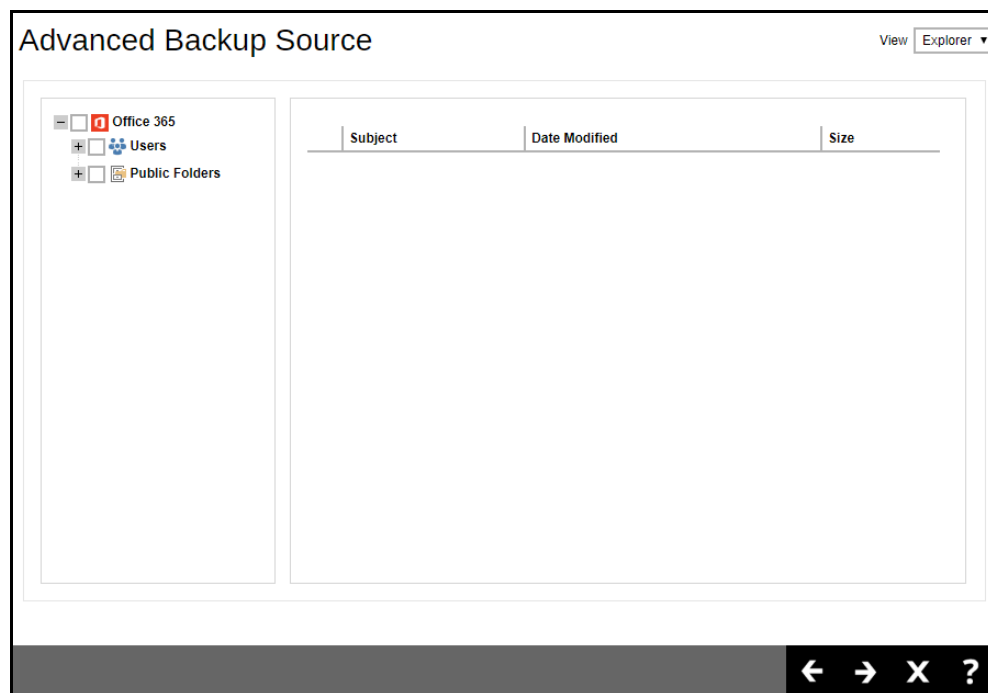
For AhsayOBM users, these are the following sources available:

- Users: include Outlook, OneDrive, and Personal Sites
- Public Folders: include public folder
- Site Collections: include personal site and site collection



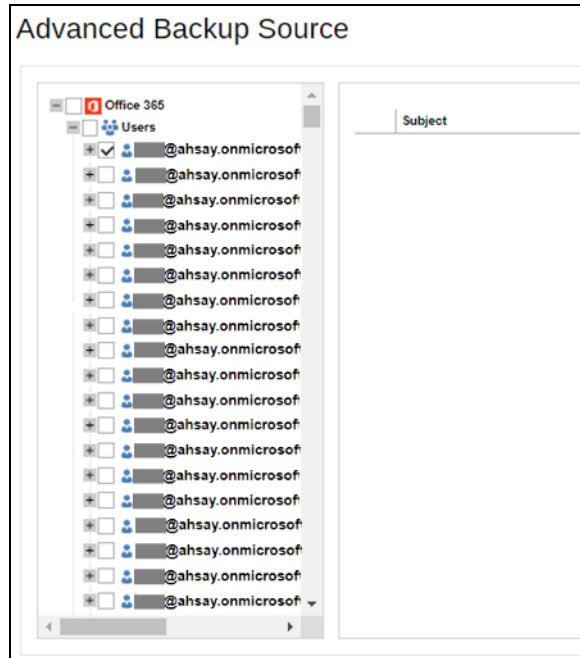
For AhsayACB users, these are the following sources available:

- Users: include Outlook, OneDrive, and Personal Sites
- Public Folders: include public folder

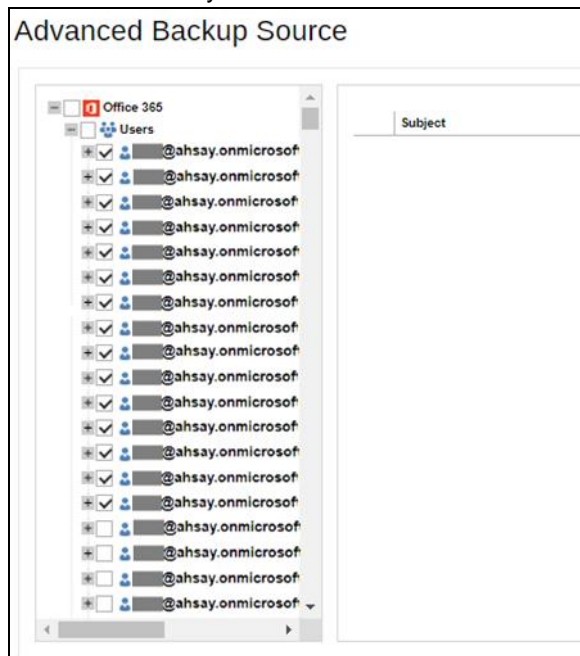


If you will select a large number of items to backup, like 1000 items, you need to click on these 1000 items to select/deselect them individually. Now there is a shortcut that you can use to lessen the burden of selecting/deselecting every 1000 item. You can select/deselect all 1000 items at once by 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.

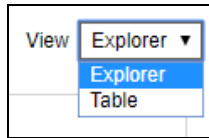


- ii. Scroll down to the 15th user.
- iii. Hold the Shift key then click the 15th user. All the 15 users are now selected.



Press  at the bottom right corner to proceed when you are done with the selection.

You also have an option if you want to view the Advanced Backup Source screen by Explorer or Table.



Explorer view

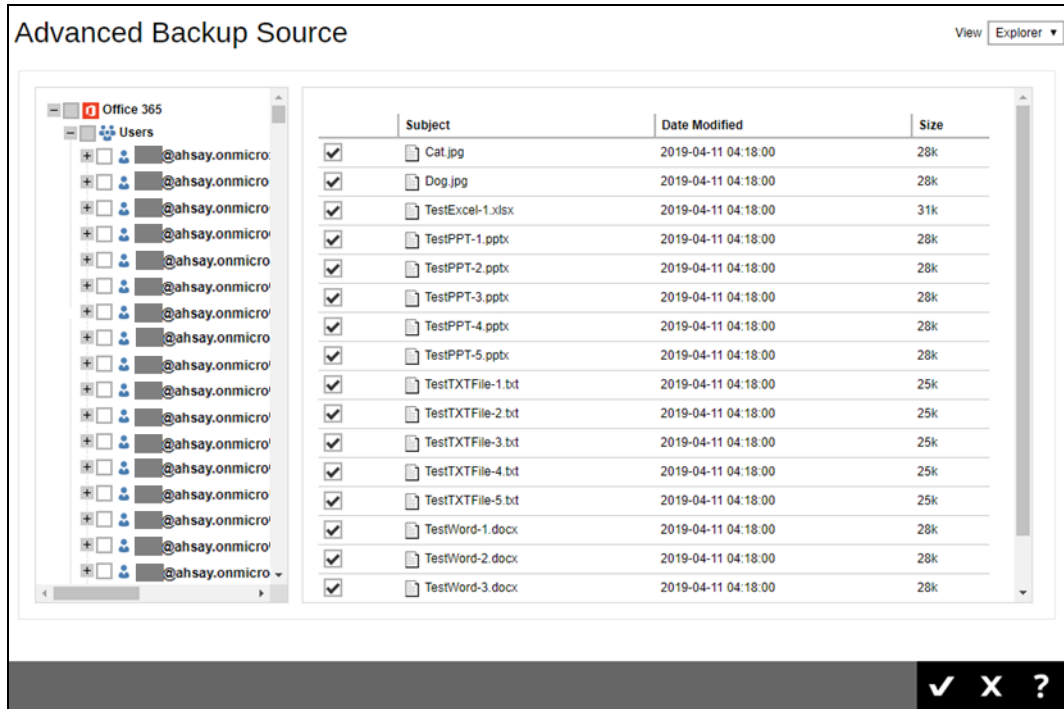




Table view

Click the **Add** button or plus sign icon to add Selected and Deselected Sources.




7. Press  at the bottom right corner to continue.
8. If you would like the backup set to run at a specified time interval of your choice, turn this feature on by sliding the on/off switch in the **Schedule** menu.

Schedule


Run scheduled backup for this backup set









Click the  button to add a schedule.





Schedule

Run scheduled backup for this backup set


Manage schedule

<input type="checkbox"/>	Name	Type
<input type="checkbox"/>		

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.

Backup Schedule

Client version < 8.3.3.50 does not support periodic schedule, periodic schedule will work as normal schedule.

Details

Name

Type

Start backup
at :

Stop

☒ Run Retention Policy after backup

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

Backup Schedule

Client version < 8.3.3.50 does not support periodic schedule, periodic schedule will work as normal schedule.

Details

Name
Weekly-1

Type
Weekly ▼

Backup on these days of the week
☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☒ Sat

Start backup
at ▼ 19 ▼ : 00 ▼

Stop
until full backup completed ▼

☒ Run Retention Policy after backup

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

Backup Schedule

Client version < 8.3.3.50 does not support periodic schedule, periodic schedule will work as normal schedule.

Details

Name
Monthly-1

Type
Monthly ▼

Backup on the following day every month
☐ 1 ▼
☒ Last ▼ Sunday ▼

Start backup at
20 ▼ : 00 ▼

Stop
until full backup completed ▼

☒ Run Retention Policy after backup

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

Backup Schedule

Client version < 8.3.3.50 does not support periodic schedule, periodic schedule will work as normal schedule.

Details

Name

Type

Backup on the following day once

Start backup at
 :

Stop

☒ Run Retention Policy after backup

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

Start backup

☒ Run Retention Policy after backup

1 minute
2 minutes
3 minutes
4 minutes
5 minutes
6 minutes
10 minutes
12 minutes
15 minutes
20 minutes
30 minutes
1 hour
2 hours
3 hours
4 hours
6 hours
8 hours
12 hours

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

Figure 1.1 – Periodic schedule every 4 hours Monday - Friday during business hours

Backup Schedule

Client version < 8.3.3.50 does not support periodic schedule, periodic schedule will work as normal schedule.

Details

Name
Weekly-1

Type
Weekly

Backup on these days of the week
☐ Sun ☒ Mon ☒ Tue ☒ Wed ☒ Thu ☒ Fri ☐ Sat

Start backup
every 4 hours

☒ Run Retention Policy after backup

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

Backup Schedule

Client version < 8.3.3.50 does not support periodic schedule, periodic schedule will work as normal schedule.

Details

Name
Weekly-1

Type
Weekly

Backup on these days of the week
☒ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☒ Sat

Start backup
at 21 : 00

Stop
until full backup completed

☒ Run Retention Policy after backup

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

Click  to save the configured backup schedule settings.


Click  to proceed. Multiple backup schedules can be created.

9. To add a destination, select from the existing storage destinations listed on the drop-down list as provided by your backup service provider.

Backup destination is preset to the AhsayCBS or Predefined Destination.



In the sample screenshot above, the backup service provider has setup four (4) available destinations (i.e. ColdStor, AWSComStor, GCS-Predefined-storage, and AhsayCBS).

Press  at the bottom right corner to proceed when you are done with the setting.

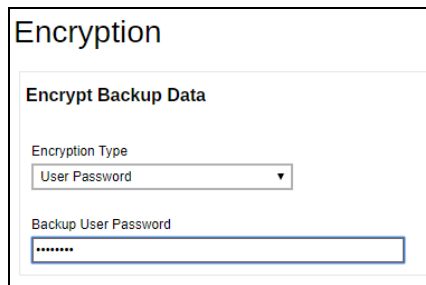
10. By default, the **Encrypt Backup Data** option is enabled with the Encryption Type preset as **Default** which provides the most secure protection.



The screenshot shows a window titled "Encryption". Inside, there's a section "Encrypt Backup Data" with a toggle switch that is turned on. Below it, the "Encryption Type" is set to "Default (Machine Generated Random)" in a dropdown menu. Other options visible are "User Password" and "Custom". At the bottom right of the window are navigation icons: back, save, close, and help.

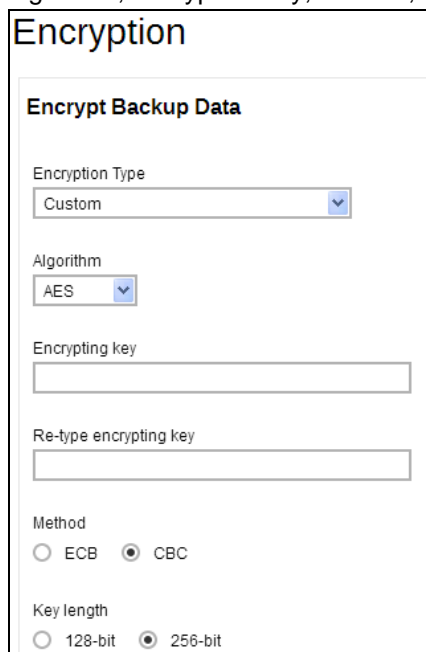
You can choose from one of the following three Encryption Type options:

- **Default (Machine Generated Random)** – 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 was 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.




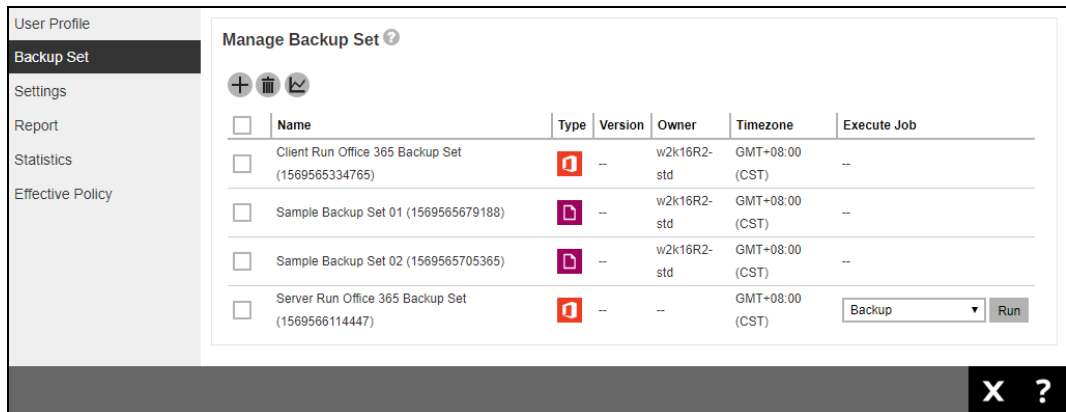
This screenshot shows the "Encryption" window with "User Password" selected in the "Encryption Type" dropdown. Below it, there is a text field for "Backup User Password" containing several asterisks to represent a masked password.

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



This screenshot shows the "Encryption" window with "Custom" selected in the "Encryption Type" dropdown. It displays additional configuration options: "Algorithm" is set to "AES", "Encrypting key" and "Re-type encrypting key" are empty text fields, "Method" has radio buttons for "ECB" and "CBC" (with "CBC" selected), and "Key length" has radio buttons for "128-bit" and "256-bit" (with "256-bit" selected).

11. Click  at the bottom right corner to confirm creating this backup set.

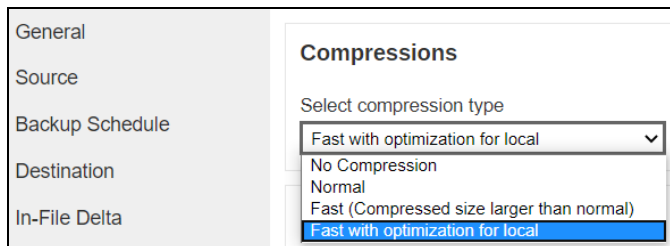


<input type="checkbox"/>	Name	Type	Version	Owner	Timezone	Execute Job
<input type="checkbox"/>	Client Run Office 365 Backup Set (1569565334765)		--	w2k16R2-std	GMT+08:00 (CST)	--
<input type="checkbox"/>	Sample Backup Set 01 (1569565679188)		--	w2k16R2-std	GMT+08:00 (CST)	--
<input type="checkbox"/>	Sample Backup Set 02 (1569565705365)		--	w2k16R2-std	GMT+08:00 (CST)	--
<input type="checkbox"/>	Server Run Office 365 Backup Set (1569566114447)		--	--	GMT+08:00 (CST)	<div>Backup <input type="button" value="Run"/></div>

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

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

- No Compression
- Normal
- Fast
- Fast with optimization for local



General

Source

Backup Schedule

Destination

In-File Delta

Compressions

Select compression type

Fast with optimization for local ▼

No Compression

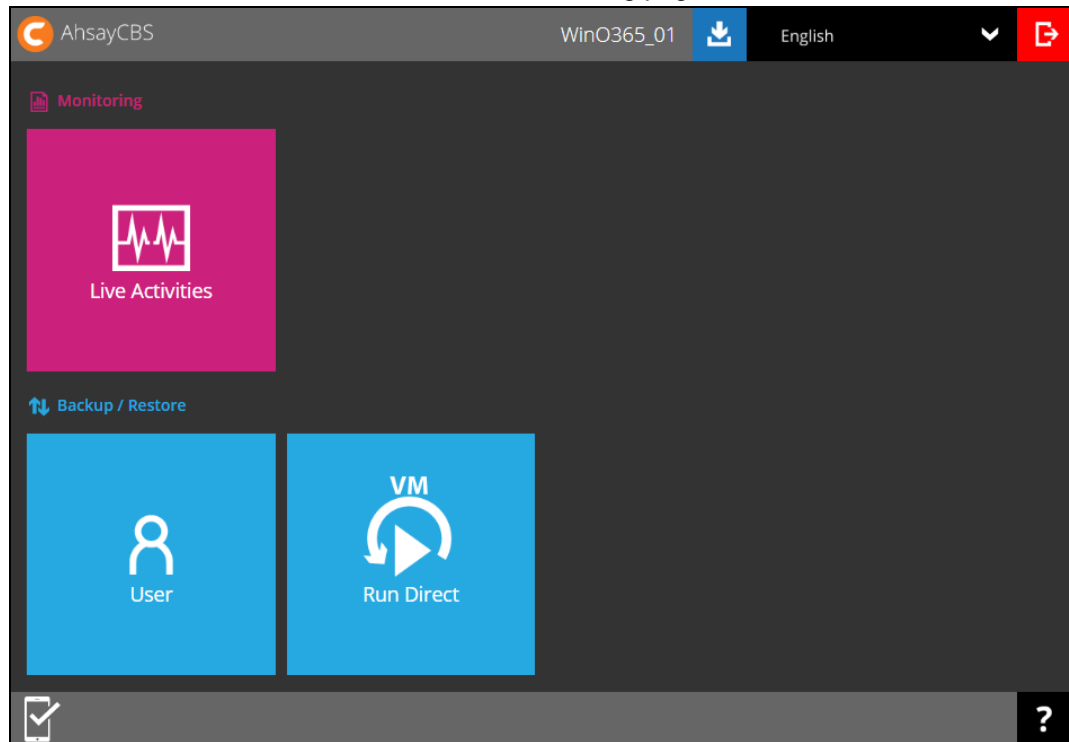
Normal

Fast (Compressed size larger than normal)

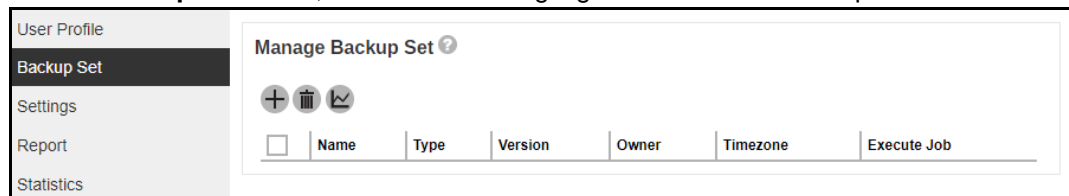
Fast with optimization for local

4.2 Hybrid Authentication

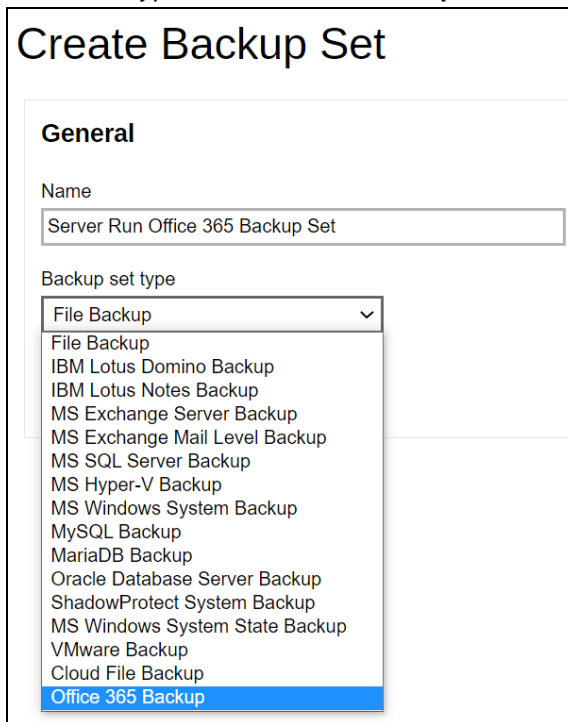
1. Log in to the User Web Console according to the instructions in [Login to AhsayCBS User Web Console](#).
2. Click the User icon on the User Web Console landing page.



3. On the **Backup Set** menu, click the + icon highlighted to create a backup set.



4. Select the type as **Office 365 Backup**, then name the backup set.



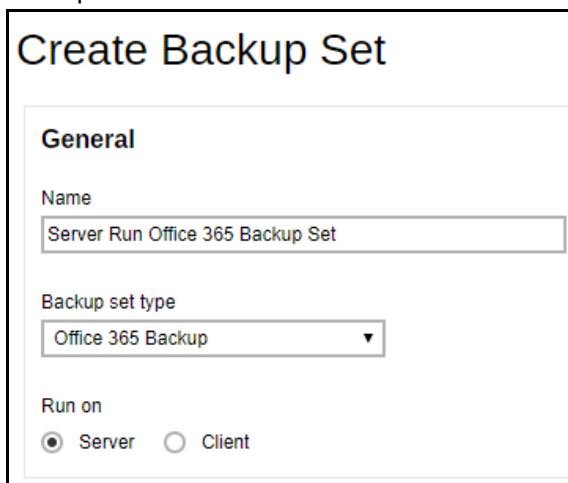
Create Backup Set

General

Name
Server Run Office 365 Backup Set

Backup set type
File Backup
File Backup
IBM Lotus Domino Backup
IBM Lotus Notes Backup
MS Exchange Server Backup
MS Exchange Mail Level Backup
MS SQL Server Backup
MS Hyper-V Backup
MS Windows System Backup
MySQL Backup
MariaDB Backup
Oracle Database Server Backup
ShadowProtect System Backup
MS Windows System State Backup
VMware Backup
Cloud File Backup
Office 365 Backup

5. On the same menu under **Run on**, select **Server** to create a Run on Server (Agentless) backup set.



Create Backup Set

General

Name
Server Run Office 365 Backup Set

Backup set type
Office 365 Backup

Run on
☒ Server ☐ Client

NOTES

- If you choose to run the backup set on the AhsayCBS server, you won't be able to back up, restore or manage your backups on the AhsayOBM once the backup set is created.
- This setting **CANNOT** be altered once the backup set is created. If you wish to change the backup method later, you will have to create a new backup set and start over the configurations again.
- For backup sets created in **Run on Server** backup type, the backup destination is restricted to either AhsayCBS or a predefined destination (if setup by your backup service provider). If you wish to back up to other cloud destinations or back up to multiple destinations, the backup set should be created in **Run on Client** backup type instead.

To create a backup set using Hybrid Authentication:

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

Create Backup Set

General

Name

Backup set type

Run on
☒ Server ☐ Client

Office 365

Username

Account password

App password
(Required if Multi-Factor Authentication is enforced)

Region

☐ Access the Internet through Proxy

[Sign up for Office 365 Backup](#)

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

Create Backup Set

General

Name

Backup set type

Run on
☒ Server ☐ Client

Office 365

Username

Account password

App password
(Required if Multi-Factor Authentication is enforced)

Region

☐ Access the Internet through Proxy

[Sign up for Office 365 Backup](#)

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

Office 365 Multi-Factor Authentication

A sms is sent to your mobile device, please type in the code shown in the sms message


[Use another method to authenticate](#)


or

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

Office 365 Multi-Factor Authentication

Select an authentication method

 **Text +XX XXXXXXXXXX15**

 **Call +XX XXXXXXXXXX15**

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

Office 365 Multi-Factor Authentication


A sms is sent to your mobile device, please type in the code shown in the sms message

[Use another method to authenticate](#)

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

Office 365 Multi-Factor Authentication

Please answer the phone call to continue

 Waiting for response

[Use another method to authenticate](#)

A message will be displayed indicating account was verified.

125 [REDACTED] says

Verified

OK

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 AhsayCBS user web console 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.

Click [Authorize] and in the pop-up browser window, sign in your Microsoft account and authorize the backup application (if necessary), copy and paste the authorization code to the textbox and hit [OK] to complete the authentication.

Authorize

Cancel

Sign in to your Microsoft account.

 Microsoft

Sign in

██████████@ahsay.onmicrosoft.com

No account? [Create one!](#)

[Can't access your account?](#)

[Sign-in options](#)

Back

Next

 Microsoft

← ██████████@ahsay.onmicrosoft.com

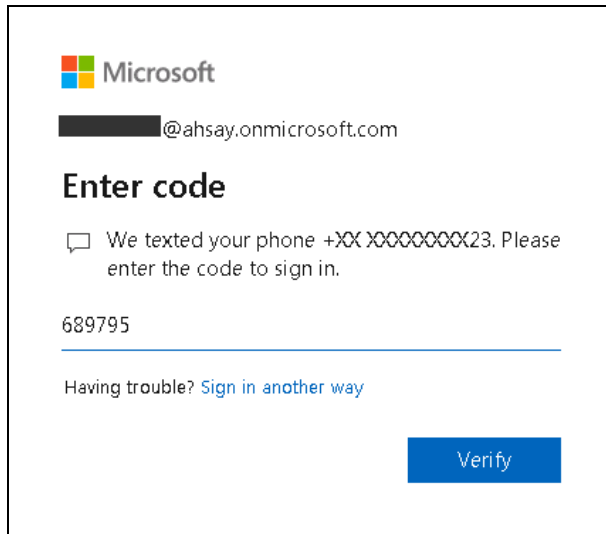
Enter password

.....

[Forgot my password](#)

Sign in

If MFA is enforced, enter the validation code sent to your mobile device and click **Verify**.



The screenshot shows a Microsoft login interface. At the top is the Microsoft logo. Below it is a placeholder email address ending in @ahsay.onmicrosoft.com. The heading "Enter code" is followed by a message: "We texted your phone +XX XXXXXXXX23. Please enter the code to sign in." Below this is a text input field containing the number "689795". A link "Having trouble? Sign in another way" is present. A blue "Verify" button is at the bottom right.

NOTE

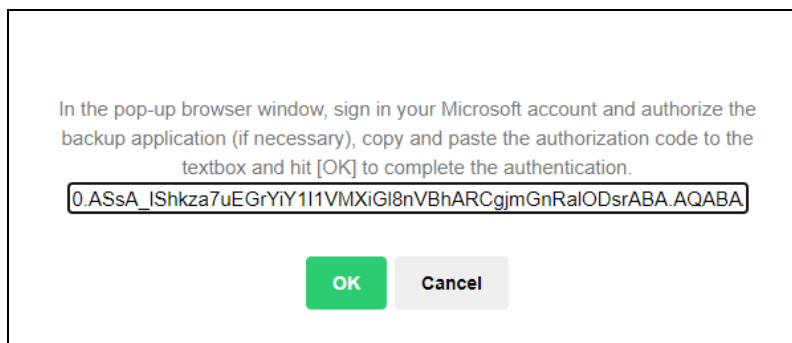
The verification code is only required if the MFA status of an Office 365 account is enforced.

Copy the authorization code.



The screenshot displays the "Authorization Code for Microsoft 365". It features the Ahsay logo at the top. The authorization code "0.ASsA_IShkza7uEGrYiY1I1VMXiGI8nVBhARCgjmGnR:" is shown in red text within a light gray box. Below the box, a message states: "Please copy and paste the above Authorization Code into Ahsay's product to complete the setup."

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



The screenshot shows a confirmation dialog box. It contains the text: "In the pop-up browser window, sign in your Microsoft account and authorize the backup application (if necessary), copy and paste the authorization code to the textbox and hit [OK] to complete the authentication." Below this text is a text input field containing the authorization code "0.ASsA_IShkza7uEGrYiY1I1VMXiGI8nVBhARCgjmGnRaIODsrABA.AQABA". At the bottom are two buttons: a green "OK" button and a gray "Cancel" button.

Test completed successfully is displayed when the validation is successful.

Create Backup Set

General

Name

Backup set type

Run on
☒ Server ☐ Client

Office 365

Username

Account password

App password
(Required if Multi-Factor Authentication is enforced)

Region

☐ Access the Internet through Proxy

✓ Test completed successfully

[Sign up for Office 365 Backup](#)

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 AhsayCBS user web console 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.

6. Select the **Backup Source** in this menu. Select the desired Outlook, OneDrive, Personal Site, Public Folders or Site Collections for backup. Check the box will back up all, i.e. check the box of Outlook will back up the mailboxes of all the users.

Backup Source

Select the items and folders that you want to backup

☐ Outlook

☐ OneDrive

☐ Personal Site

☐ Public Folders

☐ Site Collections

[I would like to choose the items to backup](#)

Or click **I would like to choose the items to backup** to choose the detailed items to backup.

For AhsayOBM users, these are the following sources available:

- Users: include Outlook, OneDrive, and Personal Sites
- Public Folders: include public folder
- Site Collections: include personal site and site collection

Advanced Backup Source

View Explorer

☐ Office 365

☐ Users

☐ Public Folders

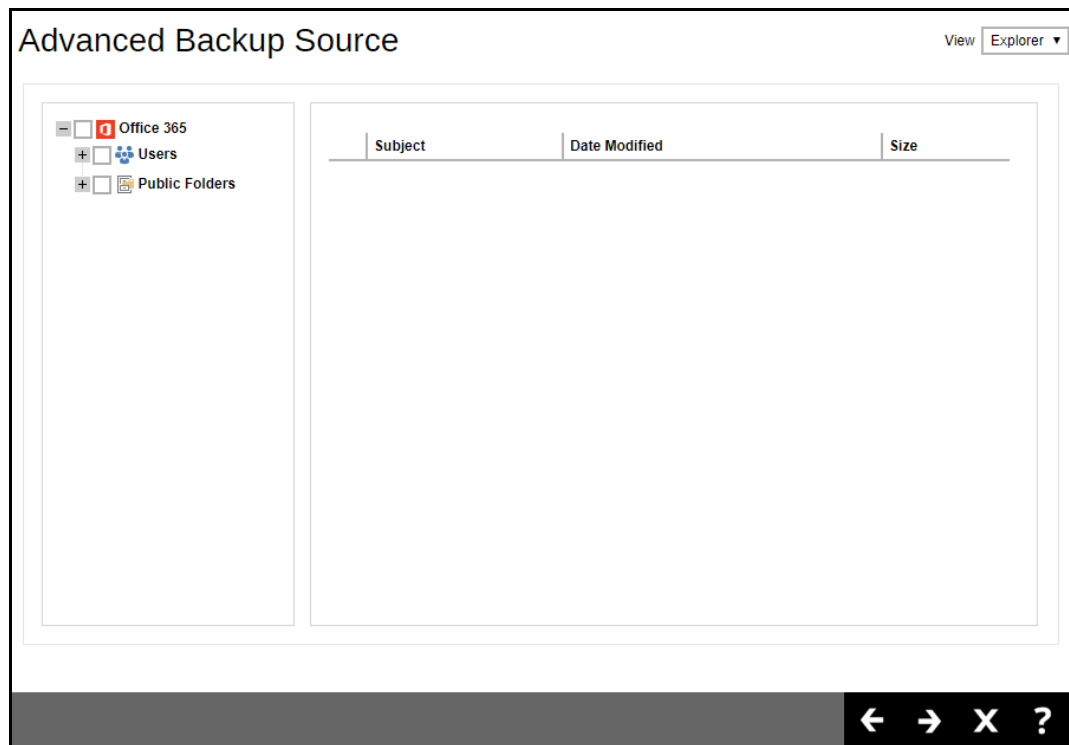
☐ Site Collections

Subject	Date Modified	Size
---------	---------------	------

✓ X ?

