Ahsay Backup

Ahsay Cloud Backup Suite v9

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

Ahsay Systems Corporation Limited

2 May 2023

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

Copyright Notice

© 2023 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 365 are registered trademarks of Microsoft Corporation.

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

OpenJDK is a registered trademark of Oracle America, Inc.

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.

Debian is a registered trademark of Software in the Public Interest, Inc.

Rocky is a registered trademark of Rocky Brands.

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	Version
25 January 2022	▪ Ch. 5 – updated screenshot to show Migrate Data option	9.1.0.0
18 March 2022	▪ Ch. 1.3 – removed space freeing up ▪ Ch. 2.16.3 – added space freeing up limitation	9.1.0.0
27 June 2022	▪ Ch. 1 & 2 – changed Office 365 to Microsoft 365 ▪ Ch. 3 – updated steps on creating backup set ▪ Ch. 6 – updated restore instructions	9.3.0.0
15 July 2022	▪ Ch. 3 – added note regarding backup of Teams Chat and Teams Channel	9.3.0.0
8 August 2022	▪ Ch. 2.15 – added Teams Chat limitations	9.3.0.0
3 November 2022	▪ Ch. 3 – added permission request and exclude filter screenshots and instructions ▪ Ch. 7 – added Delete corrupted data blocks permanently description	9.5.0.0
2 May 2023	▪ Ch. 2.9 and 2.10 – updated steps for assigning permission	9.5.4.0

Table of Contents

1 Overview 1

What is this software? 1

1.1 System Architecture 1

1.2 Why should I use AhsayCBS Run on Server (Agentless) solution to back up my Microsoft 365 data? 2

1.3 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 Microsoft 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 Microsoft 365 License Requirements 11

2.9 Microsoft 365 Permission Requirements for AhsayOBM 12

2.9.1 Assigning Global Admin Role to Accounts 13

2.9.2 Granting Term Store Administrator Role 15

2.9.3 Granting Permission to Discovery Management Group 16

2.9.4 Granting Permission to Accounts for Creating Backup Set 18

2.9.5 Granting Permission to restore all share link types to alternate location in Microsoft 365 19

2.10 Microsoft 365 Permission Requirements for AhsayACB 22

2.10.1 Assigning Global Admin Role to Accounts 22

2.10.2 Granting Permission to Discovery Management Group 25

2.10.3 Granting Permission to Accounts for Creating Backup Set 27

2.11 Data Synchronization Check (DSC) Setup 29

2.12 Authentication 31

2.13 Supported Services 33

2.14 Maximum Supported File Size 41

2.14.1 AhsayOBM 41

2.14.2 AhsayACB 41

2.15 Limitations 42

2.15.1 AhsayOBM 42

2.15.2 AhsayACB 65

2.15.3 AhsayCBS Run on Server (Agentless) 73

2.16 Best Practices and Recommendations 74

3 Creating a Microsoft 365 Backup Set 80

AhsayOBM 89
AhsayACB 94

4 Overview of Microsoft 365 Backup Process 104

4.1 Periodic Data Integrity Check (PDIC) Process 105
4.2 Backup Set Index Handling Process 107
4.2.1 Start Backup Job 107
4.2.2 Completed Backup Job 108
4.3 Data Validation Check Process 109

5 Running Backup Job 110

6 Restoring Microsoft 365 Backup Set 113

From Users 114
From Teams 124
From SharePoint Sites 128
From Public Folders 129

7 Running a Data Integrity Check 143

8 Deleting Backup Data 145

9 Contact Ahsay 147

9.1 Technical Assistance 147
9.2 Documentation 147

Appendix 148

Appendix A: Example Scenarios for Microsoft 365 License Requirement and Usage 148
Appendix B: Example for backup of large numbers of Microsoft 365 users 153
Appendix C: Setting Multi-Factor Authentication (MFA) in Microsoft 365 Admin Center 156
Appendix D: Example Scenario for Backup Set Maintenance 167
Appendix E: Example Scenario for Data Synchronization Check (DSC) with sample backup reports 168
Appendix F: How to view Item count and Storage used in Microsoft 365 Admin Center 173
Appendix G: Re-Authentication of Microsoft 365 Backup Set 178

1 Overview

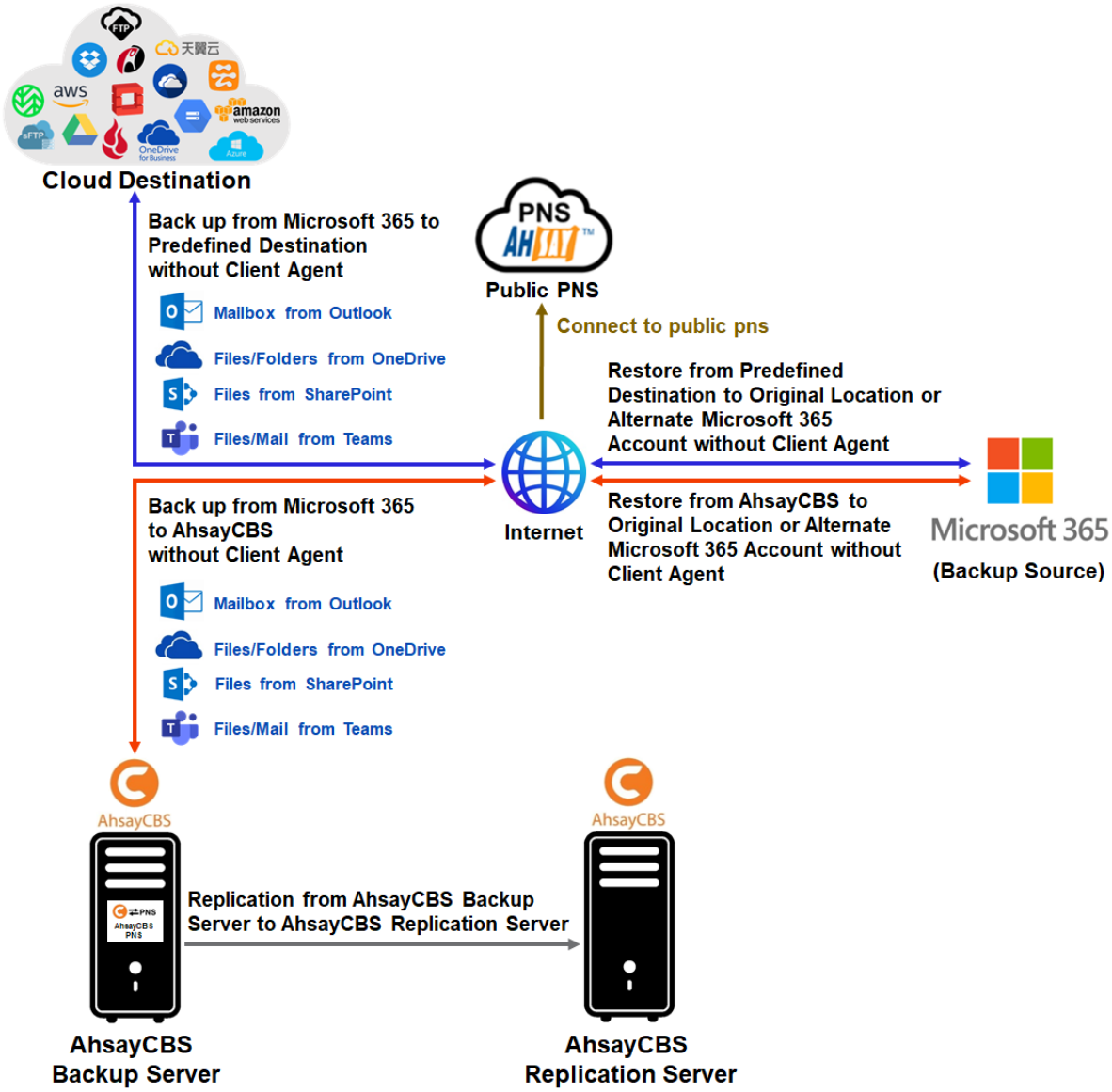
What is this software?

Ahsay Cloud Backup Suite v9 allows you to back up your Microsoft 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.

1.1 System Architecture

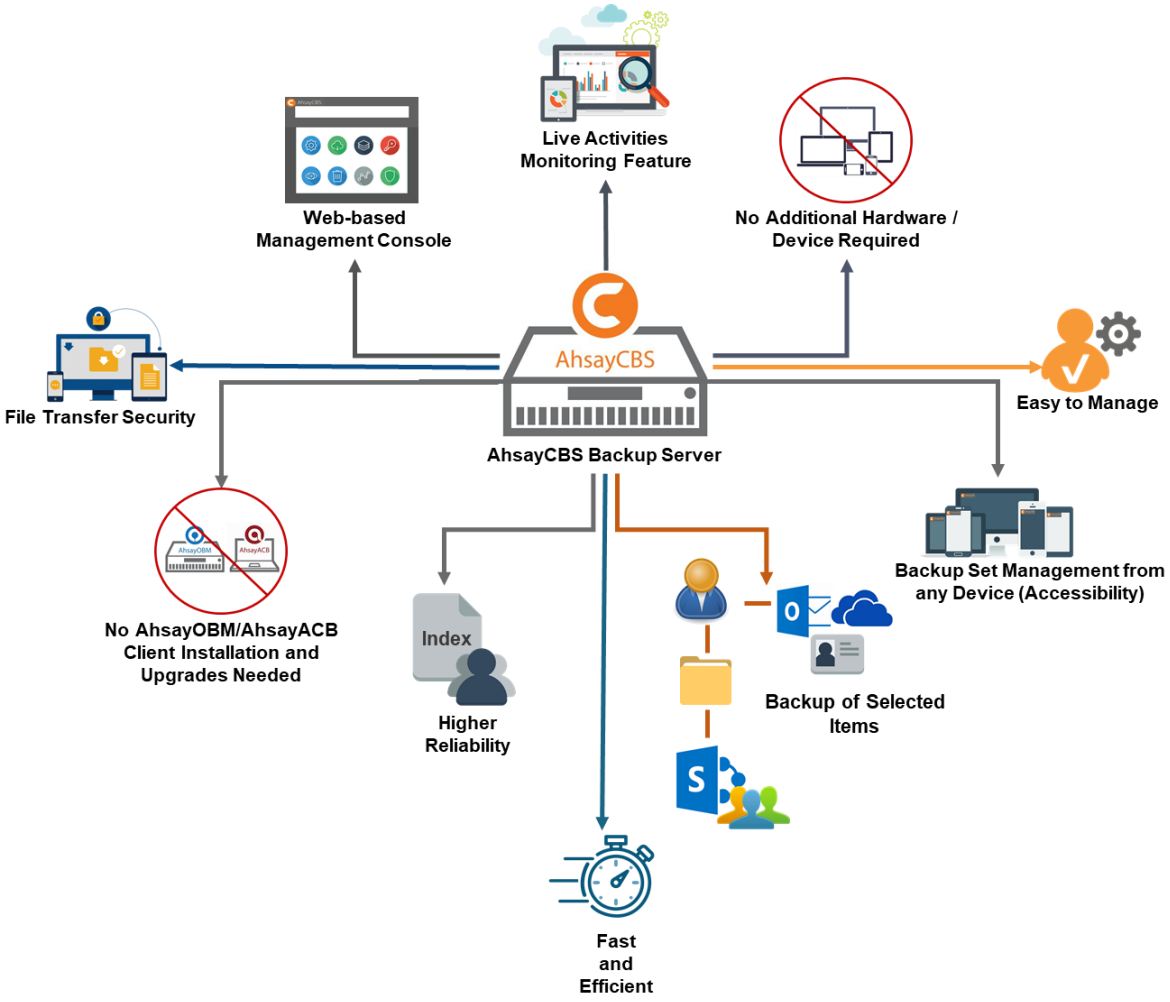
For agentless backup and restore, the AhsayCBS backup server connects to the Microsoft 365 directly through the Internet without the need to deploy additional backup agents on the customers site.

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.



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

We are committed to bringing you a comprehensive Run-on Server (Agentless) Microsoft 365 backup and recovery solution. Below are some key areas that can help 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 Change Key API has significantly improved backup performance of backup jobs, which means backup sets with a large number of Microsoft 365 accounts for 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
- View the status of the restore process that is currently running

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 Microsoft 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 Microsoft 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 content or just one item.
  - Restore items to the original location or an alternate location.

Fast and Efficient

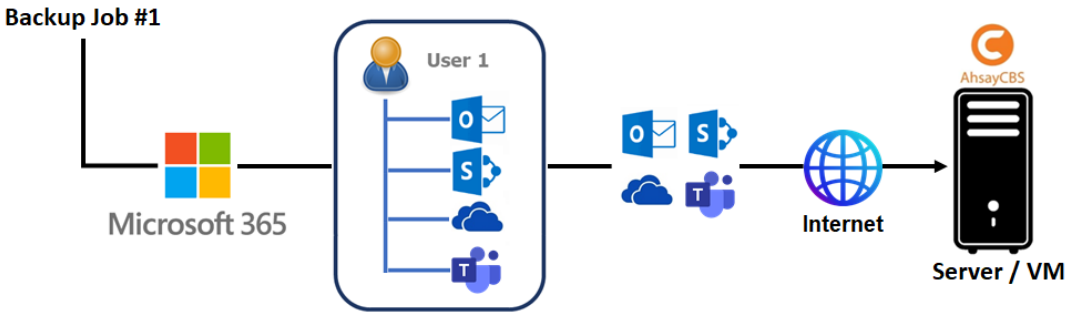
We understand that backup could be a time and resources consuming process, which is why AhsayCBS is designed with advanced technologies to make backup a fast and efficient process.

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.

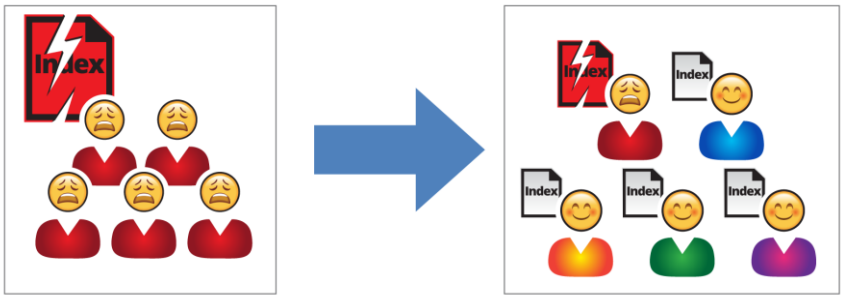
  The default setting for Microsoft 365 backup sets supports a total of 4 threads per backup job.

  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 (Microsoft 365) to the backup destination (AhsayCBS server).

High Level of Security

We understand your Microsoft 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 Microsoft 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:

- Aliyun
- CTYun
- Amazon S3
- AWS S3 Compatible Cloud Storage
- Wasabi
- Backblaze
- Google Cloud Storage
- Google Drive
- Microsoft Azure
- Microsoft OneDrive
- Microsoft OneDrive for Business
- Rackspace
- OpenStack
- Dropbox
- FTP
- SFTP

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 Microsoft 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 Microsoft 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 Microsoft 365 backup set, and the tool to use (web console or client agent) when performing a backup and restore:

	Run on Server Microsoft 365 Backup Set	Run on Client Microsoft 365 Backup Set
General Settings	✓	✓
Backup Source	✓	✓
Backup Schedule	✓	✓
Destination	AhsayCBS or Predefined Destinations only	AhsayCBS, Predefined Destinations, Standard and Local
Multiple Destinations	✘	✓
Deduplication	✓	AhsayOBM
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	✘	✓
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 Microsoft 365 Backup Set	Run on Client Microsoft 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 v9 User Guide - Microsoft 365 Backup & Restore for Windows

AhsayOBM v9 User Guide - Microsoft 365 Backup & Restore for Mac

AhsayACB v9 User Guide - Microsoft 365 Backup & Restore for Windows

AhsayACB v9 User Guide - Microsoft 365 Backup & Restore for Mac

1.3 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) Microsoft 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 Microsoft 365 Backup & Restore

Requirements
Requirements for Microsoft 365 backup set

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

Part 2: Performing a Microsoft 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 a Microsoft 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 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 and Delete Backup Data).

Who should read this document?

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

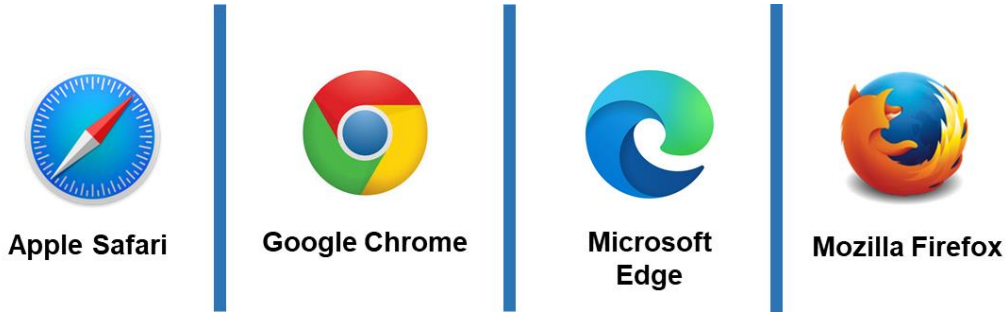
2 Preparing for Backup and Restore

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 or LAN access to the internal AhsayCBS server.

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 Microsoft 365

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

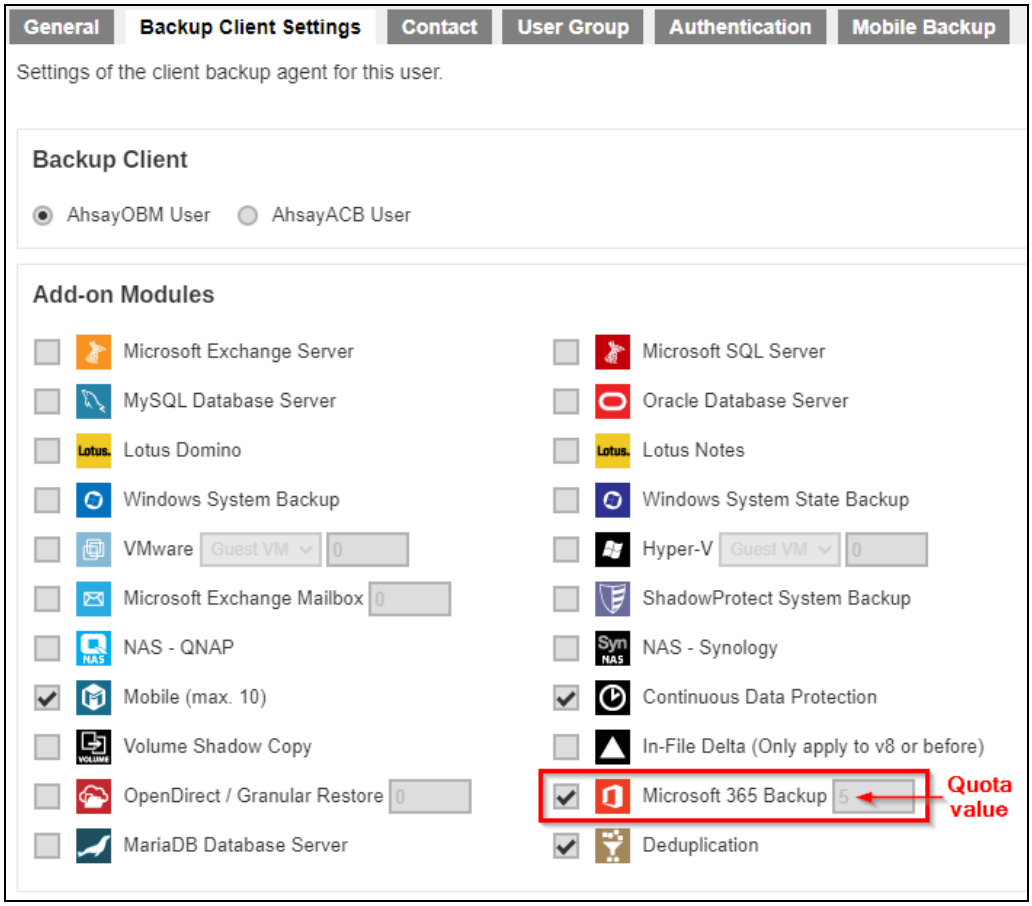
2.6 Add-on Module Requirements

- Microsoft 365 Add-on Module

  Make sure that the Microsoft 365 Backup feature has been enabled as an add-on module in your AhsayOBM and AhsayACB user account and there is enough Microsoft 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 Microsoft 365 with licenses.

AhsayOBM User with five (5) licenses



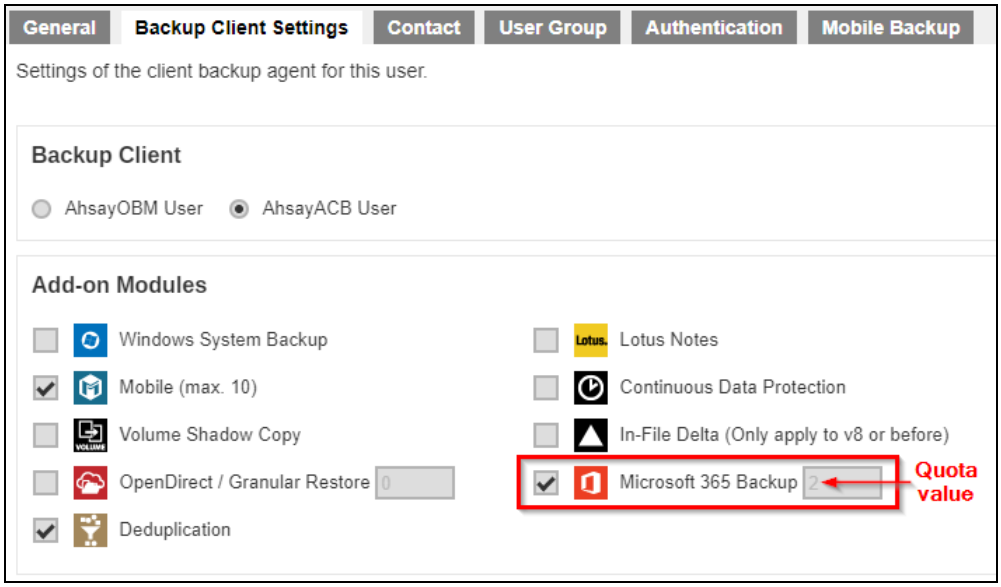
The Ahsay licenses for the Microsoft 365 module are calculated by the number of unique licensed or unlicensed Microsoft 365 user accounts. If same Microsoft 365 account is backed up on multiple backup sets with an AhsayOBM user account, it would be counted as one Microsoft 365 license.

- Each licensed or unlicensed Microsoft 365 user account selected for backup requires one Microsoft 365 license.
- Each Equipment Mailbox, Room Mailbox, or Shared Mailbox selected for backup requires one Microsoft 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 zero Microsoft 365 license but a minimum of one Microsoft 365 license is needed to perform a backup. The Microsoft 365 license is only needed to start the backup but it will not be counted as used license.

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

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

AhsayACB User with two (2) licenses



NOTE

- Please be reminded that a maximum of two (2) modules are allowed for Microsoft 365 Backup on AhsayACB. If you wish to back up more than two Microsoft 365 users, consider using AhsayOBM instead. Please contact your backup service provider for more details.
- Each AhsayACB Microsoft 365 backup set is limited to one Microsoft 365 user account. Therefore, when you backup two Microsoft 365 user accounts it will require two separate backup sets.

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

2.7 Backup Quota Requirement

Make sure that your AhsayACB or AhsayOBM user account has sufficient quota assigned to accommodate the storage of the Microsoft 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 Microsoft 365 Organization in the Microsoft 365 Admin Centre. Please refer to this link: Appendix F: How to view Item count and Storage used in Microsoft 365 Admin Center

2.8 Microsoft 365 License Requirements

Microsoft 365 Subscription Plan

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

Microsoft 365 Business	**Microsoft 365 Business Essentials**
Microsoft 365 Business Premium	**Microsoft 365 Enterprise E1**
Microsoft 365 Enterprise E3	**Microsoft 365 Enterprise E4**
Microsoft 365 Enterprise E5	**Microsoft 365 Education**

- **Microsoft 365 Subscription Status**

  Make sure your Microsoft 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 Microsoft 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 365 Subscription Status.

- **Restore Requirement**

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

  - Requires Exchange License

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

  - Requires SharePoint License

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

2.9 Microsoft 365 Permission Requirements for AhsayOBM

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

- **Global Admin Role**

  The Microsoft 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.

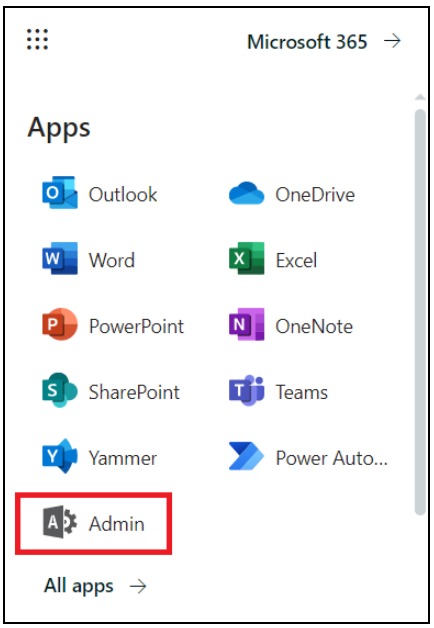
  - ApplicationImpersonation
  - Legal Hold
  - Mailbox Import Export
  - Mailbox Search
  - Public Folders

Otherwise, proceed to grant all necessary permissions to the Microsoft user account as shown in the following chapters 2.9.1, 2.9.2, 2.9.3, 2.9.4, and 2.9.5.

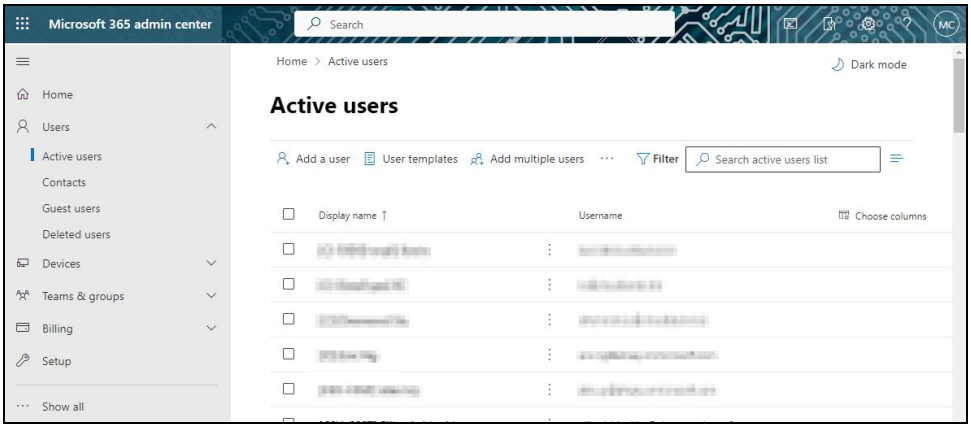
2.9.1 Assigning Global Admin Role to Accounts

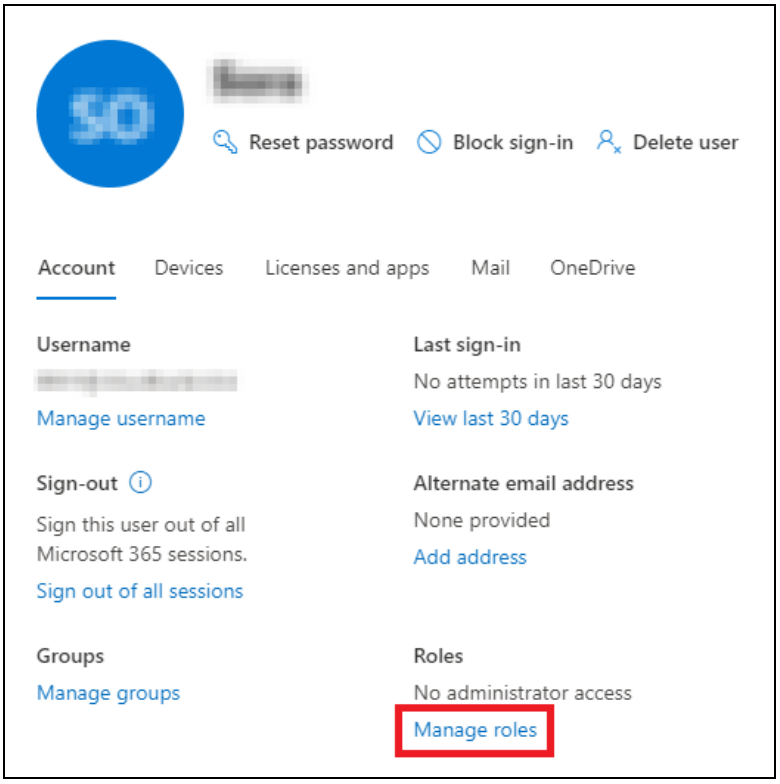
To assign the Global Admin role to accounts, follow the steps below:

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

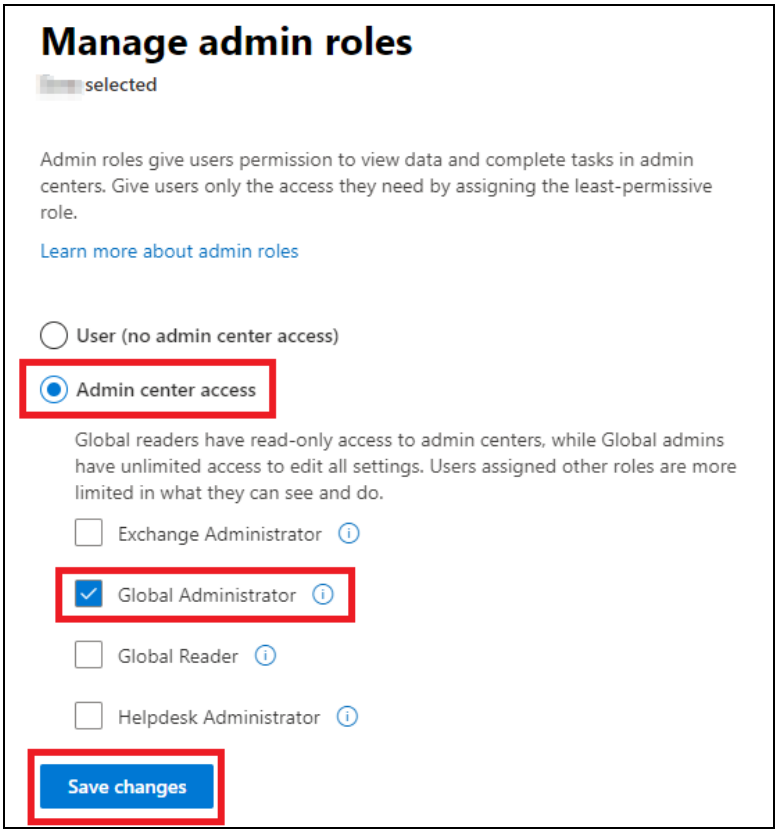


ii. In the Microsoft 365 admin center, on the left panel click **Users**. Find the user you want to assign the Global Admin and select **Manage roles**.





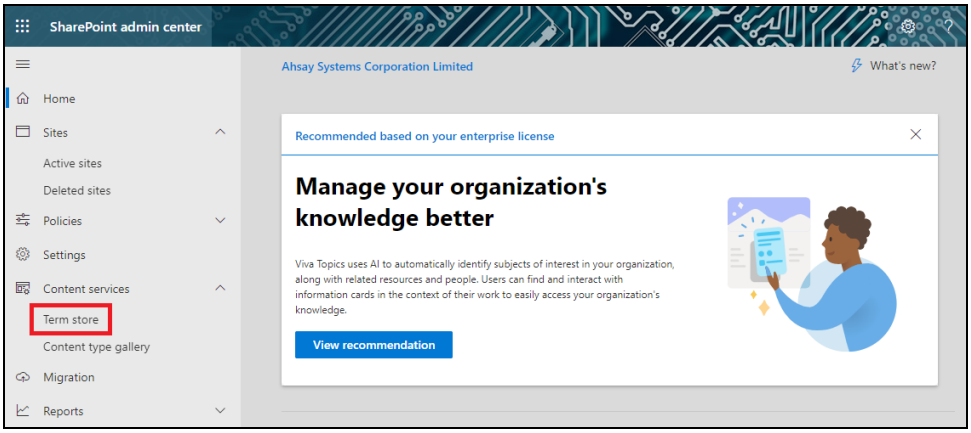
iii. In the Manage roles window, select **Admin center access** then check the box beside **Global admin**. Click **Save Changes** to save the role you assigned.



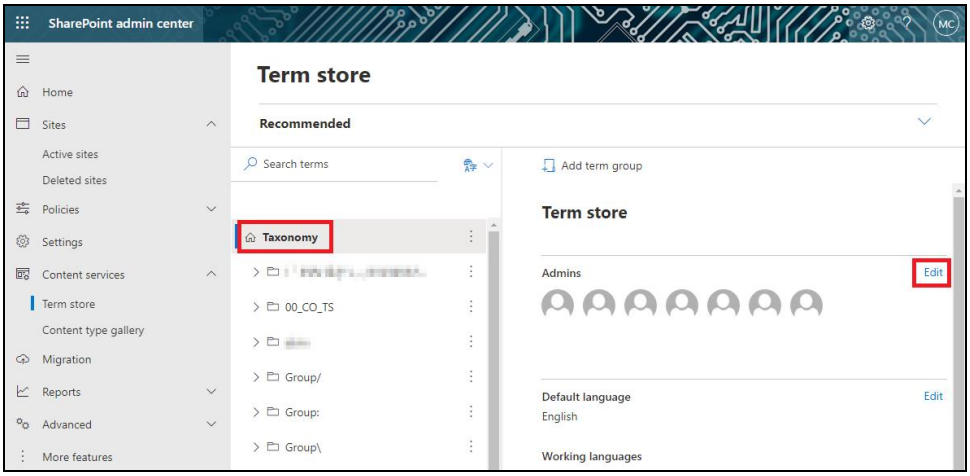
2.9.2 Granting Term Store Administrator Role

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

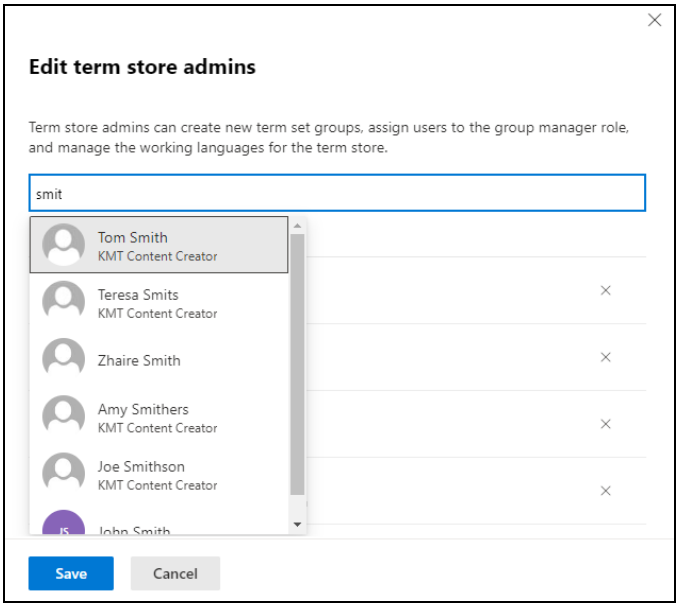
i. In the SharePoint admin center, under **Content services**, click **Term store**.



ii. In the tree view pane in the middle, select **Taxonomy**. Then click **Edit** in the Term store section on the right.



iii. The “Edit term store admins” panel appears. Enter the names or email addresses of the Microsoft 365 user who you want to add as term store admins then click **Save**.

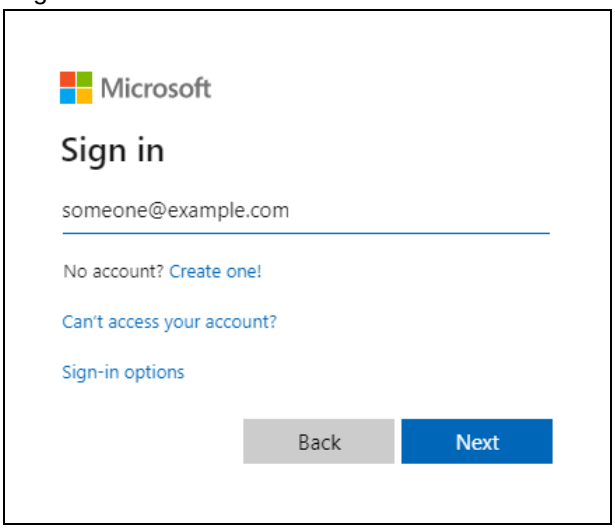


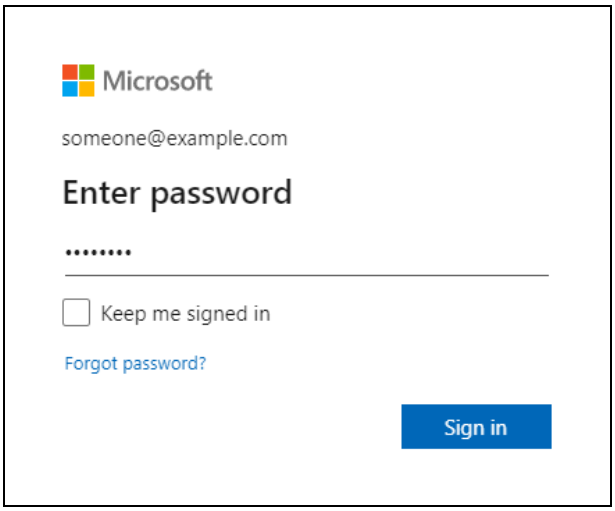
2.9.3 Granting Permission to Discovery Management Group

This permission allows users added under the **Permissions** 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 **Assigned** section.

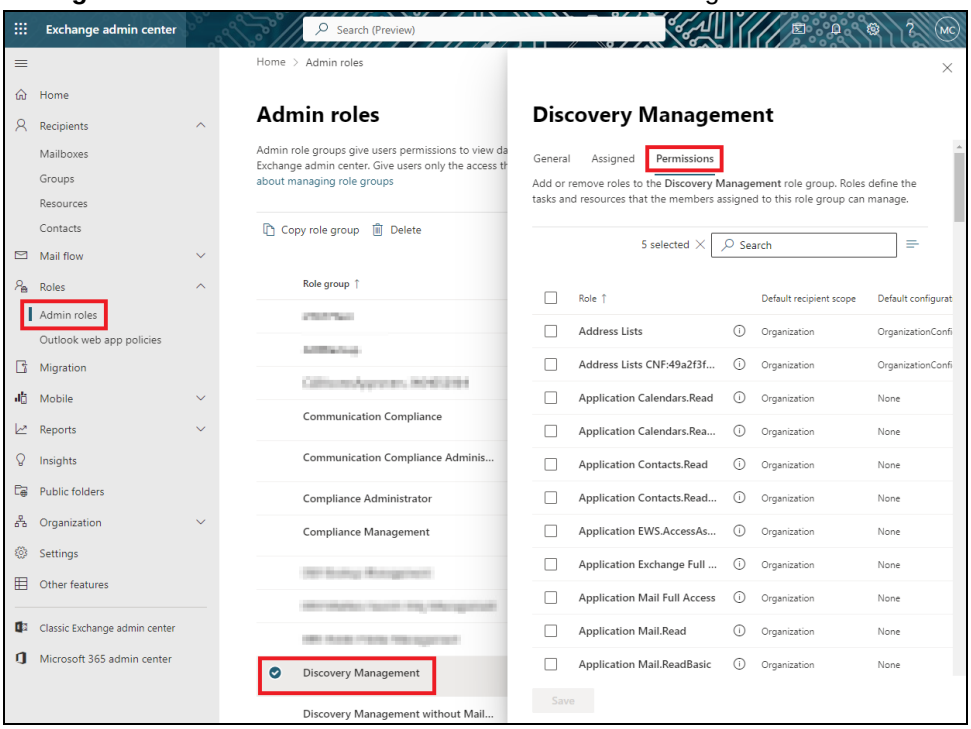
i. Open https://admin.exchange.microsoft.com/

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



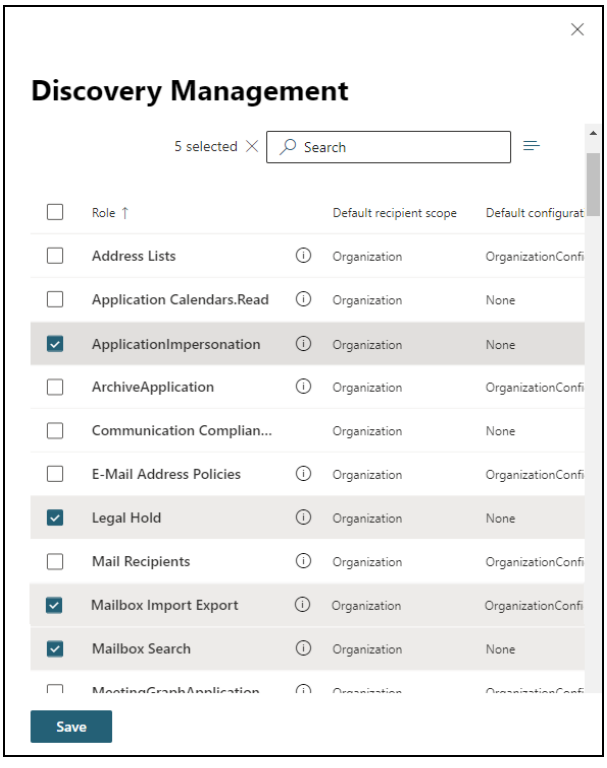


iii. Select **Admin roles** which is under Roles on the left, then click on **Discovery Management** in the middle. Click on **Permissions** on the right.



iv. Tick the box beside the roles you want to add. These are the following roles:

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

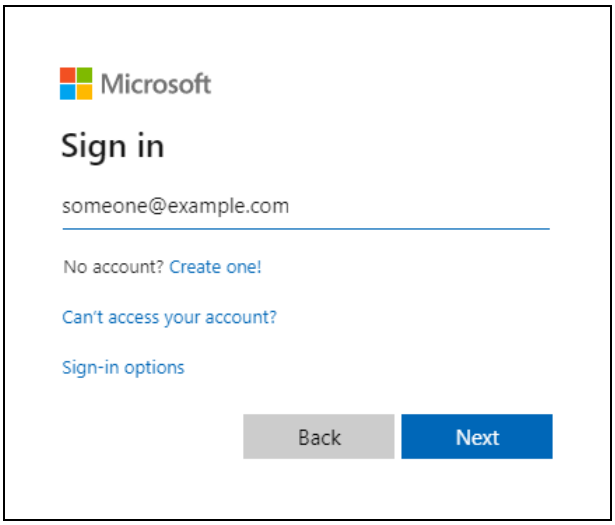


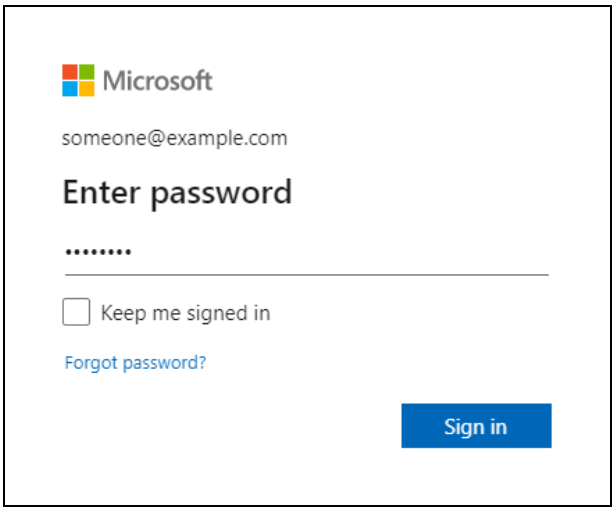
v. Click **Save** to confirm and click ✕ to exit the setting.

2.9.4 Granting Permission to Accounts for Creating Backup Set

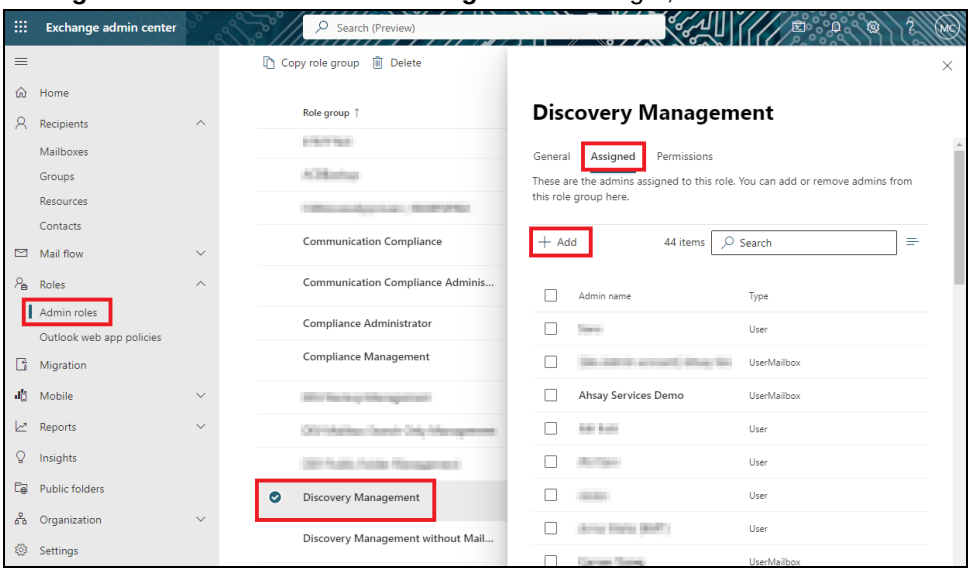
i. Open https://admin.exchange.microsoft.com/

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

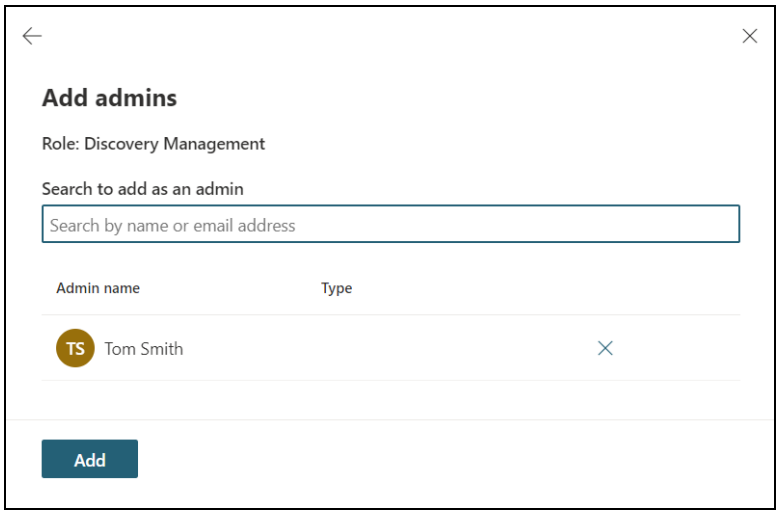




iii. Select **Admin roles** which is under Roles on the left, then click on **Discovery Management** in the middle. Click **Assigned** on the right, then click **Add**.



iv. You can now add users to this group. Search by name or email address then click **Add** once done.



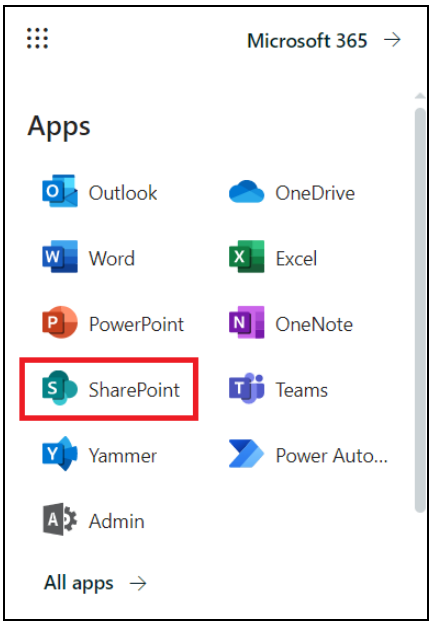
2.9.5 Granting Permission to restore all share link types to alternate location in Microsoft 365

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

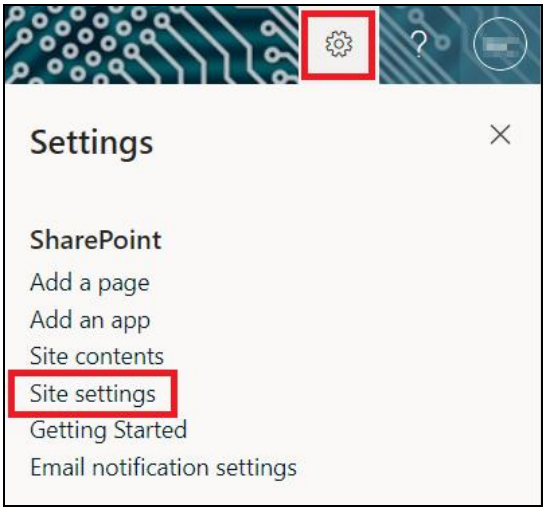
- Allowing anonymous users to access application pages

i. Click the App launcher in the upper left side.