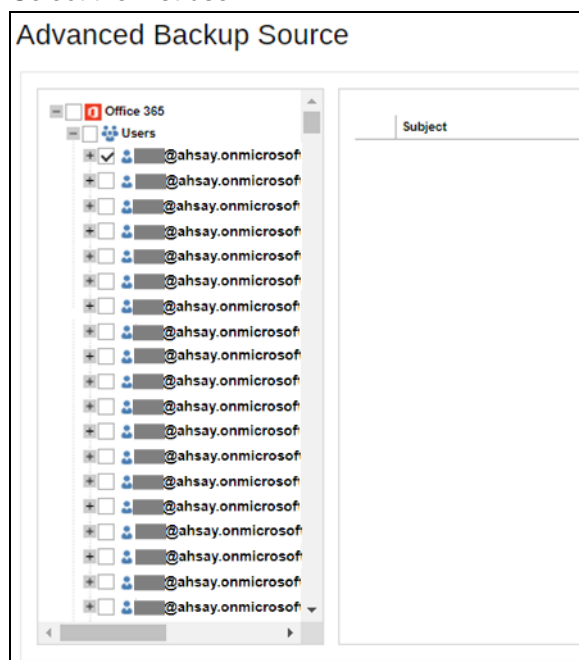
For AhsayACB users, these are the following sources available:

- Users: include Outlook, OneDrive, and Personal Sites
- Public Folders: include public folder

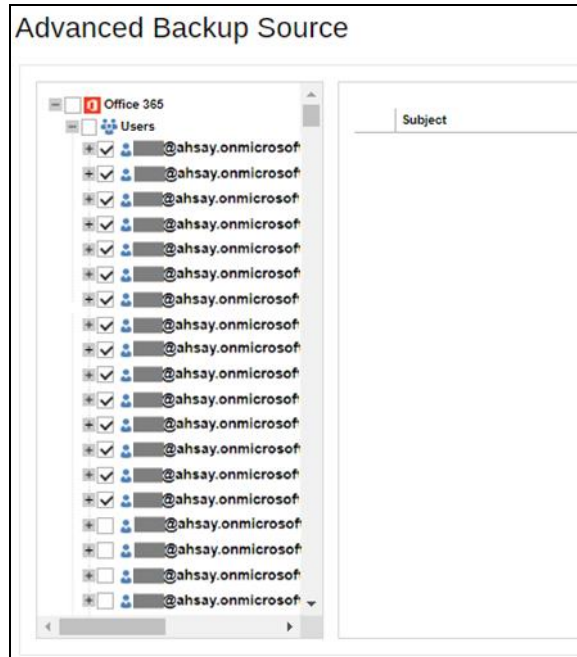



If you will select a large number of items to backup, like 1000 items, you need to click on these 1000 items to select/deselect them individually. Now there is a shortcut that you can use to lessen the burden of selecting/deselecting every 1000 item. You can select/deselect all 1000 items at once by 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:

- Select the first user.

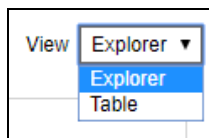


- ii. Scroll down to the 15th user.
- iii. Hold the Shift key then click the 15th user. All the 15 users are now selected.



Press  at the bottom right corner to proceed when you are done with the selection.

You also have an option if you want to view the Advanced Backup Source screen by Explorer or Table.



Explorer view

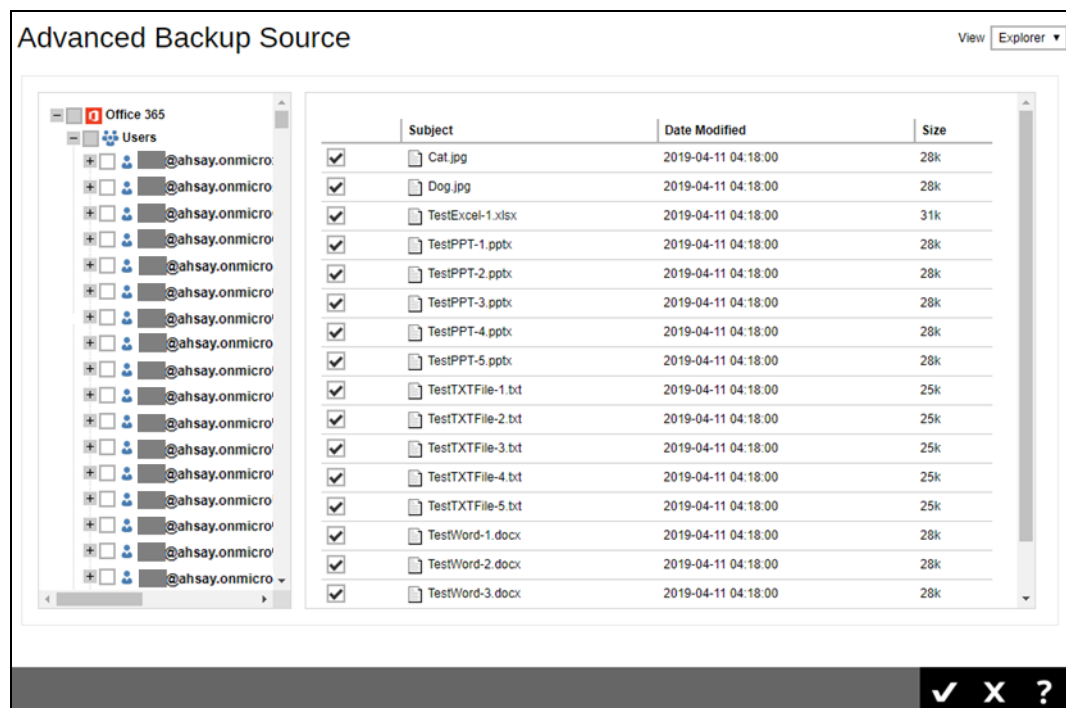


Table view

Click the **Add** button or plus sign icon to add Selected and Deselected Sources.

Advanced Backup Source

View Table

Other Selected Source

+ -

☐ Path

Deselected Source

+ -

☐ Path

Advanced Backup Source

View Table

Other Selected Source

+ -

☐ Path


☐ Office 365/Users/[redacted] OneDrive/D913_TestFiles

☐ Office 365/Users/[redacted] Outlook/Inbox

Deselected Source

+ -


☐ Path

- Press  at the bottom right corner to continue.
- If you would like the backup set to run at a specified time interval of your choice, turn this feature on by sliding the on/off switch in the **Schedule** menu.

Schedule

Run scheduled backup for this backup set

← → X ?

Click the  button to add a schedule.

Schedule

Run scheduled backup for this backup set

Manage schedule

+ -

☐ Name

Type

← → X ?

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.

Backup Schedule

Client version < 8.3.3.50 does not support periodic schedule, periodic schedule will work as normal schedule.

Details

Name
Daily-1

Type
Daily ▼

Start backup
at ▼ 18 ▼ : 00 ▼

Stop
until full backup completed ▼

☒ Run Retention Policy after backup

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

Backup Schedule

Client version < 8.3.3.50 does not support periodic schedule, periodic schedule will work as normal schedule.

Details

Name
Weekly-1

Type
Weekly ▼

Backup on these days of the week
☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☒ Sat

Start backup
at ▼ 19 ▼ : 00 ▼

Stop
until full backup completed ▼

☒ Run Retention Policy after backup

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

Backup Schedule

Client version < 8.3.3.50 does not support periodic schedule, periodic schedule will work as normal schedule.

Details

Name
Monthly-1

Type
Monthly ▼

Backup on the following day every month

☐ 1 ▼

☒ Last ▼ Sunday ▼

Start backup at
20 ▼ : 00 ▼

Stop
until full backup completed ▼

☒ Run Retention Policy after backup

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

Backup Schedule

Client version < 8.3.3.50 does not support periodic schedule, periodic schedule will work as normal schedule.

Details

Name
Custom-1

Type
Custom ▼

Backup on the following day once

2020 December ▼ 31 ▼

Start backup at
21 ▼ : 00 ▼

Stop
until full backup completed ▼

☒ Run Retention Policy after backup

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

The screenshot shows a 'Start backup' section with a dropdown menu set to 'every'. The dropdown list is open, showing options from '1 minute' to '12 hours'. The '1 minute' option is currently selected and highlighted in blue. To the left of the dropdown, there is a checkbox labeled 'Run Retention Policy after backup' which is checked.

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

Figure 1.1 – Periodic schedule every 4 hours Monday - Friday during business hours

The screenshot shows the 'Backup Schedule' configuration page. At the top, it says 'Client version < 8.3.3.50 does not support periodic schedule, periodic schedule will work as normal schedule.' Below this is a 'Details' section with the following fields:

- Name:** Weekly-1
- Type:** Weekly
- Backup on these days of the week:** Sun (unchecked), Mon (checked), Tue (checked), Wed (checked), Thu (checked), Fri (checked), Sat (unchecked).
- Start backup:** every 4 hours
- Run Retention Policy after backup:** (checked)

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

The screenshot shows the 'Backup Schedule' configuration window. At the top, a note states: 'Client version < 8.3.3.50 does not support periodic schedule, periodic schedule will work as normal schedule.' Below this is a 'Details' section. The 'Name' field contains 'Weekly-1'. The 'Type' dropdown is set to 'Weekly'. Under 'Backup on these days of the week', checkboxes for Sun, Mon, Tue, Wed, Thu, Fri, and Sat are shown, with 'Sun' and 'Sat' checked. The 'Start backup' section shows a dropdown set to 'at', followed by '21' and '00' in separate boxes, indicating a time of 21:00. The 'Stop' dropdown is set to 'until full backup completed'. At the bottom, the checkbox 'Run Retention Policy after backup' is checked.

- **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.

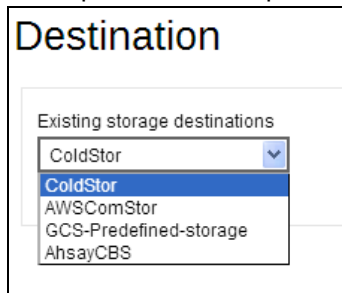
- **Run Retention Policy after backup** – if enabled, retention policy job will run to remove files from the backup destination(s) which have exceeded the retention policy after performing a backup job.

Click  to save the configured backup schedule settings.


Click  to proceed. Multiple backup schedules can be created.

9. To add a destination, select from the existing storage destinations listed on the drop-down list as provided by your backup service provider.

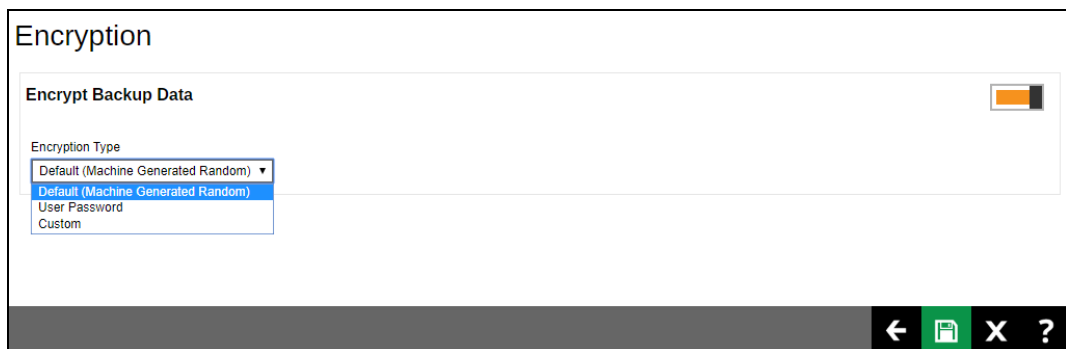
Backup destination is preset to the AhsayCBS or Predefined Destination.



In the sample screenshot above, the backup service provider has setup four (4) available destinations (i.e. ColdStor, AWSComStor, GCS-Predefined-storage, and AhsayCBS).

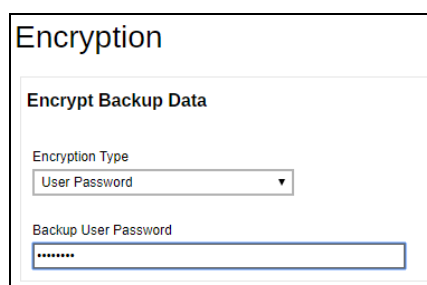
Press  at the bottom right corner to proceed when you are done with the setting.

10. By default, the **Encrypt Backup Data** option is enabled with the Encryption Type preset as **Default** which provides the most secure protection.



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

- **Default (Machine Generated Random)** – 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 was 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.

Encryption

Encrypt Backup Data

Encryption Type


Algorithm

Encrypting key

Re-type encrypting key

Method
☐ ECB ☒ CBC

Key length
☐ 128-bit ☒ 256-bit

11. Click  at the bottom right corner to confirm creating this backup set.

User Profile
Backup Set
Settings
Report
Statistics
Effective Policy

Manage Backup Set ?

+
-
↺

<input type="checkbox"/>	Name	Type	Version	Owner	Timezone	Execute Job
<input type="checkbox"/>	Client Run Office 365 Backup Set (1569565334765)		--	w2k16R2-std	GMT+08:00 (CST)	--
<input type="checkbox"/>	Sample Backup Set 01 (1569565679188)		--	w2k16R2-std	GMT+08:00 (CST)	--
<input type="checkbox"/>	Sample Backup Set 02 (1569565705365)		--	w2k16R2-std	GMT+08:00 (CST)	--
<input type="checkbox"/>	Server Run Office 365 Backup Set (1569566114447)		--	--	GMT+08:00 (CST)	<input type="text" value="Backup"/> <input type="button" value="Run"/>

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

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

- No Compression
- Normal
- Fast
- Fast with optimization for local

General
Source
Backup Schedule
Destination
In-File Delta

Compressions

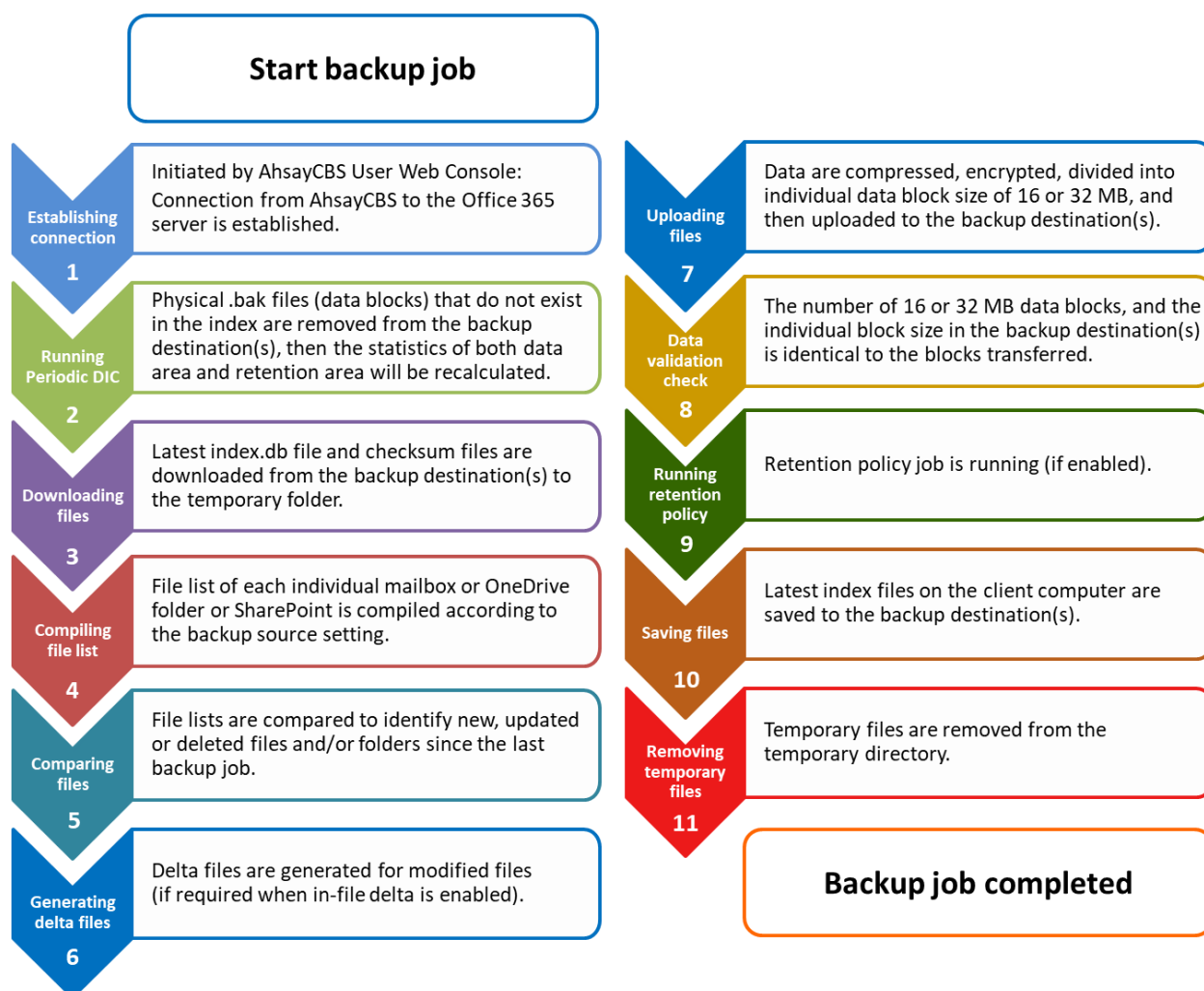
Select compression type

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 2, 3, 8, and 10, please refer to the following chapters.

- [Periodic Data Integrity Check \(PDIC\) Process \(Step 2\)](#)
- [Backup Set Index Handling Process](#)
 - [Start Backup Job \(Step 3\)](#)
 - [Completed Backup Job \(Step 10\)](#)
- [Data Validation Check Process \(Step 8\)](#)



5.1 Periodic Data Integrity Check (PDIC) Process

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

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

PDIC schedule = %BackupSetID% modulo 5

or

%BackupSetID% mod 5

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

0	Monday
1	Tuesday
2	Wednesday
3	Thursday
4	Friday

NOTE: The PDIC schedule cannot be changed.

Example:

Backup set ID: 1594627447932

Calculation: 1594627447932 mod 5 = 2

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

In this example:

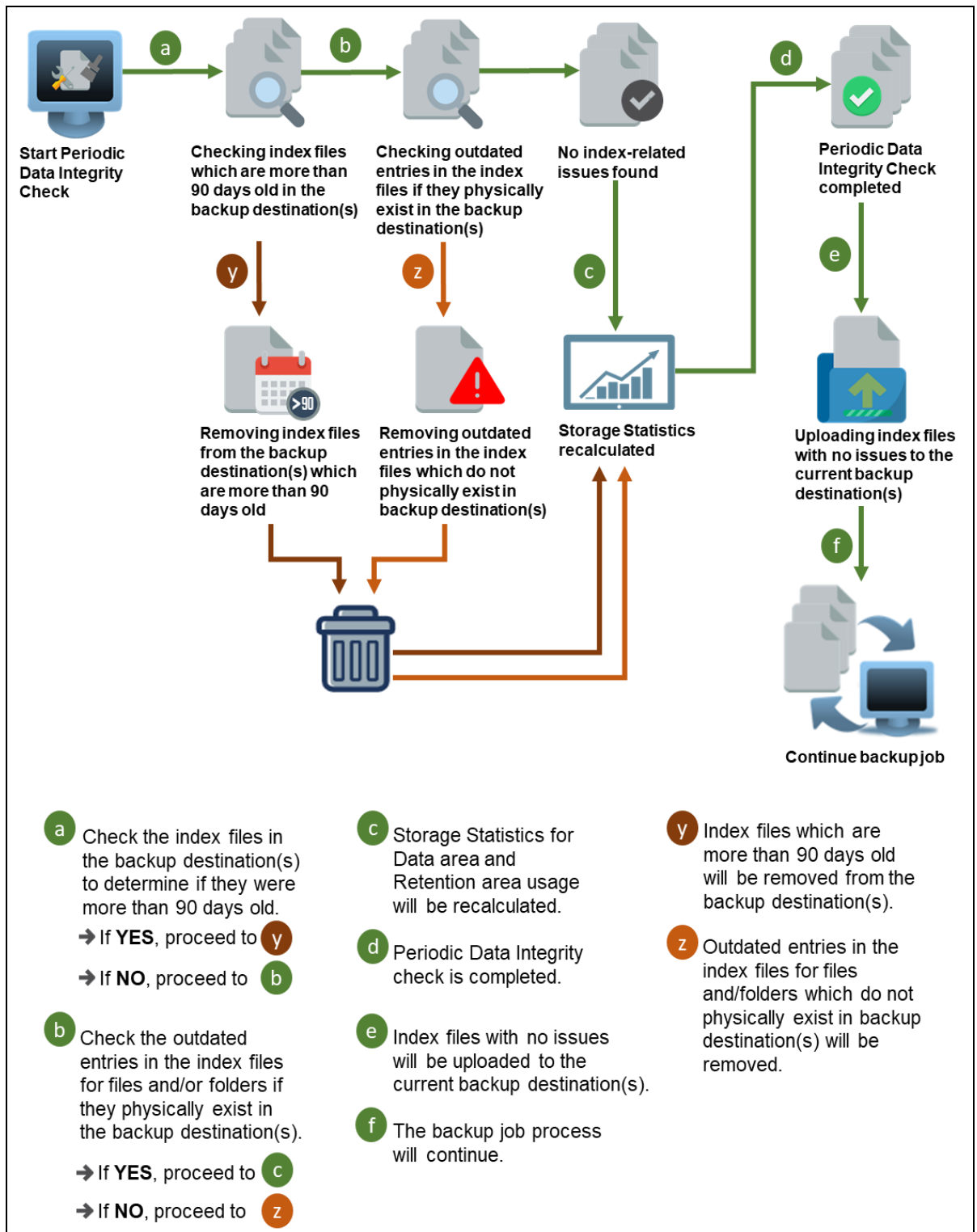
- the PDIC will run on the first backup job that falls on Wednesday; or
- if there is no active backup job(s) running from Monday to Friday, then the PDIC will run on the next available backup job.

NOTE

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

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

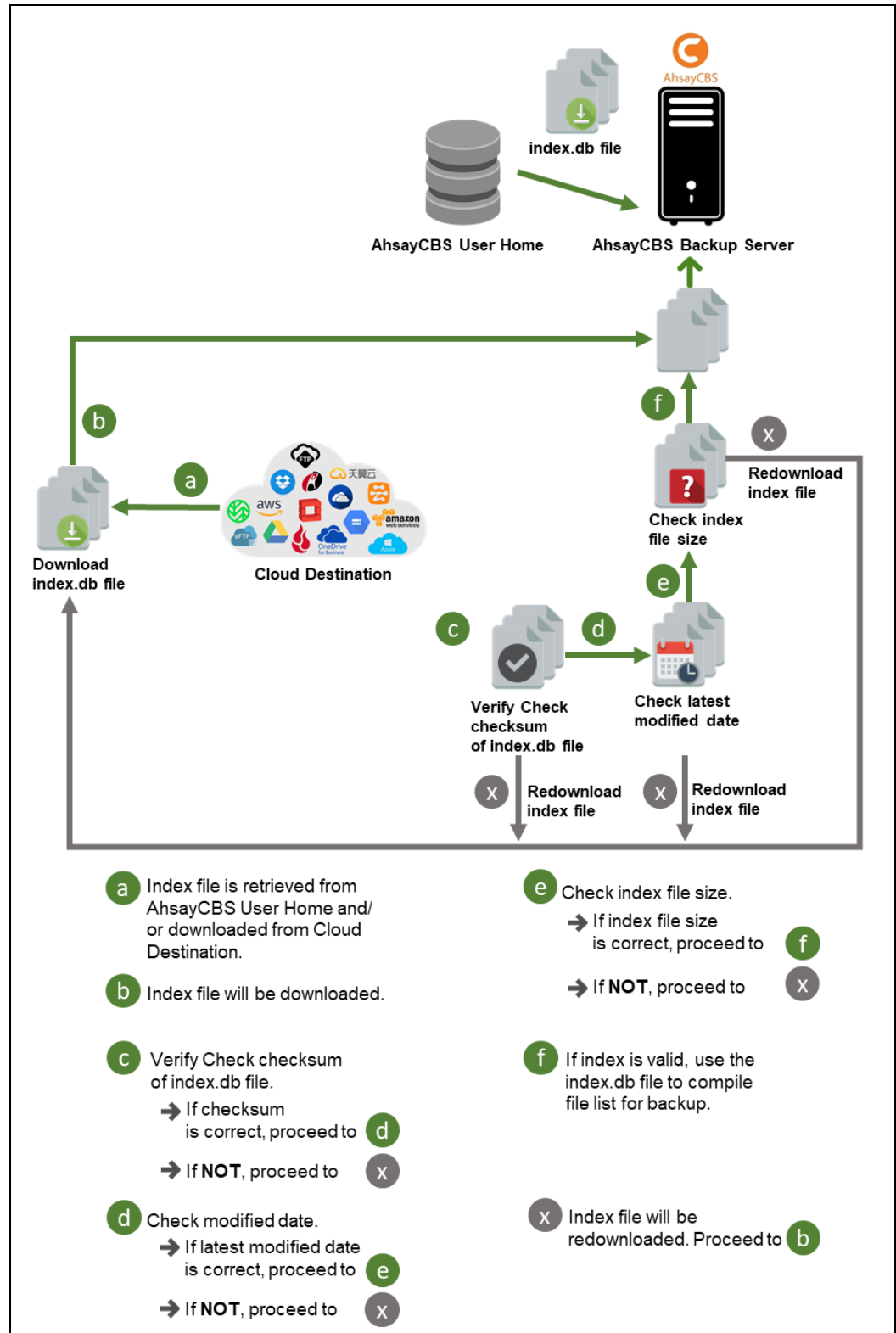
1. If AhsayCBS was upgraded to v8.5 (or above) from an older version v7, or pre-8.3.6.0 version. In this case, the PDIC job will run on the first backup job after upgrade.
2. If backup jobs for a backup set are not run on a regular daily backup schedule (for example: on a weekly or monthly schedule),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



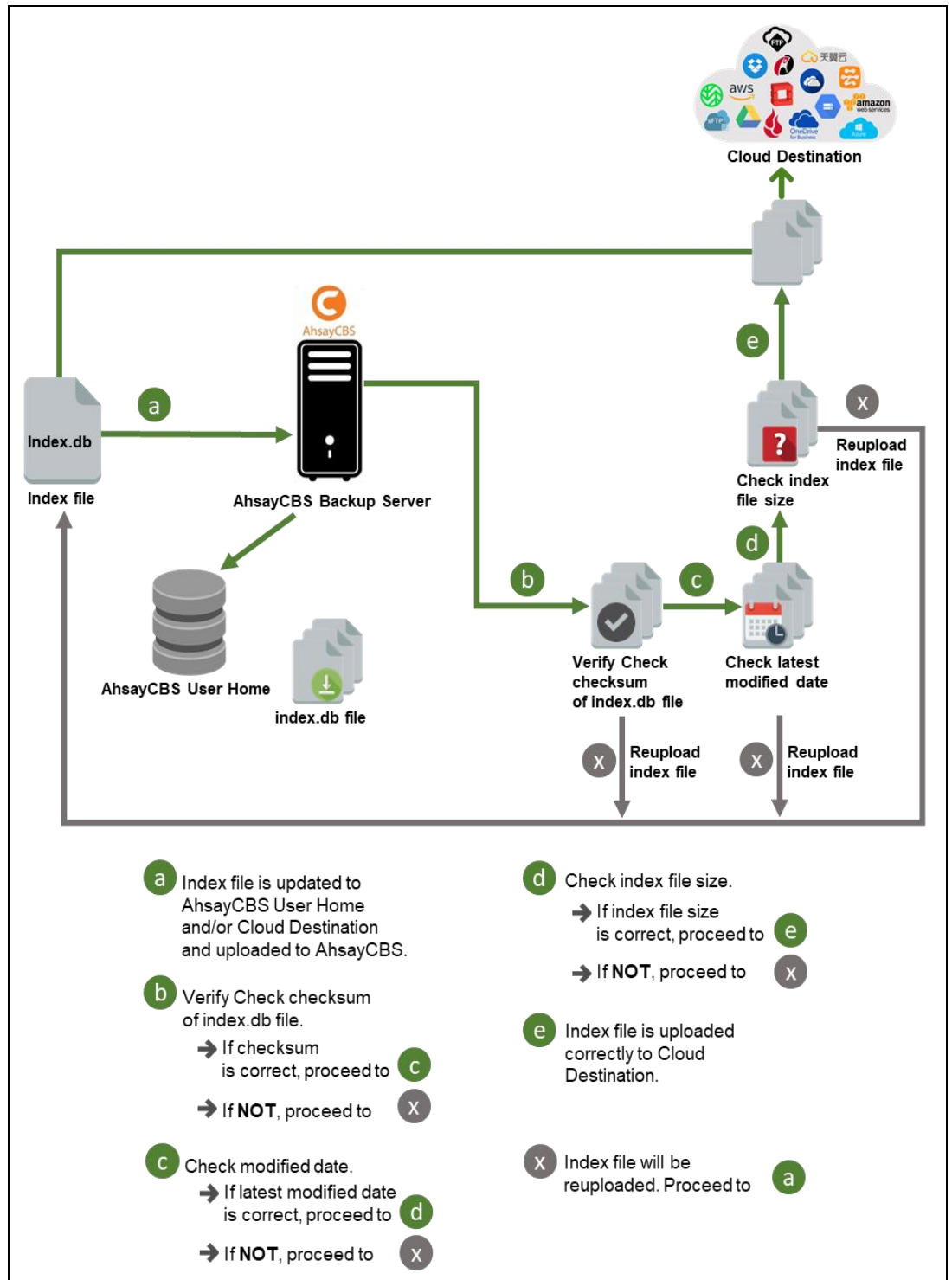
5.2 Backup Set Index Handling Process

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

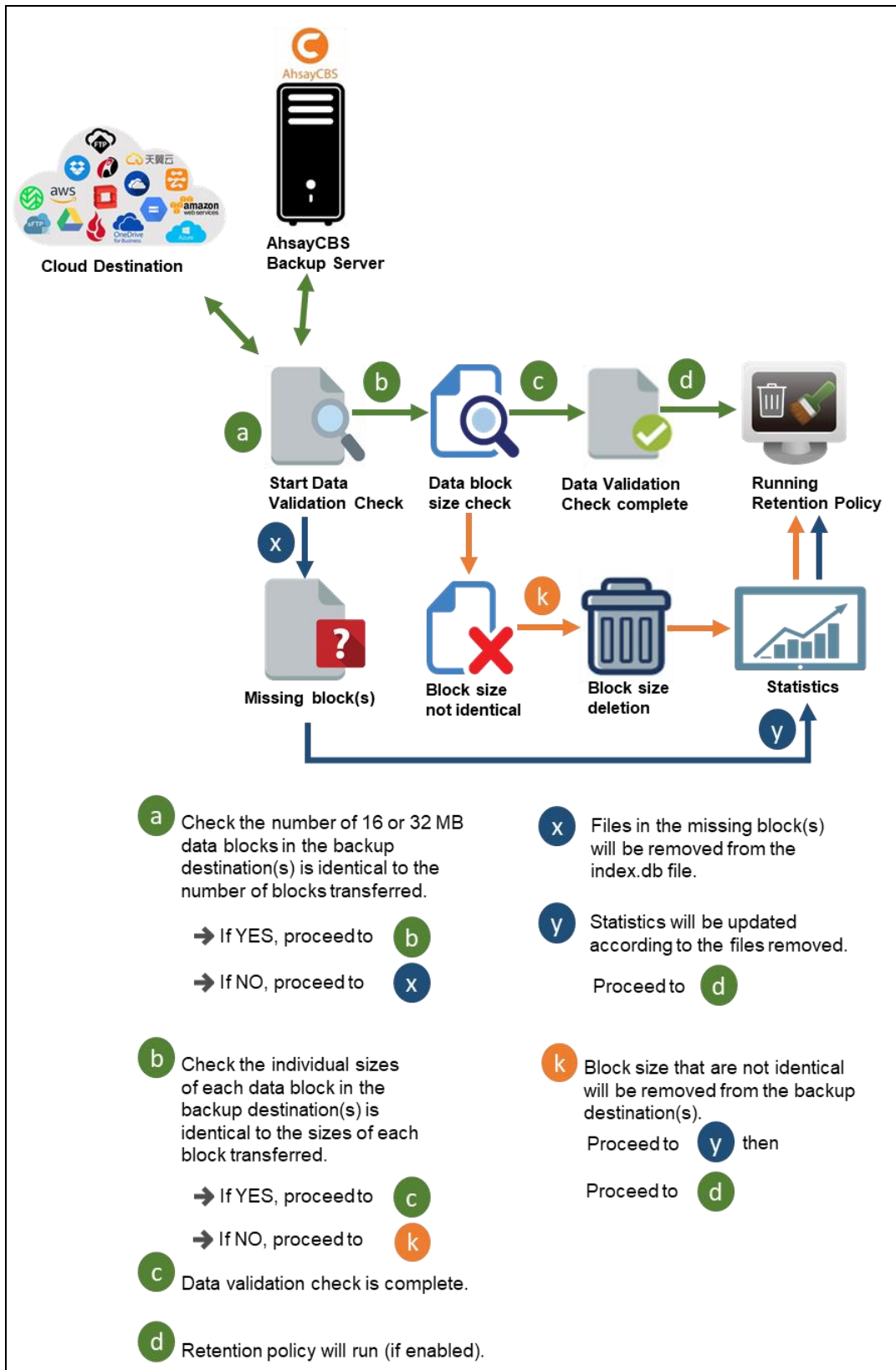


5.2.2 Completed Backup Job



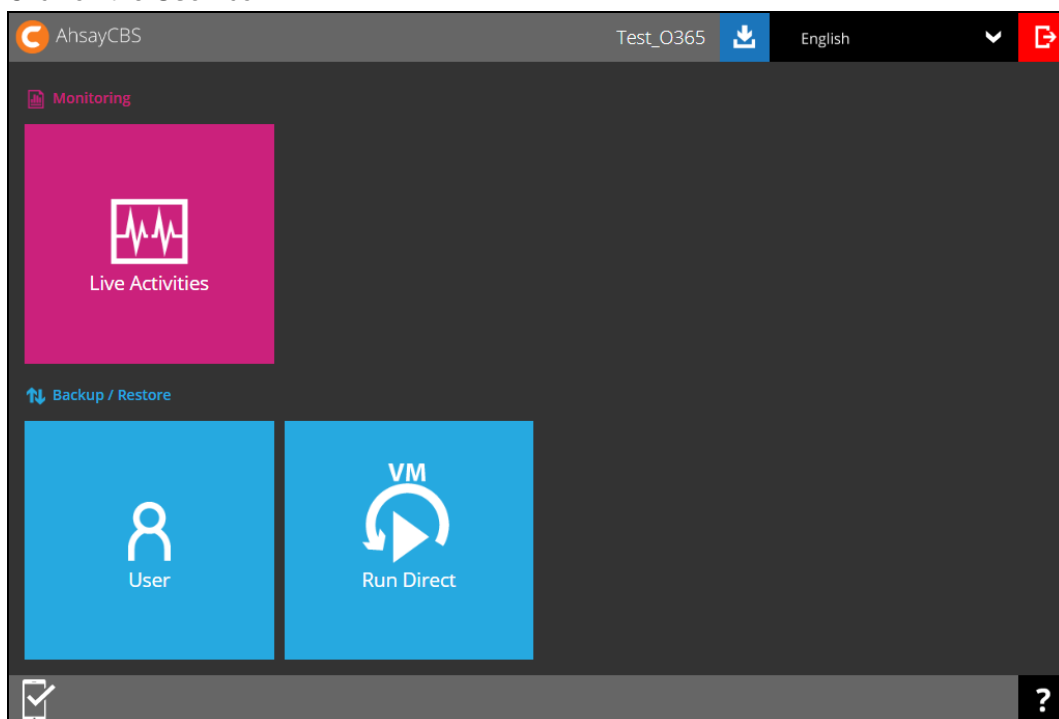
5.3 Data Validation Check Process

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.