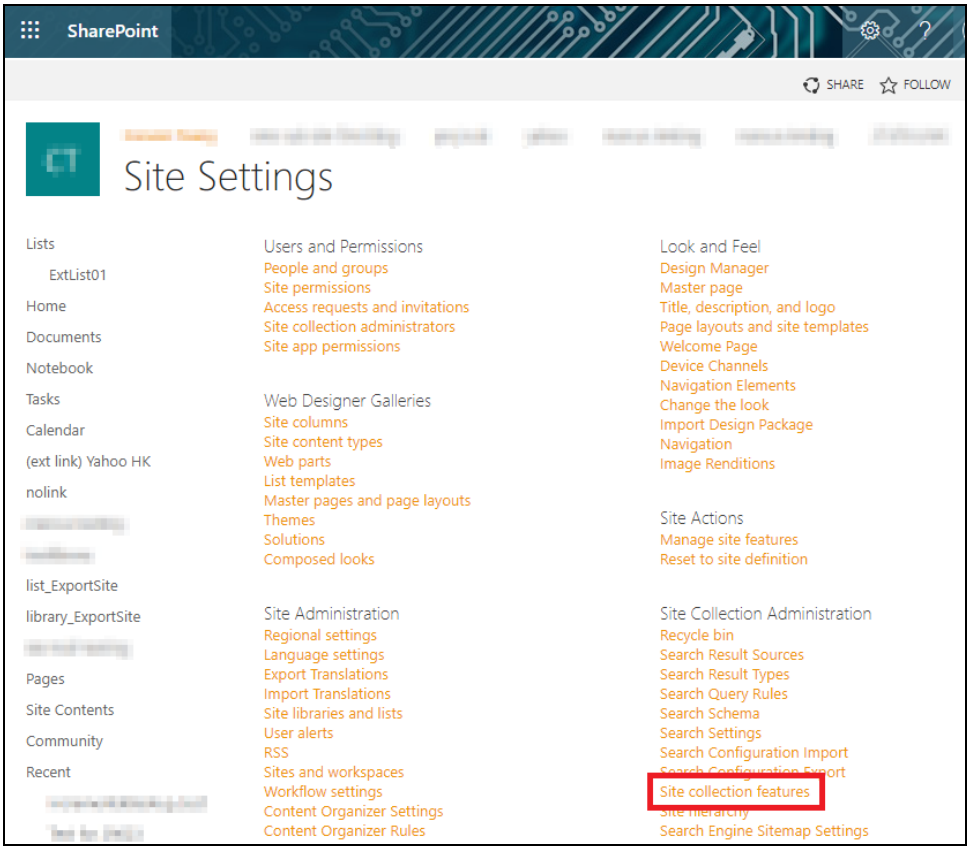
ii. Click **SharePoint** to go to the SharePoint page.



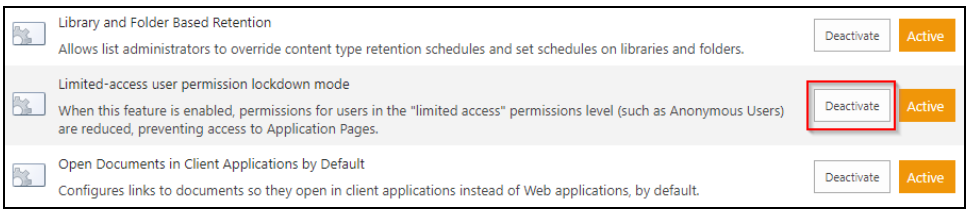
iii. Click **Settings** > **Site Settings**.



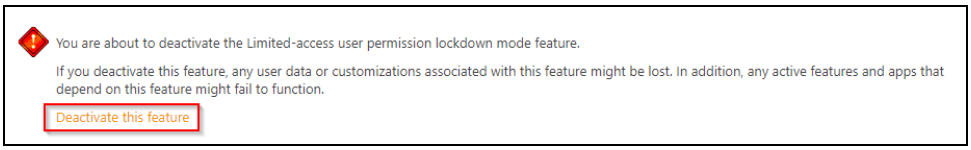
iv. Under Site Collection Administration, click **Site collection features**.



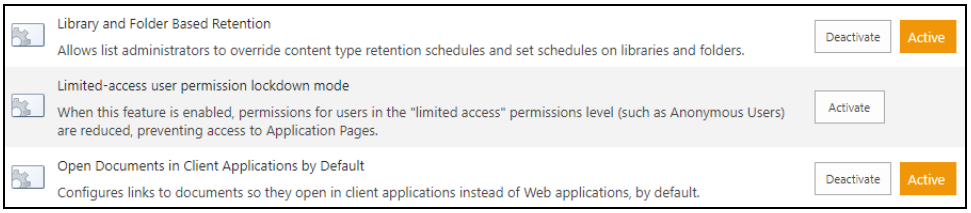
v. Scroll down and look for "**Limited-access user permission lockdown mode**", click the **Deactivate** button.



vi. Click **Deactivate this feature**.

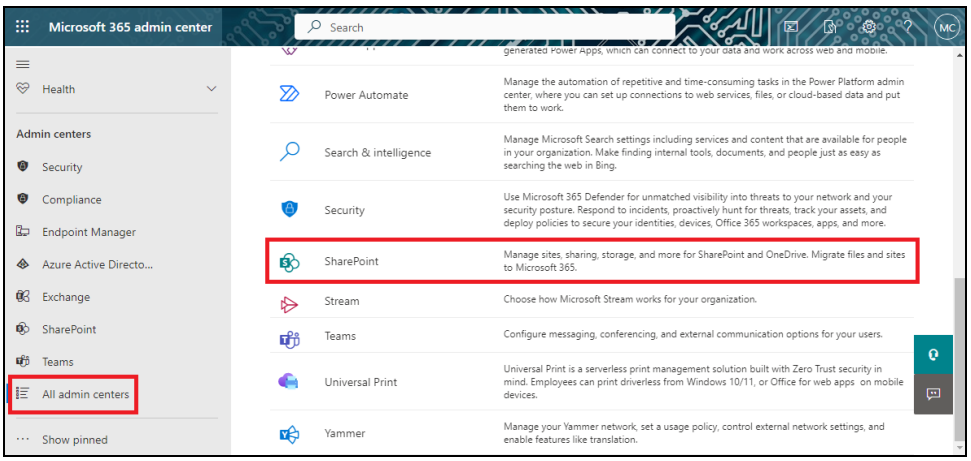


Once deactivated, the Deactivate button will no longer be available.

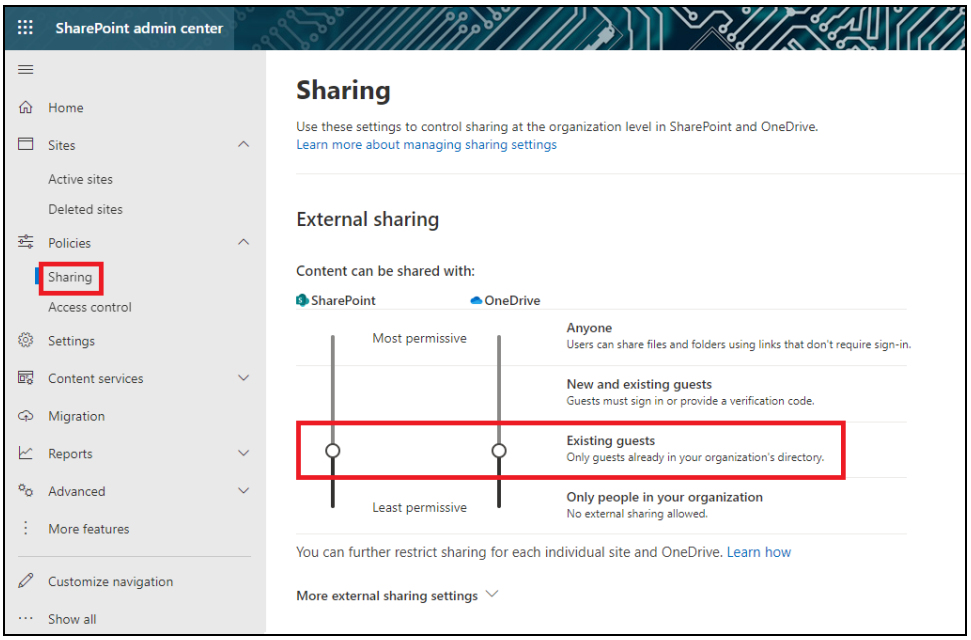


- Allowing sharing to external users

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



ii. Go to **Policies** > **Sharing**. Under <u>External sharing</u> the button must be in line with "**Existing guests**" and click **Save**.



2.10 Microsoft 365 Permission Requirements for AhsayACB

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

- **Global Admin Role**

  The Microsoft 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.

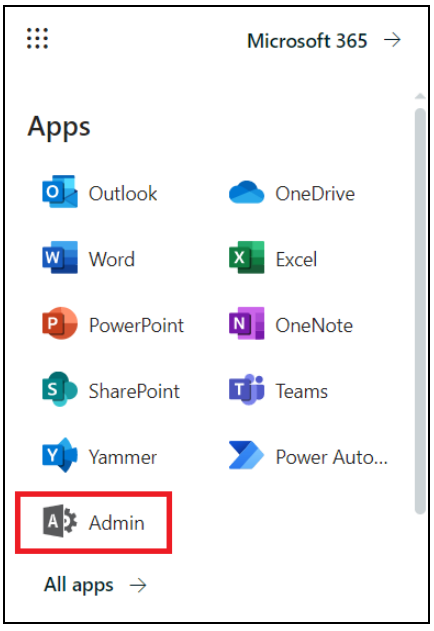
  - Mailbox Search
  - Public Folders

Otherwise, proceed to grant all necessary permissions to the Microsoft user account as shown in the following chapters 2.10.1, 2.10.2 and 2.10.3.

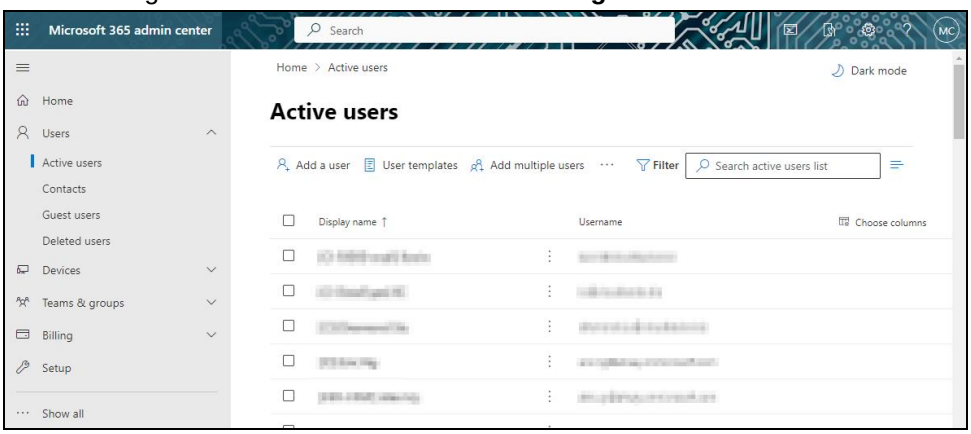
2.10.1 Assigning Global Admin Role to Accounts

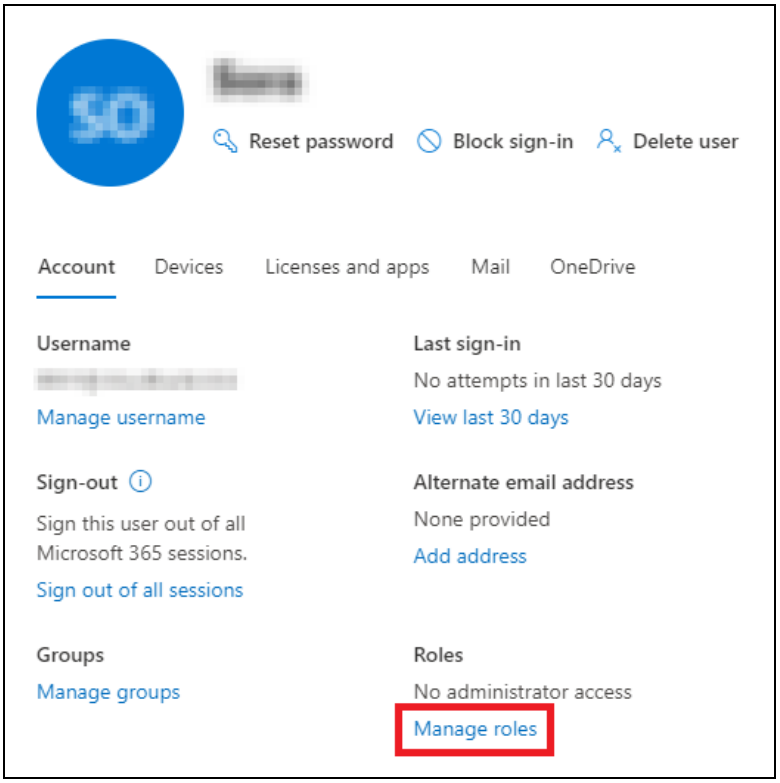
To assign the Global Admin role to accounts, follow the steps below:

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

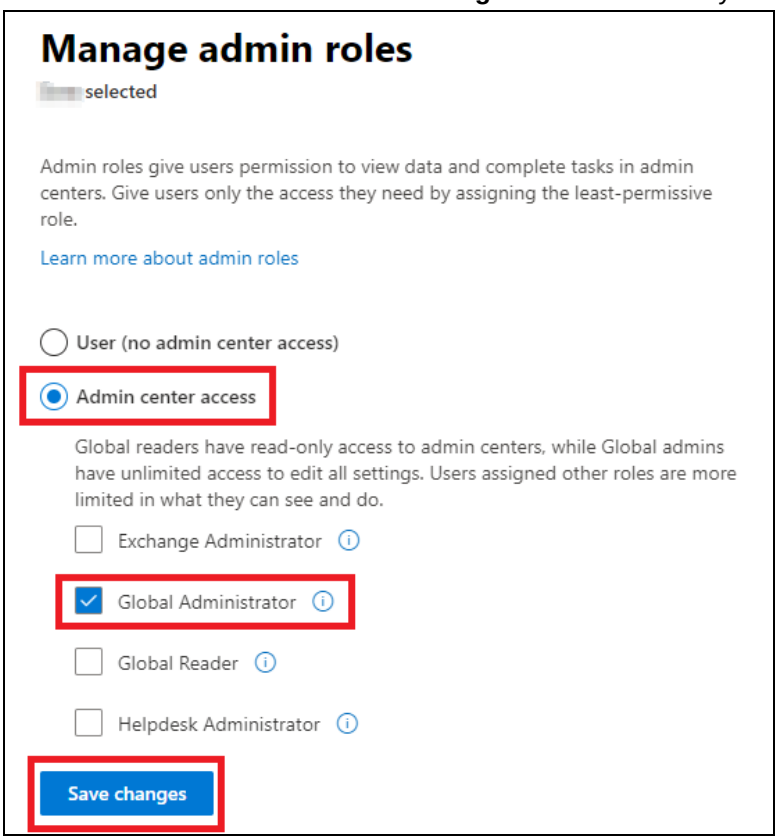


ii. In the Microsoft 365 admin center, on the left panel click **Users**. Find the user you want to assign the Global Admin and select **Manage roles**.





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

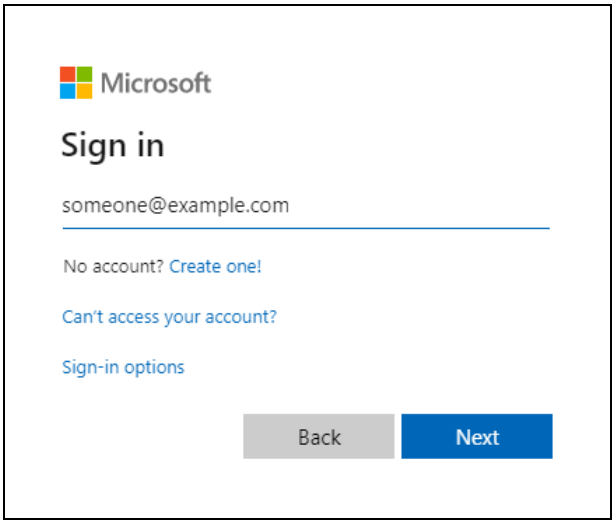


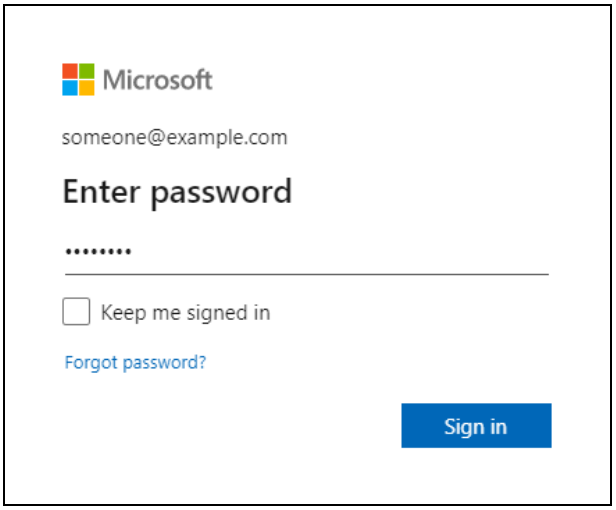
2.10.2 Granting Permission to Discovery Management Group

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.

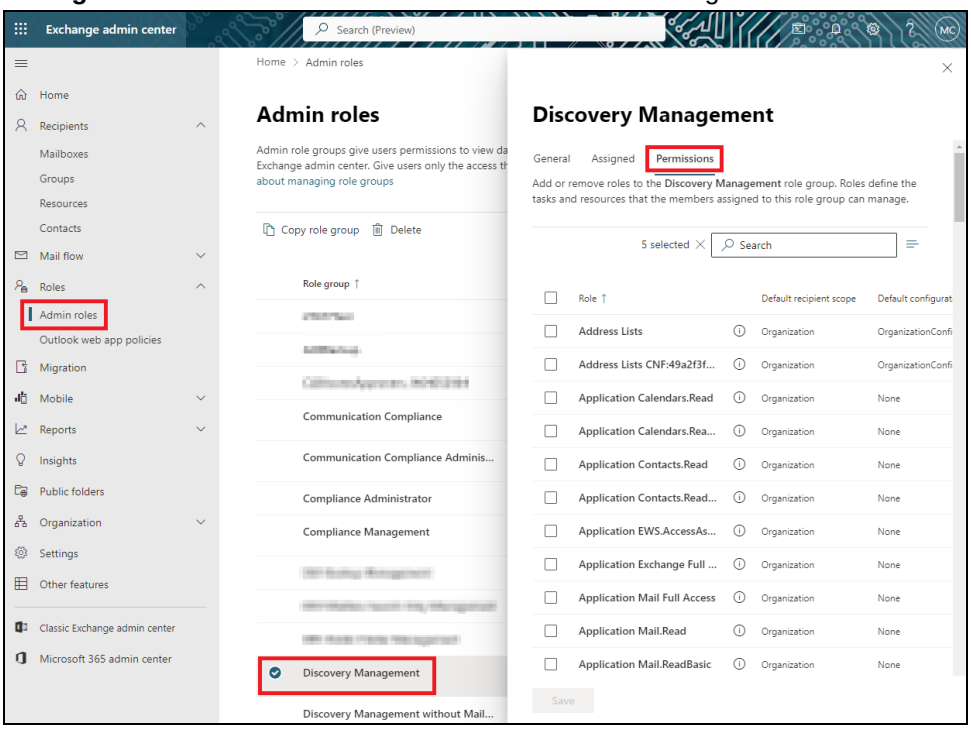
i. Open https://admin.exchange.microsoft.com/

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



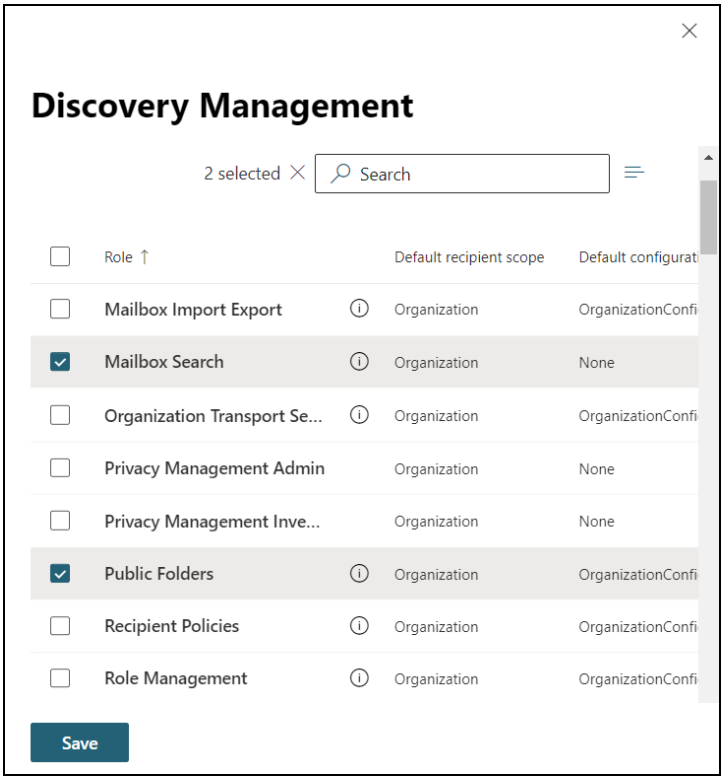


iii. Select **Admin roles** which is under Roles on the left, then click on **Discovery Management** in the middle. Click on **Permissions** on the right.



iv. Tick the box beside the roles you want to add. These are the following roles:

- Mailbox Search
- Public Folders

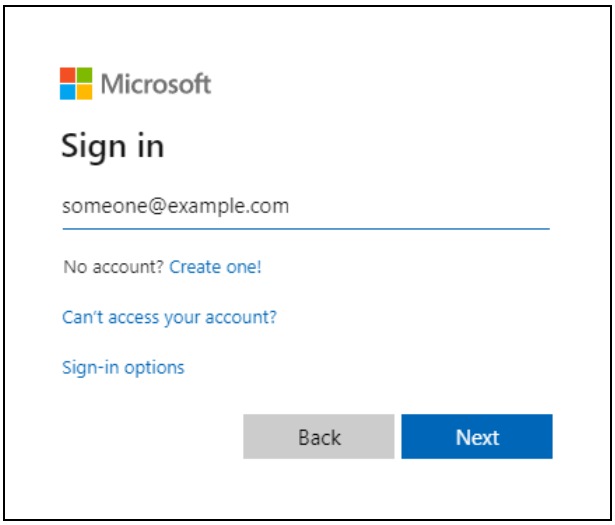


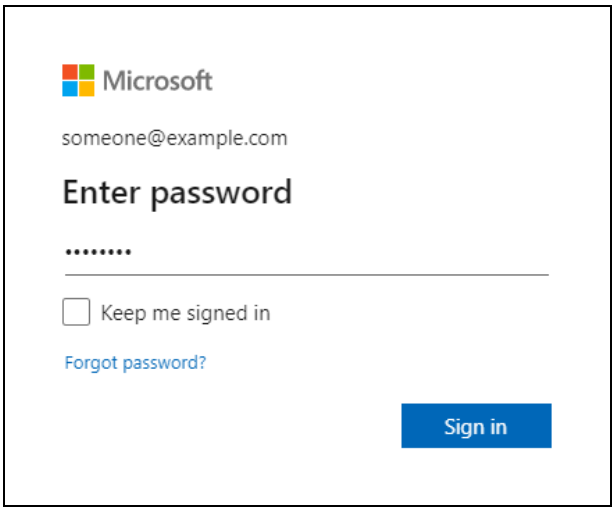
v. Click **Save** to confirm and click ✕ to exit the setting.