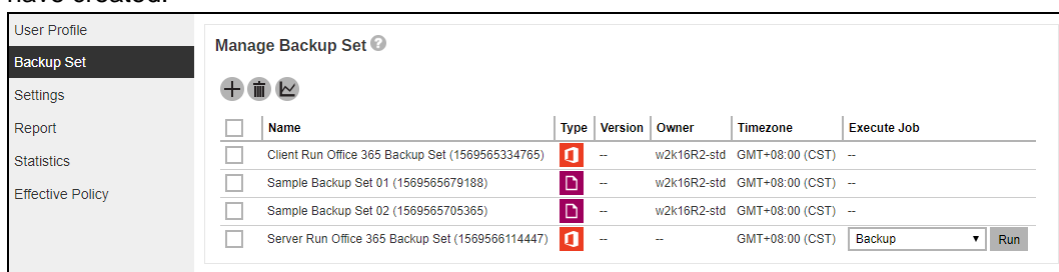


6 Running Backup Job

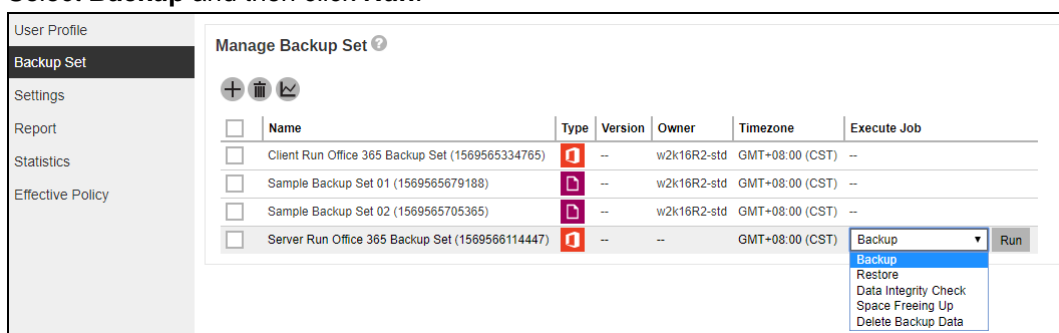
1. Log in to the User Web Console according to the instructions in [Login to User Web Console](#).
2. Click on the **User** icon.



3. Under the **Backup Set > Manage Backup Set** menu, you should see the backup set you have created.



4. Click the drop-down menu on the backup set that you would like to start a backup for. Select **Backup** and then click **Run**.



User Profile
Backup Set
Settings
Report
Statistics
Effective Policy

Manage Backup Set

+
-
↺

<input type="checkbox"/>	Name	Type	Version	Owner	Timezone	Execute Job
<input type="checkbox"/>	Client Run Office 365 Backup Set (1569565334765)		--	w2k16R2-std	GMT+08:00 (CST)	--
<input type="checkbox"/>	Sample Backup Set 01 (1569565679188)		--	w2k16R2-std	GMT+08:00 (CST)	--
<input type="checkbox"/>	Sample Backup Set 02 (1569565705365)		--	w2k16R2-std	GMT+08:00 (CST)	--
<input type="checkbox"/>	Server Run Office 365 Backup Set (1569566114447)		--	--	GMT+08:00 (CST)	<div>Backup</div> <div>Run</div>

- Modify the **In-file Delta type** and **Retention Policy** settings if necessary.


Backup

In-File Delta type

☒ Full
☐ Differential
☐ Incremental

Retention Policy

☐ Run Retention Policy after backup

- Click  at the bottom right corner to start the backup.
- You will see the status showing **Backup is Running** when the backup is in progress.

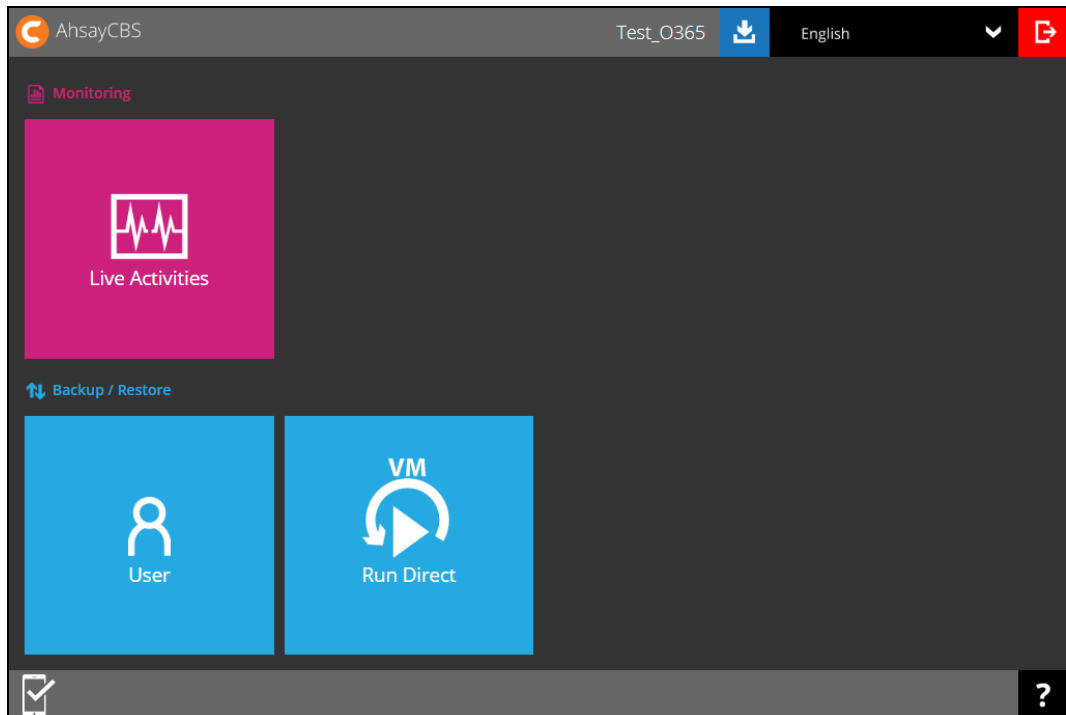
User Profile
Backup Set
Settings
Report
Statistics
Effective Policy

Manage Backup Set

+
-
↺

<input type="checkbox"/>	Name	Type	Version	Owner	Execute Job
<input type="checkbox"/>	Client Run Office 365 Backup Set (1569565334765)		--	w2k16R2-std	--
<input type="checkbox"/>	Sample Backup Set 01 (1569565679188)		--	w2k16R2-std	--
<input type="checkbox"/>	Sample Backup Set 02 (1569565705365)		--	w2k16R2-std	--
<input type="checkbox"/>	Server Run Office 365 Backup Set (1569566114447)		--	--	<div>Backup is Running</div> <div>Stop</div>

8. If you want to monitor the backup status, you need to go to **Live Activities** to watch the process.



AhsayCBS

Backup Status **Restore Status**

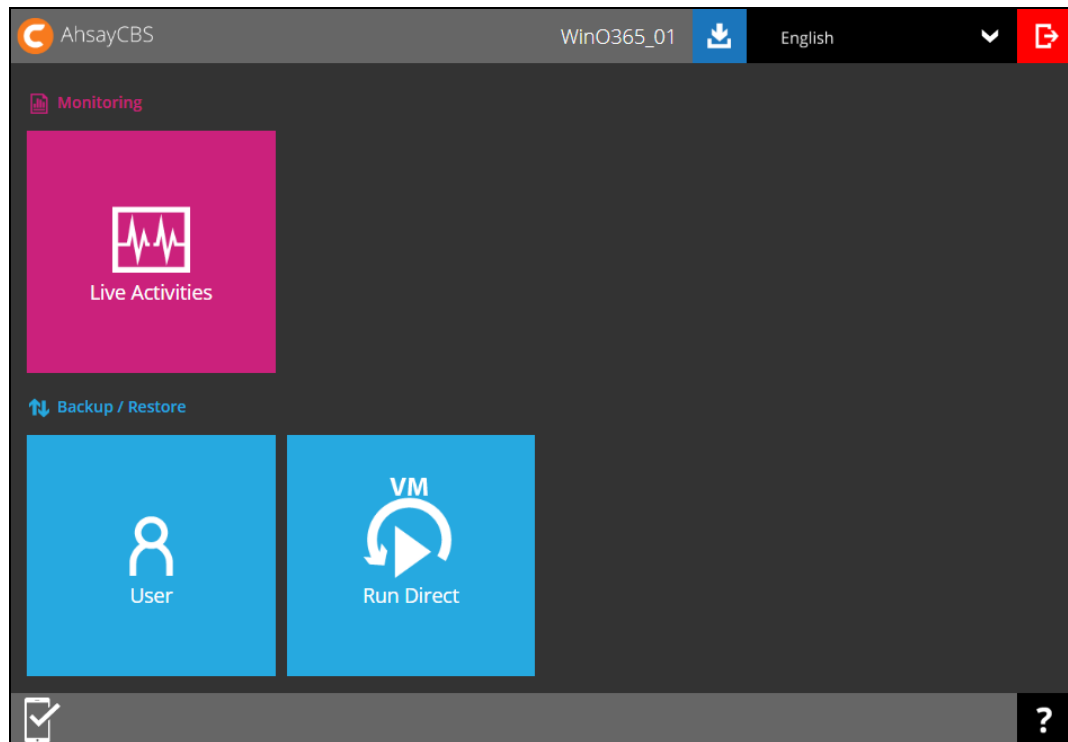
Backup jobs that are currently running or finished within 1 hour.

Login Name (Alias)	Owner	Backup Set	Destination	Progress	Estimated Time Left	Current File	Transfer Rate
Test_O365 ()	--	Client Run Office 365 Backup Set	AhsayCBS	33 %	51 min 21 sec	Office 365/Site Collections/ahsay-my.sharepoint.com/personal/yuk...say/1446099856193/blocks/2015-10-29-14-30-05/0/000000_00001d.bak	19Mibit/s
Test_O365 ()	--	Server Run Office 365 Backup Set	AhsayCBS	0 %	1 min 14 sec	Office 365/Site Collections/ahsay-my.sharepoint.com/personal/yuk_support_cloudbacko_biz/All Files/_vti_history/4096/Documents/TestFiles/Dog.jpg	42Mibit/s

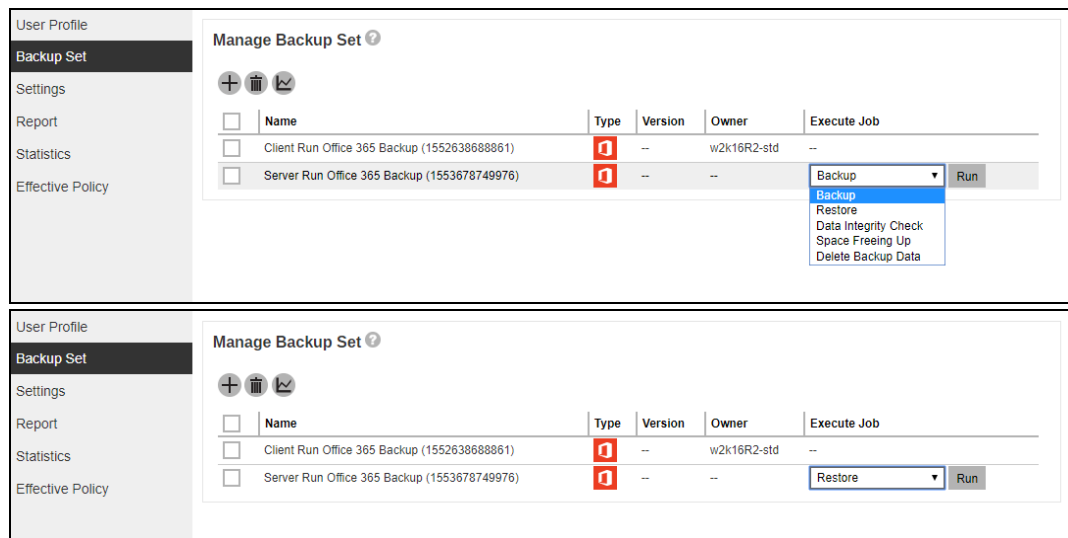
7 Restoring Office 365 Backup Set

7.1 Restore Backup with AhsayCBS User Web Console

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



3. You should see the backup set you would like to restore under **Backup Set > Manage Backup Set**. Click on the drop-down menu on the backup set you would like to restore, then select **Restore** and click **Run**.



4. Choose where the items to be restored from. Select to restore from **Users** or **Site Collections**. Click **Next** to continue.

7.1.1 From Users

For the backup data from Users

Choose Where The Items To Be Restored From

Restore items from

☒ Users

☐ 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 Your Items To Be Restored

Select What To Restore

Choose from files as of job ▾ 2019-03-29 ▾ Latest ▾

Show filter

Office 365

Public Folders

Users

@ahsay.onmicro

OneDrive

Outlook

Personal Site

File	Size	Last Modified
------	------	---------------

← → X ?

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

7.1.1.1 Original location

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.

Choose Where The Items To Be Restored

Restore Items To

☒ Original location

☐ Alternate location

☐ Alternate Office 365 account

[Show advanced option](#)

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.

Choose Where The Items To Be Restored

Restore Items To


☒ Original location

☐ Alternate location

☐ Alternate Office 365 account

☐ Verify checksum of in-file delta files during restore

[Hide advanced option](#)

Click  to start the restoration.

7.1.1.2 Alternate location

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.

Choose Where The Items To Be Restored

Restore Items To

☐ Original location

☒ Alternate location

☐ Alternate Office 365 account

[Show advanced option](#)

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.

Choose Where The Items To Be Restored

Restore Items To

☐ Original location

☒ Alternate location

☐ Alternate Office 365 account

☐ Verify checksum of in-file delta files during restore


[Hide advanced option](#)

[<](#) [>](#) [X](#) [?](#)

Alternate location

Office 365 account

[<](#) [>](#) [X](#) [?](#)

Click  to start the restoration.

7.1.1.3 Alternate Office 365 Account

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 and Password and choose the region for the other Office 365 account.

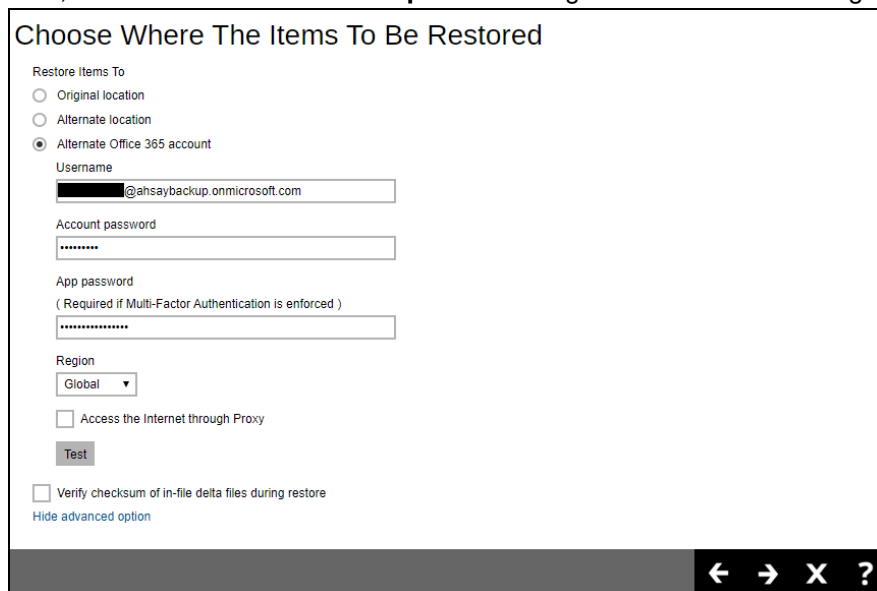
If the MFA of an alternate Office 365 account is enabled, then you are required to input the App password. Otherwise, restoration will not be able to proceed as it is mandatory.

Choose from the following **Region**:



A dropdown menu titled "Region" with a downward arrow icon. The menu is open, showing four options: "Global" (selected and highlighted in blue), "China", and "Germany".

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



A dialog box titled "Choose Where The Items To Be Restored". It contains the following fields and options:

- Restore Items To**
 - ☐ Original location
 - ☐ Alternate location
 - ☒ Alternate Office 365 account
- Username**
[Redacted]@ahsaybackup.onmicrosoft.com
- Account password**
[Redacted]
- App password**
(Required if Multi-Factor Authentication is enforced)
[Redacted]
- Region**
Global (dropdown menu)
- ☐ Access the Internet through Proxy
- Test** (button)
- ☐ Verify checksum of in-file delta files during restore
- [Hide advanced option](#)

At the bottom right, there is a navigation bar with icons: back, forward, close, and help.

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.

Choose Where The Items To Be Restored

Restore Items To

☐ Original location

☐ Alternate location

☒ Alternate Office 365 account

Username

Account password

App password

(Required if Multi-Factor Authentication is enforced)

Region

☐ Access the Internet through Proxy

☐ Verify checksum of in-file delta files during restore

[Hide advanced option](#)

← → ✕ ?

Press Test to validate the account. An alert message with OK message will show when the validation is successful, then click **OK** to continue.

Choose Where Th

10.90.10.12 says

OK

Restore Items To

☐ Original location

☐ Alternate location

☒ Alternate Office 365 account

Username

Account password

App password

(Required if Multi-Factor Authentication is enforced)

Region

☐ Access the Internet through Proxy


☐ Verify checksum of in-file delta files during restore

[Hide advanced option](#)

Alternate location

Office 365 account

← ↺ × ?

Click  to start the restoration.

7.1.2 From Site Collections

Choose Where The Items To Be Restored From

Restore items from

☐ Users

☒ 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 Your Items To Be Restored

Select What To Restore

Choose from files as of job

2019-03-29

Latest

Show filter

- ☒ Office 365
- ☒ Site Collections
 - ☒ ahsay-my.sharepoint

File	Size	Last Modified

← → X ?

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

8.1.2.1 Original location

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

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](#)

← ↺ ✕ ?

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.

Mode

Overwrite when exist ▼

Overwrite when exist

Skip when exist

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

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](#)

← ↺ ✕ ?

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.

Choose Where The Items To Be Restored

Restore Items To

☒ Original location

☐ Alternate location

☐ Alternate Office 365 account

Mode

Overwrite when exist ▾

☐ Verify checksum of in-file delta files during restore

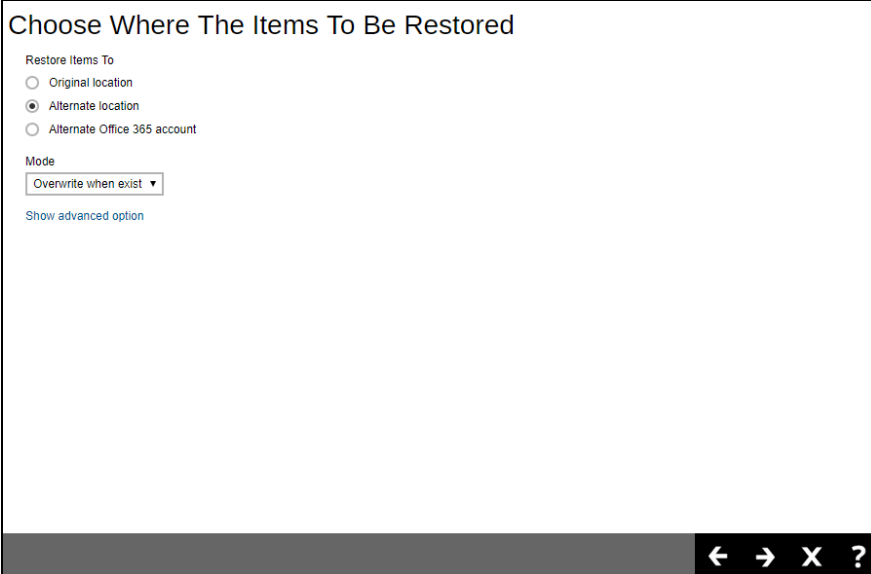
[Hide advanced option](#)

← ↺ ✕ ?

Click  to proceed.

8.1.2.2 Alternate Location

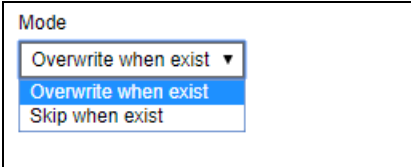
Choose from the following three (3) options on where you want your items to be restored. Select the **Alternate location**.



The screenshot shows a dialog box titled "Choose Where The Items To Be Restored". Inside, under the heading "Restore Items To", there are three radio button options: "Original location", "Alternate location" (which is selected), and "Alternate Office 365 account". Below this, there is a "Mode" section with a dropdown menu currently set to "Overwrite when exist". A link labeled "Show advanced option" is positioned below the mode dropdown. At the bottom right of the dialog box, there is a dark grey bar containing navigation icons: a left arrow, a right arrow, an 'X' for close, and a question mark for help.

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.



This is a close-up of the "Mode" dropdown menu. The dropdown is open, showing three options: "Overwrite when exist" (highlighted in blue), "Overwrite when exist", and "Skip when exist".

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

Choose Where The Items To Be Restored

Restore Items To

☐ Original location

☒ Alternate location

☐ Alternate Office 365 account

Mode

[Show advanced option](#)

← → ✕ ?

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.

Choose Where The Items To Be Restored

Restore Items To

☐ Original location

☒ Alternate location

☐ Alternate Office 365 account

Mode

☐ Verify checksum of in-file delta files during restore

[Hide advanced option](#)

← → ✕ ?

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.

Alternate location

Office 365 account
[redacted]@ahsaybackup.onmicrosoft.com

Site Collection / Site
[dropdown menu] **Change**

Change Site Collection / Site

Office 365

- Site Collections
 - ahsay.my.sharepoint.com
 - ahsay.sharepoint.com
 - ahsay.sharepoint.com/search
 - ahsay.sharepoint.com/sites/BlogDemo
 - ahsay.sharepoint.com/sites/CI
 - ahsay.sharepoint.com/sites/CIteam01
 - ahsay.sharepoint.com/sites/CIteam Site
 - ahsay.sharepoint.com/sites/CItestsite
 - ahsay.sharepoint.com/sites/DEV
 - ahsay.sharepoint.com/sites/DevTest
 - ahsay.sharepoint.com/sites/Dev_u_o_x_SITE
 - ahsay.sharepoint.com/sites/EdenClassic1
 - ahsay.sharepoint.com/sites/EdenClassic2
 - ahsay.sharepoint.com/sites/EdenClassic3
 - ahsay.sharepoint.com/sites/EdenCommunity

✓ X

Alternate location

Office 365 account
[redacted]@ahsaybackup.onmicrosoft.com

Site Collection / Site
Office 365/Site Collections/ahsay.sharepoint.com/sites/TestSr **Change**

← ↺ X ?

Click  to proceed.

8.1.2.3 Alternate Office 365 Account

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 and Password and choose the region for the other Office 365 account.

Choose Where The Items To Be Restored

Restore Items To

- ☐ Original location
- ☐ Alternate location
- ☒ Alternate Office 365 account

Username
[Redacted]@ahsaybackup.onmicrosoft.com

Account password
[Redacted]

App password
(Required if Multi-Factor Authentication is enforced)
[Redacted]

Region
Global

☐ Access the Internet through Proxy

Test

Mode
Overwrite when exist

[Show advanced option](#)

Choose from the following **Region**:

Region

Global

Global

China

Germany

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.

Mode

Overwrite when exist

Overwrite when exist

Skip when exist

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

Choose Where The Items To Be Restored

Restore Items To

☐ Original location

☐ Alternate location

☒ Alternate Office 365 account

Username

*****@ahsaybackup.onmicrosoft.com

Account password

App password

(Required if Multi-Factor Authentication is enforced)

Region

Global

☐ Access the Internet through Proxy

Test

Mode

Overwrite when exist

Show advanced option

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.

Choose Where The Items To Be Restored

Restore Items To

☐ Original location

☐ Alternate location

☒ Alternate Office 365 account

Username

*****@ahsaybackup.onmicrosoft.com

Account password

App password

(Required if Multi-Factor Authentication is enforced)

Region

Global

☐ Access the Internet through Proxy

Test

Mode

Overwrite when exist

☐ Verify checksum of in-file delta files during restore

Hide advanced option

Press **Test** to validate the account. An alert message with OK message will show when the validation is successful, then click **OK** to continue.

Choose Where To Restore

10.90.10.12 says
OK

OK

Restore Items To

☐ Original location
☐ Alternate location
☒ Alternate Office 365 account

Username

Account password

App password

(Required if Multi-Factor Authentication is enforced)

Region

☐ Access the Internet through Proxy

Mode

☐ Verify checksum of in-file delta files during restore
[Hide advanced option](#)

← → X ?

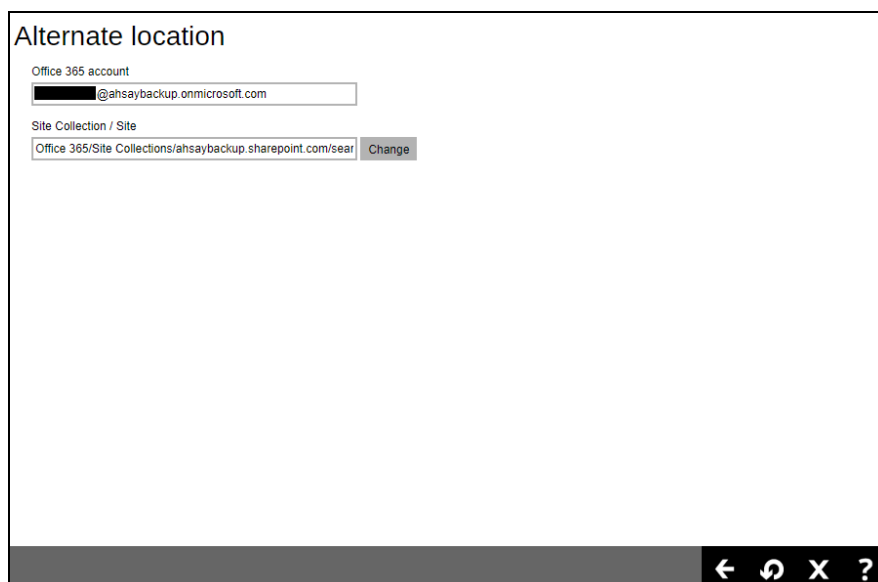
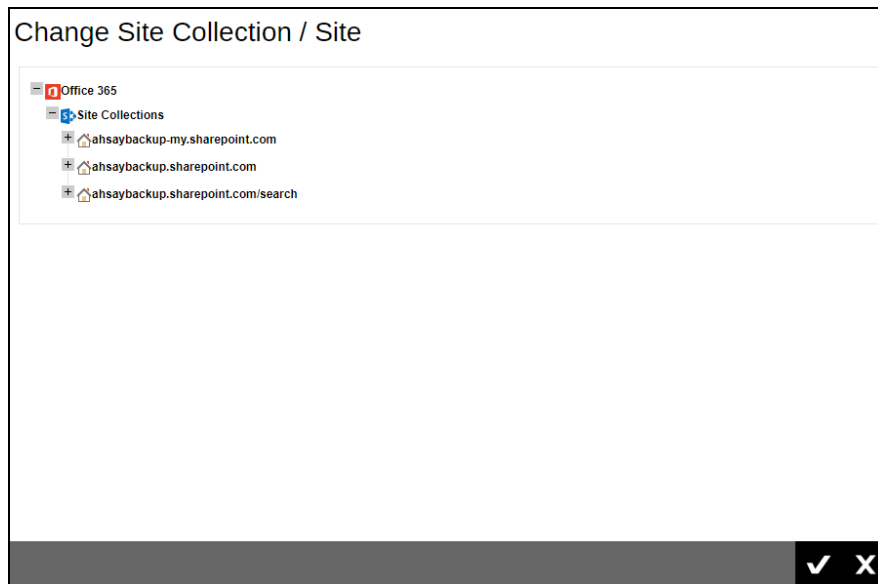
Click **Change** to select an alternate Site Collection / Site on which the data will be restored. Click on the dropdown arrow to view the available Sites.

Alternate location

Office 365 account

Site Collection / Site

← ↺ X ?



Click  to proceed.

1. You will see the status showing **Restore is Running** when the restore is in progress.

Name	Type	Version	Owner	Execute Job
Client Run Office 365 Backup (1552638688861)	Client	--	w2k16R2-std	--
Server Run Office 365 Backup (1553678749976)	Server	--	--	Restore is Running Stop

2. If you want to monitor the backup status, you need to go to **Live Activities** to watch the process.

Monitoring

Live Activities

Backup / Restore

User Run Direct

Login Name (Alias)	Owner	Backup Set	Destination	Progress	Estimated Time Left	Current File	Transfer Rate
WinO365_01 ()	--	Server Run Office 365 Backup	AhsayCBS	0 %	0 sec		0bit/s

8 Running a Data Integrity Check

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

- **AhsayOBM / Ahsay ACB User**

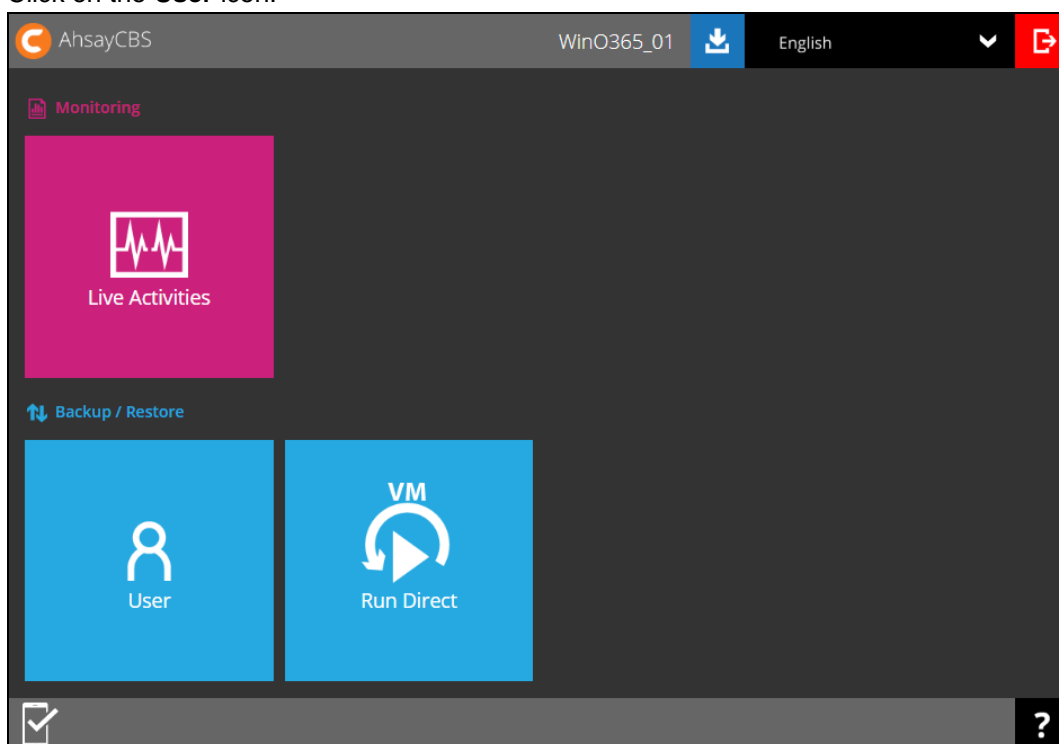
This option allows the AhsayOBM and AhsayACB users to perform data integrity check, but the results check cannot be reviewed. It will only be available upon request from your backup service provider.

Please contact your backup service provider for more information.

- **Backup Service Provider**

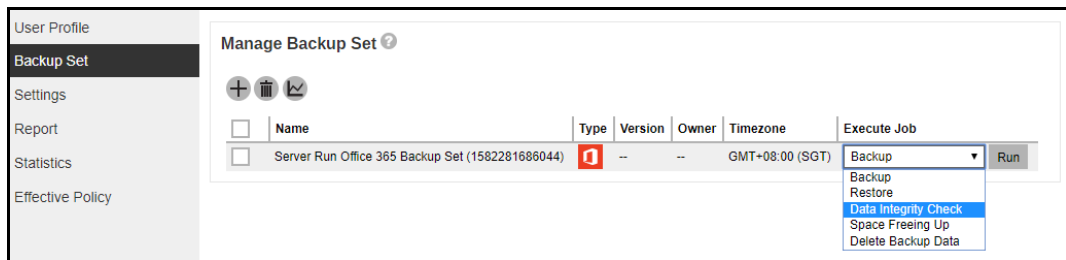
This is the recommended option, the AhsayOBM and AhsayACB users to request their backup service provider to perform data integrity check and provide them with a report of the results and or solution.

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



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



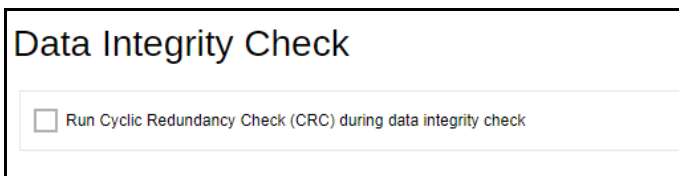



Run Cyclic Redundancy Check (CRC)

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

If there is a discrepancy, this indicates that the files on the backup destination(s) are corrupted. These corrupted files will be removed from the backup destination(s). If these files still exist on the backup server on the next backup job, the AhsayCBS will upload the latest copy.

However, if the corrupted files are in the retention area, they will not be backed up again as the source file has already been deleted from the backup server.



4. Click the  icon to begin the data integrity check process.

During a backup job, a Periodic Data Integrity Check (PDIC) will be performed as part of the backup process. This feature provides an additional regular data integrity check of the backup data.

9 Performing a Space Freeing Up

Space Freeing Up can be done in two (2) ways.

- **AhsayOBM / Ahsay ACB User**

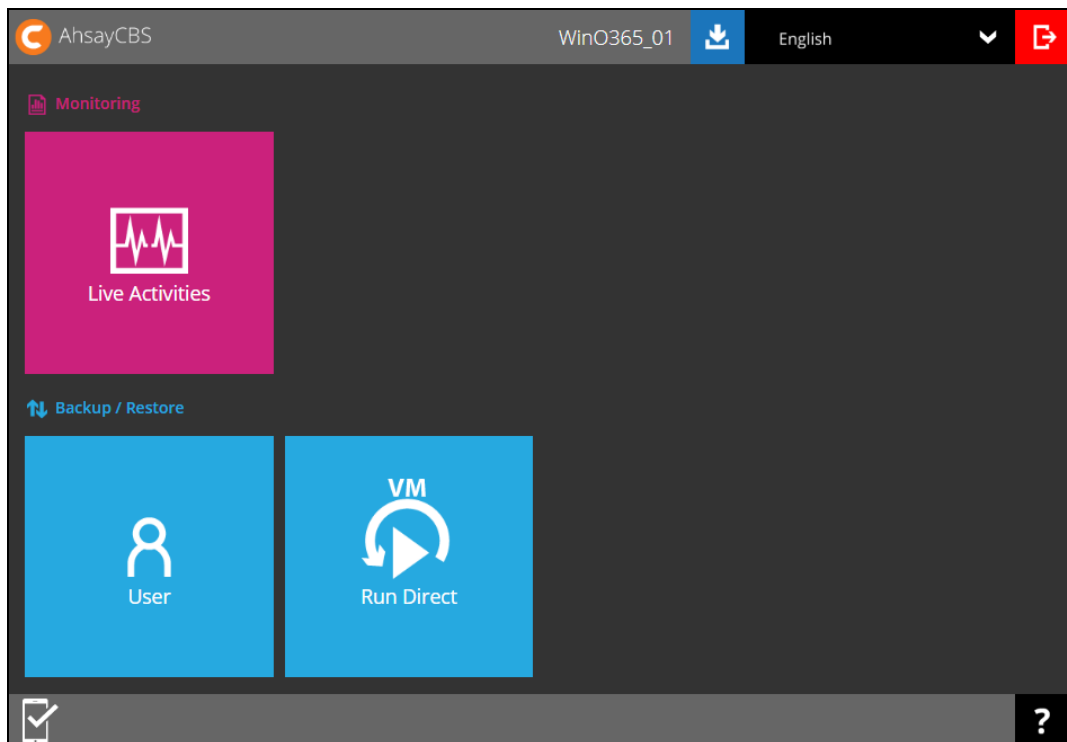
This option allows the AhsayOBM and AhsayACB users to perform space freeing up, but the results check cannot be reviewed. It will only be available upon request from your backup service provider.

Please contact your backup service provider for more information.

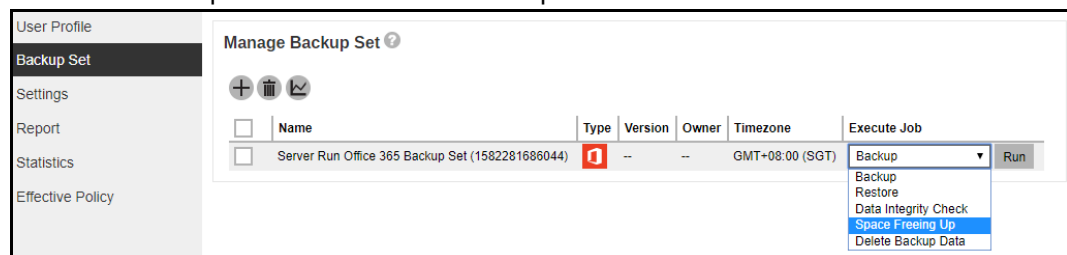
- **Backup Service Provider**

This is the recommended option, the AhsayOBM and AhsayACB users to request their backup service provider to perform space freeing up and provide them with a report of the results and or solution.

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



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




User Profile
Backup Set
Settings
Report
Statistics

Manage Backup Set ?

+
-
↺

<input type="checkbox"/>	Name	Type	Version	Owner	Timezone	Execute Job
<input type="checkbox"/>	Server Run Office 365 Backup Set (1582281686044)		--	--	GMT+08:00 (SGT)	Space Freeing Up Run

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

User Profile
Backup Set
Settings
Report
Statistics

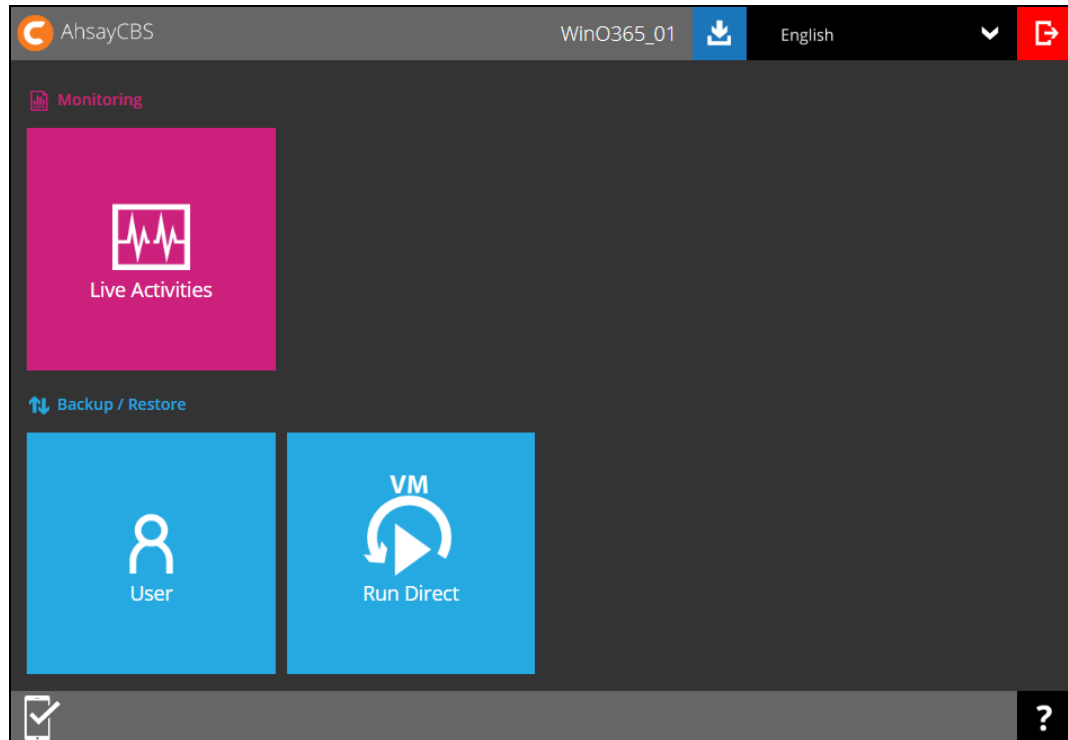
Manage Backup Set ?

+
-
↺

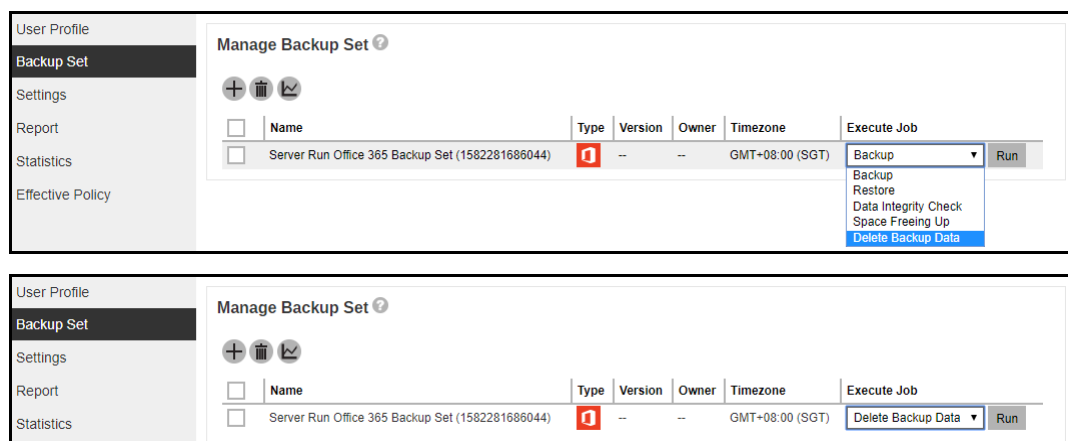
<input type="checkbox"/>	Name	Type	Version	Owner	Timezone	Execute Job
<input type="checkbox"/>	Server Run Office 365 Backup Set (1582281686044)		--	--	GMT+08:00 (SGT)	Space Freeing Up is Running Stop

10 Deleting Backup Data

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



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



4. Click the **Confirm** button to delete all files. Otherwise, click the **Cancel** button.

The screenshot shows the 'Manage Backup Set' interface with a warning dialog box. The dialog box has a yellow warning icon and the text 'Warning' in orange. Below it, the text reads 'Delete all files (Server Run Office 365 Backup Set - AhsayCBS)?'. At the bottom of the dialog are two buttons: 'Confirm' (red) and 'Cancel' (grey).

The background interface shows a sidebar with 'User Profile', 'Backup Set', 'Settings', 'Report', 'Statistics', and 'Effective Policy'. The main area is titled 'Manage Backup Set' and contains a table with columns: Name, Type, Version, Owner, Timezone, and Execute Job. The table has one row with the following data:

Name	Type	Version	Owner	Timezone	Execute Job
Server Run Office 365 Backup Set (1582281686044)	1	--	--	GMT+08:00 (SGT)	Delete Backup Data is Running

NOTE

Delete backup data action is not reversible. It will physically delete the selected backup data regardless of the defined retention policy settings. Therefore, make sure to select the correct backup data to be deleted before you proceed.

11 Contact Ahsay

11.1 Technical Assistance

To contact Ahsay support representatives for technical assistance, visit the Partner Portal:

<https://www.ahsay.com/partners/>

Also use the Ahsay Wikipedia for resource such as Hardware Compatibility List, Software Compatibility List, and other product information:

<https://wiki.ahsay.com/>

11.2 Documentation

Documentations for all Ahsay products are available at:

https://www.ahsay.com/jsp/en/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

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, three 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.

Backup Set Name	Files and/or Folders
Backup Set A	Folder01 <ul style="list-style-type: none">○ microsoftword01.docx○ powerpointpresentation01.pptx○ spreadsheet01.xls○ notepad01.txt○ picture01.jpg○ picture02.jpg
Backup Set B	Folder01 <ul style="list-style-type: none">○ microsoftword01.docx○ powerpointpresentation01.pptx○ spreadsheet01.xls○ notepad01.txt○ picture01.jpg○ picture02.jpg
	Folder02
	Folder03
Backup Set C	Folder01 <ul style="list-style-type: none">○ microsoftword01.docx○ powerpointpresentation01.pptx○ spreadsheet01.xls○ notepad01.txt○ picture01.jpg○ picture02.jpg
	Folder02
	Folder03 <ul style="list-style-type: none">○ microsoftword02.docx○ powerpointpresentation02.pptx○ spreadsheet02.xls○ notepad02txt○ picture05.jpg○ picture06.jpg

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 one (1) 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 <ul style="list-style-type: none"> ○ 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 <ul style="list-style-type: none"> ○ 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 not 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

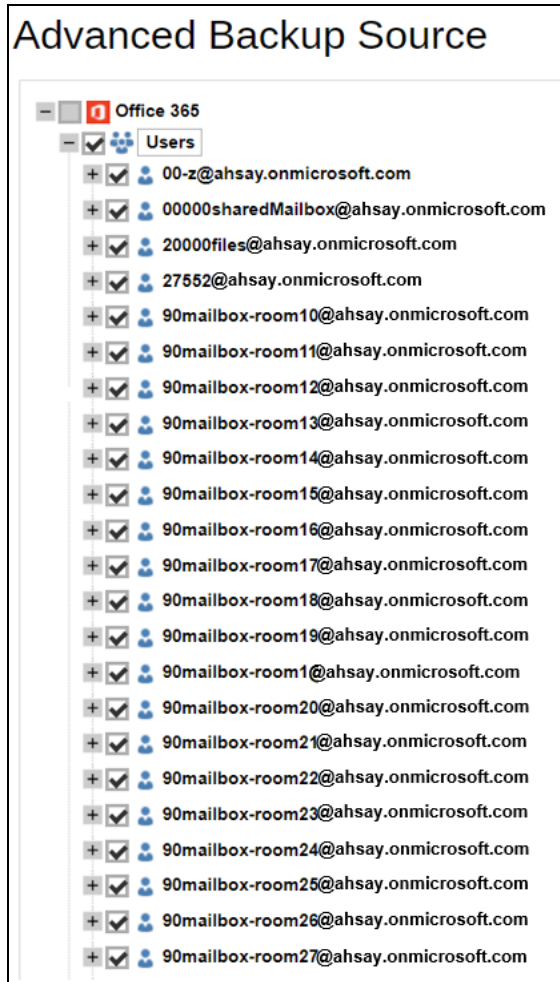
Backup Set Name	User Number
Backup -Set-1	No.1 – 2000
Backup -Set-2	No.2001 – 4000
Backup -Set-3	No. 4001 – 6000
Backup -Set-4	No. 6001 – 8000
Backup -Set-5	No. 8001 – 10000

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

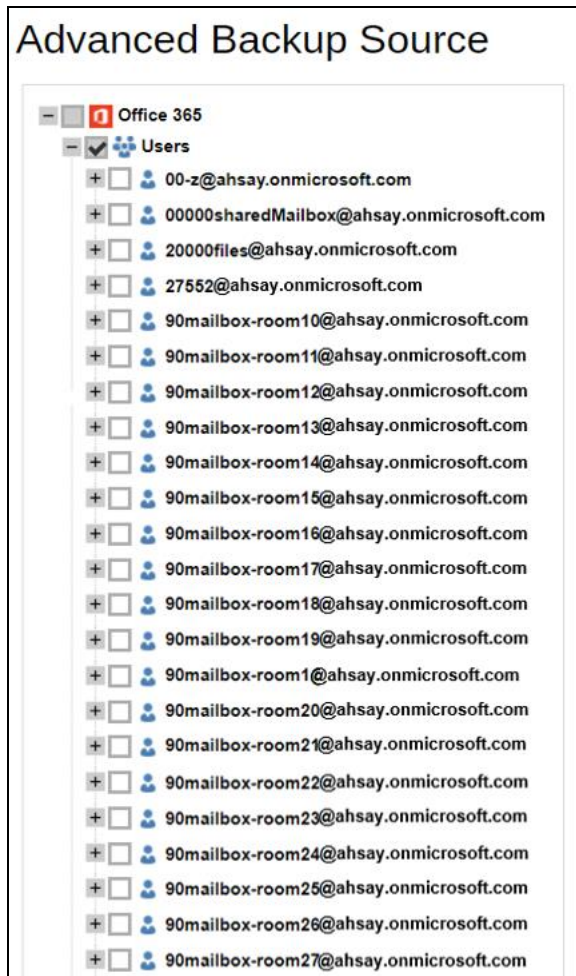
Backup Set Name	User Number
Backup -Set-1	No.1 – 1000
Backup -Set-2	No.1001 – 2000
Backup -Set-3	No. 2001 – 3000
Backup -Set-4	No. 3001 – 4000
Backup -Set-5	No. 4001 – 5000
Backup -Set-6	No. 5001 – 6000
Backup -Set-7	No. 6001 – 7000
Backup -Set-8	No. 7001 – 8000
Backup -Set-9	No. 8001 – 9000
Backup -Set-10	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 9,000 Office 365 users.

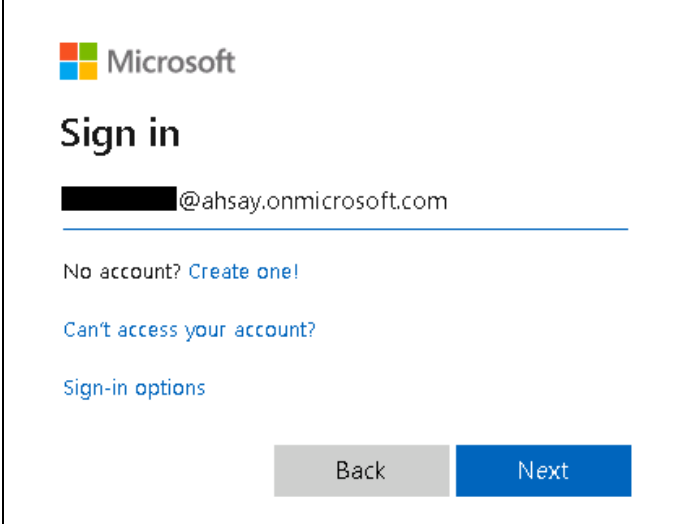


Appendix C: Setting Multi-Factor Authentication (MFA) in Microsoft 365 Admin Center

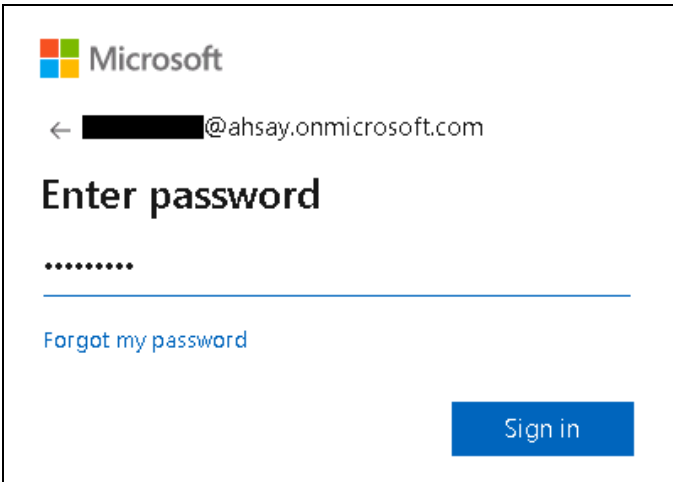
What is a Multi-Factor Authentication (MFA)? It is an authentication method wherein a user will be granted an access only after successfully presenting two or more evidences or proof of personal information or identification. It also adds second layer of security to users upon logging in.

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

1. Login using an Office 365 Administrator credentials.

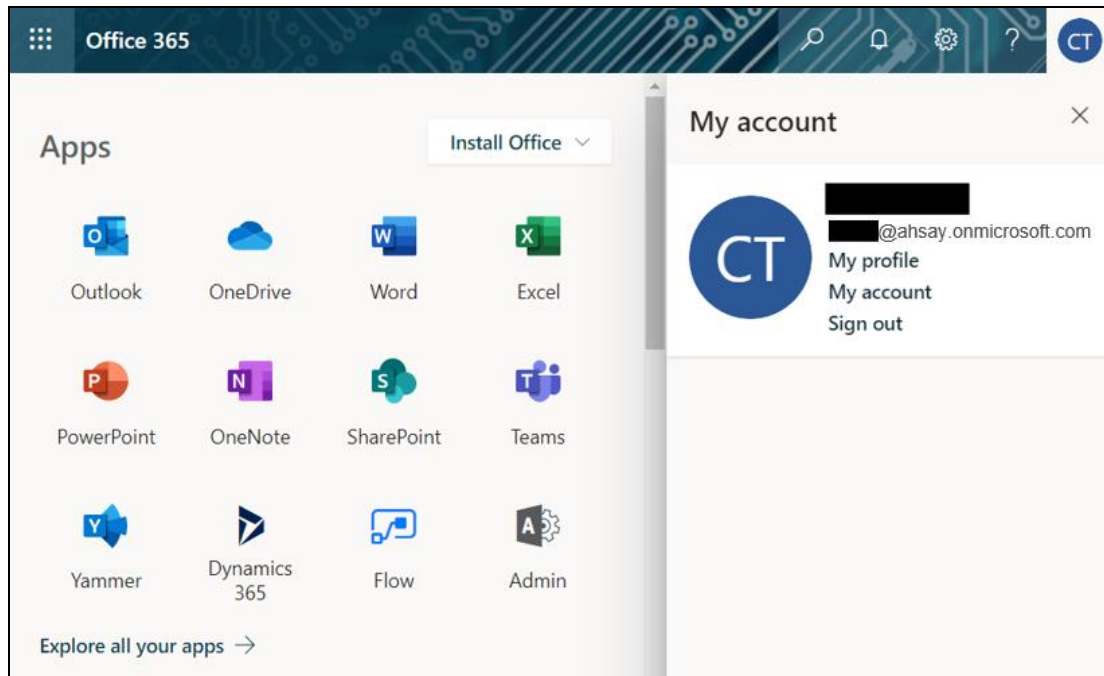
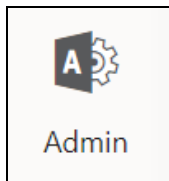


The image shows the Microsoft sign-in page. At the top is the Microsoft logo. Below it is the heading "Sign in". There is a text input field containing a redacted email address followed by "@ahsay.onmicrosoft.com". Below the input field are three links: "No account? [Create one!](#)", "[Can't access your account?](#)", and "[Sign-in options](#)". At the bottom right are two buttons: a grey "Back" button and a blue "Next" button.

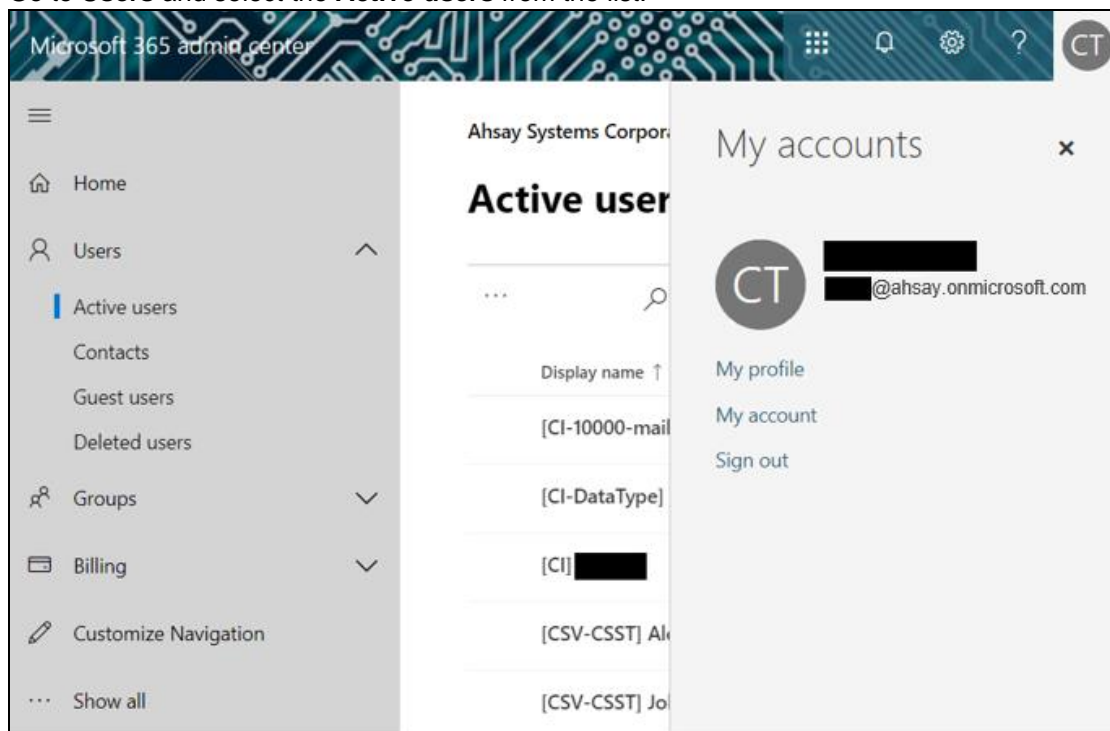


The image shows the Microsoft "Enter password" screen. At the top is the Microsoft logo. Below it is a back arrow followed by a redacted email address and "@ahsay.onmicrosoft.com". The heading "Enter password" is displayed. Below it is a password input field with dots. At the bottom left is a link "[Forgot my password](#)". At the bottom right is a blue "Sign in" button.

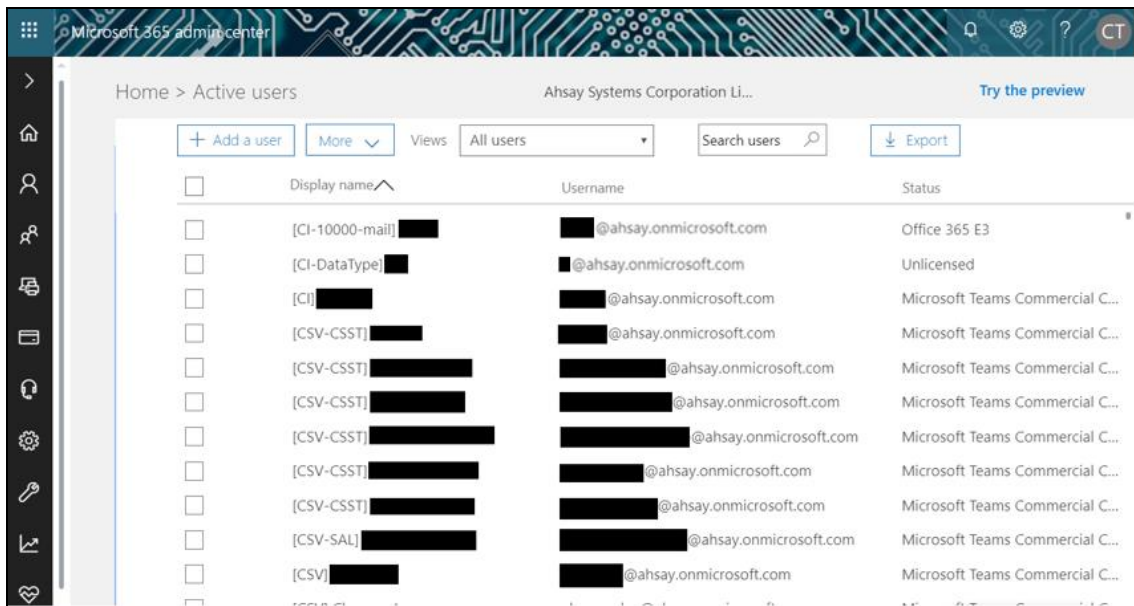
2. Click the **Admin Center** icon.



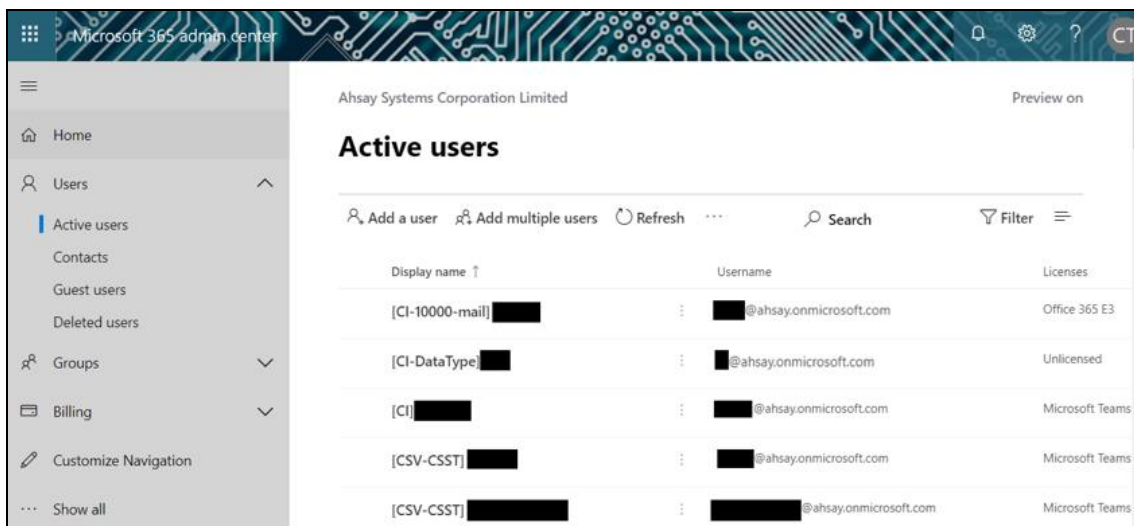
3. Go to **Users** and select the **Active users** from the list.



4. There are two (2) modes of viewing the Active users.
Classic Mode – This is the default mode upon entering the Active users screen.



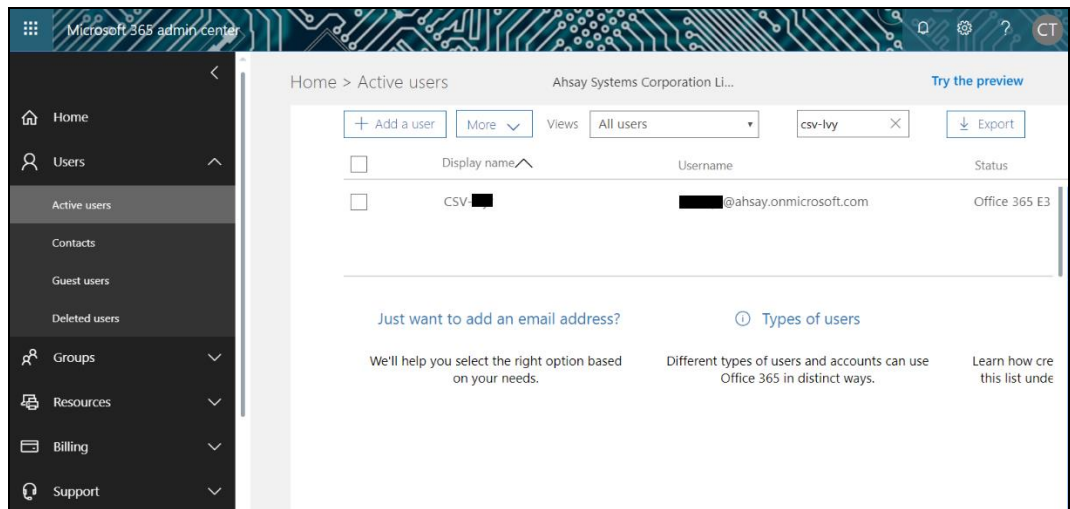
Preview Mode – This is a new feature in the Office 365 Admin Center that offers simplification to manage your Microsoft 365 and Office 365 services. It also has all the capabilities of the classic mode.