2.10.3 Granting Permission to Accounts for Creating Backup Set

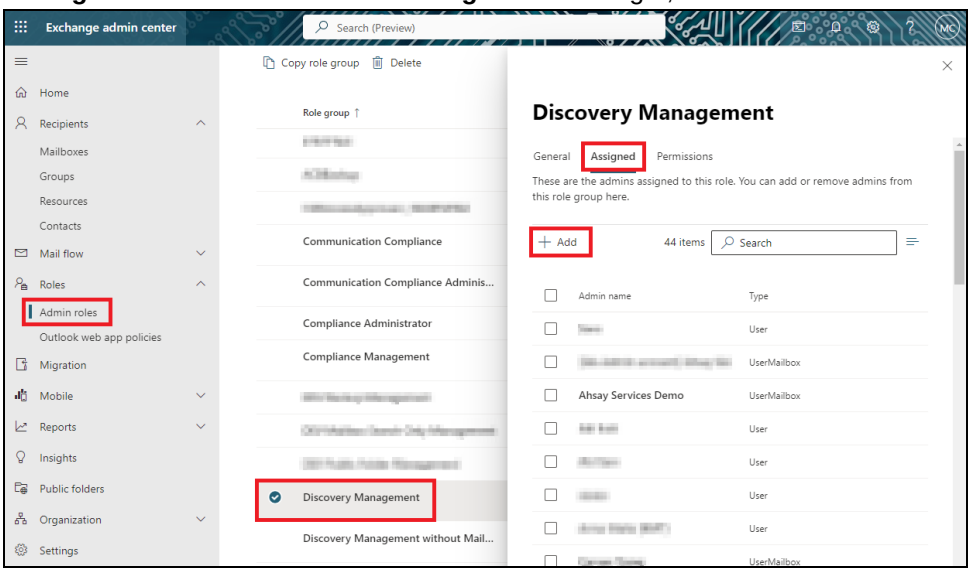
i. Open https://admin.exchange.microsoft.com/

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

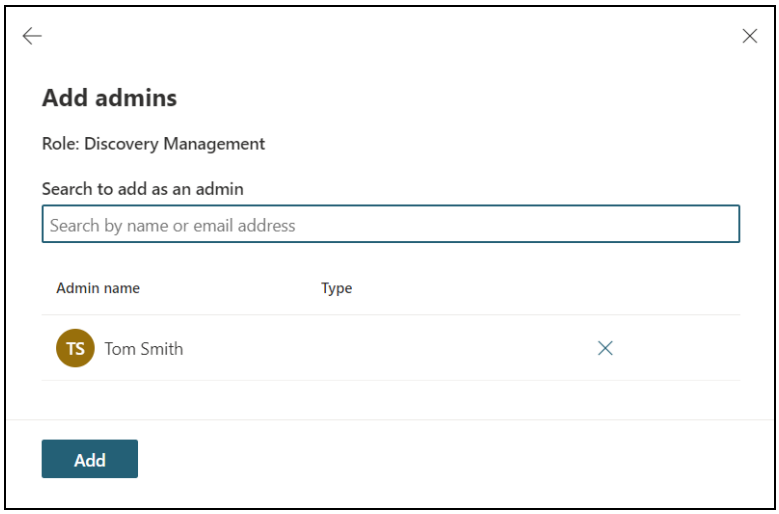




iii. Select **Admin roles** which is under Roles on the left, then click on **Discovery Management** in the middle. Click **Assigned** on the right, then click **Add**.



iv. You can now add users to this group. Search by name or email address then click **Add** once done.



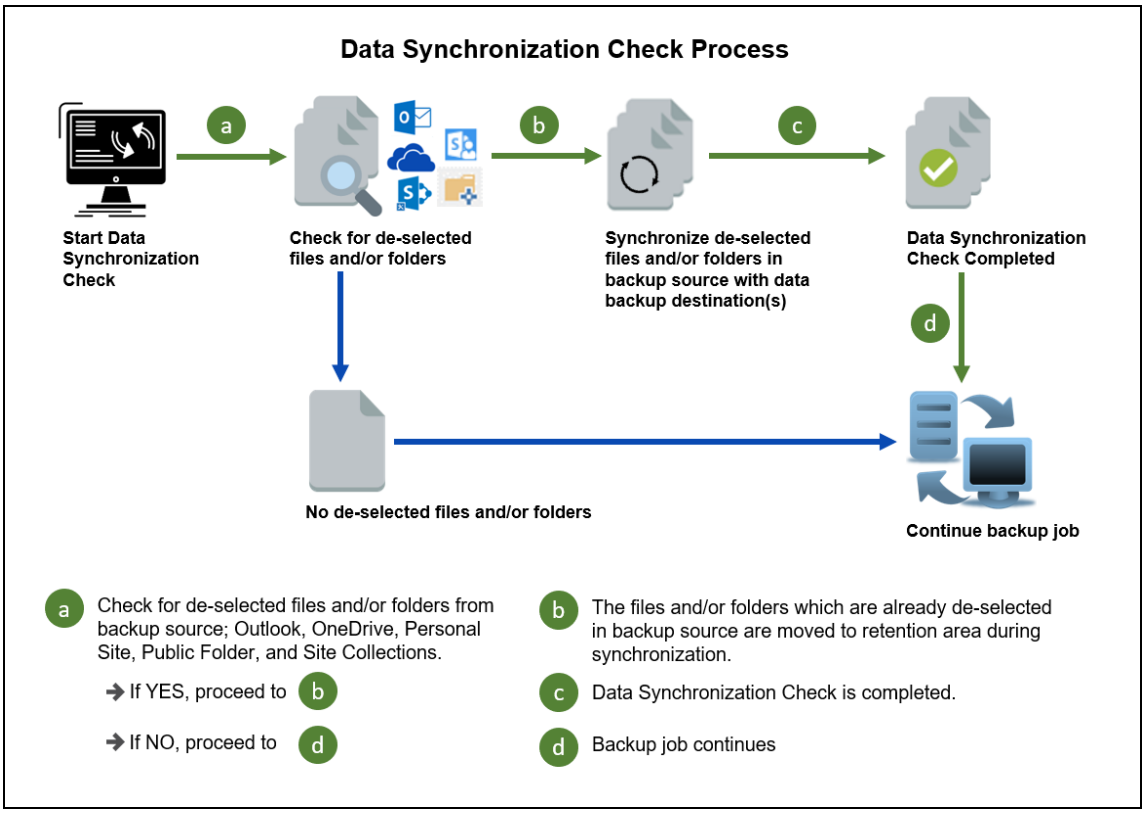
2.11 Data Synchronization Check (DSC) Setup

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 Microsoft 365 user accounts or Site Collections. Un-selected individual Microsoft 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 Microsoft 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 DSC.

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


Data Synchronization Check Process
a
b
c
Start Data Synchronization Check
Check for de-selected files and/or folders
Synchronize de-selected files and/or folders in backup source with data backup destination(s)
Data Synchronization Check Completed
d
No de-selected files and/or folders
Continue backup job
a Check for de-selected files and/or folders from backup source; Outlook, OneDrive, Personal Site, Public Folder, and Site Collections.
→ If YES, proceed to b
→ If NO, proceed to d
b The files and/or folders which are already de-selected in backup source are moved to retention area during synchronization.
c Data Synchronization Check is completed.
d Backup job continues

2.12 Authentication

To comply with Microsoft's product roadmap for Microsoft 365, Basic Authentication (Authentication using Microsoft 365 login credentials) will no longer be utilized. Instead, all new Microsoft 365 backup sets created will use Modern 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 Microsoft 365 login credentials. In order to use Modern Authentication, the Microsoft 365 account is registered under Global region and the Microsoft 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 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 Modern Authentication please refer to Appendix G: Re-Authentication of Microsoft 365 Backup Set. After the upgrade to AhsayCBS v9.1.0.0 or above, the backup and restore process of existing Microsoft 365 backup sets still using Basic Authentication will not be affected during this transition period since Modern Authentication is not yet enforced by Microsoft.

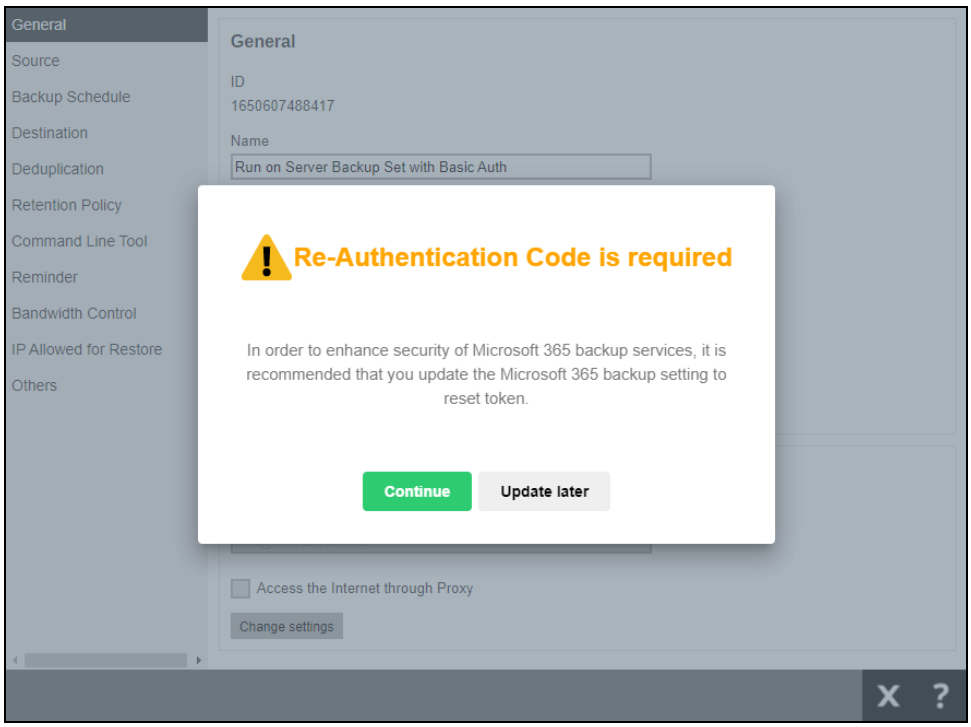
In order to migrate existing backup sets to Modern Authentication there are two (2) methods:

- The first method is the Microsoft 365 account used for the backup set is assigned the Global Admin.
- The second method is the Microsoft 365 account used for the backup set is an ordinary account. When changing the settings of the backup set, the user can ask a Microsoft 365 Global Admin to grant permission 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**.

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

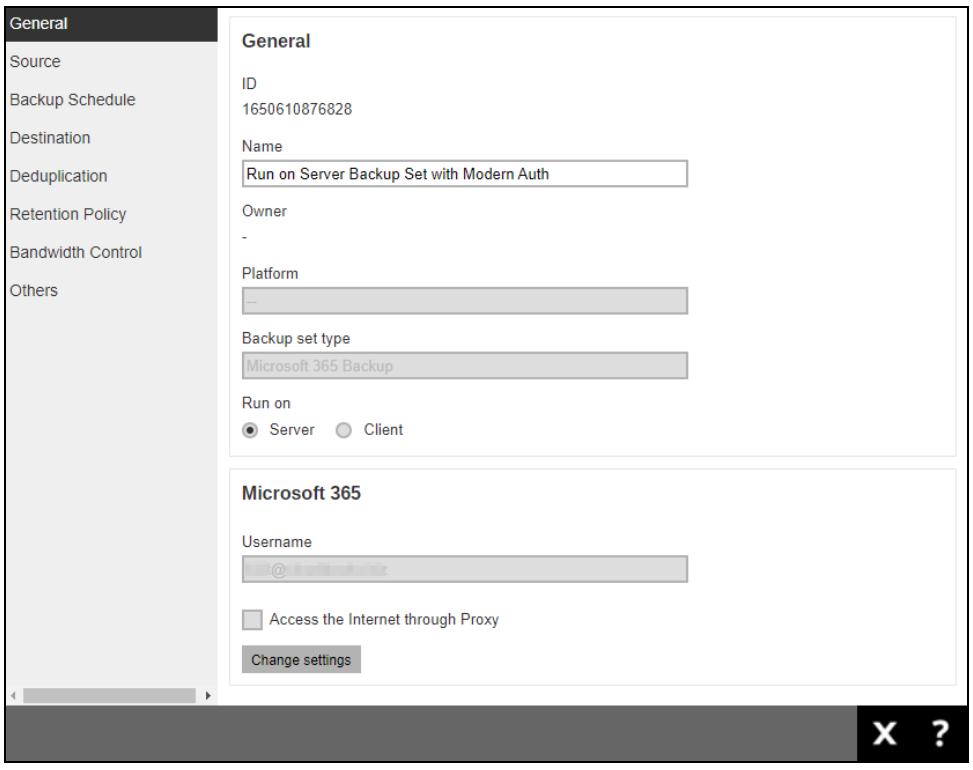
- **Basic Authentication**

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



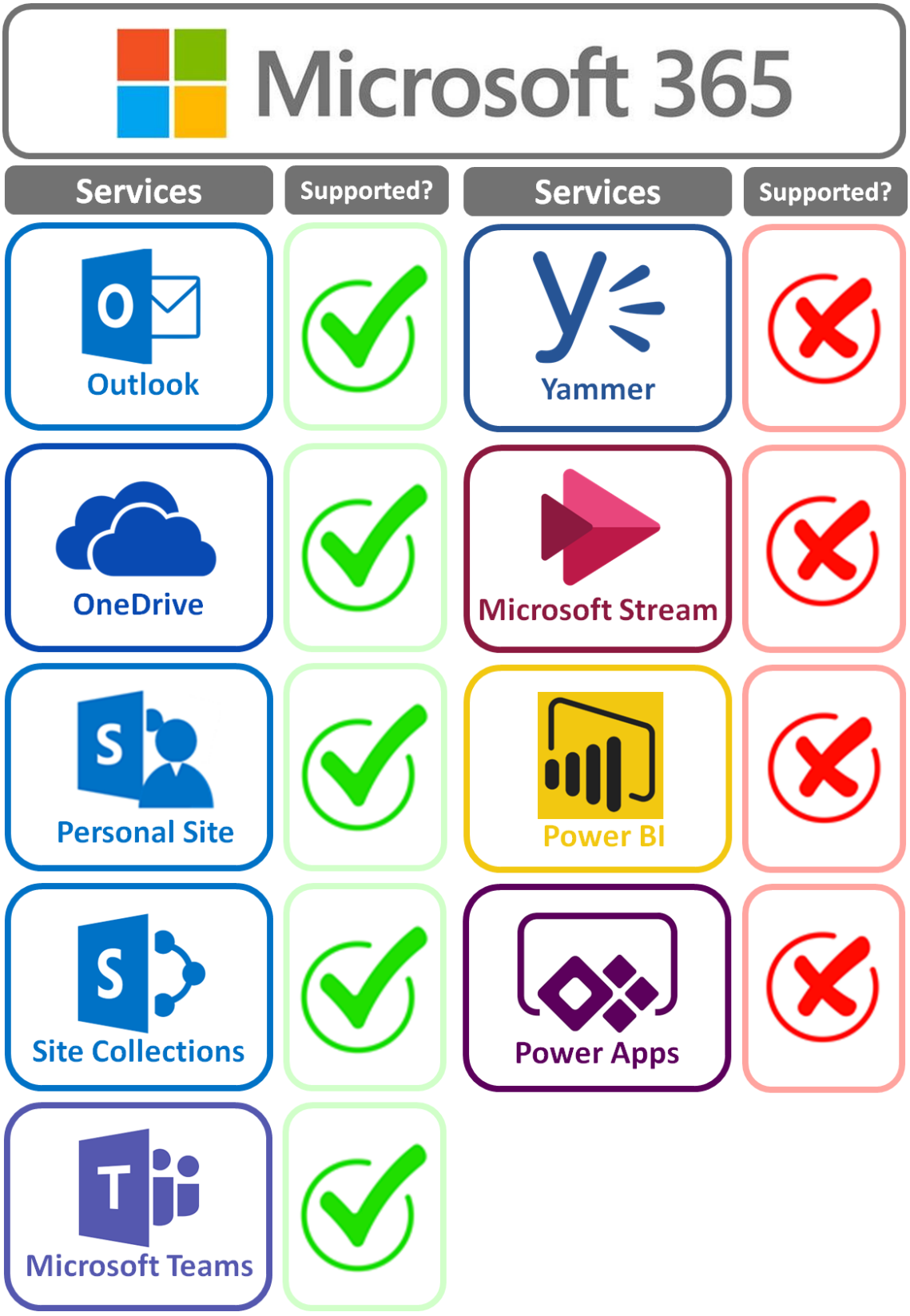
- **Modern and Hybrid Authentication**

  For backup set using Modern or Hybrid Authentication, there is no pop up authentication alert.

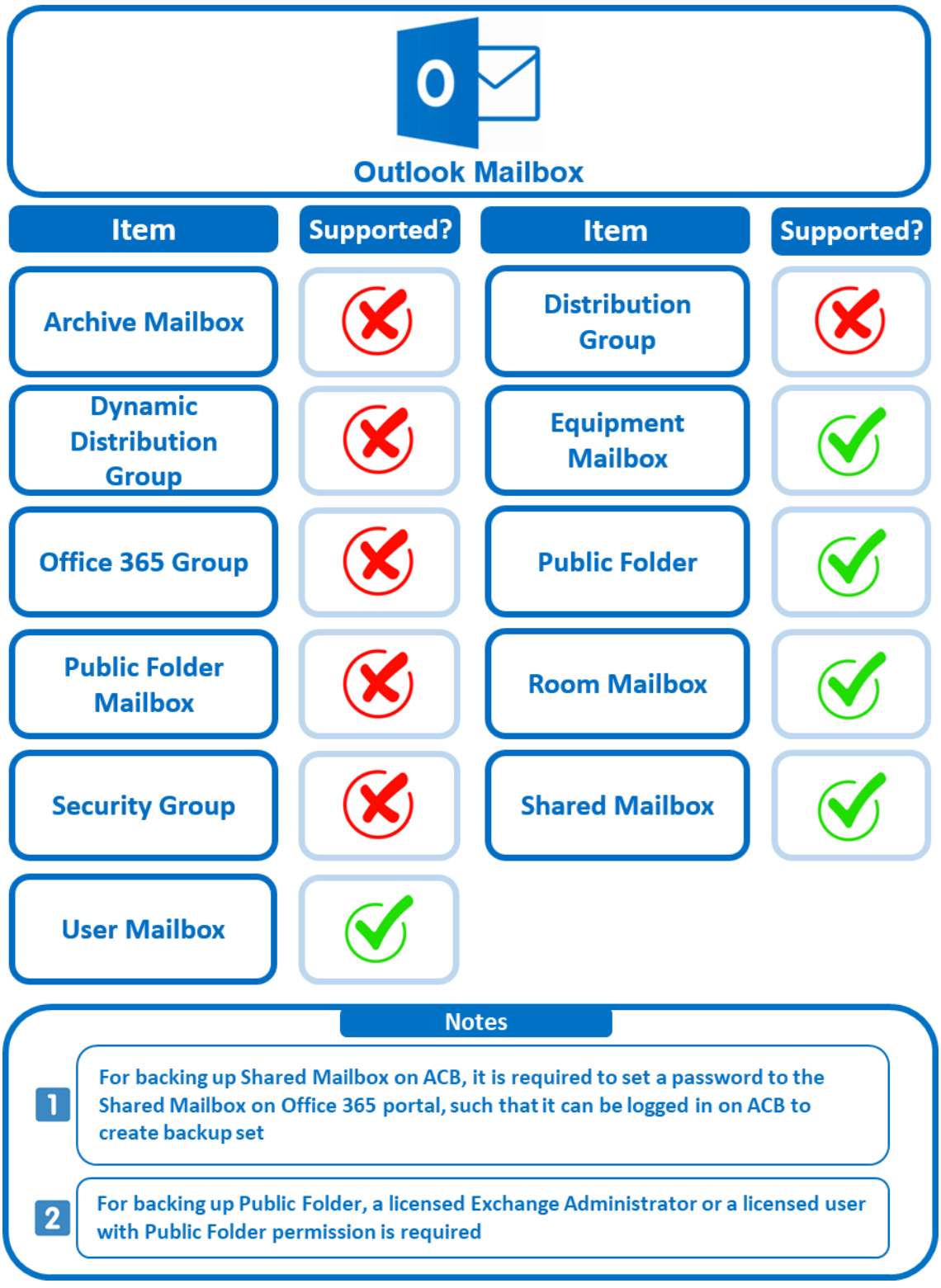


2.13 Supported Services

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



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



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

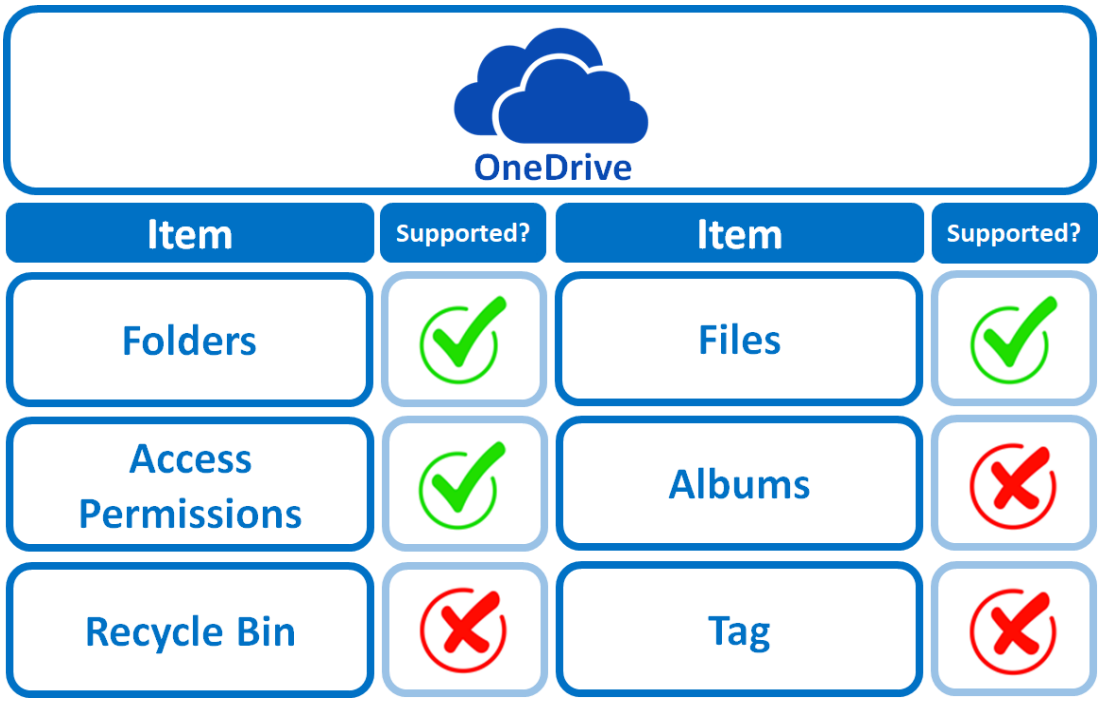
Folder Level

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	✓

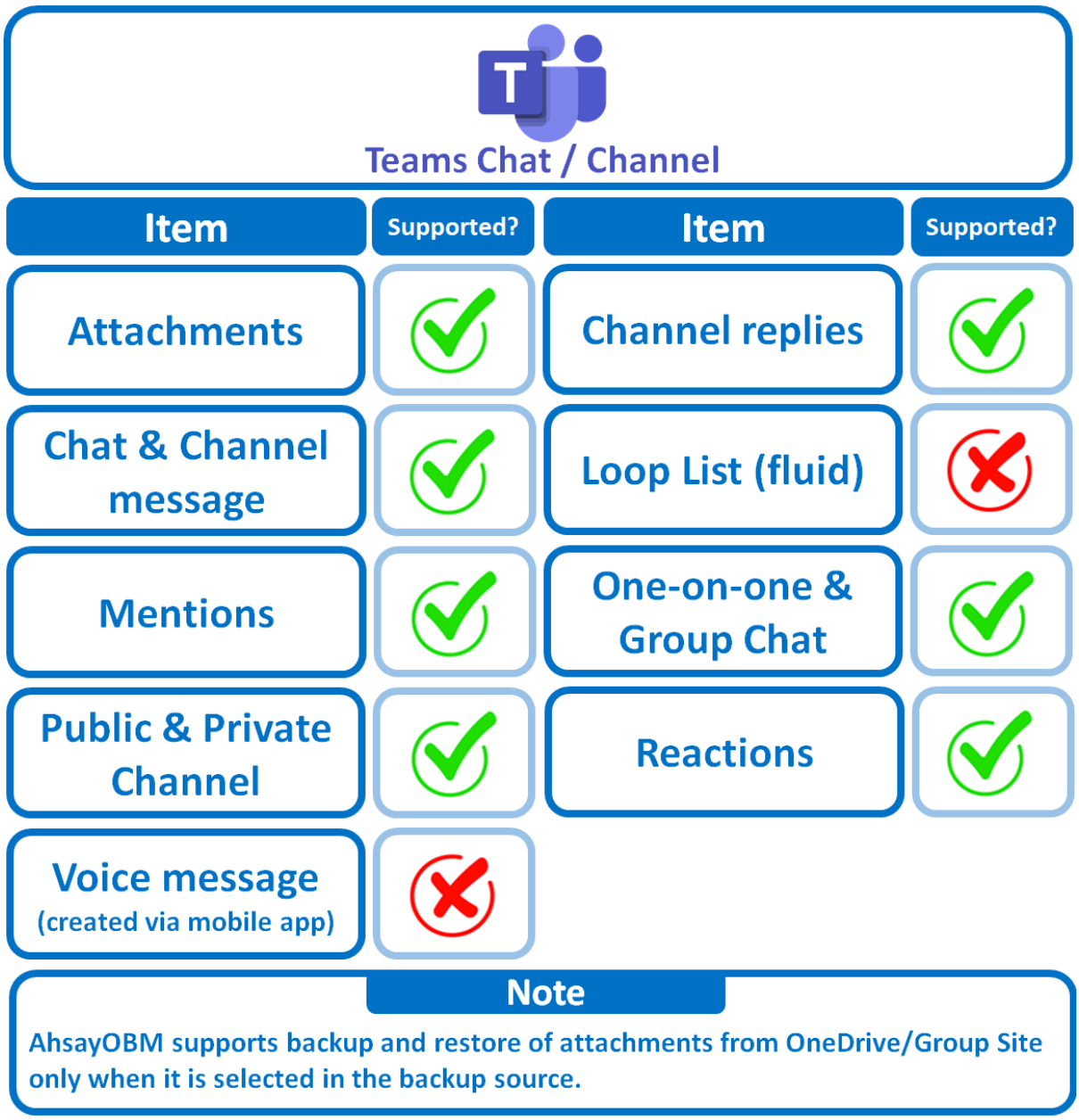
Note

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.