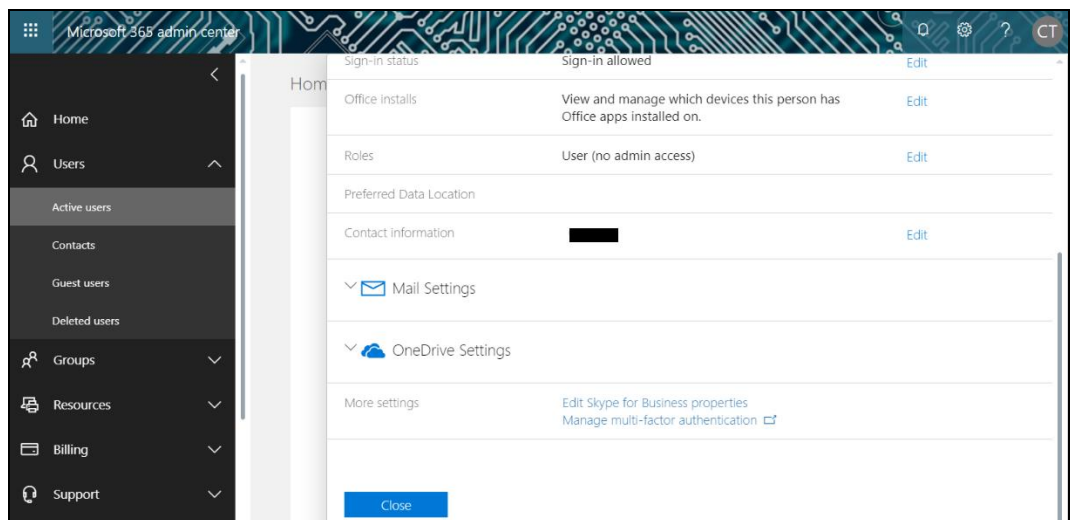
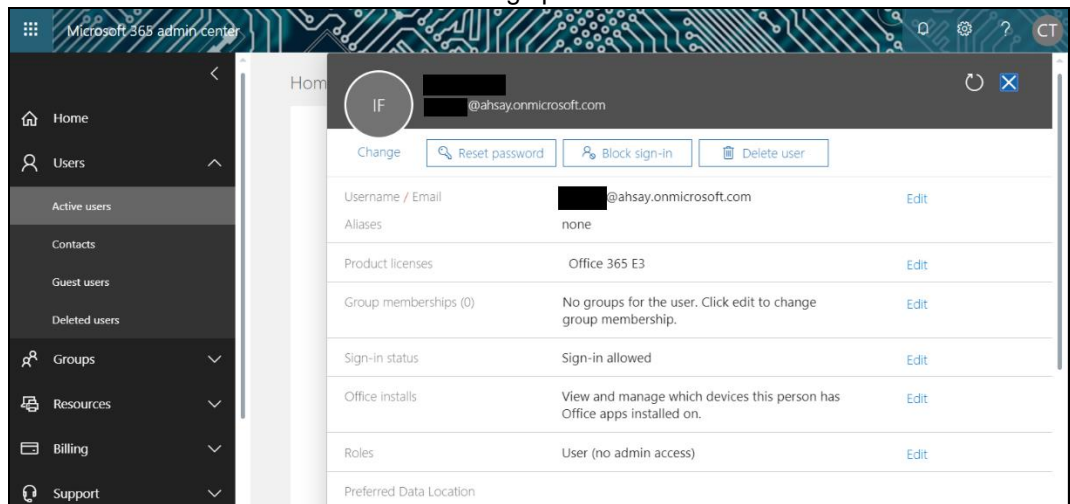
5. To go to the Multifactor Authentication screen, below are the steps for classic and preview mode.

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.



More settings

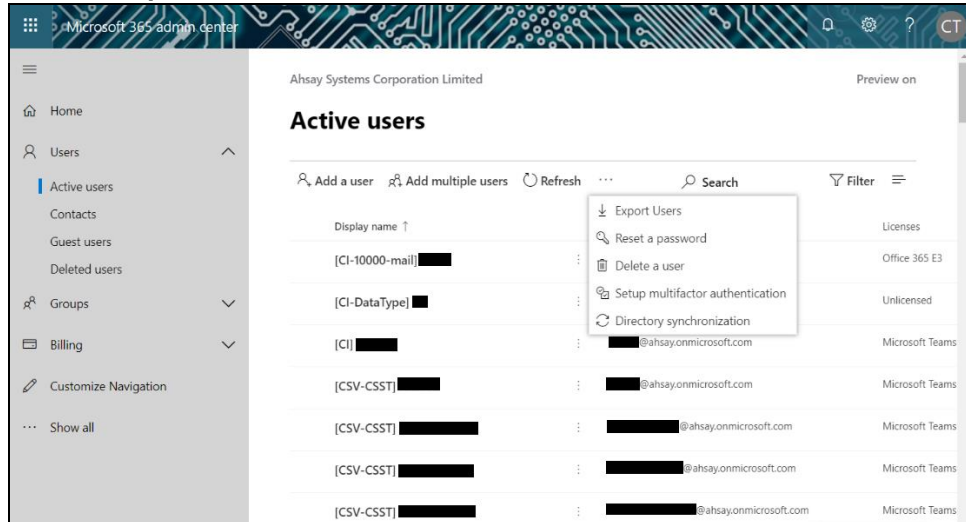
Edit Skype for Business properties
Manage multi-factor authentication [🔗](#)

For the Preview Mode:

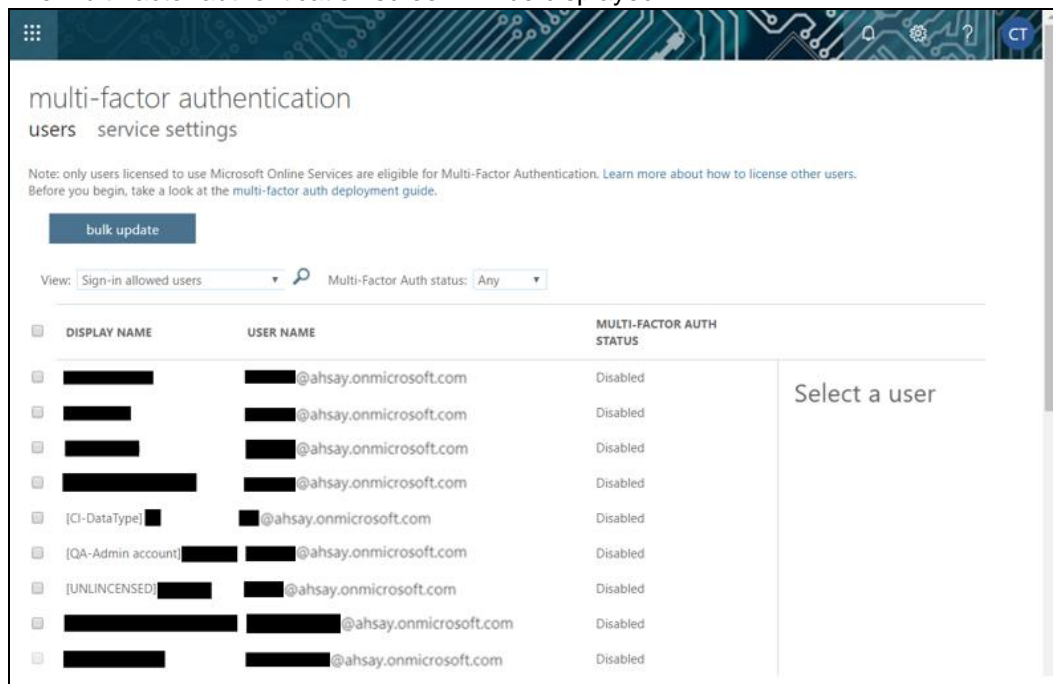
- In the Active user's screen, click the [...] ellipses.



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

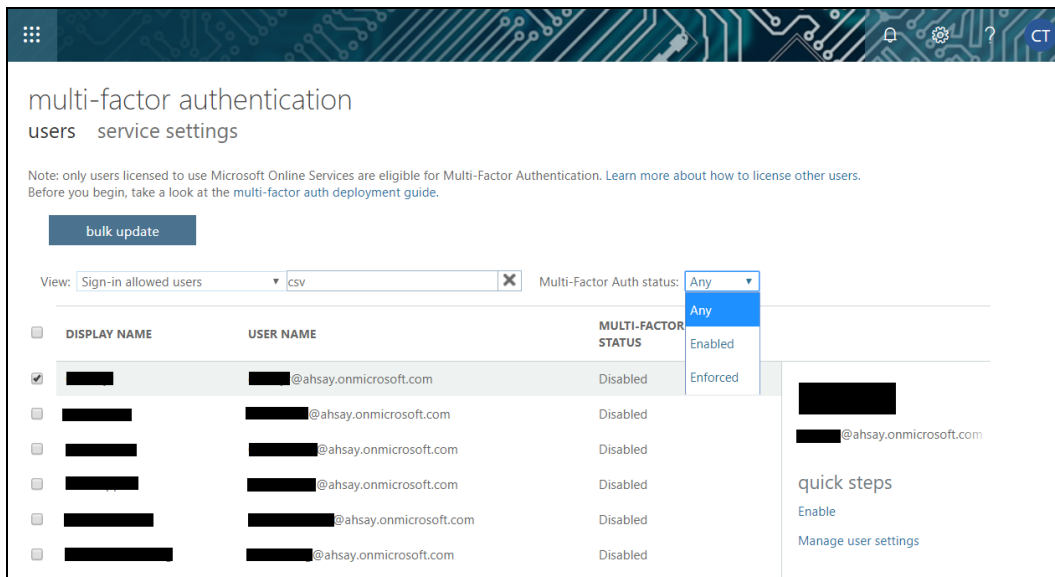


- The multi-factor authentication screen will be displayed.

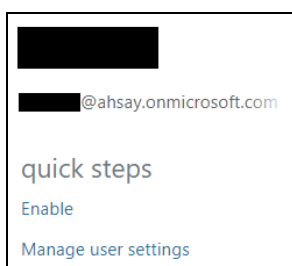
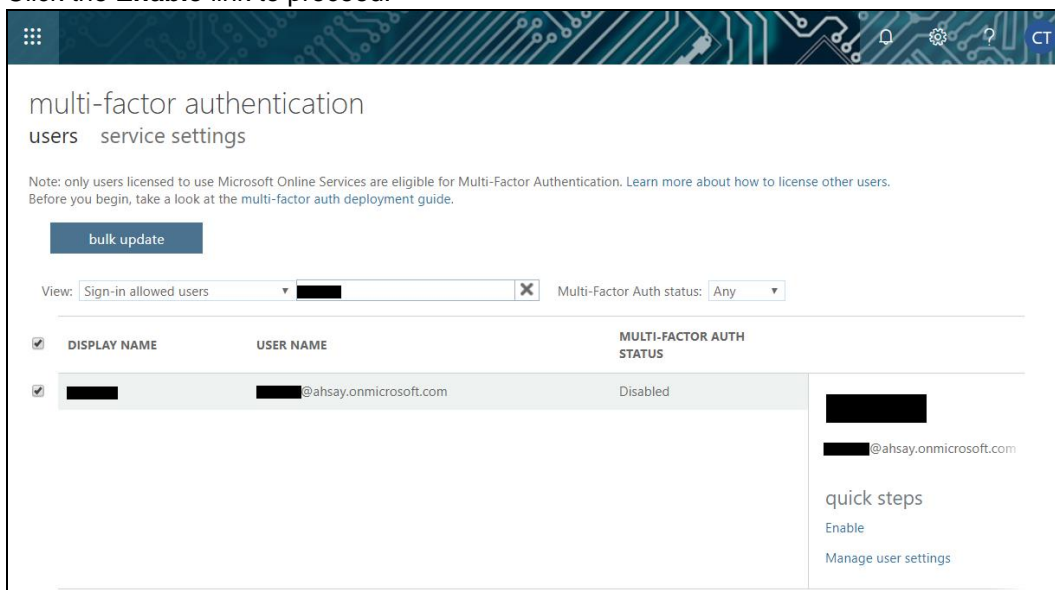


Note: The two (2) modes will go to the same screen.

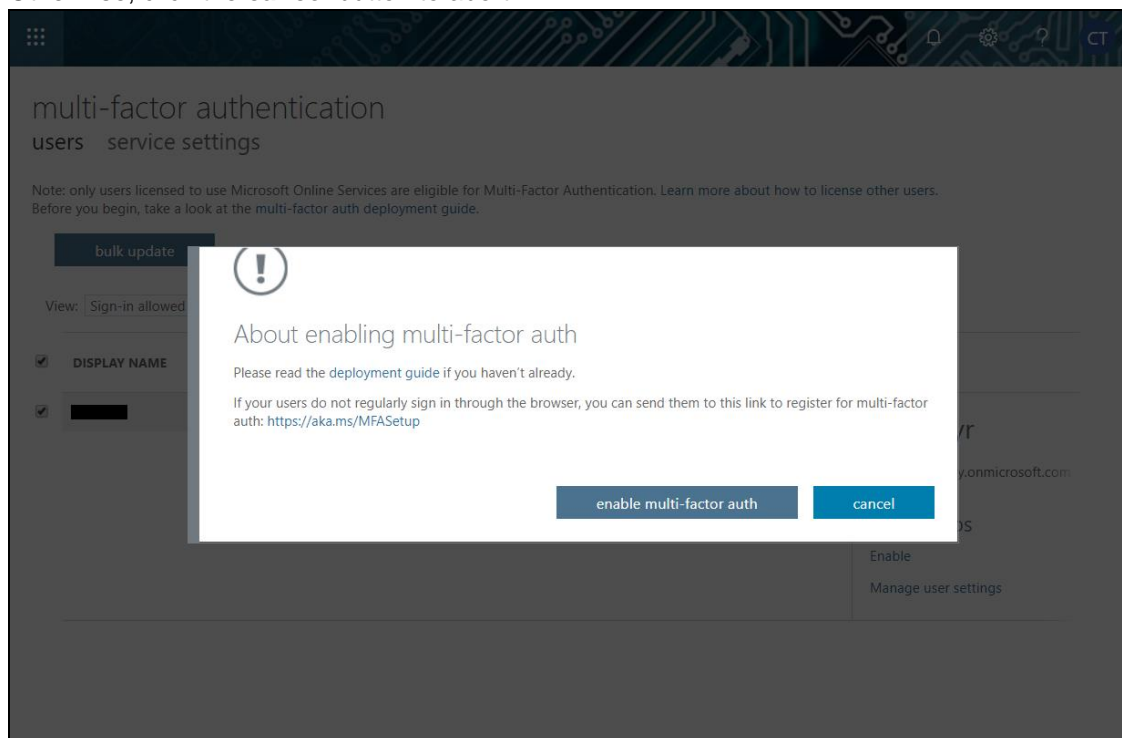
- You can search and select one or more Office 365 user accounts. There is also a drop-down list available for multi-factor authentication status namely, **Disabled**, **Enabled**, and **Enforced**.



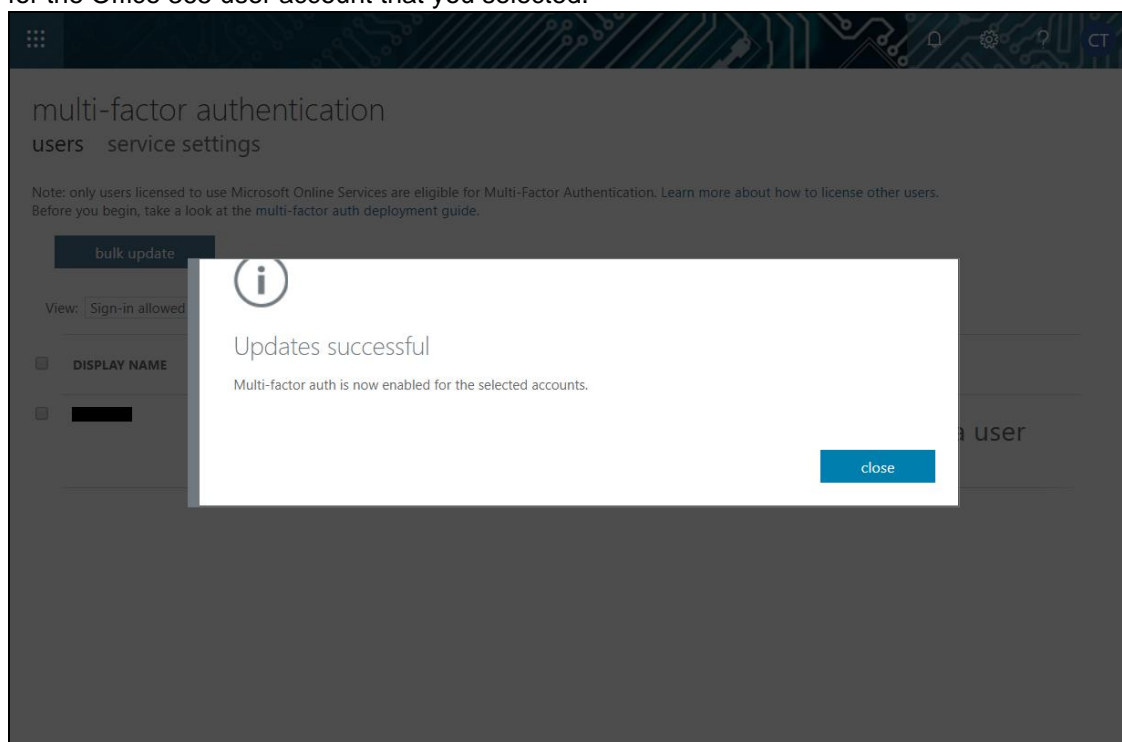
- Disabled – This status refers to the users who are not yet enrolled in the MFA. This is the default status.
 - Enabled – This status refers to the users who are enrolled in the MFA, but changes have not yet taken effect.
 - Enforced – This status refers to the users who are enrolled in the MFA has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



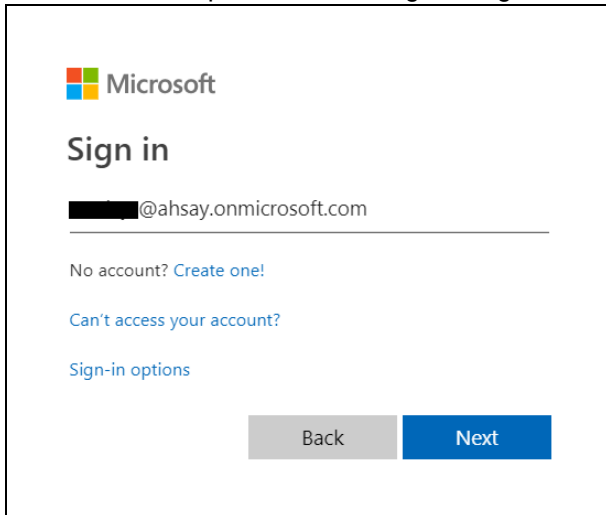
9. A warning message will be displayed. Click the **enable multi-factor auth** button to proceed. Otherwise, click the **cancel** button to abort.



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.



Microsoft

Sign in

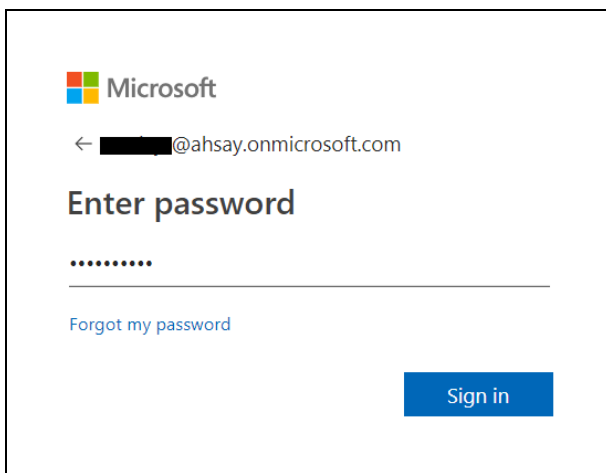
██████@ahsay.onmicrosoft.com

No account? [Create one!](#)

[Can't access your account?](#)

[Sign-in options](#)

[Back](#) [Next](#)



Microsoft

← ██████@ahsay.onmicrosoft.com

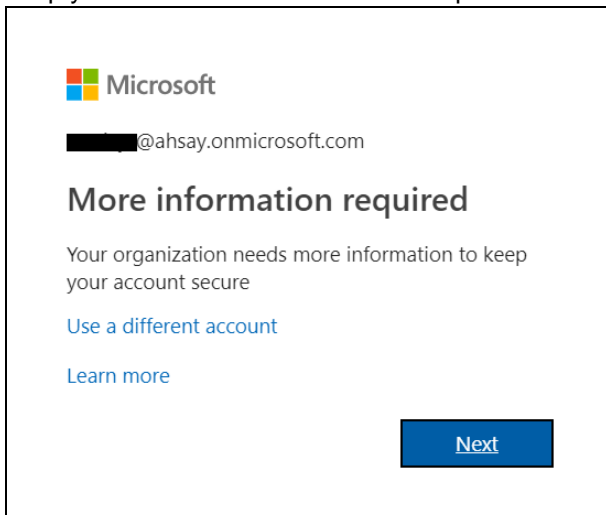
Enter password

.....

[Forgot my password](#)

[Sign in](#)

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.



Microsoft

██████@ahsay.onmicrosoft.com

More information required

Your organization needs more information to keep your account secure

[Use a different account](#)

[Learn more](#)

[Next](#)

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**.

Microsoft

Additional security verification

Secure your account by adding phone verification to your password. [View video to know how to secure your account](#)

Step 1: How should we contact you?

Authentication phone ▼

Select your country or region ▼

Phone number can contain only the digits 0-9, dash, space, period and parentheses.

Method

☐ Send me a code by text message

☒ Call me

Next

Your phone numbers will only be used for account security. Standard telephone and SMS charges will apply.

©2019 Microsoft Legal | Privacy

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

Microsoft

Additional security verification

Secure your account by adding phone verification to your password. [View video to know how to secure your account](#)

Step 1: How should we contact you?

Authentication phone ▼

Philippines (+63) ▼ 9338544479

Method

☒ Send me a code by text message

☐ Call me

Next

Your phone numbers will only be used for account security. Standard telephone and SMS charges will apply.

©2019 Microsoft Legal | Privacy

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

Microsoft

Additional security verification

Secure your account by adding phone verification to your password. [View video to know how to secure your account](#)

Step 1: How should we contact you?

Office phone ▼

Select your country or region ▼ Extension

Contact your admin if you need to update your office number. Do not use a Lync phone.

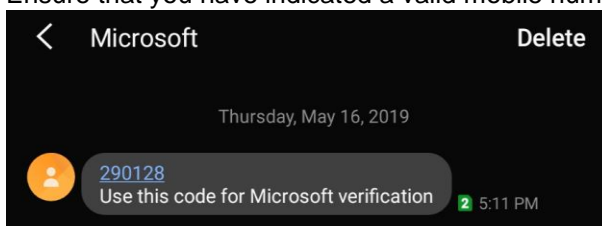
Next

Your phone numbers will only be used for account security. Standard telephone and SMS charges will apply.

© 2019 Microsoft Legal | Privacy

- 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.



Microsoft

Additional security verification

Secure your account by adding phone verification to your password. [View video to know how to secure your account](#)

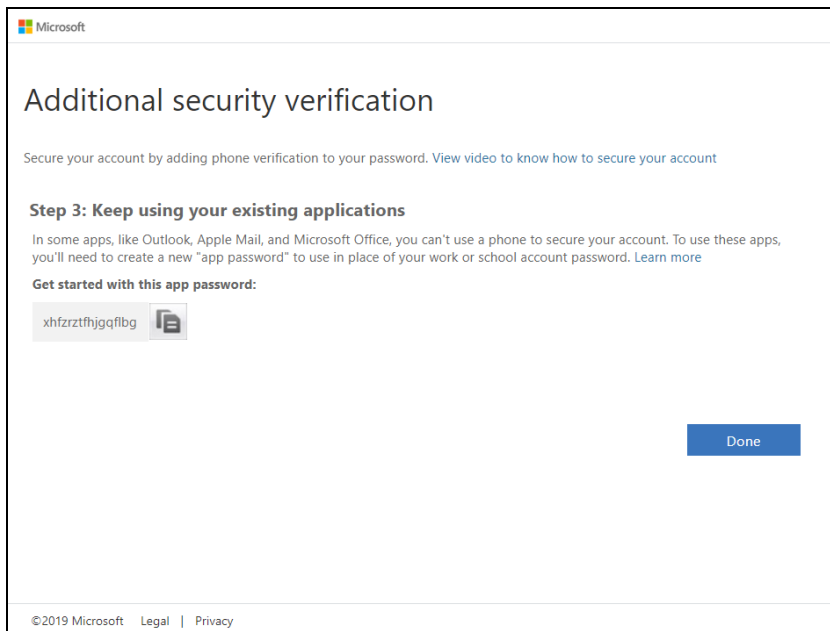
Step 2: We've sent a text message to your phone at +63 [redacted]

When you receive the verification code, enter it here

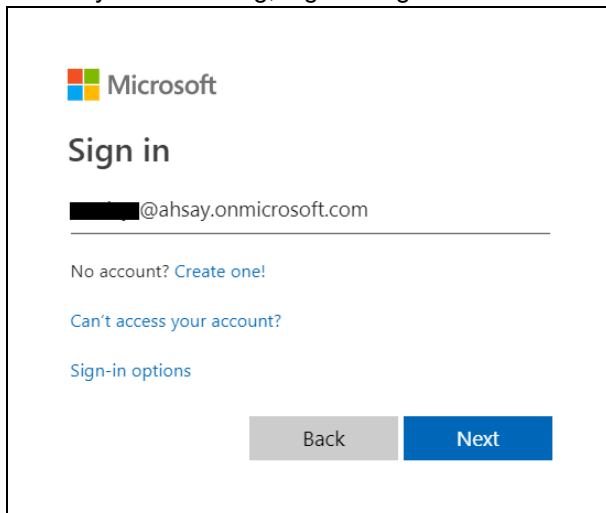
290128

Cancel Verify


© 2019 Microsoft Legal | Privacy



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

██████████@ahsay.onmicrosoft.com

Enter code

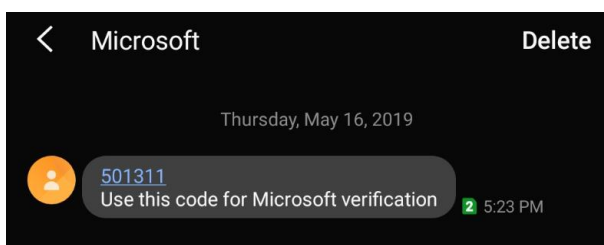
 We texted your phone +XX XXXXXXXX79. Please enter the code to sign in.


Code

Having trouble? [Sign in another way](#)

[More information](#)


Verify



 Microsoft

██████████@ahsay.onmicrosoft.com

Enter code

 We texted your phone +XX XXXXXXXX79. Please enter the code to sign in.

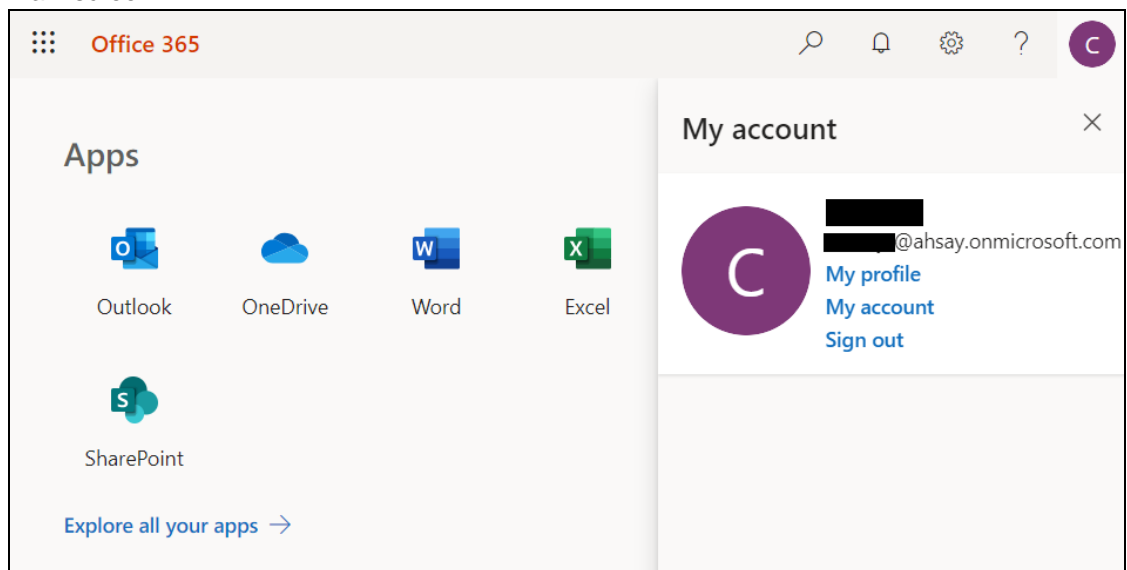
501311

Having trouble? [Sign in another way](#)

[More information](#)

Verify

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







Appendix D: Example Scenario for 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 report for the warning message.

Backup Report for This User					
			View Today ▾		
Backup Set	Destination	Start Time	End Time	Status	
 Server Run Office 365 Backup Set(1608711251295)	 AhsayCBS	28-Dec-2020 11:23 JST	28-Dec-2020 11:25 JST	Warn	
 Server Run Office 365 Backup Set(1608711251295)	 AhsayCBS	28-Dec-2020 11:19 JST	28-Dec-2020 11:21 JST	OK	

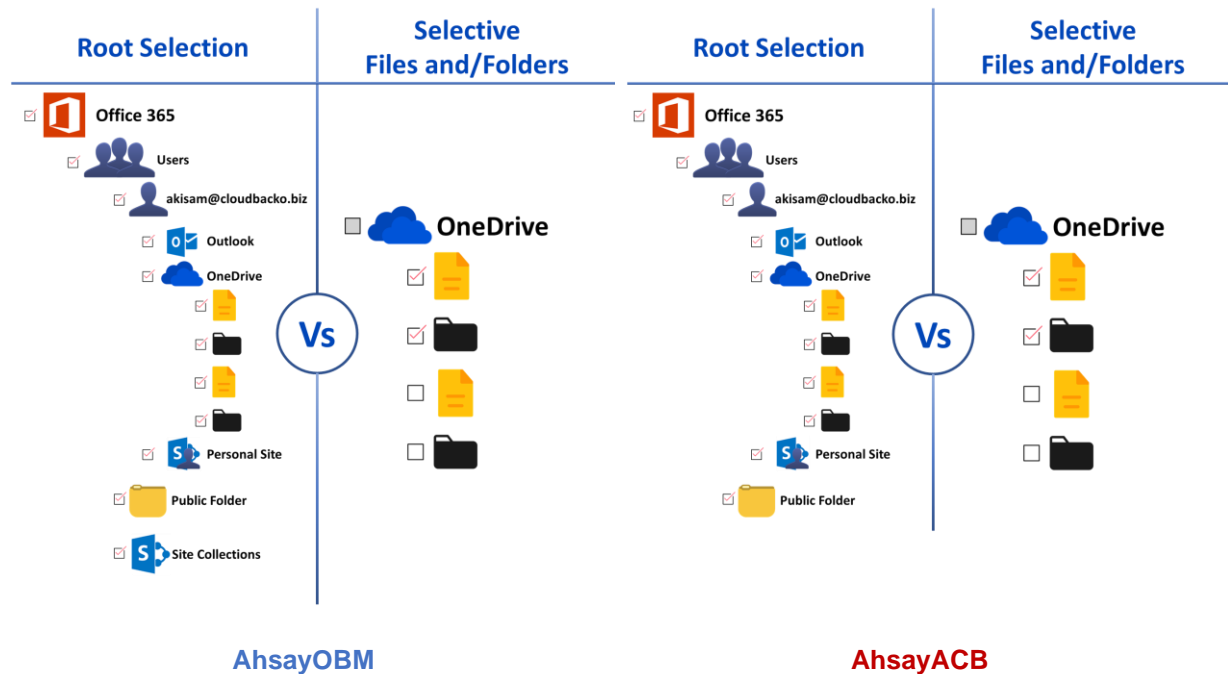
Backup report contains a warning message.

5	warn	2020/12/28 11:24:22	Backup source "Office 365/Users/[REDACTED]@ahsay.onmicrosoft.com" does not exist !
---	------	---------------------	--

Backup Logs			
No.	Type	Timestamp	Log
1	start	2020/12/28 11:23:41	Start [Ahsay Cloud Backup Suite v8.3.4.0]
2	info	2020/12/28 11:23:47	Using Temporary Directory C:\Program Files\AhsayCBS\temp\1608711251295\Local@1608712072920
3	info	2020/12/28 11:24:14	Download valid index files from backup job "Current" to "C:\Program Files\AhsayCBS\temp\1608711251295\Local@1608712072920\index".
4	info	2020/12/28 11:24:20	Office 365 Data Synchronization Check is disabled (Debug option: "Office365.DSCItemset" = -1)
5	warn	2020/12/28 11:24:22	Backup source "Office 365/Users/[REDACTED]@ahsay.onmicrosoft.com" does not exist !
6	info	2020/12/28 11:24:23	Download valid index files from backup job "Current" to "C:\Program Files\AhsayCBS\temp\1608711251295\Local@1608712072920\index\sub index\ee13ef62-567f-3023-b83d-ef00fd0e91ff".
7	info	2020/12/28 11:24:25	Start validating the presence and size of backup data in destination "AhsayCBS"...
8	info	2020/12/28 11:24:25	Finished validating the presence and size of backup data in destination "AhsayCBS"
9	info	2020/12/28 11:24:29	Download valid index files from backup job "Current" to "C:\Program Files\AhsayCBS\temp\1608711251295\Local@1608712072920\index\sub index\16c1db78-565a-3a2b-a234-0d84a739b3a5".
10	info	2020/12/28 11:24:51	Start validating the presence and size of backup data in destination "AhsayCBS"...
11	info	2020/12/28 11:24:51	File: "1608711251295/blocks/2020-12-28-11-23-34/0/000000.bak", Size: 155,808, OK
12	info	2020/12/28 11:24:51	Finished validating the presence and size of backup data in destination "AhsayCBS"
13	info	2020/12/28 11:24:56	Start validating the presence and size of backup data in destination "AhsayCBS"...
14	info	2020/12/28 11:24:56	Finished validating the presence and size of backup data in destination "AhsayCBS"
15	info	2020/12/28 11:25:00	Quota (E-mail Account): 3
16	info	2020/12/28 11:25:00	Quota (E-mail Account) used in this backup set: 1
17	info	2020/12/28 11:25:00	l.yuk.support@cloudbacko.biz

Appendix E: Example Scenario for Data Synchronization Check (DSC) with sample backup reports

Selection of root folder vs Selective files and/folders



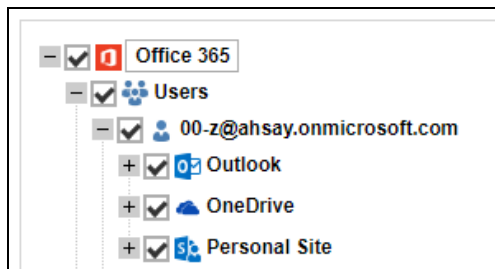
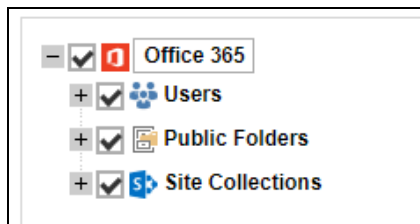
Root Selection

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 for AhsayOBM and only Public Folder for AhsayACB. On the comparison image above, the checkbox for the root folder “Office 365” is ticked.