Below are the items that you can backup or restore from Teams Chat / Channel.



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

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	✗	Manage Site Features	✗
Newsfeed	✗	Permissions and Management	✓ [2]
Picture and Libraries	✓	Report Libraries	✓
Site Collection Features	✗	Site Page	✓
Survey	✓	Version History	✓ [2]
Wiki / Page Libraries	✓		

Notes

1. For the General Settings, only the List Name can be restored.
2. 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 a Microsoft 365 backup set.

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

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

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

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

2.14 Maximum Supported File Size

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

2.14.1 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

2.14.2 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

2.15 Limitations

2.15.1 AhsayOBM

Ahsay Limitations

- **Modern Authentication**
  - Modern Authentication is only supported for Microsoft 365 account that is registered in Global region and the Microsoft 365 backup is configured to use Global region.
  - Migration to Modern Authentication is not supported on a Microsoft 365 account without a Global Admin role; or during the migration process, the Microsoft 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 during 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 Microsoft 365 organization.
- Backup and restore of all versions will be supported for **OneDrive and SharePoint Documents** only, except for ".aspx" files.

- **Teams**
  - Backup of external chat/message, attachment to system message backup (e.g. meeting recording) and backup tabs, pins for chat/channel are not supported.
  - Restore of chat/channel to original thread is not supported. Restore only as data export in HTML format, stored to local or OneDrive.
  - Refer to the table below for the limitations regarding Teams Chat backup.

	Teams Chat only without OneDrive	**Teams Chat with OneDrive**
Entire Organization	Only the chat room that include the selected users and messages sent by the selected users will be backed up. If the messages contain attachments (Files), the Files will not be backed up since OneDrive was not selected.	Only the chat room that include the selected users and messages sent by the selected users will be backed up. If the messages contain attachments (Files), only the Files of the selected users will be backed up. It will not include the Files shared by other users that were not selected for backup. This is a limitation with the Microsoft API, as the shared file is located in the other users' OneDrive, which was not selected for backup. To backup Teams Chat to include Files from all users in the chat, then all users who participated in the chat will also need to be selected for backup.
This Microsoft 365 user only	Chat rooms of the login user will be backed up, including messages from other users and from the login user. If the messages contain attachments (Files), the Files will not be backed up since they are located in OneDrive which was not selected.	Chat rooms of the login user will be backed up, including messages from other users and from the login user. If the messages contain attachments (Files), only the Files of the login user will be backed up, it will not include the files shared by other users since the other users were not selected for backup.

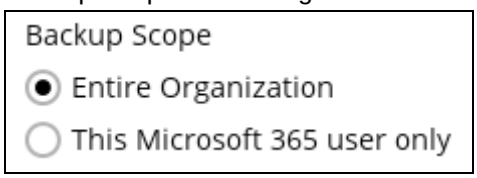
Here are some sample scenarios:

Example No. 1

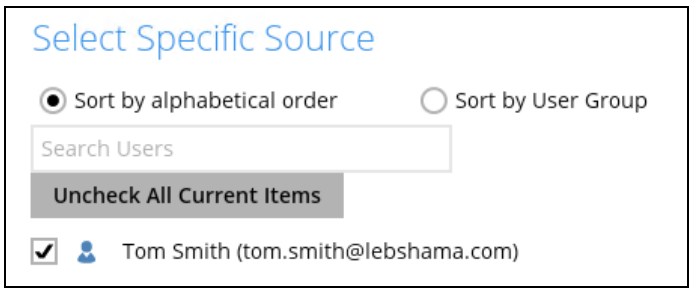
You are required to backup Microsoft 365 user: Tom

Selection:

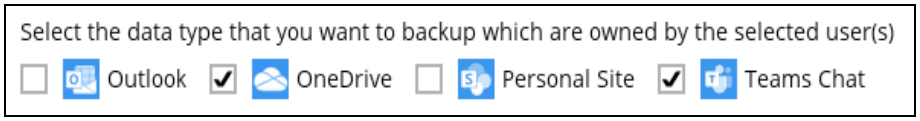
- Backup Scope: Entire Organization



- Microsoft 365 user: Tom



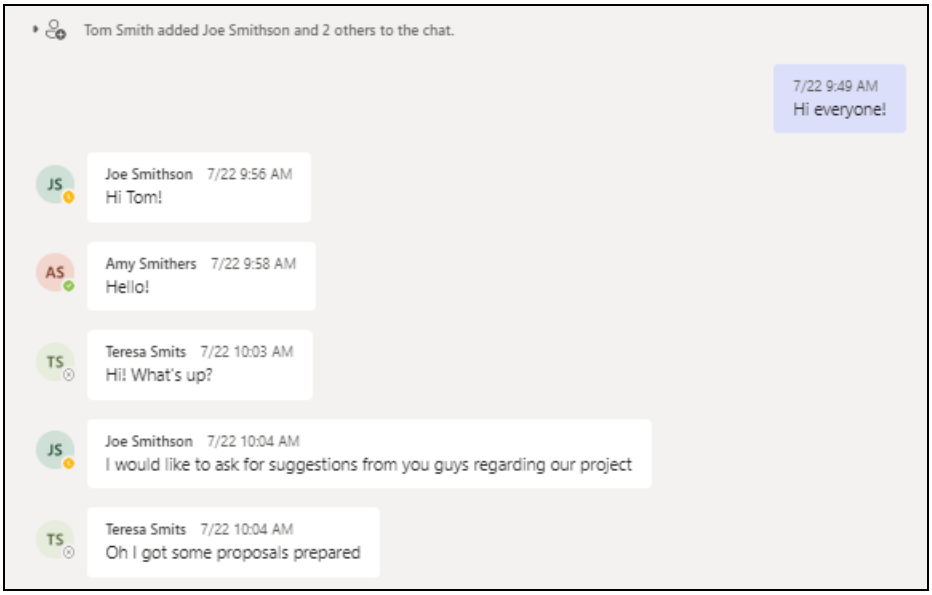
- Data type: Teams Chat (assuming no Outlook or Personal Site data) and OneDrive

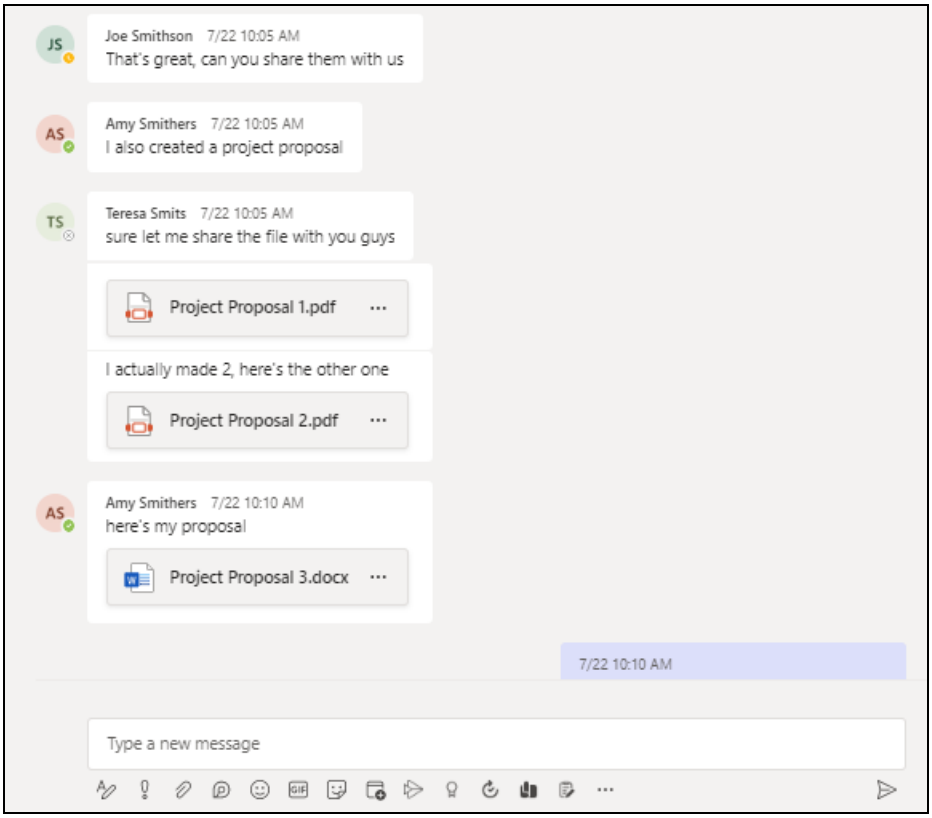


Scenario:

Tom is in a group Teams Chat which includes Amy, Joe and Teresa.

They chat about their project within the group, share files, etc.

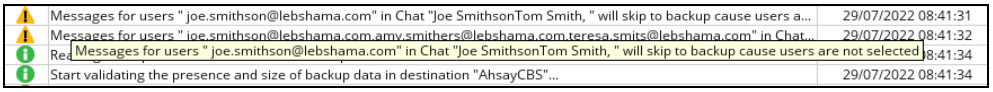




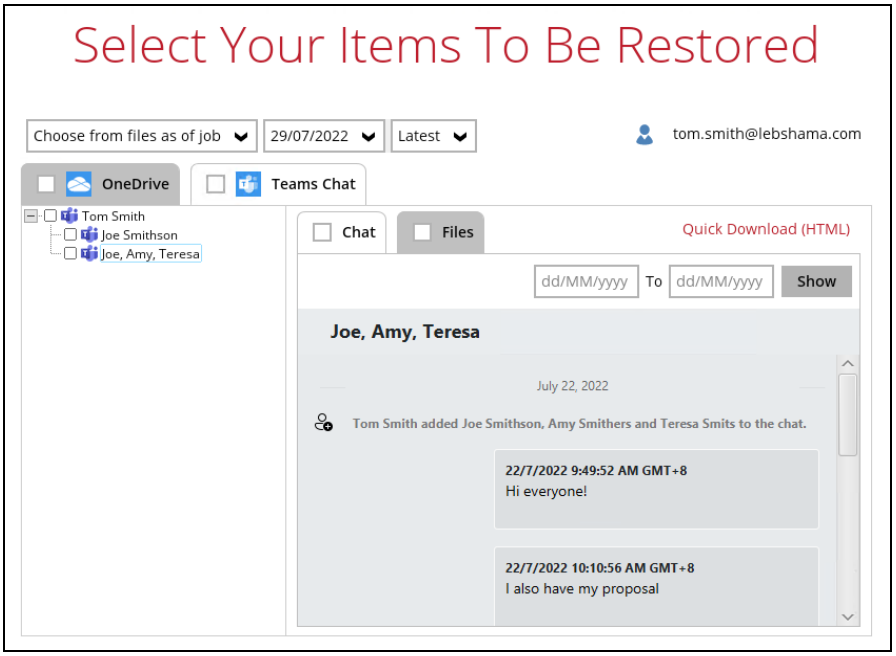
If you create a Backup Set and select only Tom; it will include only messages sent by Tom for the 1:1 group chat where Tom is included.

It will only include files that Tom had attached. It will not backup file attachments from the other three participants.

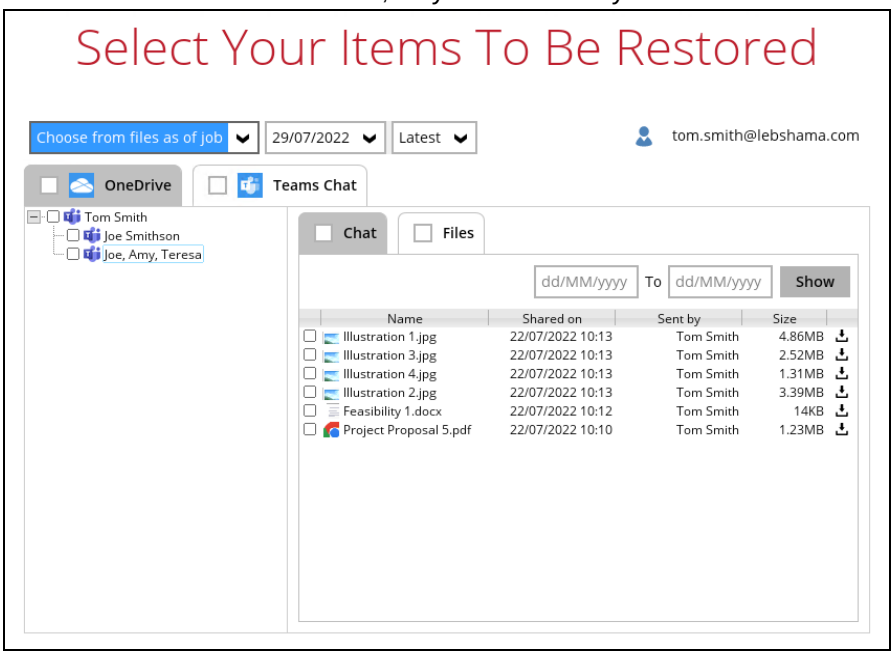
There will be Warnings after backup that items were not backed up when not all the users involved in the conversation are selected for backup. This is a sample of the warning that can be viewed from the backup report "*Messages from users joe.smithson@lebshama.com in Chat "Joe SmithsonTom Smith," will skip to backup cause users are not selected*".



When you Restore from this Backup Set to choose this group Teams Chat you will only see messages from Tom. Check the screenshot of the actual conversation above, as you can see the messages from the other users were not backed up.



You will only be able to download and/or restore files shared by Tom. This means you will need to include the other users in your Backup Set Source selection if you want to be able to download and/or restore the files they shared. In the screenshot below, only files shared by Tom will be listed.

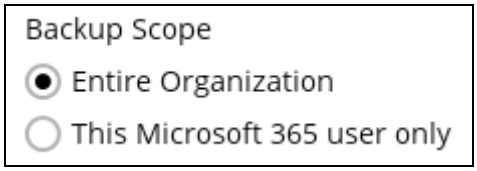


Example No. 2

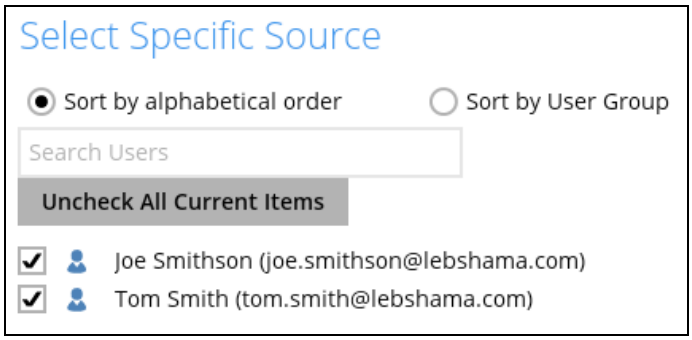
You are required to backup Microsoft 365 user: Joe.

Selection:

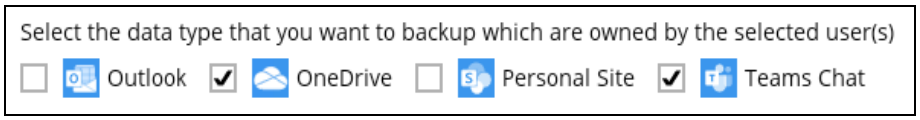
- Backup Scope: Entire Organization



- Microsoft 365 user: Joe and Tom

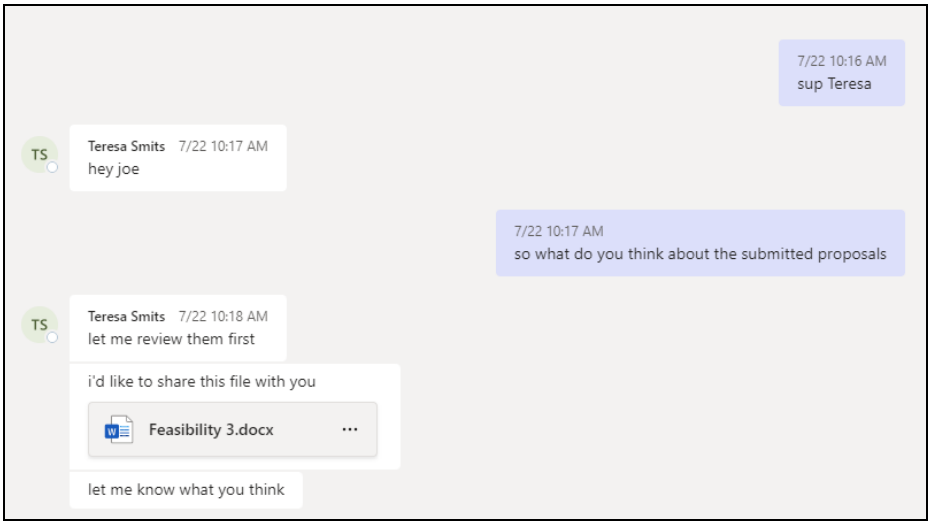


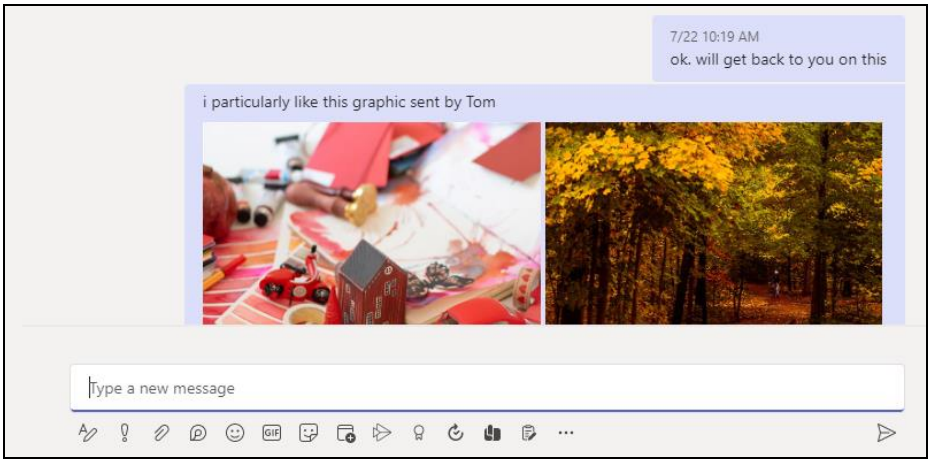
- Data type: Teams Chat (assuming no Outlook or Personal Site data) and OneDrive



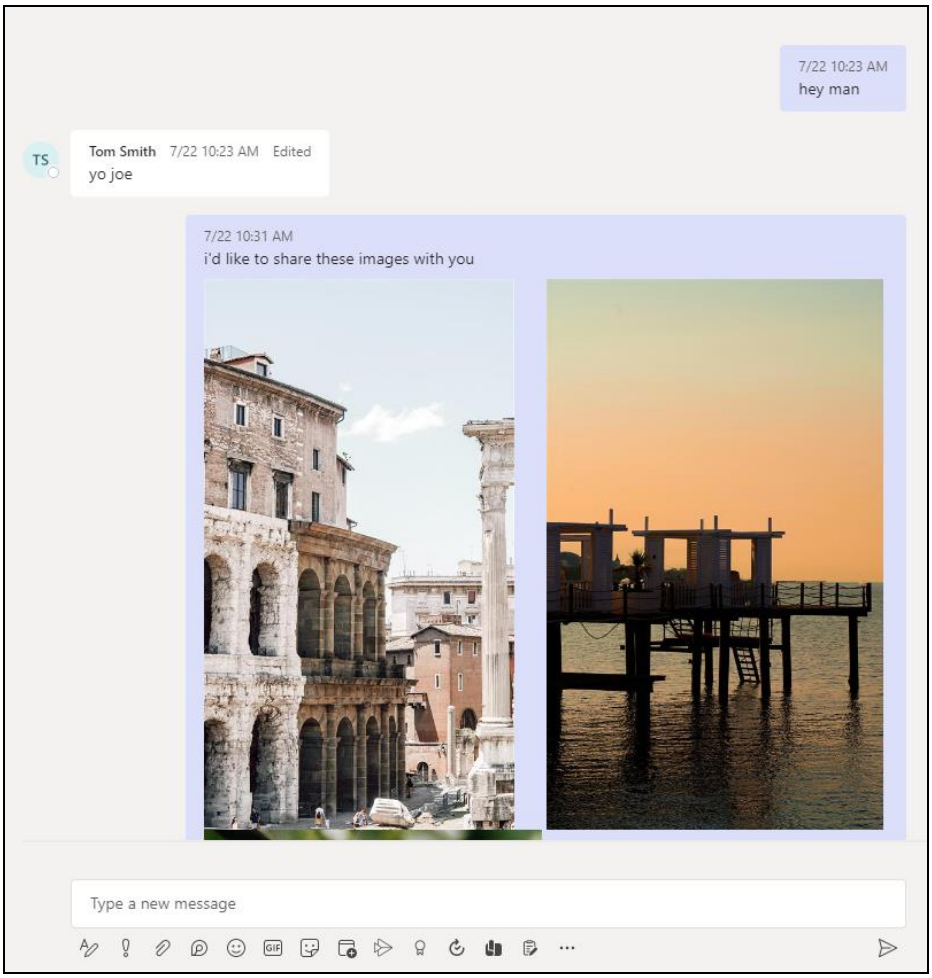
Scenario:

Joe has 1:1 chat with Teresa, and they shared files with each other.



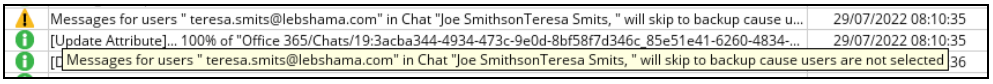


Joe has 1:1 chat with Tom, and they shared files with each other.



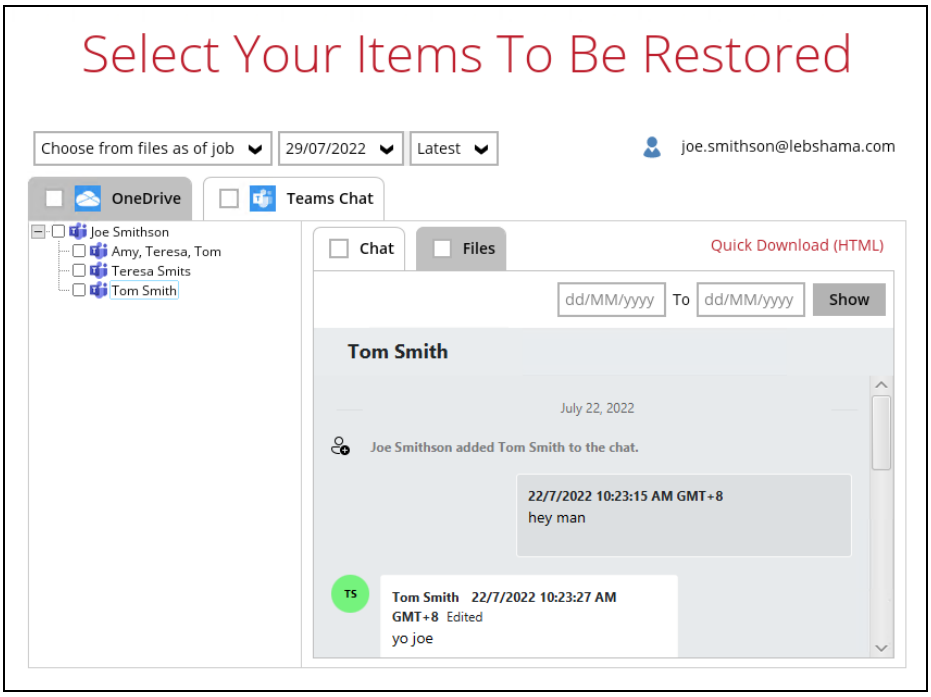
If you create a Backup Set and select only Joe and Tom, it will include Joe's chat message with Tom, and files shared by Joe and Tom. It will not include Teresa's chat message and file attachments.

There will be Warnings after backup that items were not backed up when not all the users involved in the conversation are selected for backup. This is a sample of the warning that can be viewed from the backup report "*Messages from users teresa.smits@lebshama.com in Chat "Joe SmithsonTeresa Smits," will skip to backup cause users are not selected*".

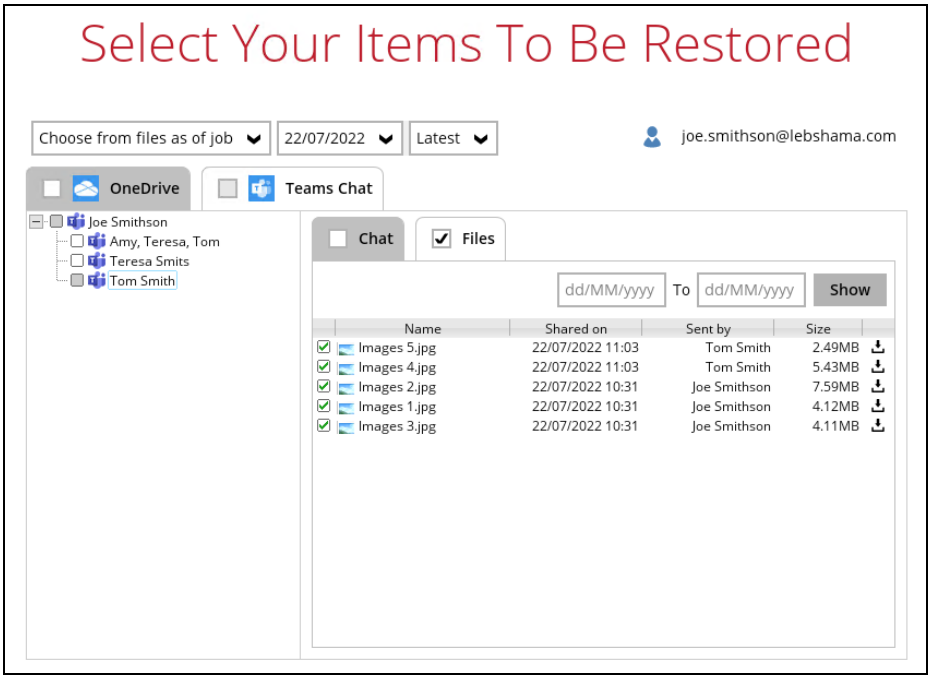


When you Restore from this Backup Set to choose from Joe's list of chats, you can open the conversation between Joe and Tom, you can also restore any files they shared with each other.

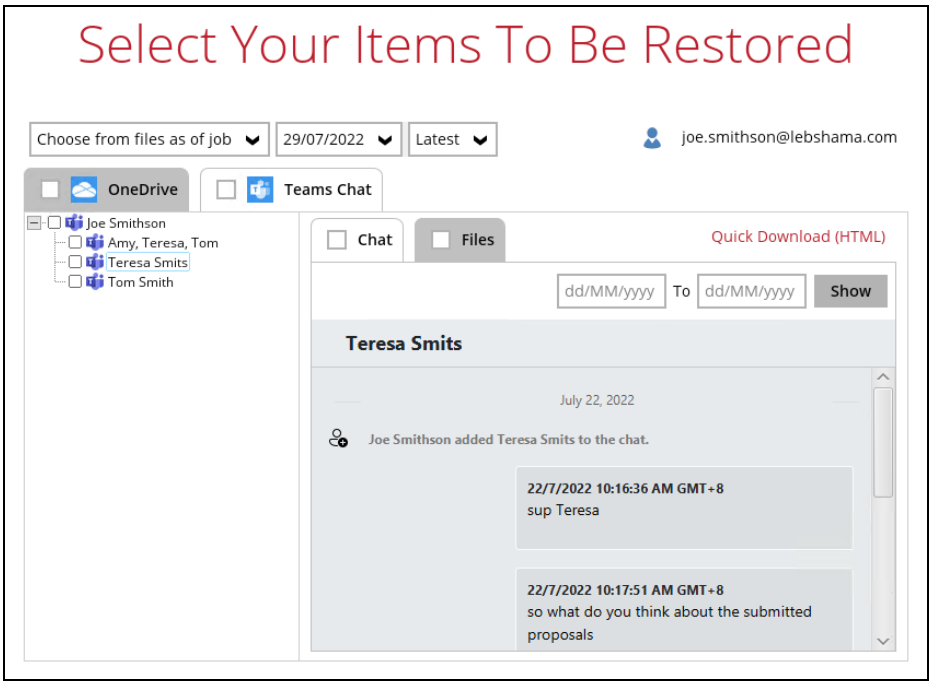
The chat displays messages from Joe and Tom.



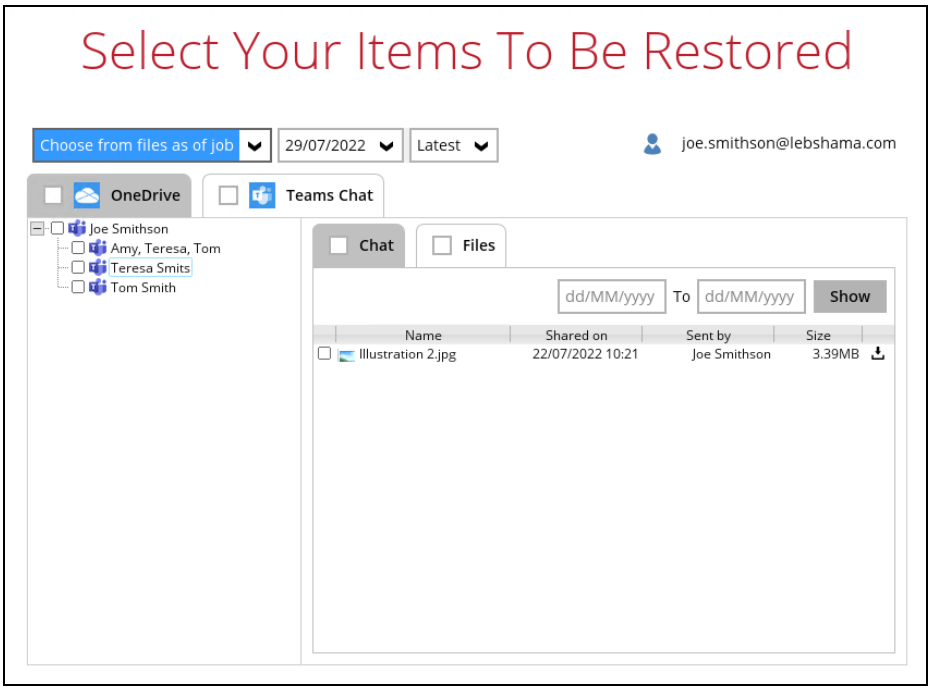
Files shared between them can also be downloaded and/or restored.



But when you click on the conversation with Teresa, you will see the chat messages from Joe only. Please refer to the screenshot of the actual chat above.



Only the file that Joe shared with Teresa will be available for download and/or restore. Files that were shared by Teresa will not be available since she was not selected in the Backup Source Selection.

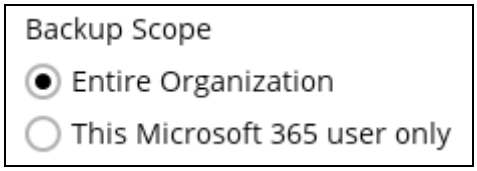


Example No. 3

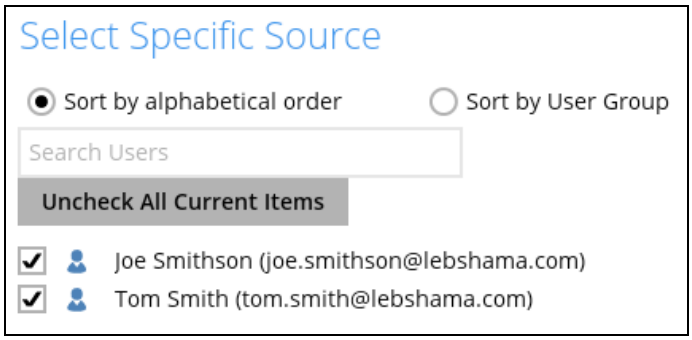
You are required to backup Microsoft 365 user: Joe.

Selection:

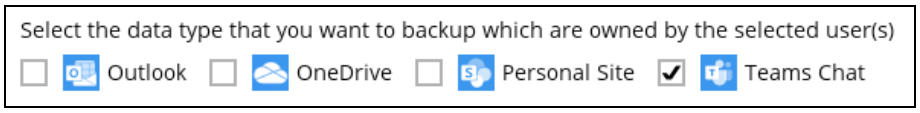
- Backup Scope: Entire Organization



- Microsoft 365 user: Joe and Tom

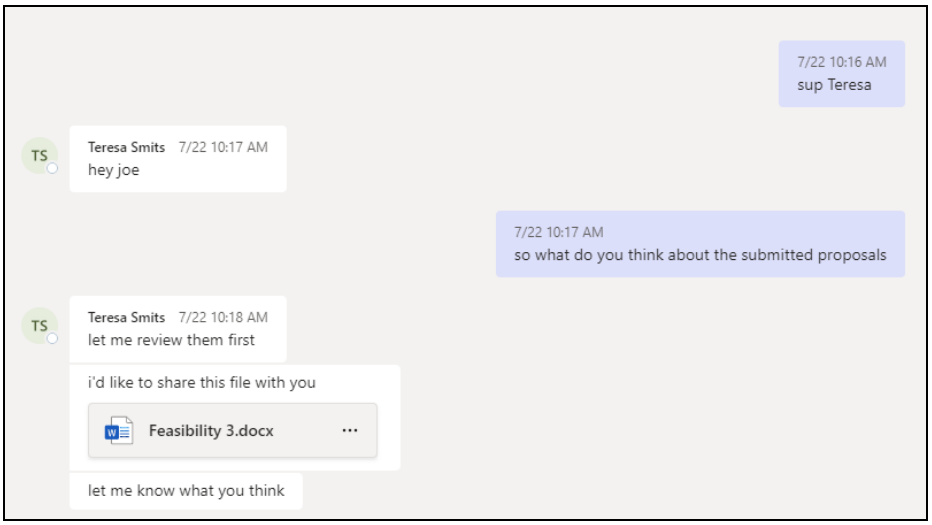


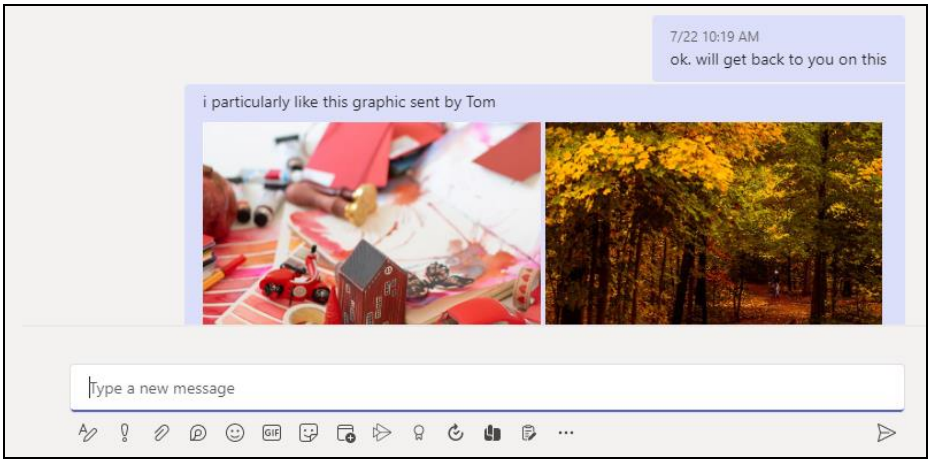
- Data type: Teams Chat



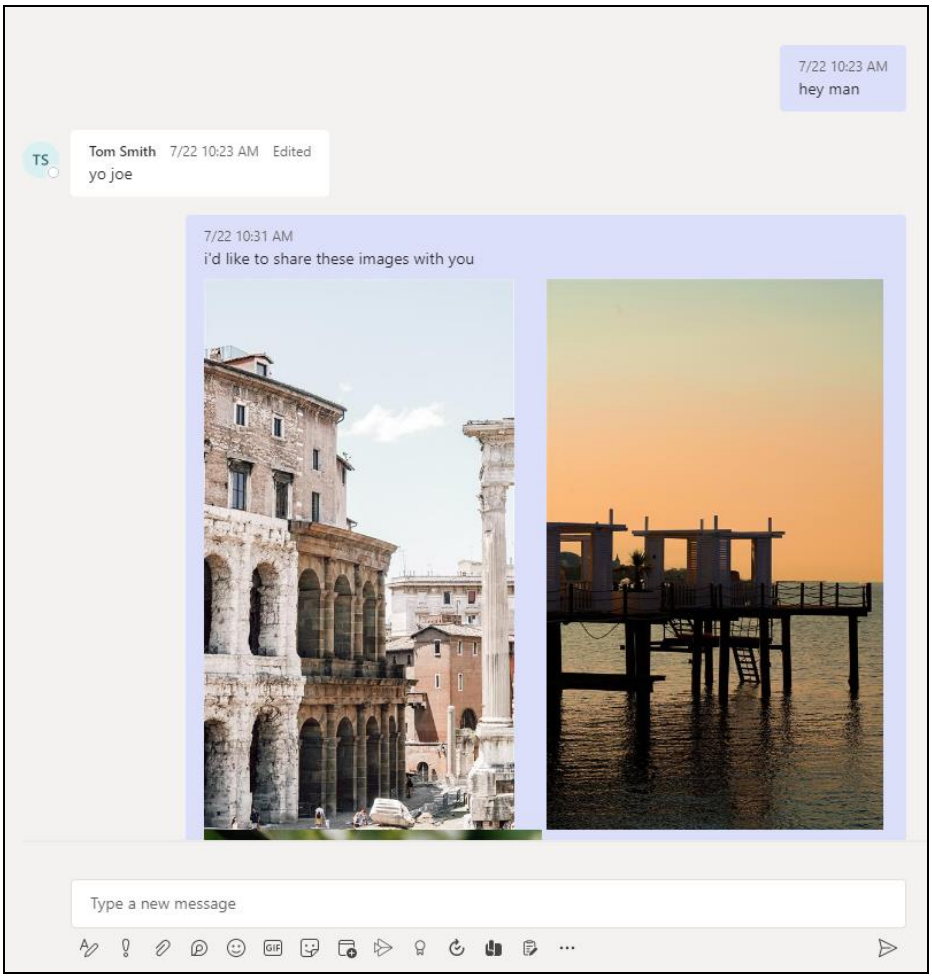
Scenario:

Joe has 1:1 chat with Teresa, and they shared files with each other.



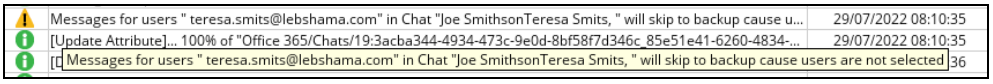


Joe has 1:1 chat with Tom, and they shared files with each other.

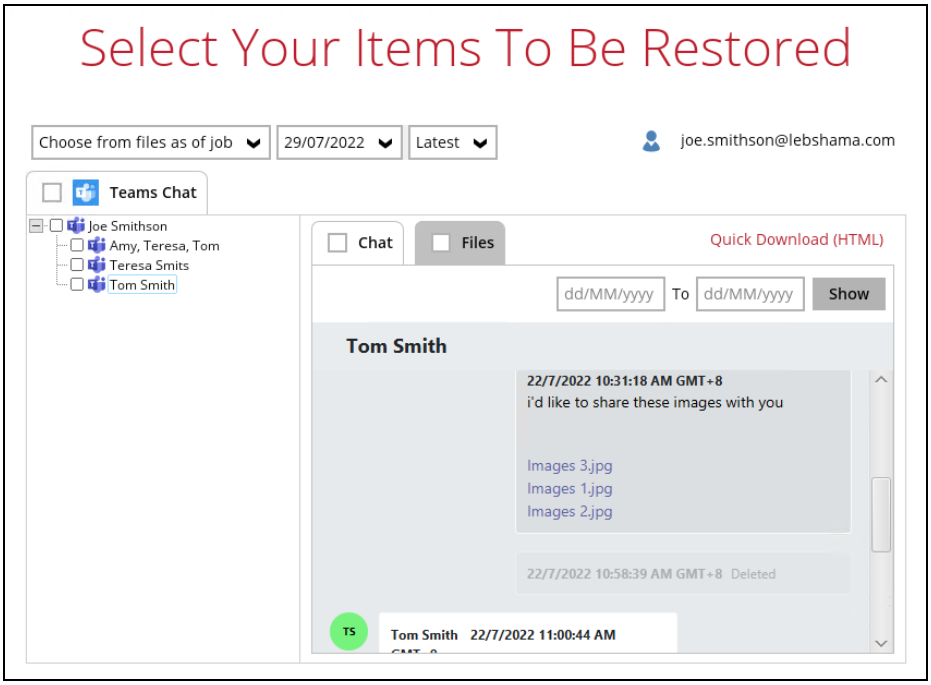


If you create a Backup Set, and select only Joe and Tom, it will include Joe's chat message with Tom. It will not include Teresa's messages as Teresa is not selected. It will also not include any files attached as OneDrive is not selected.

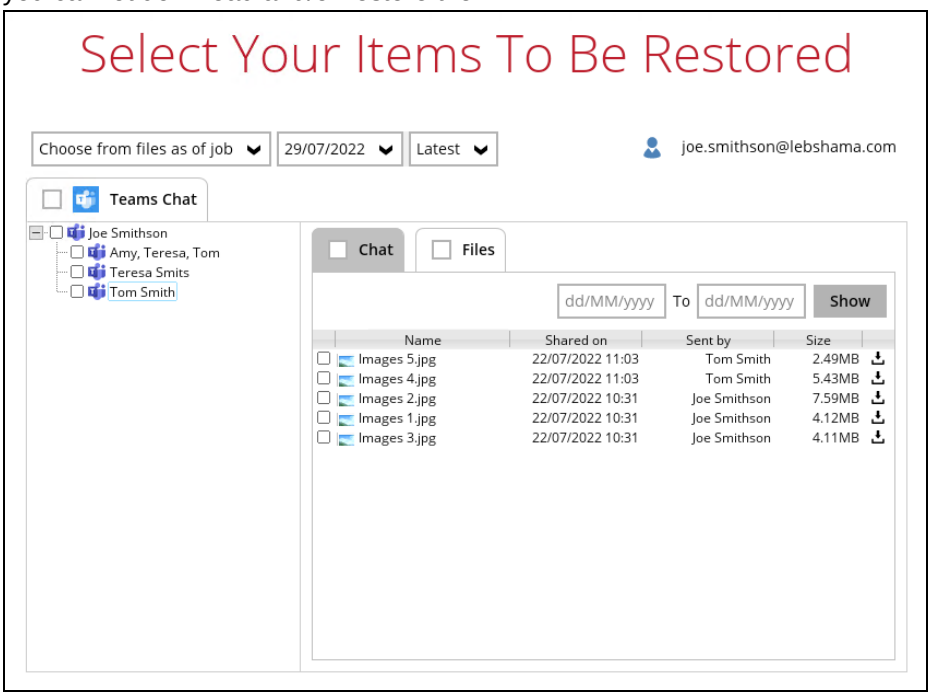
There will be Warnings after backup that items were not backed up when not all the users involved in the conversation are selected for backup. This is a sample of the warning that can be viewed from the backup report "*Messages from users teresa.smits@lebshama.com in Chat "Joe SmithsonTeresa Smits," will skip to backup cause users are not selected*".



When you Restore from this Backup Set to choose from Joe's list of chats, and open the conversation between Joe and Tom, you can only restore messages.

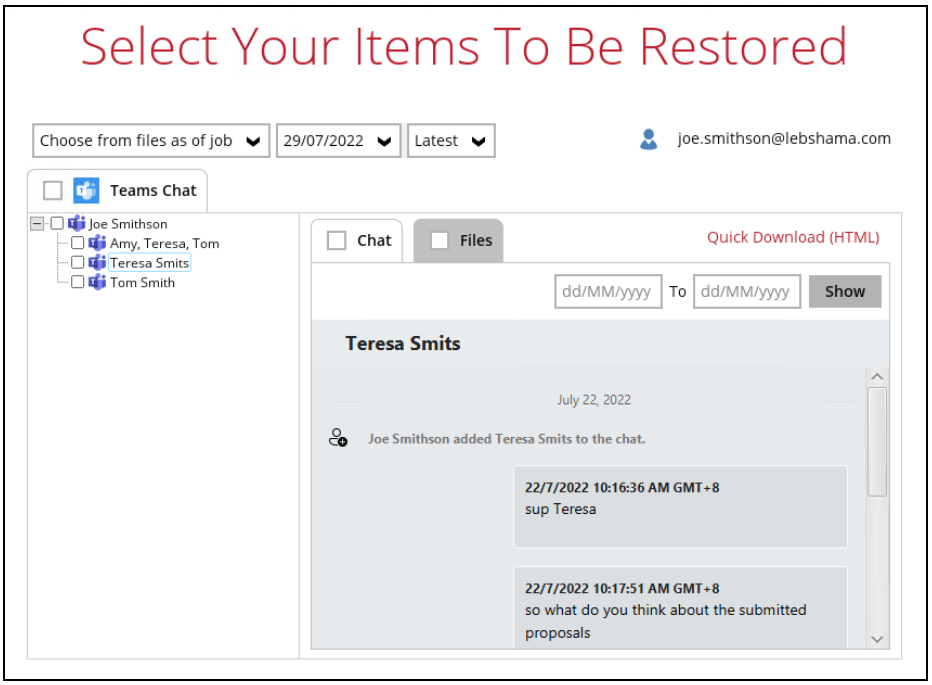


Files that they shared with each other will be listed under the Files tab, but you cannot download and/or restore them.

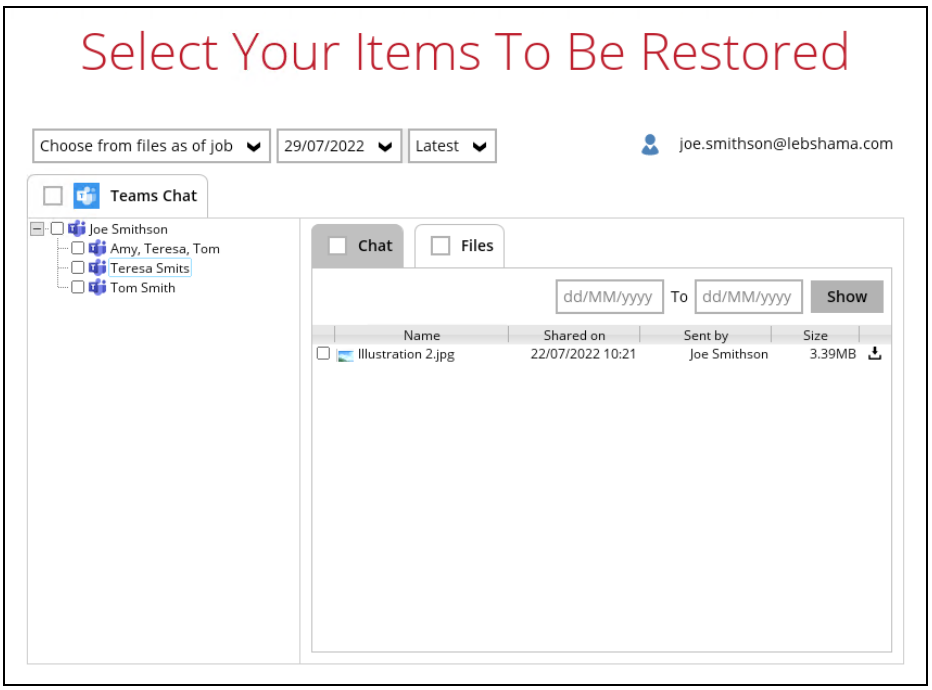


And when you click on the download button, this error message will appear because OneDrive is not a selected Data Type, which means the shared file was not backed up since file attachments are saved in OneDrive.