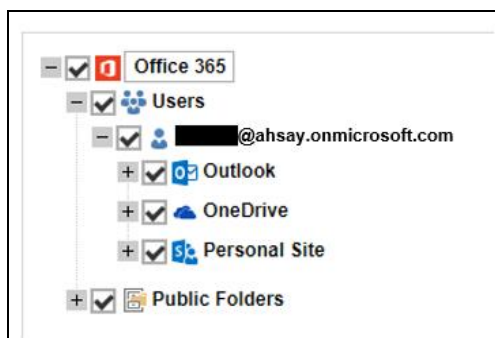
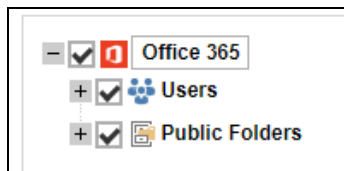
Data synchronization check is not required when using root selection backed up. As during a backup job any deleted files in the backup source will be automatically move to retention area.

Below are the sample screenshot of the backup source with root selection.

AhsayOBM



AhsayACB



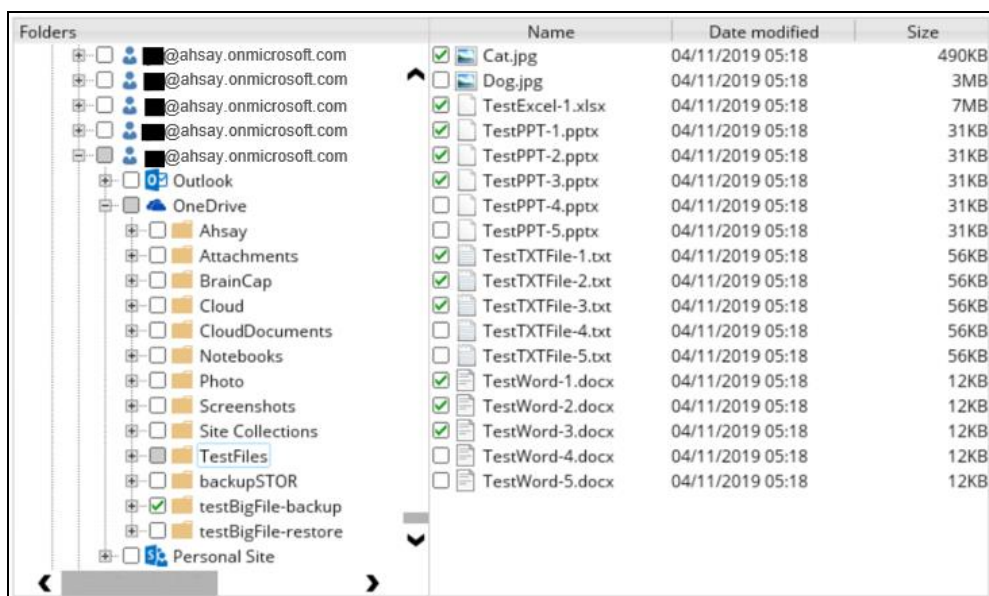
Selective Files and/or Folders

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).

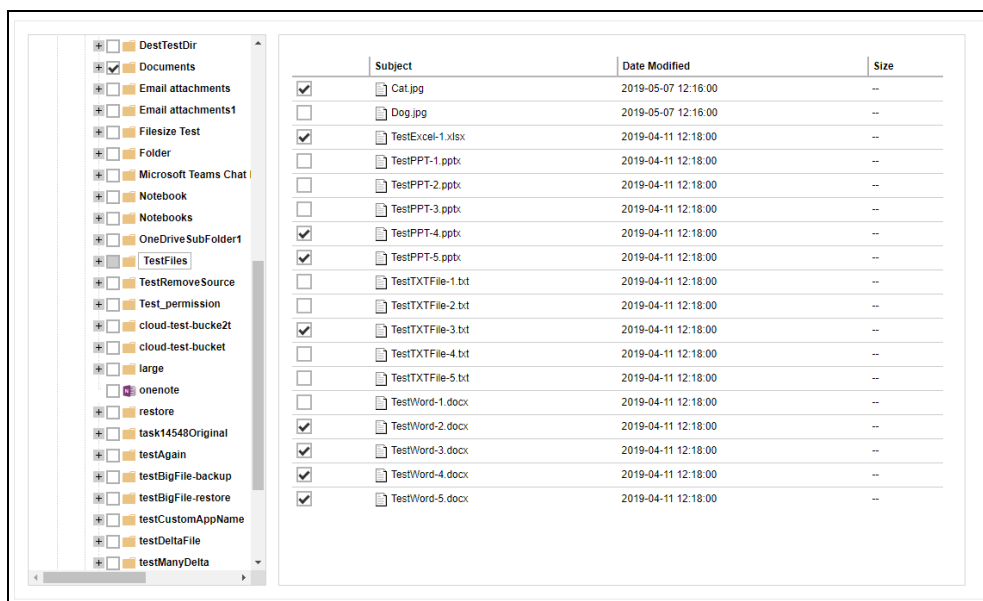
Data synchronization check is highly recommended to perform to synchronize de-selected files and/folders in the backup source with the backup destination(s). This will ensure that there will be no data build up on the backup destination(s).

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

AhsayOBM



AhsayACB



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

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

Backup Report

Backup Logs			
No.	Type	Timestamp	Log
1	start	2020/12/23 18:01:49	Start [Ahsay Cloud Backup Suite v8.3.4.0]
2	info	2020/12/23 18:01:54	Using Temporary Directory C:\Program Files\AhsayCBS\temp\1608711251295\Local@1608712072920
3	info	2020/12/23 18:02:28	Run Office 365 Data Synchronization Check (1st time)
4	info	2020/12/23 18:02:32	Backup E-mail Account: [REDACTED]@ahsay.onmicrosoft.com
5	info	2020/12/23 18:02:33	Start validating the presence and size of backup data in destination "AhsayCBS"...
6	info	2020/12/23 18:02:33	Finished validating the presence and size of backup data in destination "AhsayCBS"
7	info	2020/12/23 18:03:42	Start validating the presence and size of backup data in destination "AhsayCBS"...
8	info	2020/12/23 18:03:42	File: "1608711251295/blocks/2020-12-23-18-01-42/0/000000.bak", Size: 6,745,104, OK
9	info	2020/12/23 18:03:42	Finished validating the presence and size of backup data in destination "AhsayCBS"
10	info	2020/12/23 18:03:49	Start validating the presence and size of backup data in destination "AhsayCBS"...
11	info	2020/12/23 18:03:49	Finished validating the presence and size of backup data in destination "AhsayCBS"
12	info	2020/12/23 18:03:56	Quota (E-mail Account): 3
13	info	2020/12/23 18:03:56	Quota (E-mail Account) used in this backup set: 1
14	info	2020/12/23 18:03:56	1. [REDACTED]@ahsay.onmicrosoft.com

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

Backup Report

Backup Logs			
No.	Type	Timestamp	Log
1	start	2020/12/24 18:57:26	Start [Ahsay Cloud Backup Suite v8.3.4.0]
2	info	2020/12/24 18:57:31	Using Temporary Directory C:\Program Files\AhsayCBS\temp\1608711251295\Local@1608712072920
3	info	2020/12/24 18:57:55	Download valid index files from backup job "Current" to "C:\Program Files\AhsayCBS\temp\1608711251295\Local@1608712072920\index".
4	info	2020/12/24 18:58:02	Office 365 Data Synchronization Check will be run after 2 day(s)
5	info	2020/12/24 18:58:05	Download valid index files from backup job "Current" to "C:\Program Files\AhsayCBS\temp\1608711251295\Local@1608712072920\index\sub index\ce13cf62-567f-3023-b83d-ef00fd0e91ff".
6	info	2020/12/24 18:58:06	Start validating the presence and size of backup data in destination "AhsayCBS"...
7	info	2020/12/24 18:58:06	Finished validating the presence and size of backup data in destination "AhsayCBS"
8	info	2020/12/24 18:58:17	Download valid index files from backup job "Current" to "C:\Program Files\AhsayCBS\temp\1608711251295\Local@1608712072920\index\sub index\16c1db78-565a-3a2b-a234-0d84a739b3a5".
9	info	2020/12/24 18:58:39	Start validating the presence and size of backup data in destination "AhsayCBS"...
10	info	2020/12/24 18:58:39	File: "1608711251295/blocks/2020-12-24-18-57-18/0/000000.bak", Size: 156,816, OK
11	info	2020/12/24 18:58:39	Finished validating the presence and size of backup data in destination "AhsayCBS"
12	info	2020/12/24 18:58:45	Start validating the presence and size of backup data in destination "AhsayCBS"...
13	info	2020/12/24 18:58:45	Finished validating the presence and size of backup data in destination "AhsayCBS"
14	info	2020/12/24 18:58:49	Quota (E-mail Account): 3
15	info	2020/12/24 18:58:49	Quota (E-mail Account) used in this backup set: 1
16	info	2020/12/24 18:58:49	1. [REDACTED]@ahsay.onmicrosoft.com

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

Backup Report

Backup Logs			
No.	Type	Timestamp	Log
1	start	2020/12/27 10:48:30	Start [Ahsay Cloud Backup Suite v8.3.4.0]
2	info	2020/12/27 10:48:36	Using Temporary Directory C:\Program Files\AhsayCBS\temp\1608711251295\Local@1608712072920
3	info	2020/12/27 10:48:59	Download valid index files from backup job "Current" to "C:\Program Files\AhsayCBS\temp\1608711251295\Local@1608712072920\index".
4	info	2020/12/27 10:49:05	Run Office 365 Data Synchronization Check
5	info	2020/12/27 10:49:08	Download valid index files from backup job "Current" to "C:\Program Files\AhsayCBS\temp\1608711251295\Local@1608712072920\index\sub index\ce13cf62-567f-3023-b83d-ef00fd0e91ff".
6	info	2020/12/27 10:49:10	Start validating the presence and size of backup data in destination "AhsayCBS"...
7	info	2020/12/27 10:49:10	Finished validating the presence and size of backup data in destination "AhsayCBS"
8	info	2020/12/27 10:49:12	Download valid index files from backup job "Current" to "C:\Program Files\AhsayCBS\temp\1608711251295\Local@1608712072920\index\sub index\16c1db78-565a-3a2b-a234-0d84a739b3a5".
9	info	2020/12/27 10:49:54	Start validating the presence and size of backup data in destination "AhsayCBS"...
10	info	2020/12/27 10:49:54	File: "1608711251295/blocks/2020-12-27-10-48-23/0/000000.bak", Size: 156,960, OK
11	info	2020/12/27 10:49:54	Finished validating the presence and size of backup data in destination "AhsayCBS"
12	info	2020/12/27 10:50:01	Start validating the presence and size of backup data in destination "AhsayCBS"...
13	info	2020/12/27 10:50:01	Finished validating the presence and size of backup data in destination "AhsayCBS"
14	info	2020/12/27 10:50:06	Quota (E-mail Account): 3
15	info	2020/12/27 10:50:06	Quota (E-mail Account) used in this backup set: 1
16	info	2020/12/27 10:50:06	1. [REDACTED]@ahsay.onmicrosoft.com

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

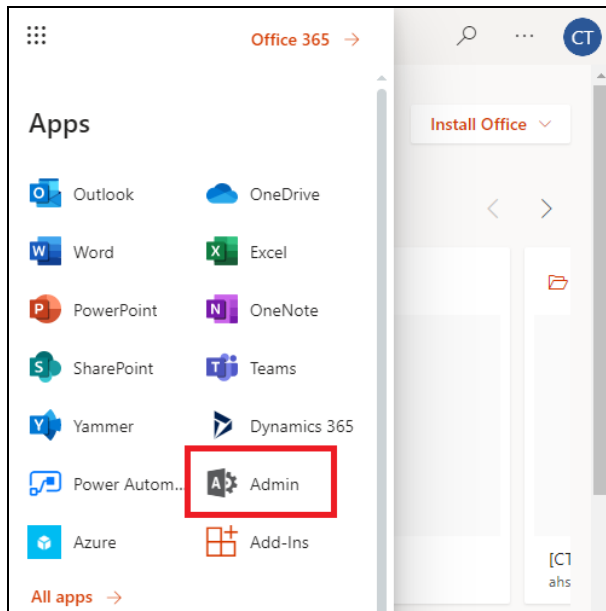
Backup Report

Backup Logs			
No.	Type	Timestamp	Log
1	start	2020/12/27 12:15:13	Start [Ahsay Cloud Backup Suite v8.3.4.0]
2	info	2020/12/27 12:15:18	Using Temporary Directory C:\Program Files\AhsayCBS\temp\1608711251295\Local@1608712072920
3	info	2020/12/27 12:15:42	Download valid index files from backup job "Current" to "C:\Program Files\AhsayCBS\temp\1608711251295\Local@1608712072920\index".
4	info	2020/12/27 12:15:49	Office 365 Data Synchronization Check is disabled (Debug option - Office365.DSCInterval = -1)
5	info	2020/12/27 12:15:51	Download valid index files from backup job "Current" to "C:\Program Files\AhsayCBS\temp\1608711251295\Local@1608712072920\index\sub index\cc13cf62-567f-3023-b83d-cf00fd0c91ff".
6	info	2020/12/27 12:15:53	Start validating the presence and size of backup data in destination "AhsayCBS"...
7	info	2020/12/27 12:15:53	Finished validating the presence and size of backup data in destination "AhsayCBS"
8	info	2020/12/27 12:15:55	Download valid index files from backup job "Current" to "C:\Program Files\AhsayCBS\temp\1608711251295\Local@1608712072920\index\sub index\16c1db78-565a-3a2b-a234-0d84a739b3a5".
9	info	2020/12/27 12:16:14	Start validating the presence and size of backup data in destination "AhsayCBS"...
10	info	2020/12/27 12:16:14	File: "1608711251295/blocks/2020-12-27-12-15-05/0/000000.bak", Size: 156,736, OK
11	info	2020/12/27 12:16:14	Finished validating the presence and size of backup data in destination "AhsayCBS"
12	info	2020/12/27 12:16:19	Start validating the presence and size of backup data in destination "AhsayCBS"...
13	info	2020/12/27 12:16:19	Finished validating the presence and size of backup data in destination "AhsayCBS"
14	info	2020/12/27 12:16:24	Quota (E-mail Account): 3
15	info	2020/12/27 12:16:24	Quota (E-mail Account) used in this backup set: 1
16	info	2020/12/27 12:16:24	1. [REDACTED]@ahsay.onmicrosoft.com

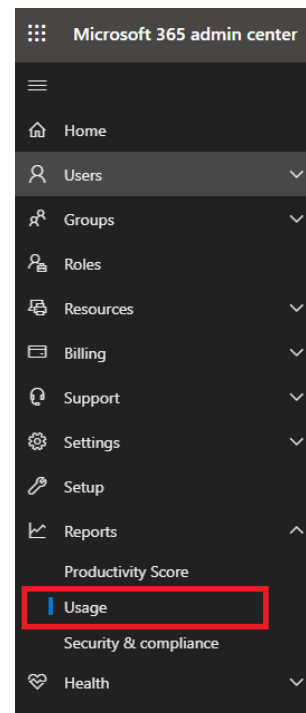
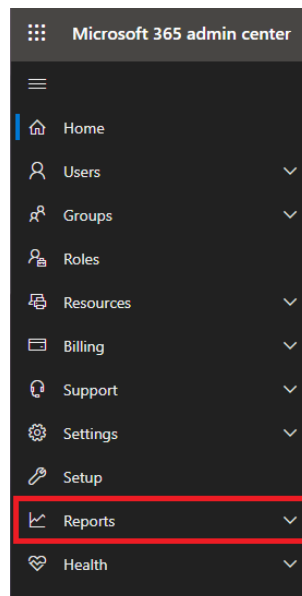
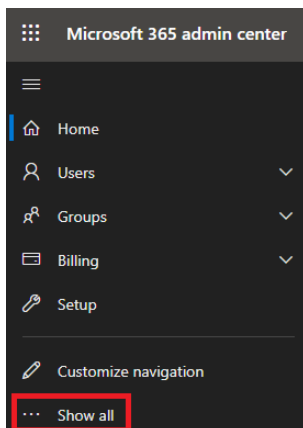
Appendix F: Steps on How to view Item count and Storage used in Microsoft 365 Admin Center

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

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

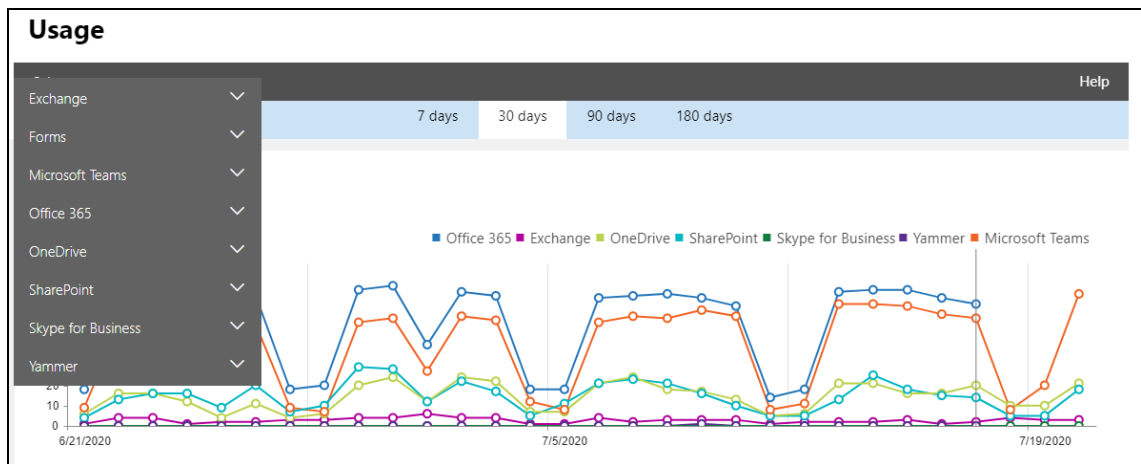
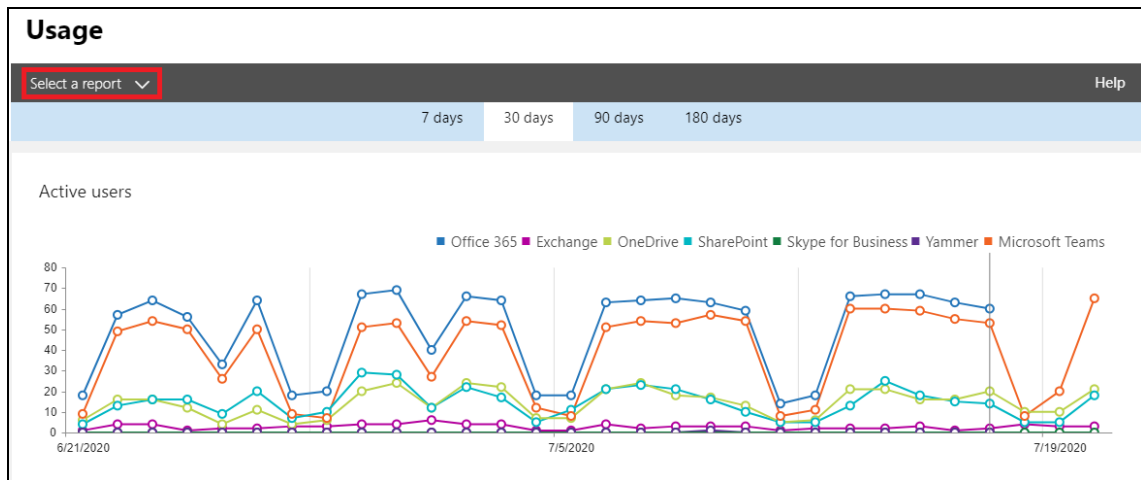


3. On the Microsoft 365 admin center, click **Show all** then click the dropdown arrow for the **Reports** and select **Usage**.

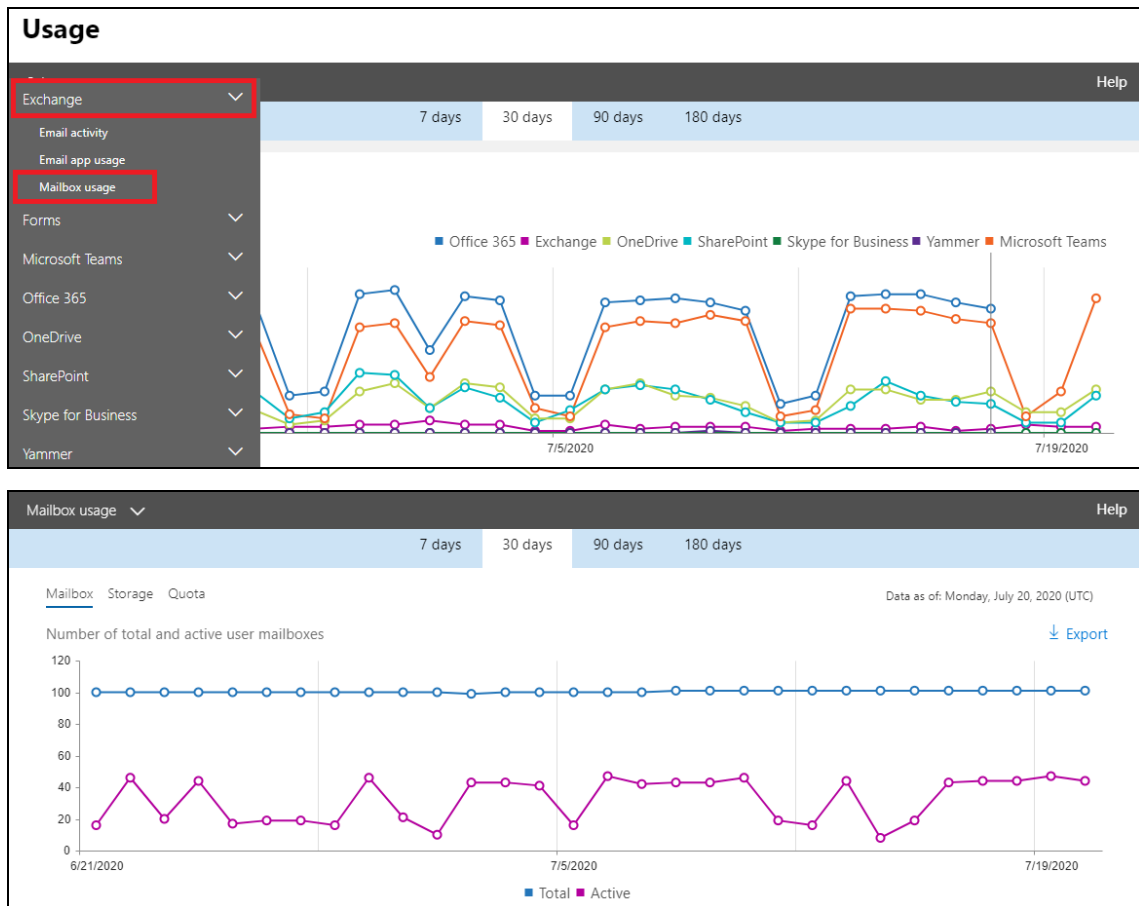


4. On the Usage screen, select a report you want to view.

Select a report ▼



5. For Exchange, go to Mailbox usage.

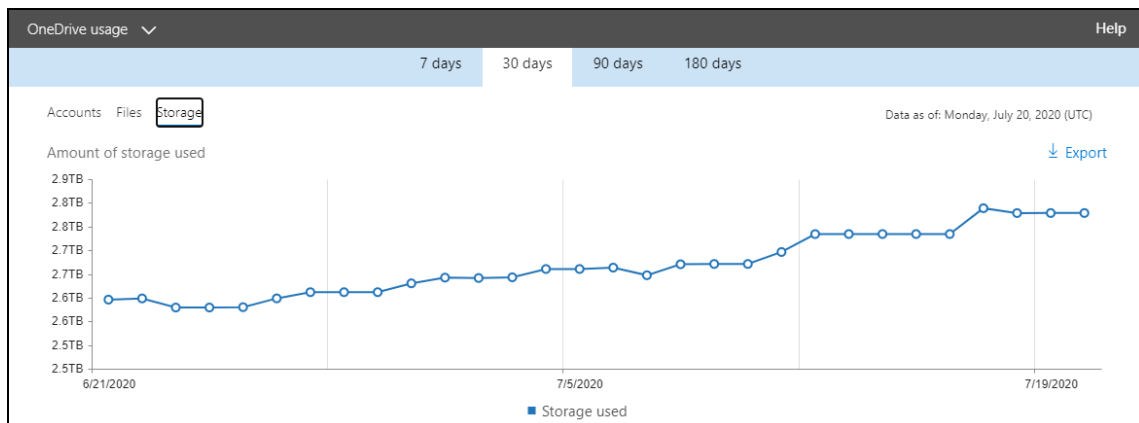
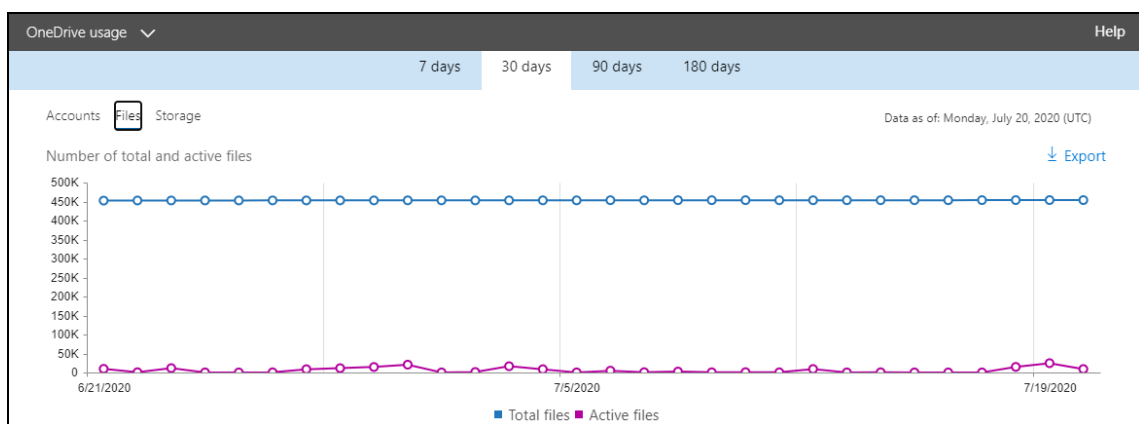
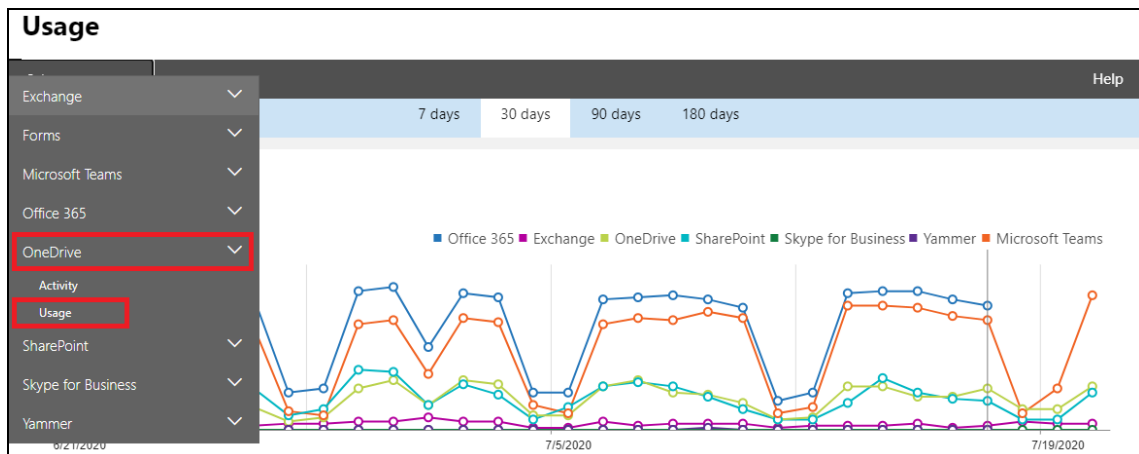


Highlighted columns are, Item count and Storage used (MB).

- **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

Details		Last activity date (UTC)		Item count	Storage used (MB)	Quota status
Username						
@ahsay.onmicrosoft.com				9,597	1,383	Good (under limits)
@ahsay.onmicrosoft.com				9,607	1,383	Good (under limits)
@ahsay.onmicrosoft.com				9,634	1,383	Good (under limits)
@ahsay.onmicrosoft.com				9,597	1,383	Good (under limits)
@ahsay.onmicrosoft.com				9,597	1,383	Good (under limits)
@ahsay.onmicrosoft.com				9,585	1,384	Good (under limits)

6. For OneDrive, go to Usage

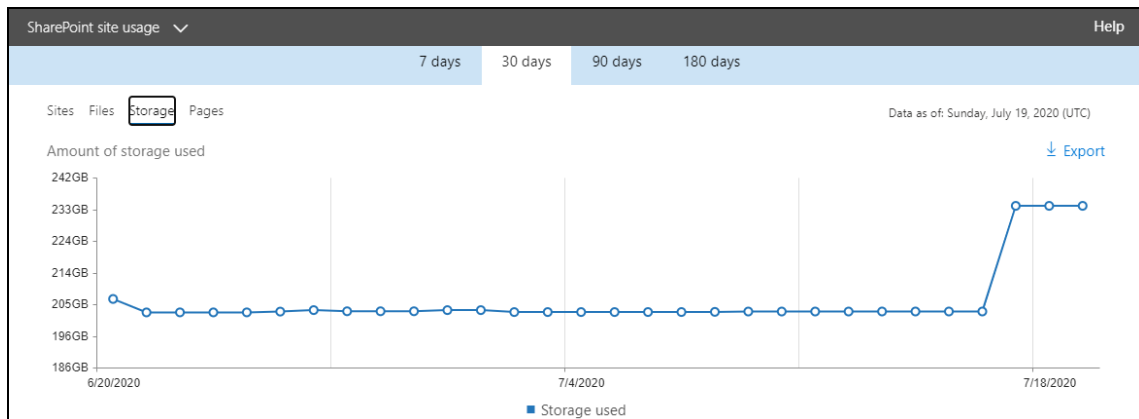
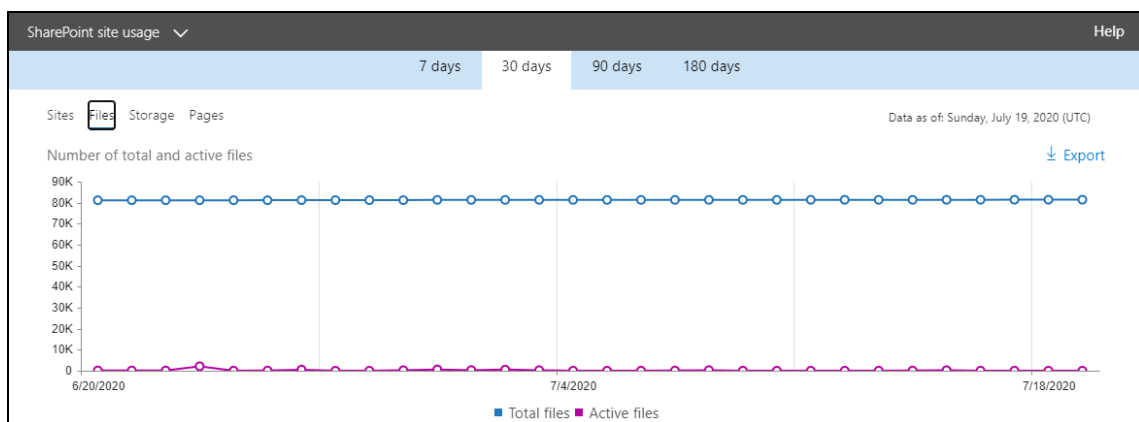
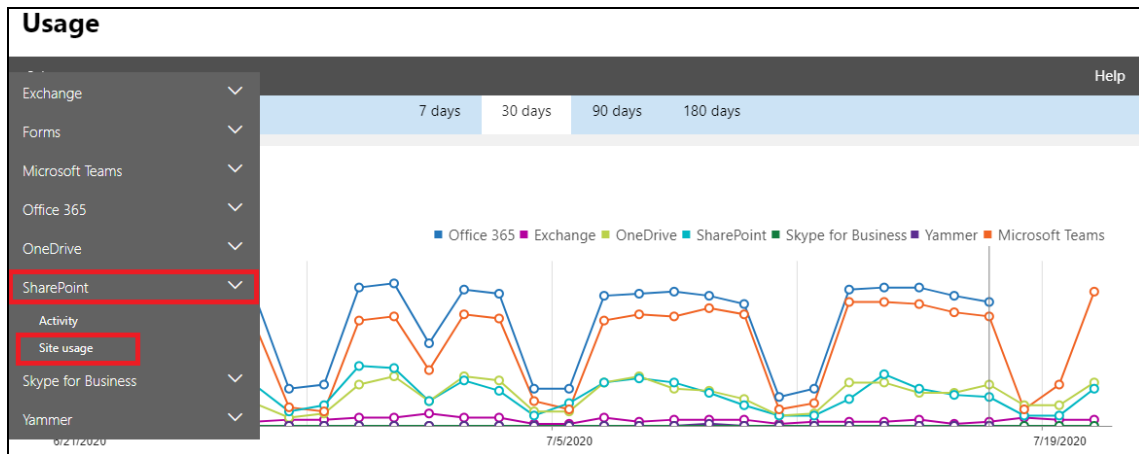


Highlighted columns are, Files and Storage used (MB).

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

URL	Owner principal name	Last activity date (UTC)	Files	Active files	Storage used (MB)
https://ahsay-my.sharepoint.com/personal/...	@ahsay.onmicrosoft.com	Tuesday, July 14, 2020	8	48	52
https://ahsay-my.sharepoint.com/personal/...	@ahsay.onmicrosoft.com	Monday, February 17, 2020	11,021	0	5,697
https://ahsay-my.sharepoint.com/personal/...	@ahsay.onmicrosoft.com	Tuesday, July 14, 2020	0	29	2
https://ahsay-my.sharepoint.com/personal/...	@ahsay.onmicrosoft.com	Monday, July 20, 2020	28,226	694	47,882
https://ahsay-my.sharepoint.com/personal/...	@ahsay.onmicrosoft.com	Tuesday, July 07, 2020	32	226	45

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

Details						Export
Site URL	Site owner principal name	Last activity date (UTC)	Files	Active files	Storage used (MB)	Page views
https://ahsay.sharepoint.c...	Test_site_001@ahsay.onmicrosoft.com	Monday, June 15, 2020	7	0	3	0
https://ahsay.sharepoint.c...	Test_site_002_1@ahsay.onmicrosoft.com	Thursday, February 13, 2020	6	0	2	0
https://ahsay.sharepoint.c...	test_site_002_2@ahsay.onmicrosoft.com	Friday, October 04, 2019	4	0	2	0
https://ahsay.sharepoint.c...	Test_site_002_4@ahsay.onmicrosoft.com	Sunday, October 06, 2019	5	0	2	0
https://ahsay.sharepoint.c...	Test_site_002@ahsay.onmicrosoft.com	Thursday, July 16, 2020	8	1	10	7
https://ahsay.sharepoint.c...	Test_site_003@ahsay.onmicrosoft.com	Thursday, February 06, 2020	6	0	3	0

Appendix G: Migrating Authentication of Office 365 Backup Set

AhsayOBM User

Starting with AhsayCBS v8.3.6.0 or above, existing backup sets must be migrated to use the 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. When migrating to Hybrid Authentication, any type of Office 365 account may be used to authorize the migration of authentication. However, when migrating an existing backup set created with an ordinary Office 365 account to Modern Authentication, an Office 365 Global Admin account 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 ordinary Office 365 account with Global Admin](#)

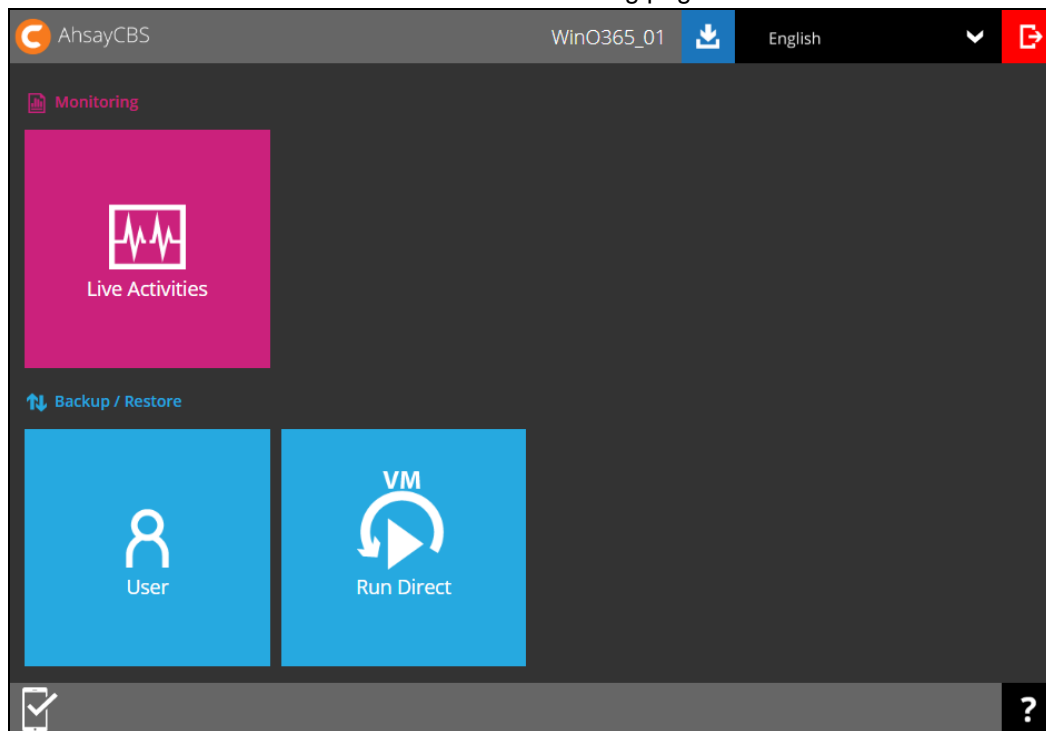
NOTE

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

- Click the **User** icon on the User Web Console landing page.



- On the **Backup Set** menu, select the backup set that you want to change to Hybrid Authentication.

User Profile
Backup Set
Settings
Report
Statistics
Effective Policy

Manage Backup Set ?

+
-
↺


<input type="checkbox"/>	Name	Type	Version	Owner	Timezone	Execute Job
<input type="checkbox"/>	Run on Server Office 365 Backup Set Basic DMFA GA (1600223557203)		--	--	GMT+09:00 (JST)	Backup Run
<input type="checkbox"/>	Run on Server Office 365 Backup Set Basic EMFA GA (1600223638593)		--	--	GMT+09:00 (JST)	Backup Run

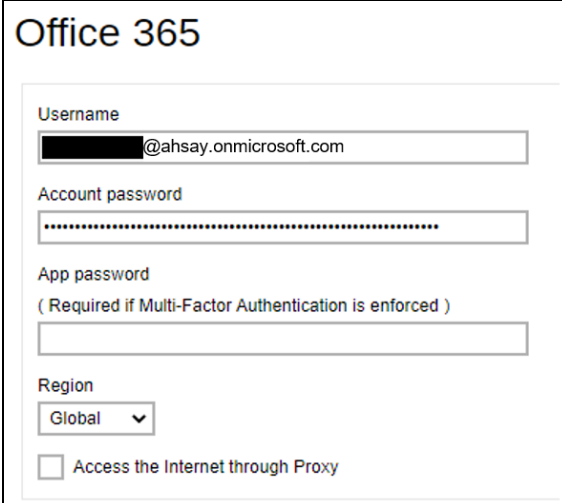
- Click **Continue**.

Authentication Code is required

In order to enhance security of Office 365 backup services, it is recommended that you update the Office 365 backup setting to use token-based authentication.

Continue
Update later

6. Leave the Username and Account password unchanged. Then click  to proceed with the authentication process.



Office 365

Username

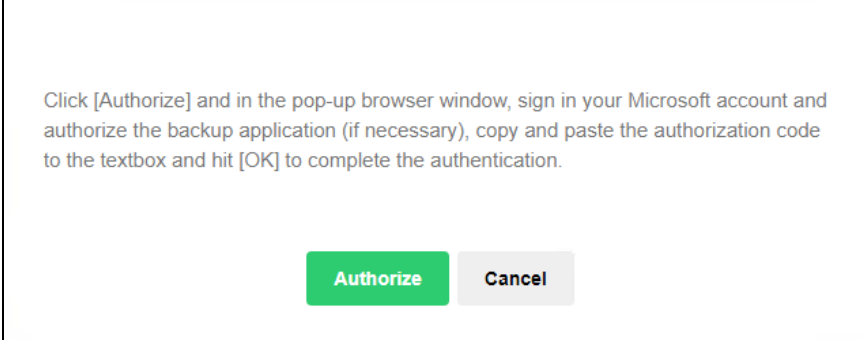
Account password

App password
(Required if Multi-Factor Authentication is enforced)

Region

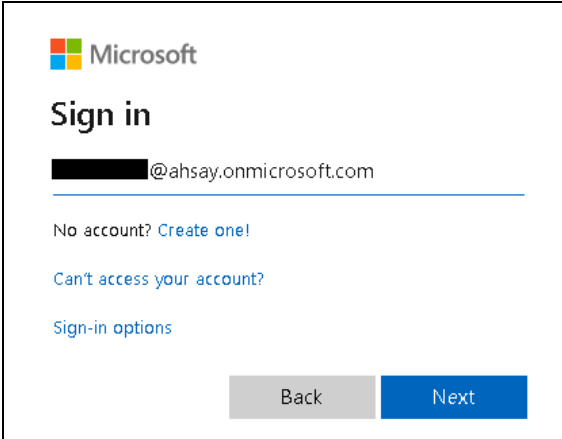
☐ Access the Internet through Proxy


7. Click **Authorize** to proceed with the authentication.



Click [Authorize] and in the pop-up browser window, sign in your Microsoft account and authorize the backup application (if necessary), copy and paste the authorization code to the textbox and hit [OK] to complete the authentication.

8. Sign in to your Microsoft account.



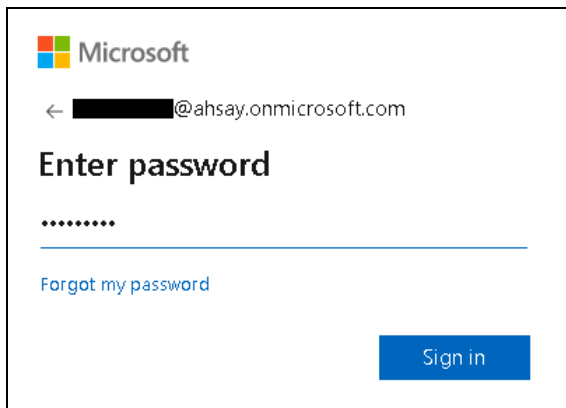
 Microsoft

Sign in

No account? [Create one!](#)

[Can't access your account?](#)

[Sign-in options](#)



Microsoft

← [redacted]@ahsay.onmicrosoft.com

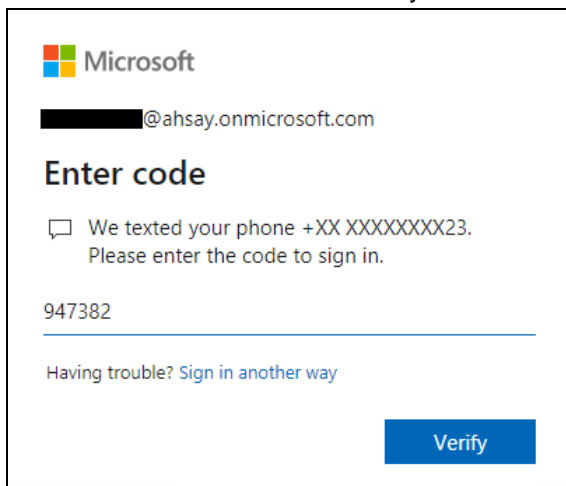
Enter password

.....

[Forgot my password](#)

Sign in


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



Microsoft

[redacted]@ahsay.onmicrosoft.com

Enter code

 We texted your phone +XX XXXXXXXX23.
Please enter the code to sign in.

947382

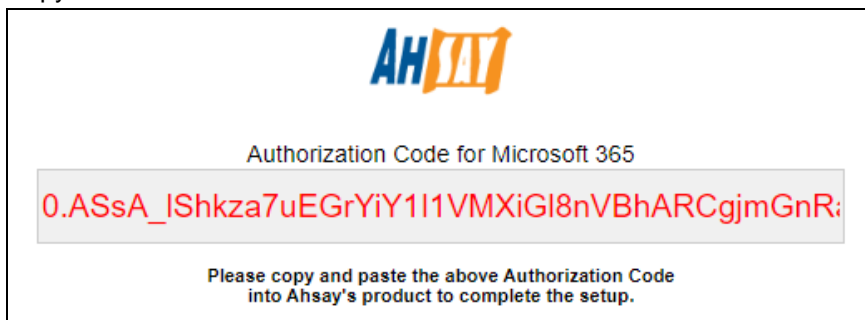
[Having trouble? Sign in another way](#)

Verify

NOTE

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

10. Copy the Authorization code.



Ahsay

Authorization Code for Microsoft 365

0.ASsA_IShkza7uEGrYiY1I1VMXiGl8nVBhARCGjmGnR:

Please copy and paste the above Authorization Code into Ahsay's product to complete the setup.

11. Go back to AhsayCBS and paste the authorization code. Then click **OK**.

In the pop-up browser window, sign in your Microsoft account and authorize the backup application (if necessary), copy and paste the authorization code to the textbox and hit [OK] to complete the authentication.

0.ASSA_IShkza7uEGrYiY1I1VMXiGI8nVBhARCgjmGnRaIODsPAAA.AQABA

OK Cancel

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

General

Source

Backup Schedule

Destination

In-File Delta

Retention Policy

Bandwidth Control

Others

General

ID
1600223557203

Name
Run on Server Office 365 Backup Set Basic DMFA GA

Owner
-

Backup set type
Office 365 Backup

Run on
☒ Server ☐ Client

Office 365

Username
[redacted]@ahsay.onmicrosoft.com

Region
Global

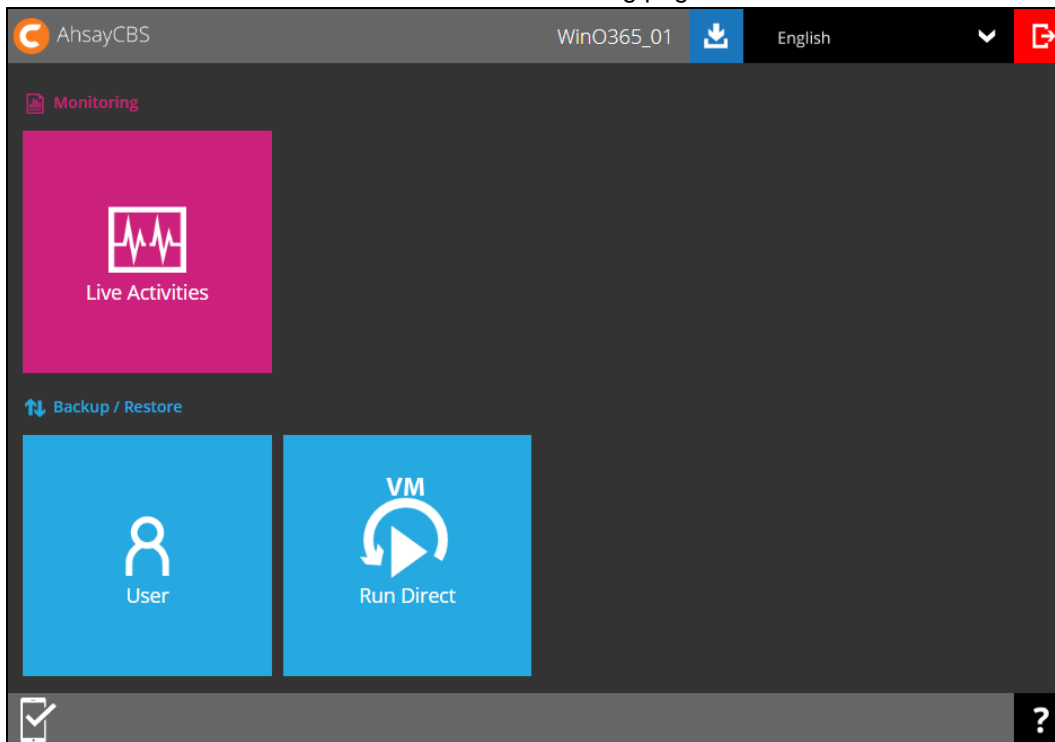
☐ Access the Internet through Proxy

Change settings

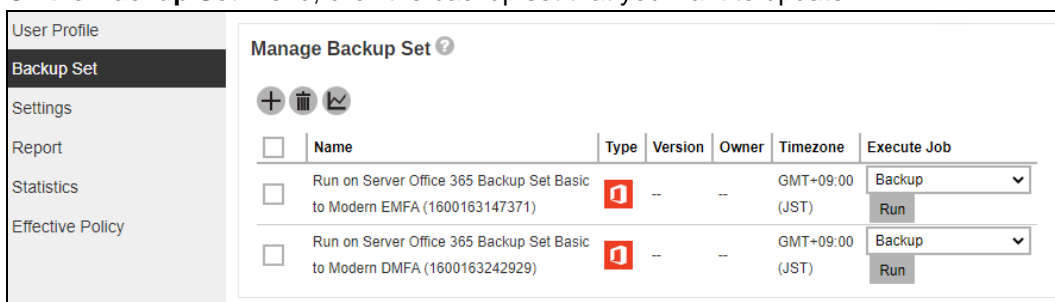
Save X ?

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


1. Log out all Office 365 account on the default browser before starting the migration of backup set.
2. Log in to the User Web Console according to the instructions in [Login to AhsayCBS User Web Console](#).
3. Click the **User** icon on the User Web Console landing page.



4. On the **Backup Set** menu, click the backup set that you want to update.




5. Click **Continue**.

**Authentication Code is required**

In order to enhance security of Office 365 backup services, it is recommended that you update the Office 365 backup setting to use token-based authentication.

Continue Update later

6. Leave the Username and Account password blank. Then click  to proceed with the authentication process.

Office 365

Username

Account password

App password


(Required if Multi-Factor Authentication is enforced)

Region

Global ▼

☐ Access the Internet through Proxy

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



This will restore Office 365 backup set using modern authentication protocol without restore functionality for SharePoint Web Parts and Metadata.


I understand the limitation and confirm to proceed Cancel

8. Click **Authorize** to proceed with the authentication.

Click [Authorize] and in the pop-up browser window, sign in your Microsoft account and authorize the backup application (if necessary), copy and paste the authorization code to the textbox and hit [OK] to complete the authentication.

Authorize **Cancel**

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

 Microsoft

Sign in


██████████@ahsay.onmicrosoft.com

[No account? Create one!](#)

[Can't access your account?](#)

[Sign-in options](#)

Back **Next**

 Microsoft

← ██████████@ahsay.onmicrosoft.com

Enter password

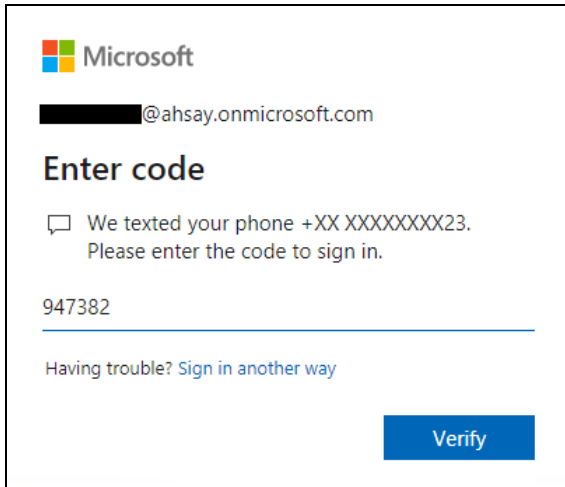
.....

[Forgot my password](#)

Sign in

10. If MFA is enforced, enter the verification code sent to your mobile device and click **Verify**.

Otherwise proceed to the next step

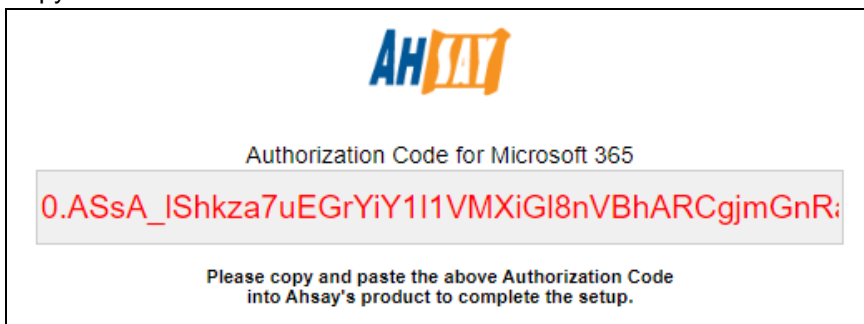


The screenshot shows a Microsoft login interface. At the top is the Microsoft logo. Below it is a blurred email address ending in @ahsay.onmicrosoft.com. The heading "Enter code" is followed by a message: "We texted your phone +XX XXXXXXXX23. Please enter the code to sign in." A text input field contains the number "947382". Below the field is a link: "Having trouble? Sign in another way". At the bottom right is a blue button labeled "Verify".

NOTE

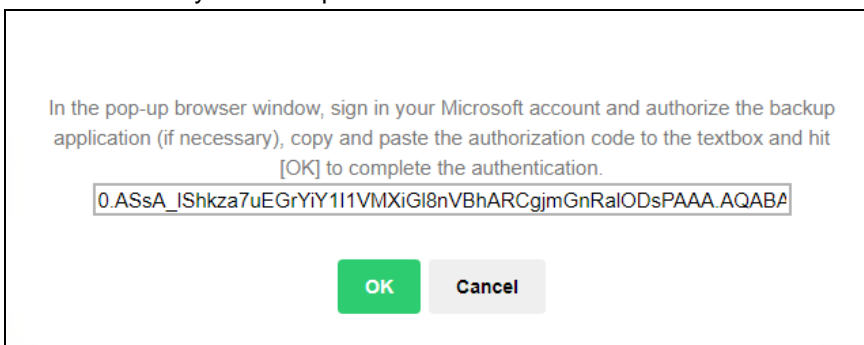
The verification code will only be required if the MFA status of an Office 365 account is enforced.

11. Copy the Authorization code.



The screenshot shows the Ahsay logo at the top. Below it is the text "Authorization Code for Microsoft 365". A red authorization code is displayed in a box: "0.ASsA_IShkza7uEGrYiY1I1VMXiGI8nVBhARCgjmGnR:". Below the code is the instruction: "Please copy and paste the above Authorization Code into Ahsay's product to complete the setup."

12. Go back to AhsayCBS and paste the code. Then click **OK**.



The screenshot shows a dialog box with the text: "In the pop-up browser window, sign in your Microsoft account and authorize the backup application (if necessary), copy and paste the authorization code to the textbox and hit [OK] to complete the authentication." Below the text is a text input field containing the code: "0.ASsA_IShkza7uEGrYiY1I1VMXiGI8nVBhARCgjmGnRaIODsPAAA.AQABA". At the bottom are two buttons: a green "OK" button and a grey "Cancel" button.

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

General

Source

Backup Schedule

Destination

In-File Delta

Retention Policy

Bandwidth Control

Others

General

ID
1600163242929

Name
Run on Server Office 365 Backup Set Basic to Modern DMFA

Owner
-

Backup set type
Office 365 Backup

Run on
☒ Server ☐ Client

Office 365

Username
[redacted]@ahsay.onmicrosoft.com

Region
Global

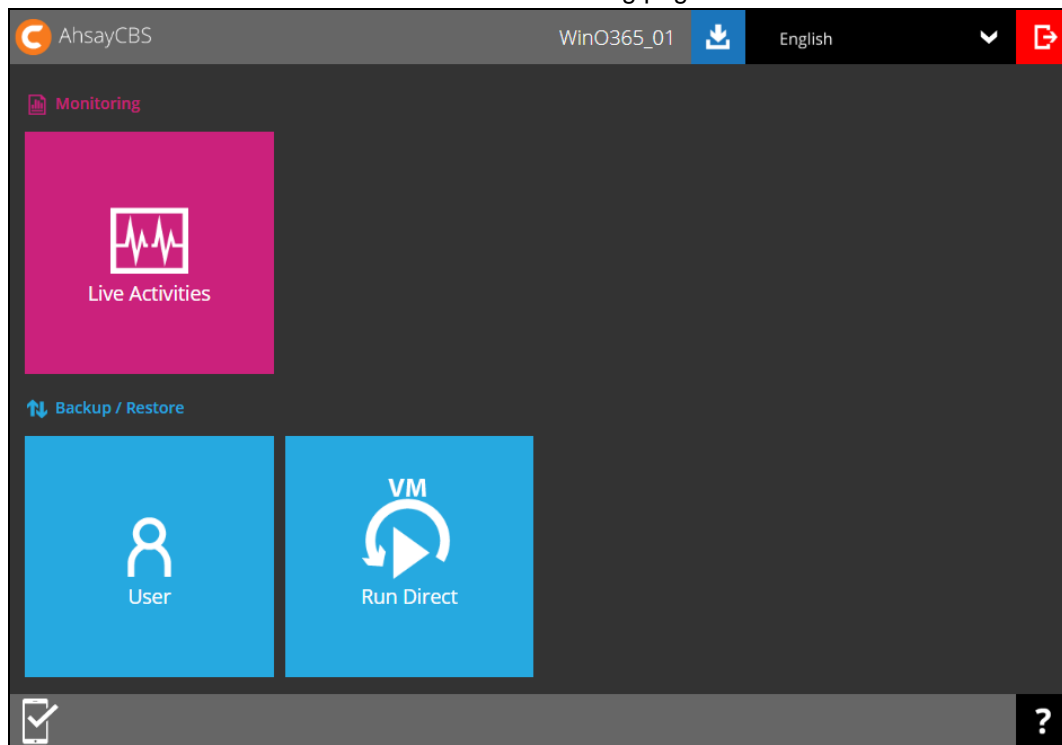
☐ Access the Internet through Proxy

Change settings

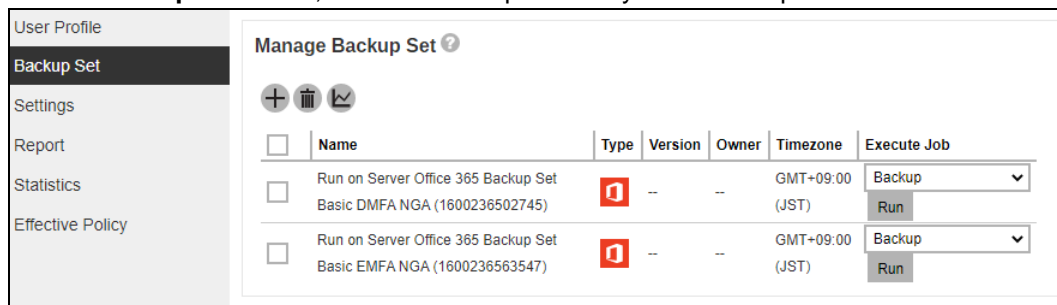
Save X ?

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


1. Logout all Office 365 account on the default browser before starting the migration of backup set.
2. Log in to the User Web Console according to the instructions in [Login to AhsayCBS User Web Console](#).
3. Click the User icon on the User Web Console landing page.



4. On the **Backup Set** menu, click the backup set that you want to update.




5. Click **Continue**.

**Authentication Code is required**

In order to enhance security of Office 365 backup services, it is recommended that you update the Office 365 backup setting to use token-based authentication.

Continue **Update later**

6. Leave the Username and Account password blank. Then click  to proceed with the authentication process.

Office 365

Username

Account password

App password


(Required if Multi-Factor Authentication is enforced)

Region

Global ▼

☐ Access the Internet through Proxy

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



This will restore Office 365 backup set using modern authentication protocol without restore functionality for SharePoint Web Parts and Metadata.


I understand the limitation and confirm to proceed **Cancel**

8. Click **Authorize** to proceed with the authentication.

Click [Authorize] and in the pop-up browser window, sign in your Microsoft account and authorize the backup application (if necessary), copy and paste the authorization code to the textbox and hit [OK] to complete the authentication.

Authorize Cancel

9. Sign in to your account.

 Microsoft

Sign in


██████████@ahsay.onmicrosoft.com

No account? [Create one!](#)

[Can't access your account?](#)

[Sign-in options](#)

Back Next

 Microsoft

← ██████████@ahsay.onmicrosoft.com

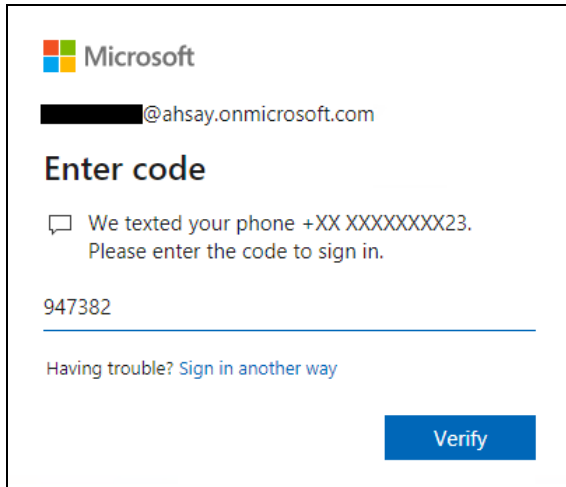
Enter password

.....

[Forgot my password](#)

Sign in

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

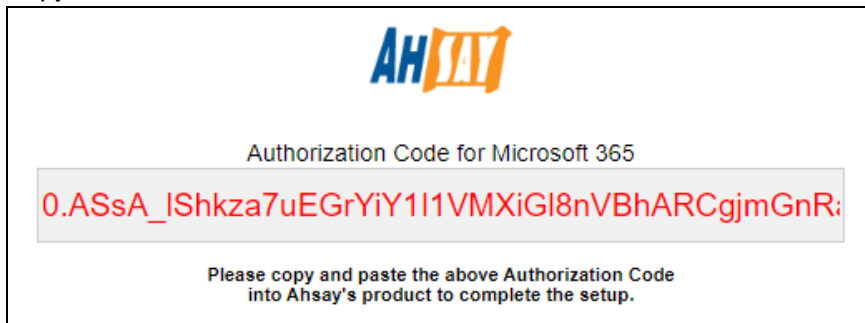


The image shows a Microsoft login interface. At the top is the Microsoft logo. Below it is the email address [REDACTED]@ahsay.onmicrosoft.com. The heading is "Enter code". A message says: "We texted your phone +XX XXXXXXXX23. Please enter the code to sign in." Below this is a text input field containing "947382". At the bottom left is a link: "Having trouble? Sign in another way". At the bottom right is a blue button labeled "Verify".

NOTE

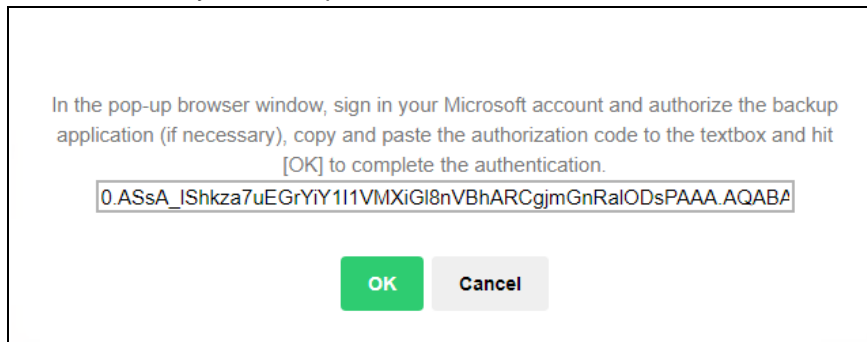
The verification code will only be required if the MFA status of an Office 365 account is enforced.

11. Copy the Authorization code.



The image shows an Ahsay interface with the Ahsay logo at the top. Below the logo is the text "Authorization Code for Microsoft 365". In the center, a red authorization code is displayed: "0.ASsA_IShkza7uEGrYiY1I1VMXiGI8nVBhARCgjmGnR:". Below the code, it says: "Please copy and paste the above Authorization Code into Ahsay's product to complete the setup."

12. Go back to AhsayCBS and paste the code. Then click **OK**.



The image shows a dialog box with the following text: "In the pop-up browser window, sign in your Microsoft account and authorize the backup application (if necessary), copy and paste the authorization code to the textbox and hit [OK] to complete the authentication." Below this text is a text input field containing the code: "0.ASsA_IShkza7uEGrYiY1I1VMXiGI8nVBhARCgjmGnRaIODsPAAA.AQABA". At the bottom are two buttons: a green "OK" button and a grey "Cancel" button.

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

The screenshot shows the 'General' settings window of Ahsay Backup Software. On the left is a sidebar with a list of settings: General (selected), Source, Backup Schedule, Destination, In-File Delta, Retention Policy, Bandwidth Control, and Others. The main area is divided into two sections. The 'General' section contains fields for ID (1600236502745), Name (Run on Server Office 365 Backup Set Basic DMFA NGA), Owner (-), Backup set type (Office 365 Backup), and Run on (Server selected, Client unselected). The 'Office 365' section contains Username (@ahsay.onmicrosoft.com), Region (Global), a checkbox for 'Access the Internet through Proxy' (unchecked), and a 'Change settings' button. At the bottom right of the window are three icons: a green 'Save' icon, a red 'X' icon, and a question mark icon.