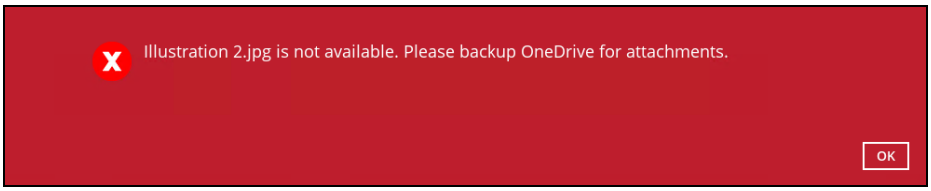
But when you click on the conversation with Teresa, you will see the chat messages from Joe only since Teresa is not selected as a backup source.



Only files shared by Joe will be listed under the Files tab, but it will not be available for download and/or restore.



This error message will be displayed when you click on the download button since OneDrive is not a selected Data Type.

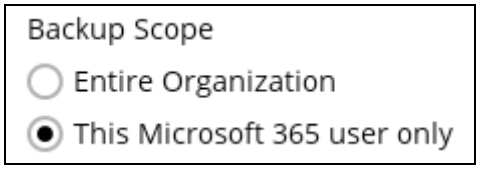


Example No. 4

You are required to backup Microsoft 365 user: Teresa.

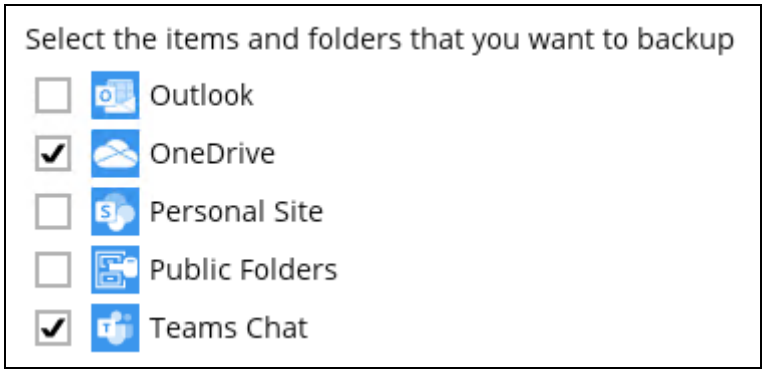
Selection:

- Backup Scope: This Microsoft 365 user only



- Microsoft 365 user: Teresa

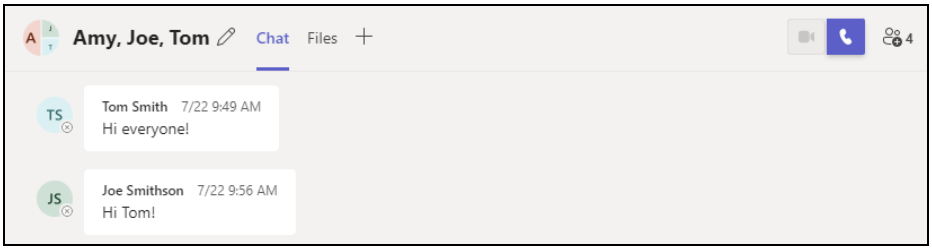
- Data type: Teams Chat (assuming no Outlook or Personal Site) and OneDrive

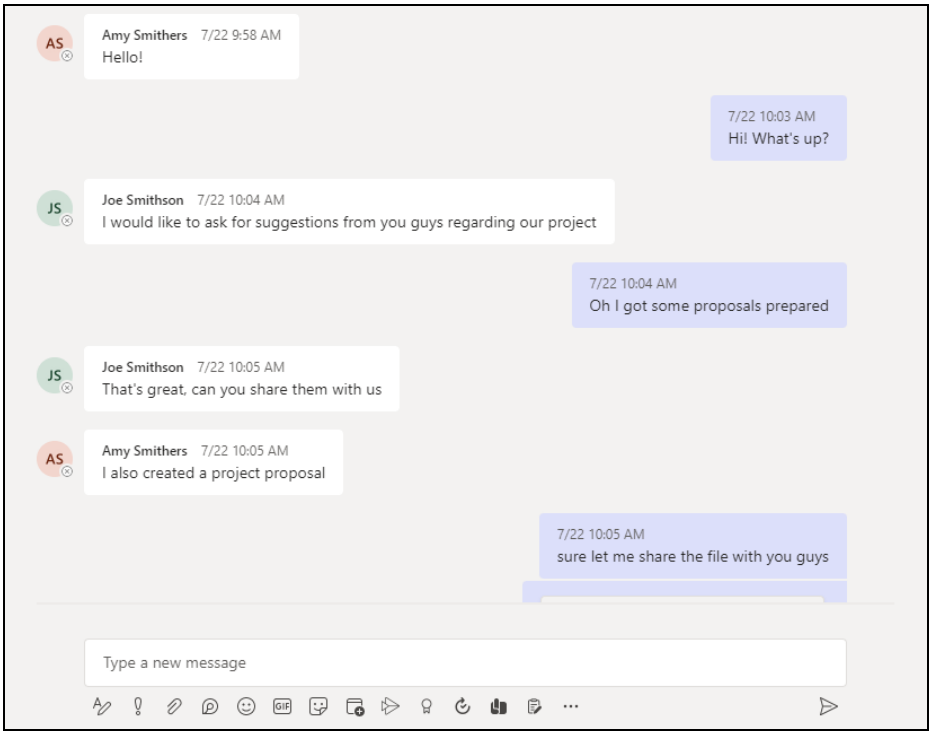


Scenario:

Teresa is in a group Teams Chat which includes Amy, Joe and Tom.

They chat about their project within the group, share files, etc.

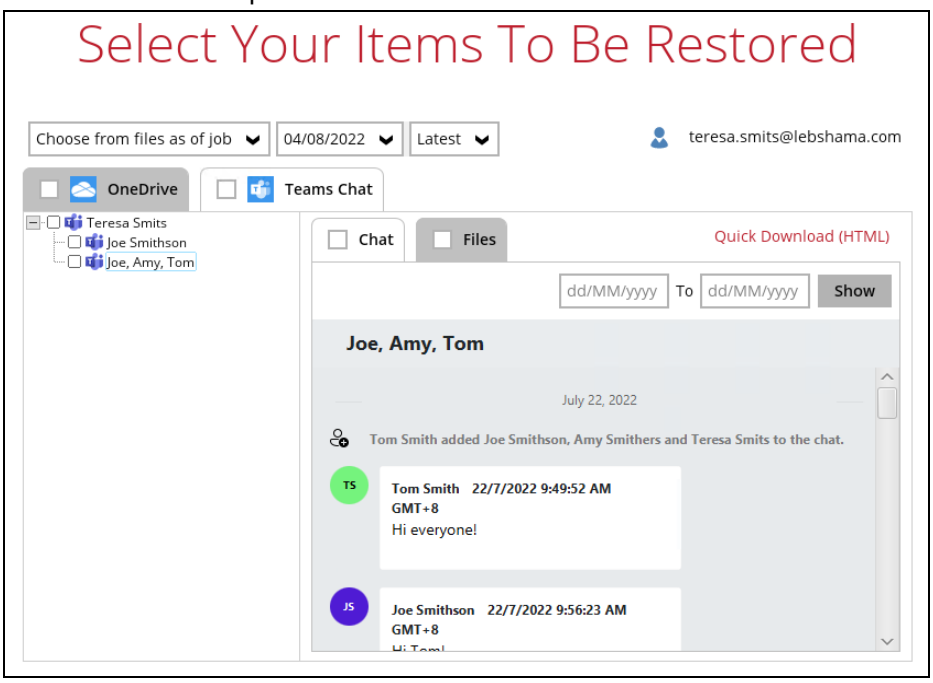




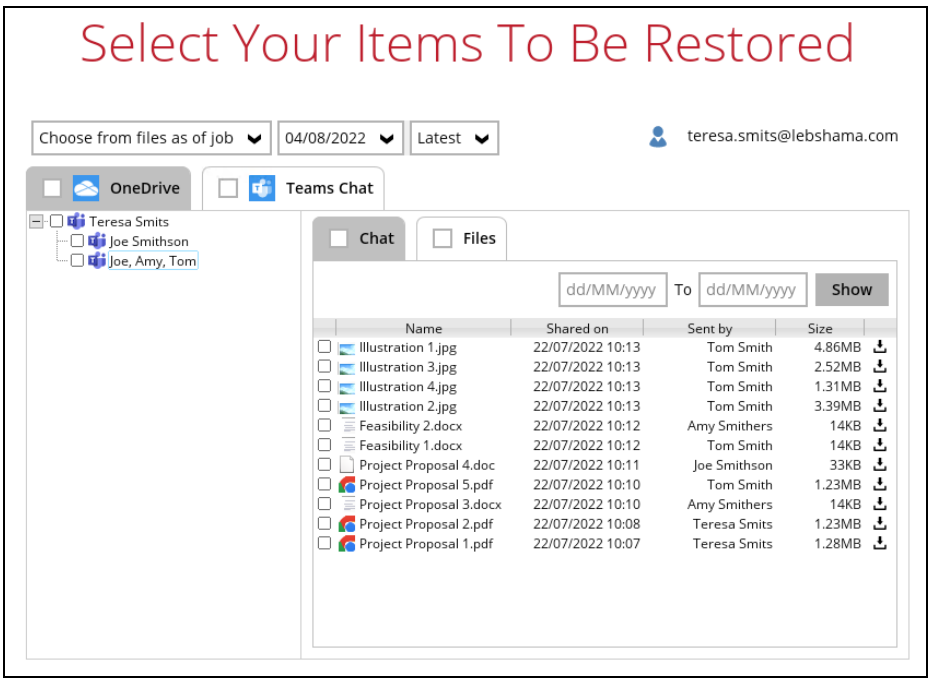
If you create a Backup Set, it will include all messages sent by Teresa as well as messages from the other users for the 1:1 group chat where Teresa is included.

It will only include files that Teresa had attached. It will not backup file attachments from the other three participants.

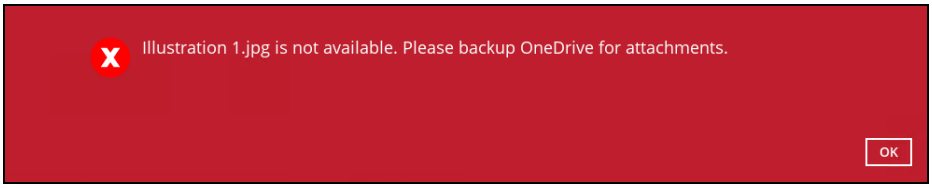
When you Restore from this Backup Set to choose this group Teams Chat you will see all the messages in the chat. Please refer to the screenshot of the actual conversation above, as you can see all the messages from all the users were backed up.



You will only be able to download and/or restore files shared by Teresa. In the screenshot below, all the files shared in the chat will be listed.



But you will not be able to download and/or restore the files shared by the other users. When you click on the download button, the message below will be displayed.

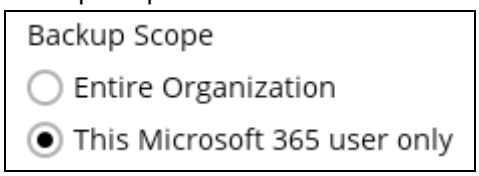


Example No. 5

You are required to backup Microsoft 365 user: Joe.

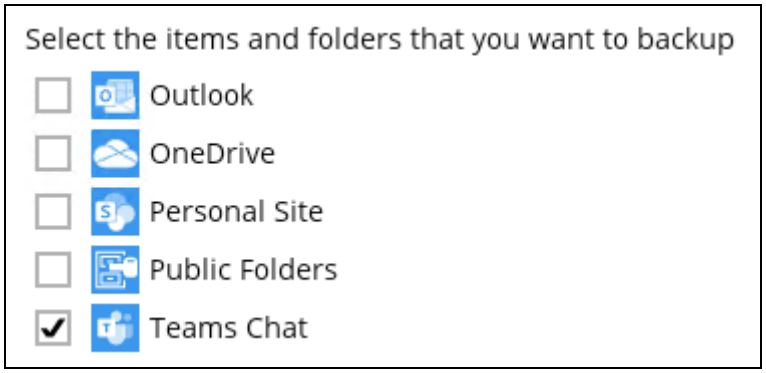
Selection:

- Backup Scope: This Microsoft 365 user only



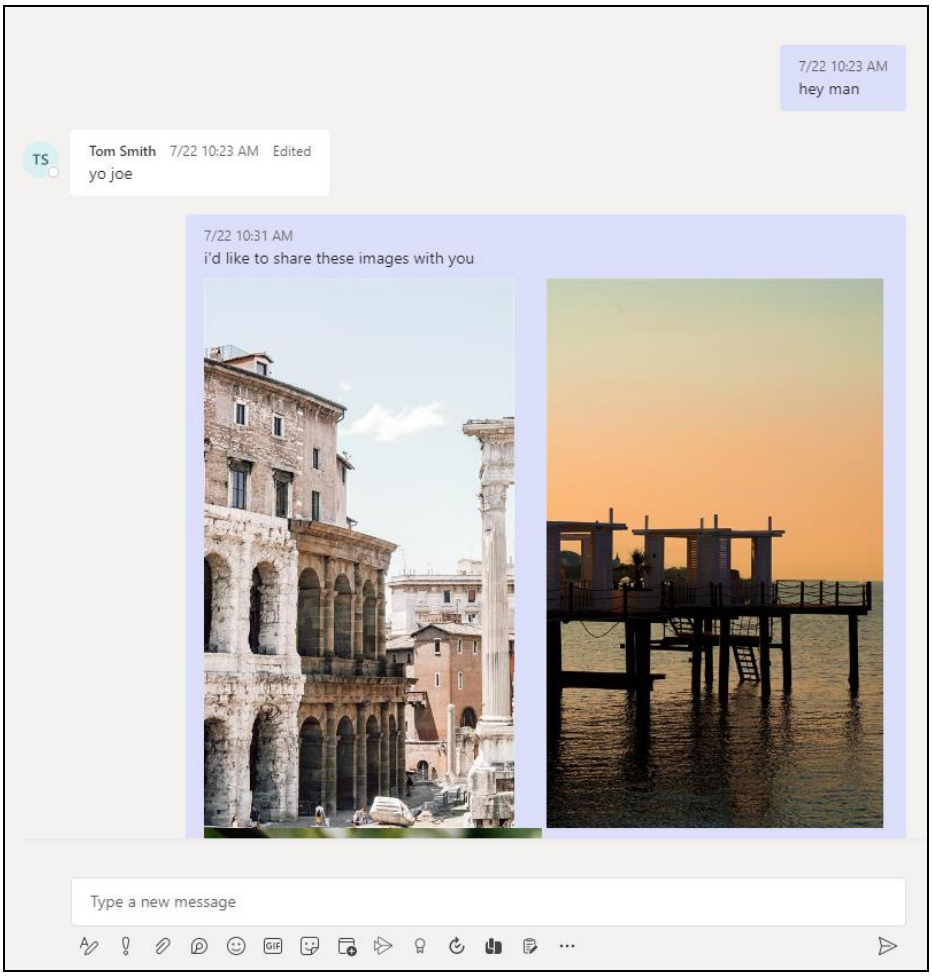
- Microsoft 365 user: Joe

- Data type: Teams Chat



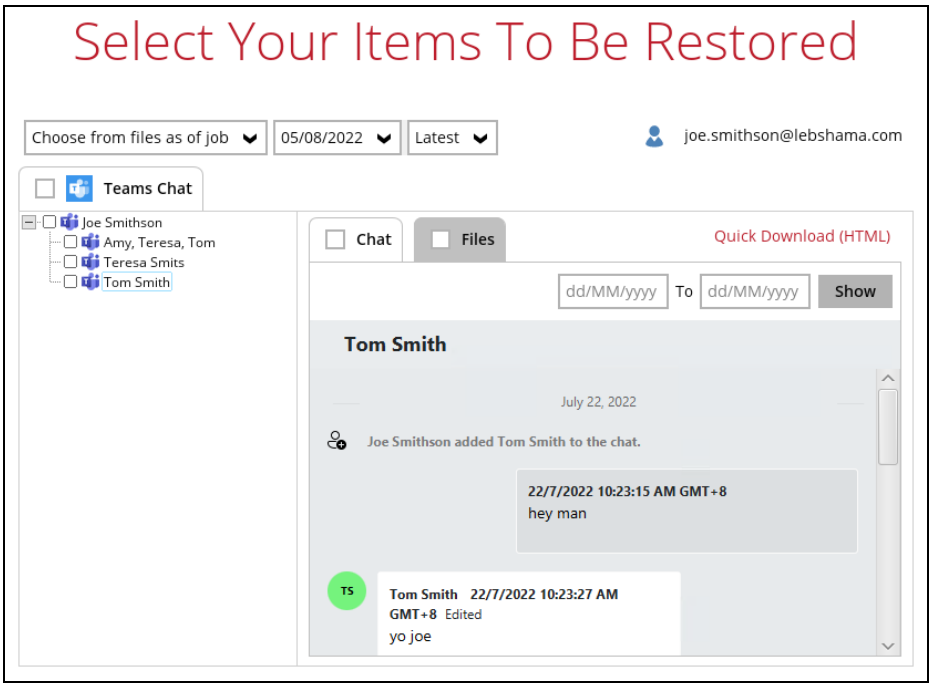
Scenario:

Joe has a 1:1 chat with Tom, and they shared files with each other.

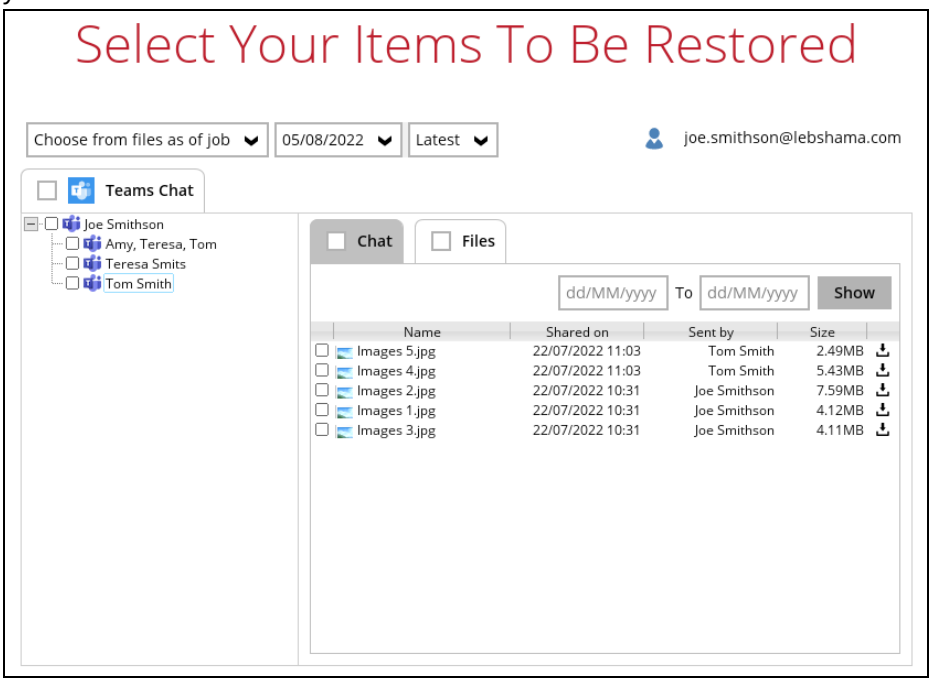


If you create a Backup Set, it will include Joe's chat message with Tom. But it will not include any files attached as OneDrive is not selected.

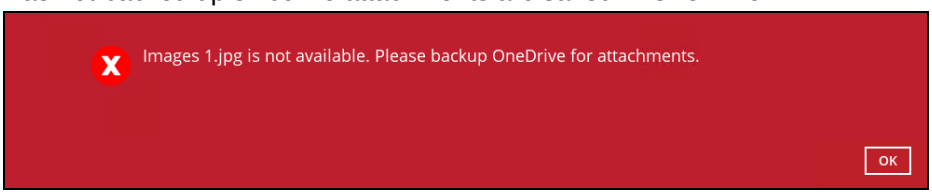
When you Restore from this Backup Set and open the conversation between Joe and Tom, you can only restore messages.



Files that they shared with each other will be listed under the Files tab, but you cannot download and/or restore them.



And when you click on the download button, this error message will appear because OneDrive is not a selected Data Type, which means the shared file was not backed up since file attachments are saved in OneDrive.



- **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 (the restored mail item is assigned a new mail ID), 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 new mail ID) created for that mail item

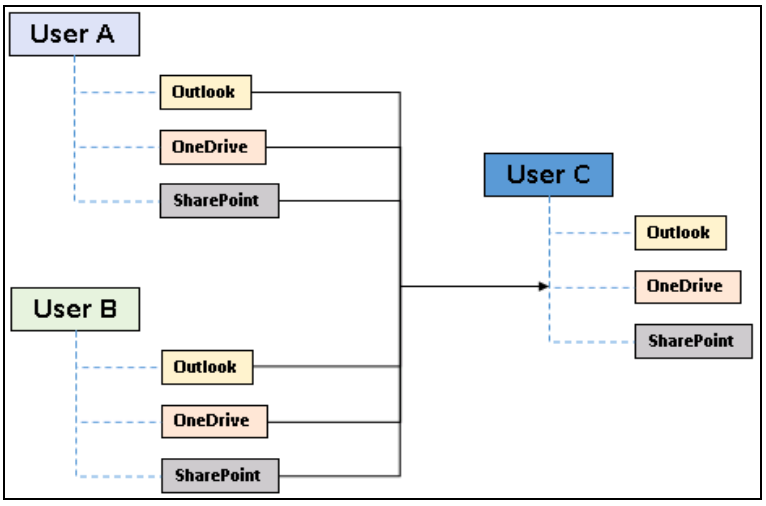
    To avoid future backup error/warning, the user will need to deselect the red item and tick the mail item again (new mail ID) in the backup source tree. This re-selection of backup source is not automatically done after you restore under *overwrite to original location* scenario.
- **Restore filter feature**

  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 Microsoft 365 account**
  - If you are trying to restore item(s) from multiple Microsoft 365 user account to an alternate Microsoft 365 user account, AhsayOBM can only restore one Microsoft 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.

2.15.2 AhsayACB

Ahsay Limitations

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

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

  Supported backup set configurations:

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

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

#	Backup Set	Microsoft 365 User Account
1	Sample Backup Set 01	user01@company-Microsoft365.com
2	Sample Backup Set 01	user01@company-Microsoft365.com
	Sample Backup Set 02	user02@company-Microsoft365.com

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

  Contact your backup service provider for more details and refer to AhsayOBM v9 User Guide - Microsoft 365 Backup & Restore for Windows.

- **Modern Authentication**

  - Modern Authentication is only supported for Microsoft 365 account that is registered in Global region and the Microsoft 365 backup is configured to use Global region.
  - Migration to Modern Authentication is not supported on a Microsoft 365 account without a Global Admin role; or during the migration process, the Microsoft 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 Microsoft 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 (the restored mail item is assigned a new mail ID), 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 new mail ID) created for that mail item.

    To avoid future backup error/warning, the user will need to deselect the red item and tick the mail item again (new mail ID) in the backup source tree. This re-selection of backup source is not automatically done after you restore under *overwrite to original location* scenario.
- **Teams**
  - Backup of external chat/message, attachment to system message backup (e.g. meeting recording) and backup tabs, pins for chat/channel are not supported.
  - Restore of chat/channel to original thread is not supported. Restore only as data export in HTML format, stored to local or OneDrive.
  - Backup and restore of channels is not supported. Also, OneDrive as a restore location is not supported, archive files can only be restored to the local machine.
  - Refer to the table below for the limitations regarding Teams Chat backup.