Setting	Value
ID	1600236502745
Name	Run on Server Office 365 Backup Set Basic DMFA NGA
Owner	-
Backup set type	Office 365 Backup
Run on	<input checked="" type="radio"/> Server <input type="radio"/> Client
Office 365	
Username	@ahsay.onmicrosoft.com
Region	Global
Access the Internet through Proxy	<input type="checkbox"/>
Change settings	Change settings

AhsayACB User

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

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

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

The following are the two (2) migration scenarios:

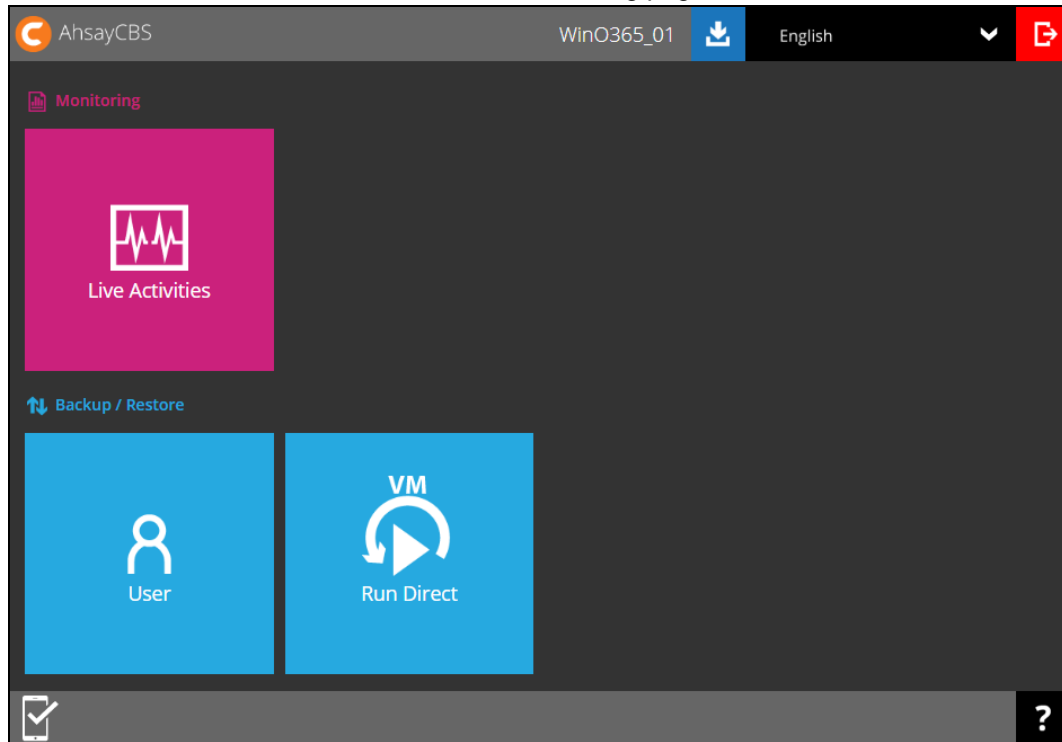
- [Basic Authentication to Hybrid Authentication](#)
- [Basic Authentication to Modern Authentication](#)

NOTE

Due to the current limitation with Microsoft API, Modern Authentication is currently not suitable for backup sets with Personal Sites 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. Log in to the User Web Console according to the instructions in [Login to AhsayCBS User Web Console](#).
3. Click the **User** icon on the User Web Console landing page.



4. On the **Backup Set** menu, click the backup set that you want to update.


User Profile	Manage Backup Set ?					
Backup Set	<div> + ✖ ↺ </div>					
Settings	<input type="checkbox"/>	Name	Type	Version	Owner	Timezone
Report	<input type="checkbox"/>	Run on Server Office 365 Backup Set		--	--	GMT+09:00 (JST)
Statistics		Basic DMFA GA (1600223557203)				Backup ▼
Effective Policy						Run
	<input type="checkbox"/>	Run on Server Office 365 Backup Set		--	--	GMT+09:00 (JST)
		Basic EMFA GA (1600223638593)				Backup ▼
						Run

5. Click **Continue**.

**Authentication Code is required**

In order to enhance security of Office 365 backup services, it is recommended that you update the Office 365 backup setting to use token-based authentication.

Continue **Update later**

6. Leave the Username and Account password unchanged. Then click  to proceed with the authentication process.

Office 365

Username

@ahsay.onmicrosoft.com

Account password

.....

App password

(Required if Multi-Factor Authentication is enforced)

Region

Global ▼

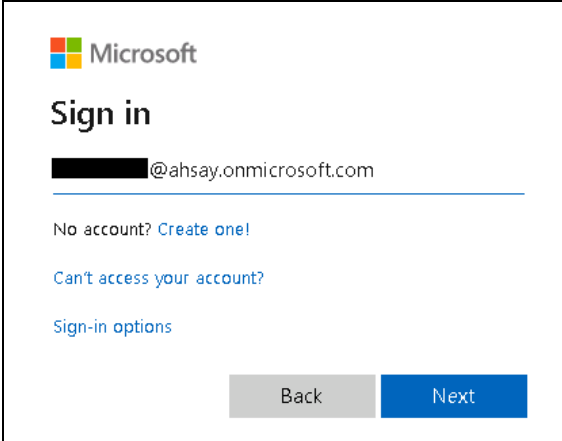
☐ Access the Internet through Proxy

7. Click **Authorize** to proceed with the authentication.

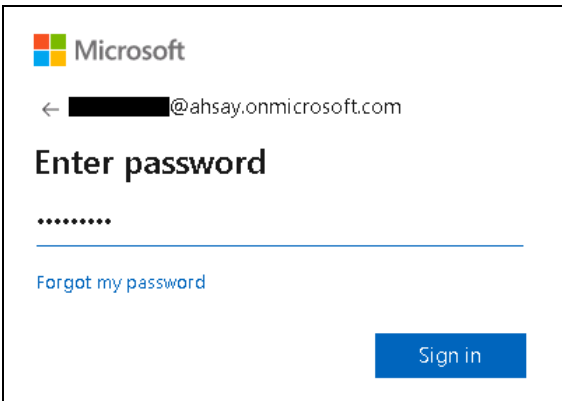
Click [Authorize] and in the pop-up browser window, sign in your Microsoft account and authorize the backup application (if necessary), copy and paste the authorization code to the textbox and hit [OK] to complete the authentication.

Authorize **Cancel**

8. Sign in to your Microsoft account.

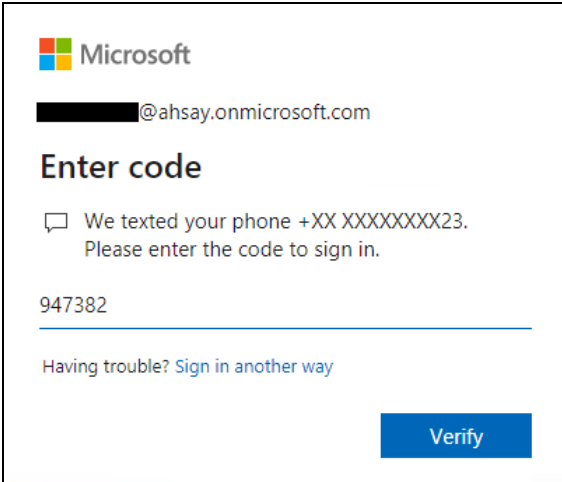


The screenshot shows the Microsoft sign-in page. At the top is the Microsoft logo. Below it is the heading "Sign in". A text input field contains the email address "████████@ahsay.onmicrosoft.com". Below the input field are three links: "No account? Create one!", "Can't access your account?", and "Sign-in options". At the bottom are two buttons: a grey "Back" button and a blue "Next" button.



The screenshot shows the Microsoft "Enter password" screen. At the top is the Microsoft logo. Below it is a back arrow and the email address "████████@ahsay.onmicrosoft.com". The heading "Enter password" is followed by a password input field with dots. Below the input field is a link "Forgot my password". At the bottom right is a blue "Sign in" button.

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



The screenshot shows the Microsoft "Enter code" screen. At the top is the Microsoft logo. Below it is the email address "████████@ahsay.onmicrosoft.com". The heading "Enter code" is followed by a message: "We texted your phone +XX XXXXXXXX23. Please enter the code to sign in." Below this is a text input field containing the code "947382". At the bottom left is a link "Having trouble? Sign in another way". At the bottom right is a blue "Verify" button.

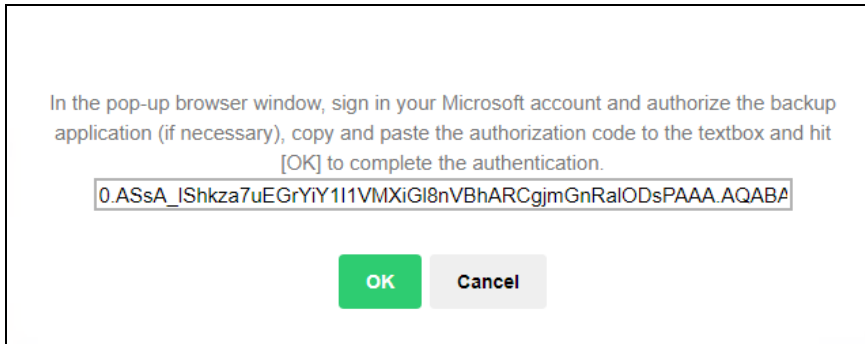
NOTE

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

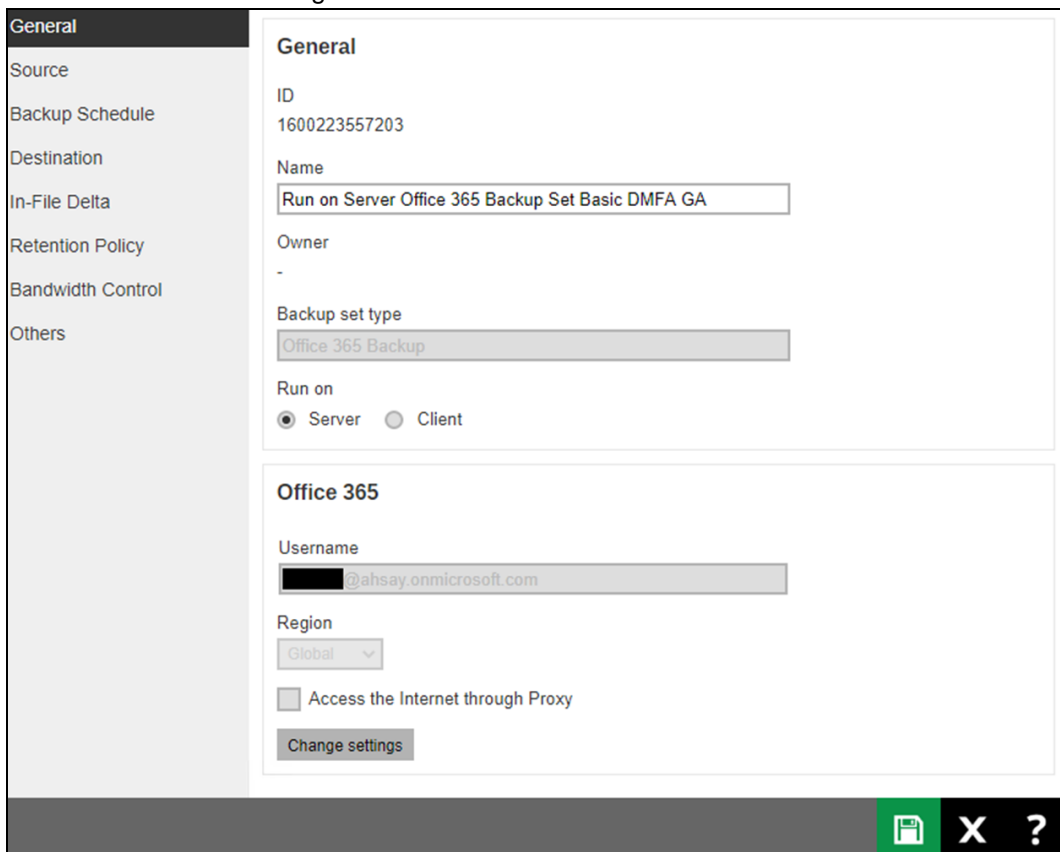
10. Copy the Authorization code.



11. Go back to AhsayCBS and paste the code. Then click **OK**.

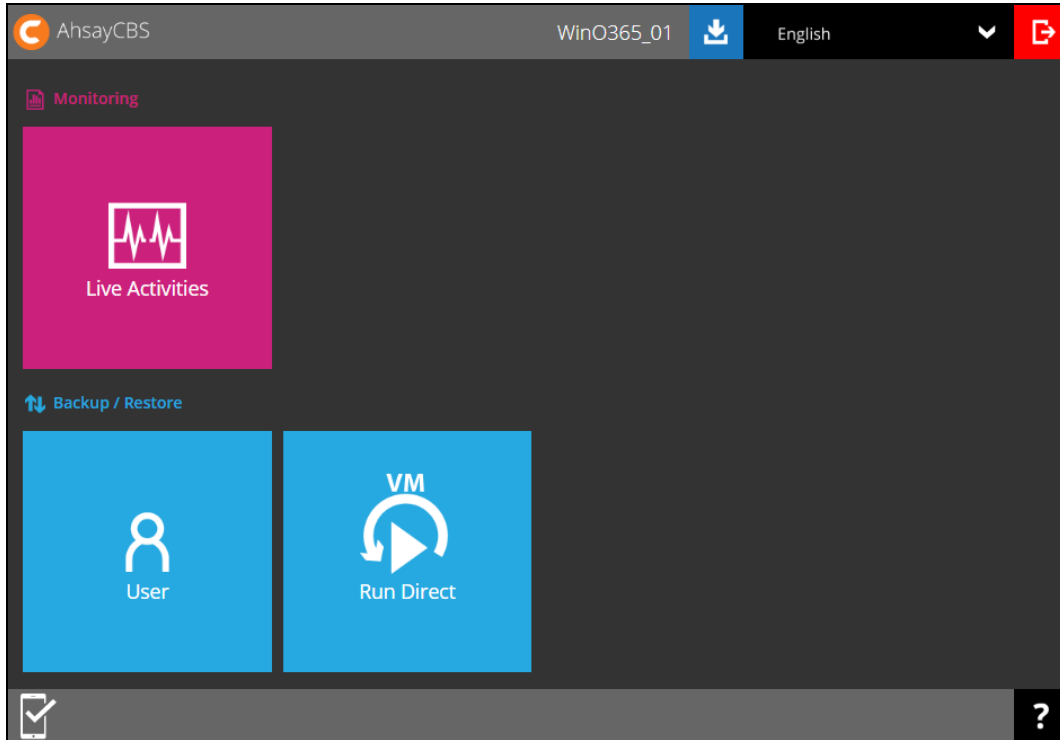


12. Click Save to finish the migration.

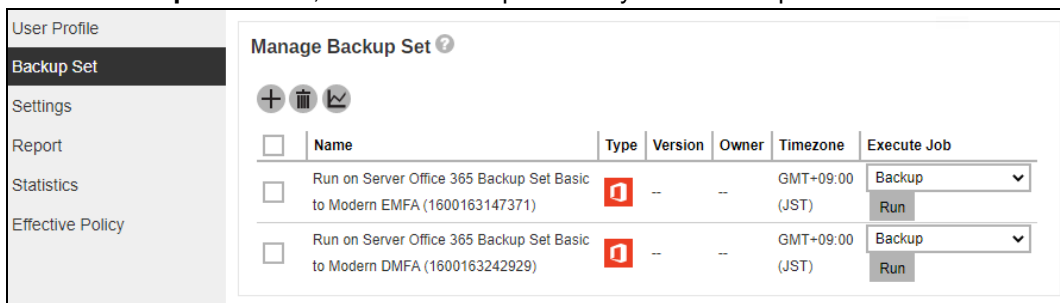


To migrate a backup set from **Basic Authentication to Modern Authentication using an ordinary Office 365 account**, follow the instructions below:


1. Logout all Office 365 account on the default browser before starting the migration of backup set.
2. Log in to the User Web Console according to the instructions in [Login to AhsayCBS User Web Console](#).
3. Click the **User** icon on the User Web Console landing page.



4. On the **Backup Set** menu, click the backup set that you want to update.




5. Click **Continue**.

**Authentication Code is required**

In order to enhance security of Office 365 backup services, it is recommended that you update the Office 365 backup setting to use token-based authentication.

Continue **Update later**

6. Leave the Username and Account password blank. Then click  to proceed with the authentication process.

Office 365

Username

Account password

App password


(Required if Multi-Factor Authentication is enforced)

Region

Global ▼

☐ Access the Internet through Proxy

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



This will restore Office 365 backup set using modern authentication protocol without restore functionality for SharePoint Web Parts and Metadata.


I understand the limitation and confirm to proceed **Cancel**

8. Click **Authorize** to proceed with the authentication.

Click [Authorize] and in the pop-up browser window, sign in your Microsoft account and authorize the backup application (if necessary), copy and paste the authorization code to the textbox and hit [OK] to complete the authentication.

Authorize **Cancel**

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

 Microsoft

Sign in


██████████@ahsay.onmicrosoft.com

[No account? Create one!](#)

[Can't access your account?](#)

[Sign-in options](#)

Back **Next**

 Microsoft

← ██████████@ahsay.onmicrosoft.com

Enter password

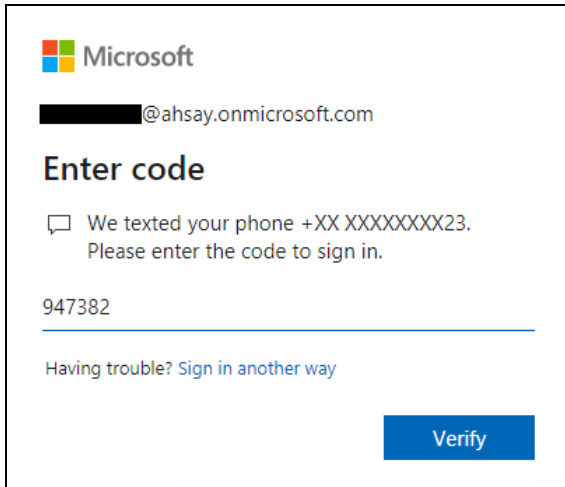
.....

[Forgot my password](#)

Sign in

10. If MFA is enforced, enter the verification code sent to your mobile device and click **Verify**.

Otherwise proceed to the next step

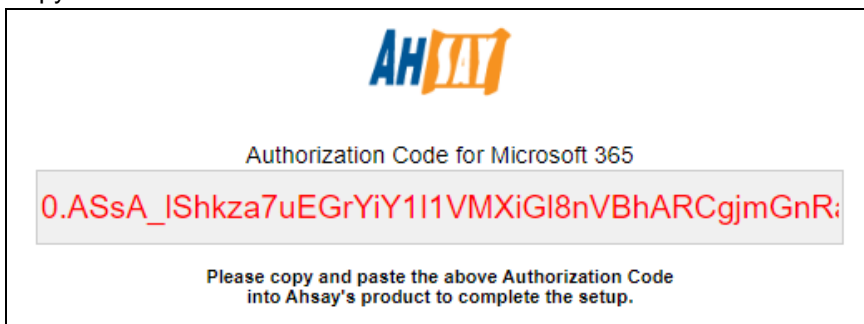


The screenshot shows a Microsoft login interface. At the top is the Microsoft logo. Below it is a blurred email address ending in @ahsay.onmicrosoft.com. The heading "Enter code" is followed by a message: "We texted your phone +XX XXXXXXXX23. Please enter the code to sign in." A text input field contains the number "947382". Below the field is a link: "Having trouble? Sign in another way". At the bottom right is a blue button labeled "Verify".

NOTE

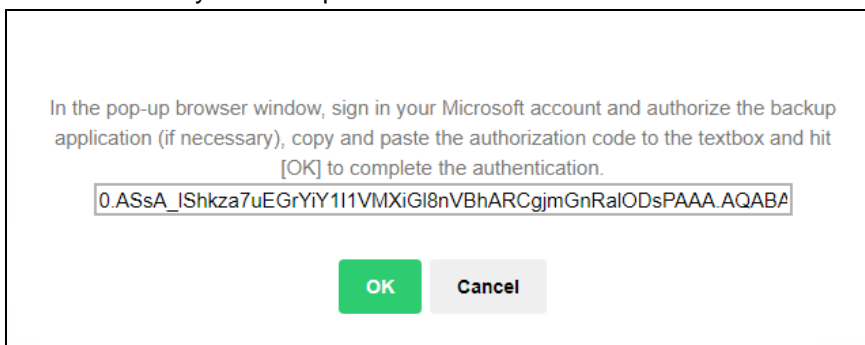
The verification code will only be required if the MFA status of an Office 365 account is enforced.

11. Copy the Authorization code.



The screenshot shows the Ahsay logo at the top. Below it is the text "Authorization Code for Microsoft 365". A red authorization code is displayed in a box: "0.ASsA_IShkza7uEGrYiY1I1VMXiGI8nVBhARCgjmGnR:". Below the box is the instruction: "Please copy and paste the above Authorization Code into Ahsay's product to complete the setup."

12. Go back to AhsayCBS and paste the code. Then click **OK**.



The screenshot shows a dialog box with the text: "In the pop-up browser window, sign in your Microsoft account and authorize the backup application (if necessary), copy and paste the authorization code to the textbox and hit [OK] to complete the authentication." Below the text is a text input field containing the code: "0.ASsA_IShkza7uEGrYiY1I1VMXiGI8nVBhARCgjmGnRaIODsPAAA.AQABA". At the bottom are two buttons: a green "OK" button and a grey "Cancel" button.

13. Click Save to finish the migration.

General

Source

Backup Schedule

Destination

In-File Delta

Retention Policy

Bandwidth Control

Others

General

ID
1600163242929

Name
Run on Server Office 365 Backup Set Basic to Modern DMFA

Owner
-

Backup set type
Office 365 Backup

Run on
☒ Server ☐ Client

Office 365

Username
[redacted]@ahsay.onmicrosoft.com

Region
Global

☐ Access the Internet through Proxy

Change settings

Save X ?

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

After upgrading to AhsayCBS 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 [2.14.1](#) and [2.14.2](#) for the complete list of backup and restore limitations using Modern Authentication.

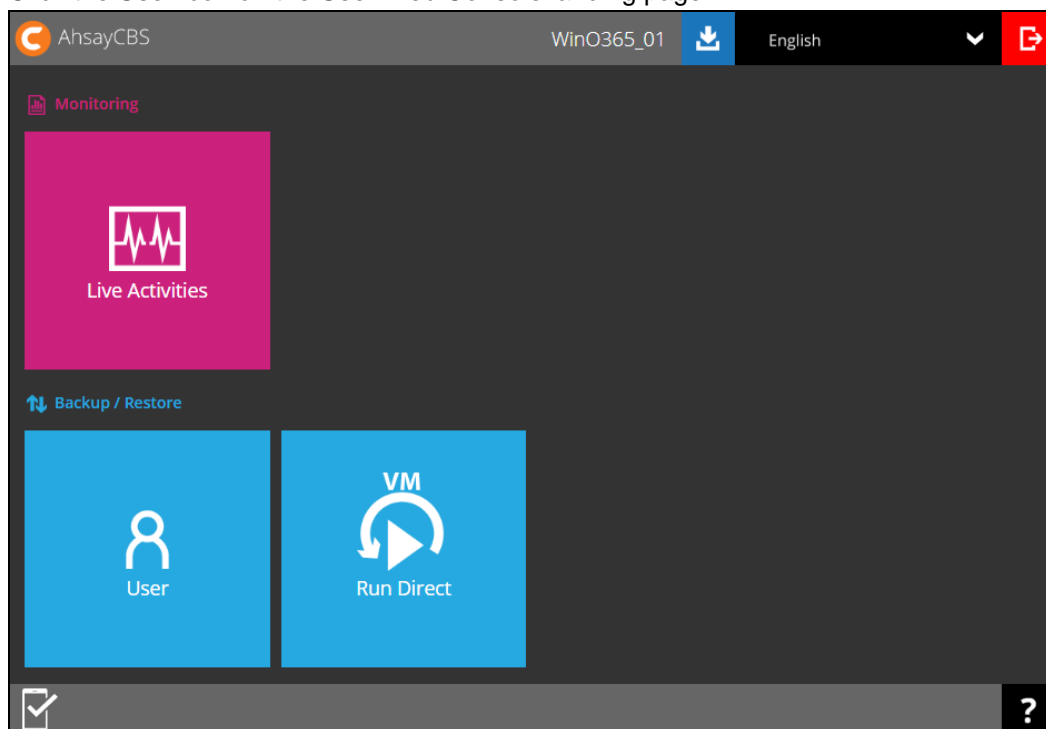
Once the backup and restore of SharePoint Web Parts and Metadata is fully supported using Modern Authentication, Office 365 backup sets using Hybrid Authentication can be changed back to Modern Authentication.

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



4. On the **Backup Set** menu, click the backup set that you want to change to Hybrid Authentication.

User Profile
Backup Set
Settings
Report
Statistics
Effective Policy

Manage Backup Set ?

+
-
↺

<input type="checkbox"/>	Name	Type	Version	Owner	Timezone	Execute Job
<input type="checkbox"/>	Run on Server Office 365 Backup Set (1600223557203)		--	--	GMT+09:00 (JST)	Backup Run
<input type="checkbox"/>	Run on Server Office 365 Backup Set Basic EMFA GA (1600223638593)		--	--	GMT+09:00 (JST)	Backup Run

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

General
Source
Backup Schedule
Destination
In-File Delta
Retention Policy
Bandwidth Control
Others

General

ID
1600223557203

Name

Owner
-

Backup set type

Run on
☒ Server
☐ Client

Office 365

Username

Region

☐ Access the Internet through Proxy

Change settings

X ?

- In the Office 365 credentials page, **input the Office 365 login account and password** then click to proceed.

Office 365

Username

Account password

App password
(Required if Multi-Factor Authentication is enforced)

Region


☐ Access the Internet through Proxy

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

Click [Authorize] and in the pop-up browser window, sign in your Microsoft account and authorize the backup application (if necessary), copy and paste the authorization code to the textbox and hit [OK] to complete the authentication.

Authorize Cancel

8. Sign in to your Microsoft account.

 Microsoft

Sign in


██████████@ahsay.onmicrosoft.com

No account? [Create one!](#)

[Can't access your account?](#)

[Sign-in options](#)

Back Next

 Microsoft

← ██████████@ahsay.onmicrosoft.com


Enter password

.....

[Forgot my password](#)

Sign in


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

 Microsoft
 [Redacted]@ahsay.onmicrosoft.com
Enter code
 We texted your phone +XX XXXXXXXX23.
 Please enter the code to sign in.
 947382
 Having trouble? [Sign in another way](#)
 Verify

NOTE

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

- Copy the Authorization code.


 Authorization Code for Microsoft 365
 0.ASsA_IShkza7uEGrYiY1I1VMXiGI8nVBhARCgjmGnR:
 Please copy and paste the above Authorization Code
 into Ahsay's product to complete the setup.

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

In the pop-up browser window, sign in your Microsoft account and authorize the backup application (if necessary), copy and paste the authorization code to the textbox and hit [OK] to complete the authentication.

0.ASsA_IShkza7uEGrYiY1I1VMXiGI8nVBhARCgjmGnRlODsPAAA.AQABA/

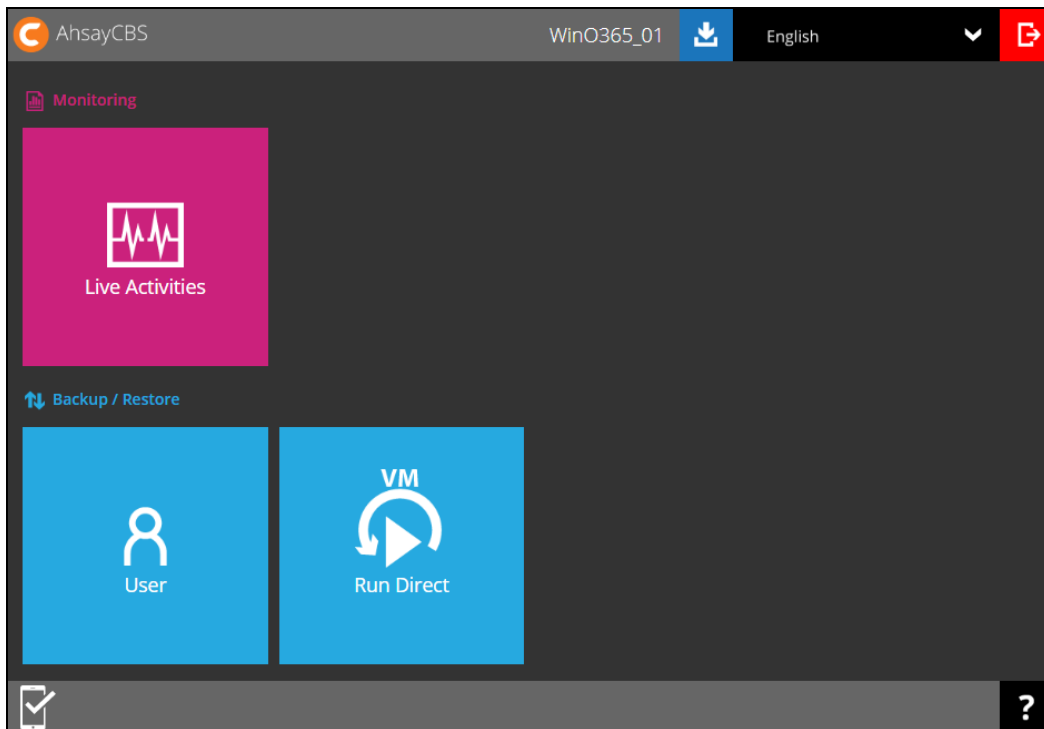
OK Cancel

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

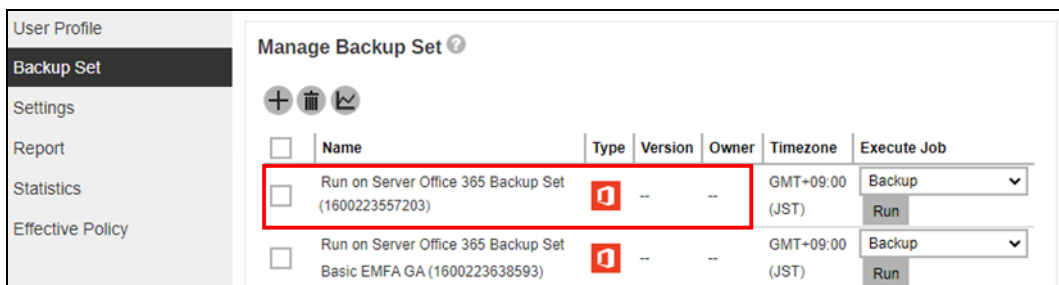
The screenshot displays the AhsayCBS configuration window. On the left is a sidebar with a list of settings: General (selected), Source, Backup Schedule, Destination, In-File Delta, Retention Policy, Bandwidth Control, and Others. The main area is divided into two sections. The top section, titled 'General', contains the following fields: ID (1600223557203), Name (Run on Server Office 365 Backup Set), Owner (-), Backup set type (Office 365 Backup), and Run on (radio buttons for Server and Client, with Server selected). The bottom section, titled 'Office 365', contains: Username (@ahsay.onmicrosoft.com), Region (Global dropdown), a checkbox for 'Access the Internet through Proxy' (unchecked), and a 'Change settings' button. At the bottom right of the window are three icons: a green save icon, a red close icon, and a yellow help icon.

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



4. On the **Backup Set** menu, click the backup set that you want to change to Modern Authentication.



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

General
Source
Backup Schedule
Destination
In-File Delta
Retention Policy
Bandwidth Control
Others

General

ID
1600223557203

Name

Owner
-

Backup set type

Run on
☒ Server
☐ Client

Office 365

Username

Region

☐ Access the Internet through Proxy

X
?

6. In the Office 365 credentials page, **remove the Account password** then click  to proceed.

Office 365

Username


Account password

App password
(Required if Multi-Factor Authentication is enforced)

Region

☐ Access the Internet through Proxy

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




This will restore Office 365 backup set using modern authentication protocol without restore functionality for SharePoint Web Parts and Metadata.

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

Click [Authorize] and in the pop-up browser window, sign in your Microsoft account and authorize the backup application (if necessary), copy and paste the authorization code to the textbox and hit [OK] to complete the authentication.

Authorize Cancel

9. Sign in to your Microsoft account.

 Microsoft

Sign in


██████████@ahsay.onmicrosoft.com

No account? [Create one!](#)

[Can't access your account?](#)

[Sign-in options](#)

Back Next

 Microsoft

← ██████████@ahsay.onmicrosoft.com


Enter password

.....

[Forgot my password](#)

Sign in


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

 Microsoft
 [Redacted]@ahsay.onmicrosoft.com
Enter code
 We texted your phone +XX XXXXXXXX23.
 Please enter the code to sign in.
 947382
 Having trouble? [Sign in another way](#)
 Verify

NOTE

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

- Copy the Authorization code.


 Authorization Code for Microsoft 365
 0.ASsA_IShkza7uEGrYiY1I1VMXiGI8nVBhARCgjmGnR:
 Please copy and paste the above Authorization Code
 into Ahsay's product to complete the setup.

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

In the pop-up browser window, sign in your Microsoft account and authorize the backup application (if necessary), copy and paste the authorization code to the textbox and hit [OK] to complete the authentication.

0.ASsA_IShkza7uEGrYiY1I1VMXiGI8nVBhARCgjmGnRlODsPAAA.AQABA

OK Cancel

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

The screenshot shows the 'General' configuration tab for a backup set. On the left is a sidebar with navigation options: General, Source, Backup Schedule, Destination, In-File Delta, Retention Policy, Bandwidth Control, and Others. The 'General' tab is active, displaying the following fields:

- General**
 - ID: 1600223557203
 - Name: Run on Server Office 365 Backup Set
 - Owner: -
 - Backup set type: Office 365 Backup
 - Run on: ☒ Server ☐ Client
- Office 365**
 - Username: [redacted]@ahsay.onmicrosoft.com
 - Region: Global (dropdown menu)
 - ☐ Access the Internet through Proxy
 - Change settings button

At the bottom right of the window, there are three icons: a green save icon, a red 'X' icon, and a question mark icon.