Teams Chat only without OneDrive	Teams Chat with OneDrive
Chat rooms of the login user will be backed up, including messages from other users and from the login user. If the messages contain attachments (Files), the Files will not be backed up since they are located in OneDrive which was not selected.	Chat rooms of the login user will be backed up, including messages from other users and from the login user. If the messages contain attachments (Files), only the Files of the login user will be backed up, it will not include the files shared by other users since the other users were not selected for backup.

Here are some sample scenarios:

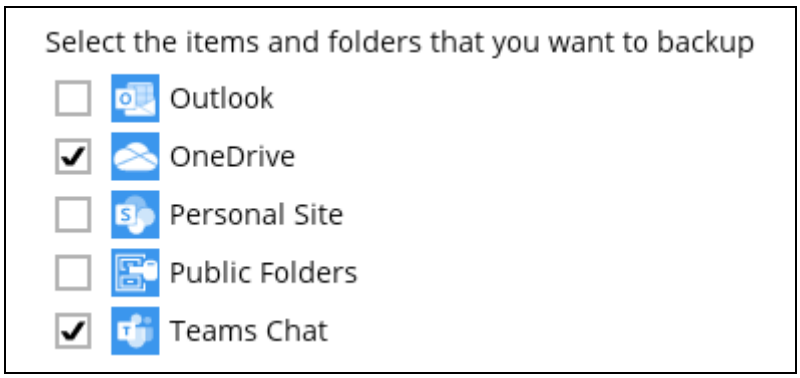
Example No. 1

You are required to backup Microsoft 365 user: Tom

Selection:

- Microsoft 365 user: Tom

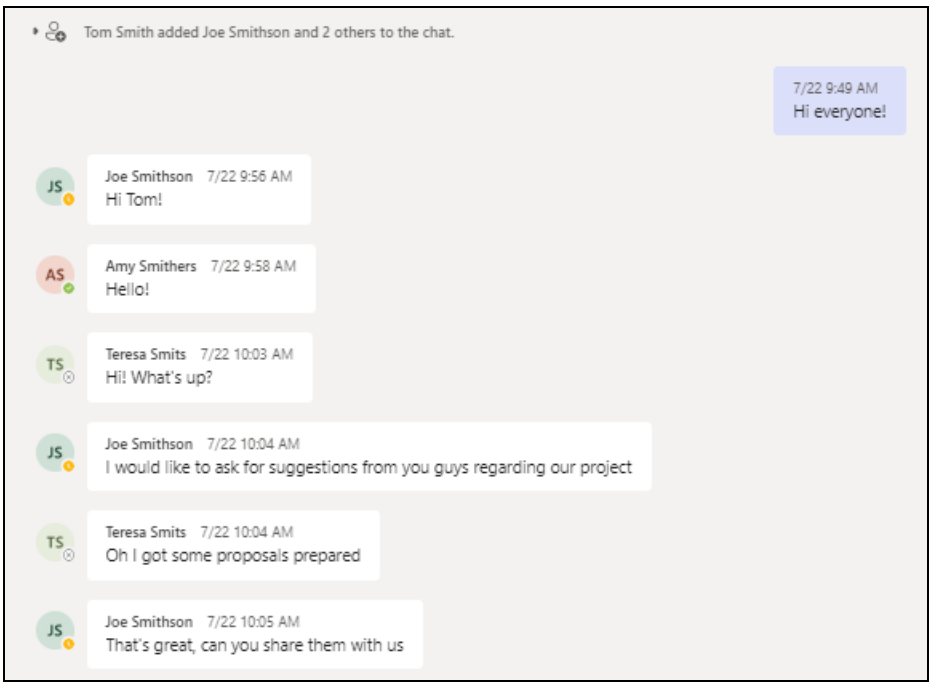
- Data type: Teams Chat (assuming no Outlook or Personal Site data) and OneDrive

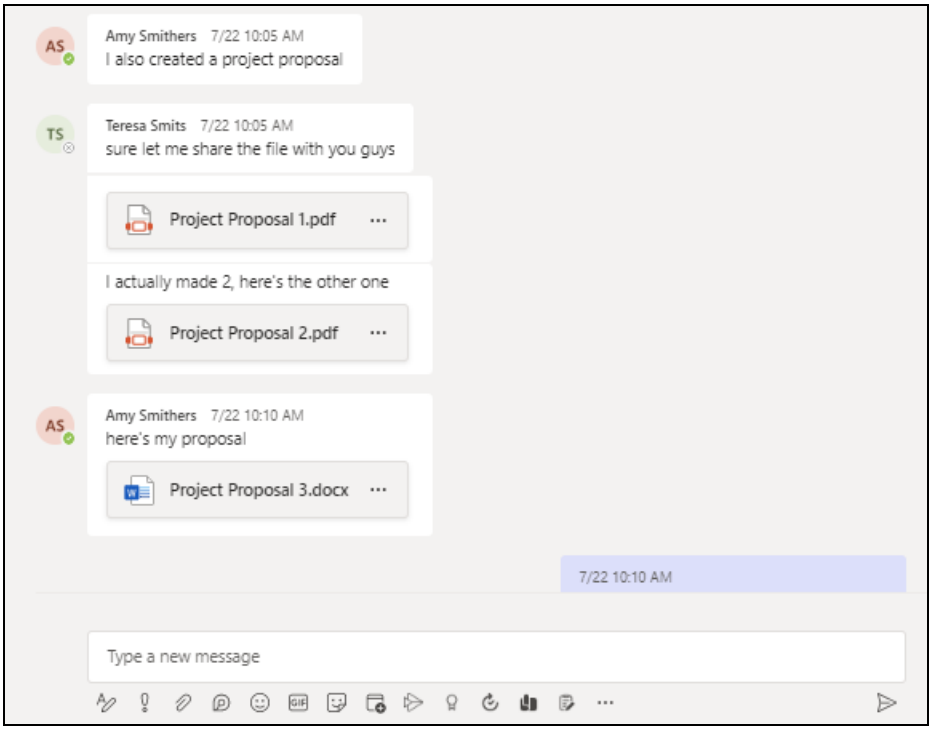


Scenario:

Tom is in a group Teams Chat which includes Amy, Joe and Teresa.

They chat about their project within the group, share files, etc.

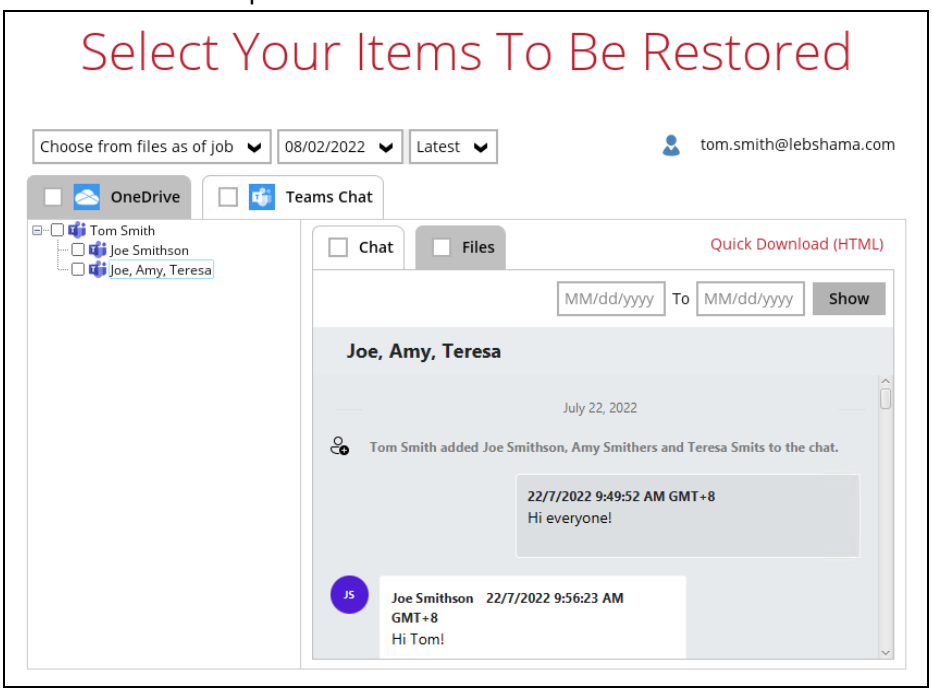




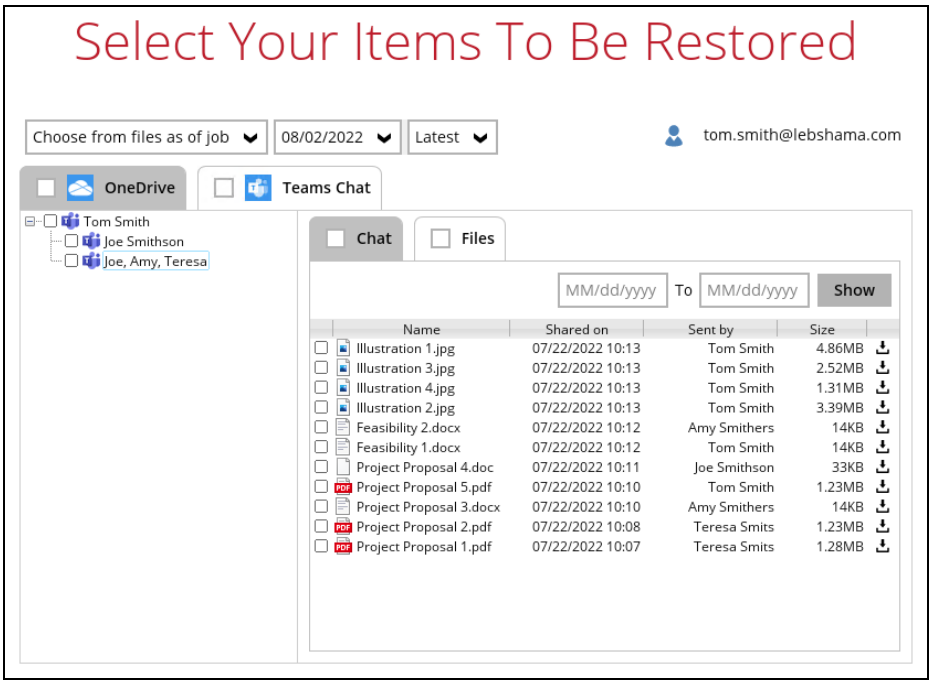
If you create a Backup Set, it will include all messages sent by Tom as well as messages from the other users for the 1:1 group chat where Tom is included.

It will only include files that Tom had attached. It will not backup file attachments from the other three participants.

When you Restore from this Backup Set to choose this group Teams Chat you will see all the messages in the chat. Please refer to the screenshot of the actual conversation above, as you can see all the messages from all the users were backed up.



You will only be able to download and/or restore files shared by Tom. In the screenshot below, all the files shared in the chat will be listed.



But you will not be able to download and/or restore the files shared by the other users. When you click on the download button, the message below will be displayed.

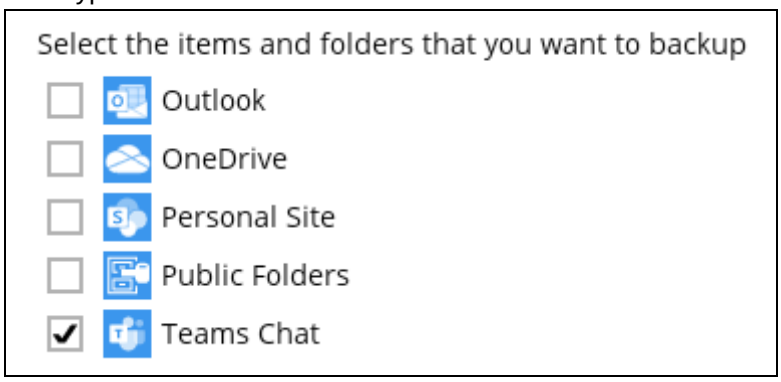
Example No. 2

You are required to backup Microsoft 365 user: Joe

Selection:

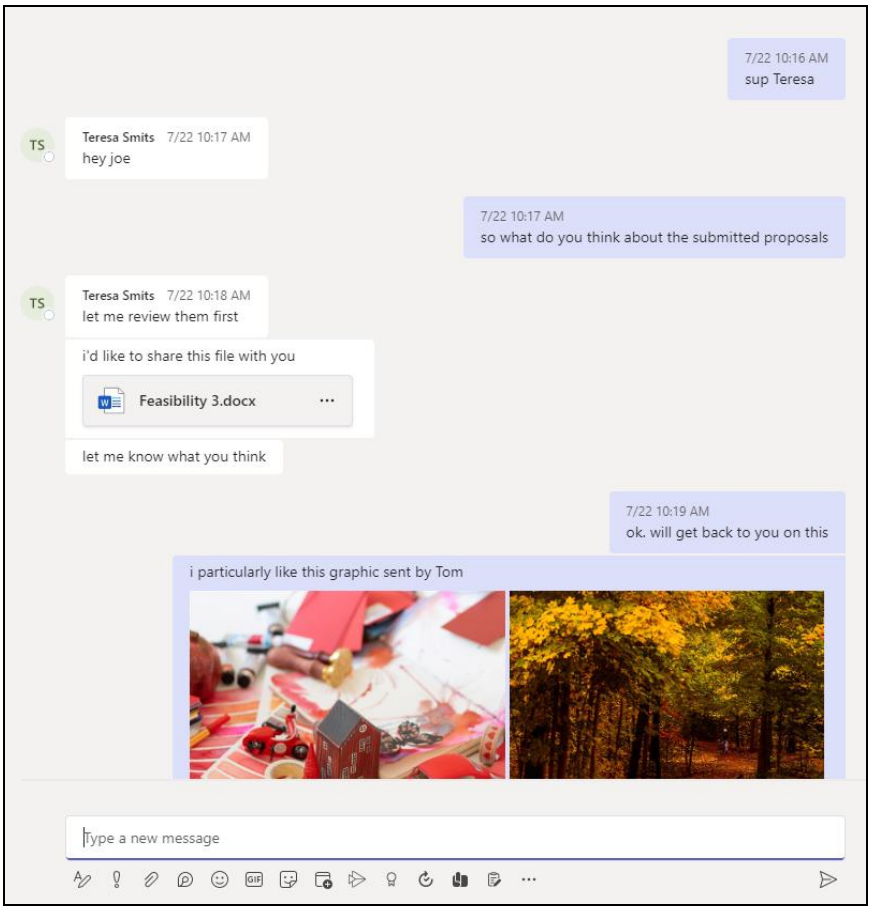
- Microsoft 365 user: Joe

- Data type: Teams Chat



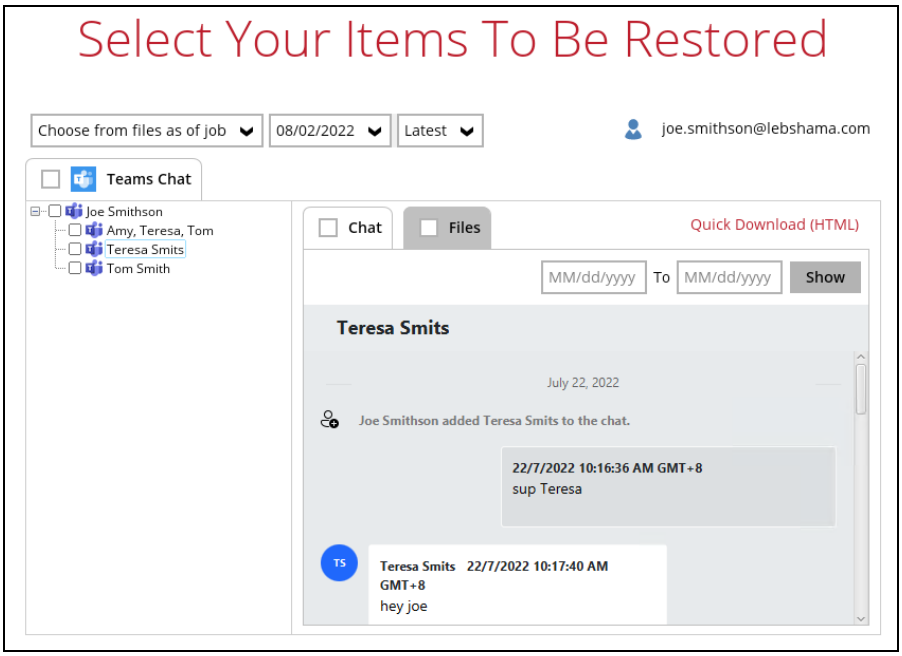
Scenario:

Joe has 1:1 chat with Teresa, and they shared files with each other.

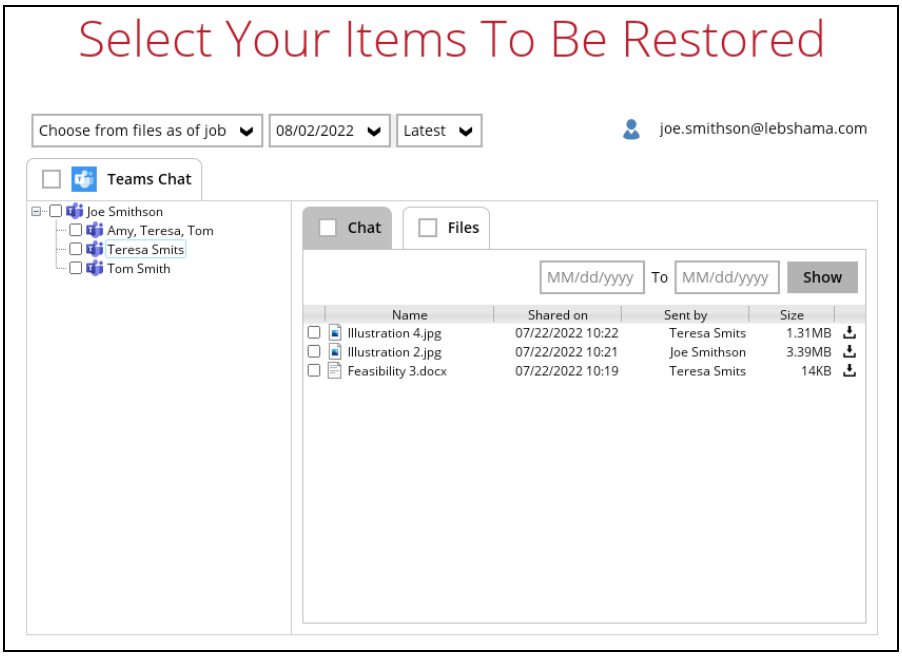


If you create a Backup Set, it will include Joe's chat message with Teresa. But it will not include any files attached as OneDrive is not selected.

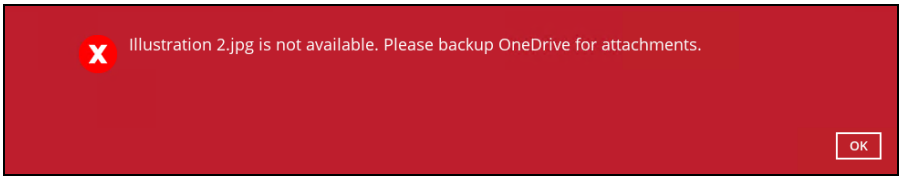
When you Restore from this Backup Set and open the conversation between Joe and Teresa, you can only restore messages.



Files that they shared with each other will be listed under the Files tab, but you cannot download and/or restore them.



And when you click on the download button, this error message will appear because OneDrive is not a selected Data Type, which means the shared file was not backed up since file attachments are saved in OneDrive.



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

2.15.3 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 Microsoft 365 restore operation and is not supported in a Run on Server Microsoft 365 restore.

- **Space Freeing up**

  Space freeing up feature is used to remove obsolete file(s) from your backup set and destination. This feature is only applicable in a Run on Client Microsoft 365 Backup Set and is not supported in a Run on Server Microsoft 365 Backup.

- **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 Microsoft 365 Backup Set and is not supported in a Run on Server Microsoft 365 Backup.

- **System Logs**

  AhsayOBM/AhsayACB backup user account does not have access to the system logs related to the Data Integrity Check operation through the AhsayCBS user console.

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

2.16 Best Practices and Recommendations

The following are some best practices or recommendations we strongly recommend you follow before you start any Microsoft 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 Microsoft 365 backups to ensure best backup performance, minimal resource usage, and lowest probability of throttling of Ahsay backup requests by Microsoft 365.

- **Recommended Number of Microsoft 365 users on a Backup Set**
  To ensure that your Microsoft 365 Run on Server backup set completes the backup job within 24 hours, it is recommended that a single Microsoft 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**
  Since Modern Authentication is already available, it is recommended that backup sets are migrated to Modern Authentication. All newly created Microsoft 365 backup sets on AhsayCBS automatically use Modern Authentication.

- **Large number of Microsoft 365 users to Backup**
  It is recommended to divide the users into multiple backup sets. A single Microsoft 365 backup set should not contain more than 2,000 Microsoft 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 Microsoft 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.

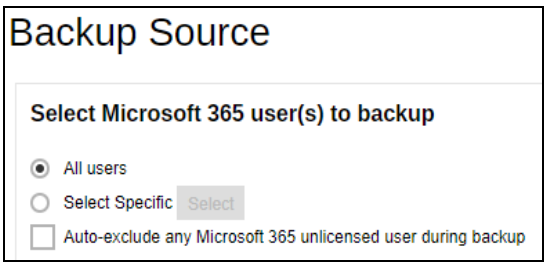
  - Hardware – to achieve optimal performance, compatible hardware requirements is a must. Ensure you have the backup machine's appropriate hardware specifications to accommodate frequency of backups,
    - so that the data is always backed up within the periodic backup interval
    - so that the backup 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 Microsoft 365 backup sets there are two approaches for backup source selection. Below are the sample screenshots of the selection All Microsoft 365 users and Selective Microsoft 365 user.

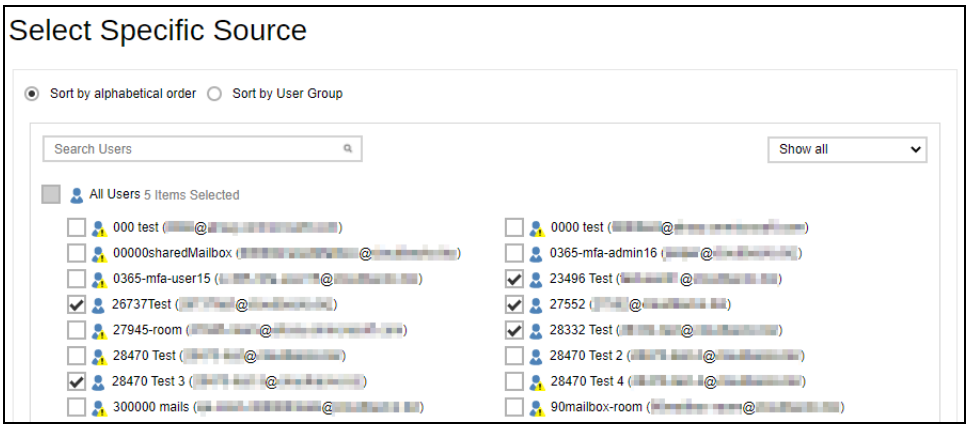
  - **All Microsoft 365 users**

    If you select "Backup all Users", all of the Microsoft 365 user accounts will automatically be selected.

  - **Selective Microsoft 365 user**

    If you select "Select Specific", you can select the users that you want to backup.

These are the Pros and Cons when selecting a backup source from all Microsoft 365 users and selective Microsoft 365 user.

	All Microsoft 365 users	Selective Microsoft 365 user
Backup Set Maintenance	The Admin does not need to manage the backup set, e.g. to select or unselect user when a Microsoft 365 user account is added or removed, the changes are automatically updated in the backup source.	The Admin will have to select or unselect users manually when a Microsoft 365 user account is added or removed, as the changes are not automatically updated in the backup source this can be very time consuming. If a Microsoft 365 user account is removed from the domain and the admin forgets to unselect the Microsoft 365 user account from the backup source, then this will cause a warning that the user does not exist. For more details on the backup set maintenance, please see, Appendix D: Example Scenario for Backup Set Maintenance
Microsoft 365 License	The backup user account must have additional Microsoft 365 license modules assigned to cover any increase in Microsoft 365 users. Otherwise, if additional users are added without sufficient modules, then this will cause backup quota exceeded warning and additional users will not be backed up. For more details on the computation on the required license, please see, Appendix A: Example Scenarios for Microsoft 365 License Requirement and Usage	This will allow the admin to easily control or manage the number of license modules used for the backup set.

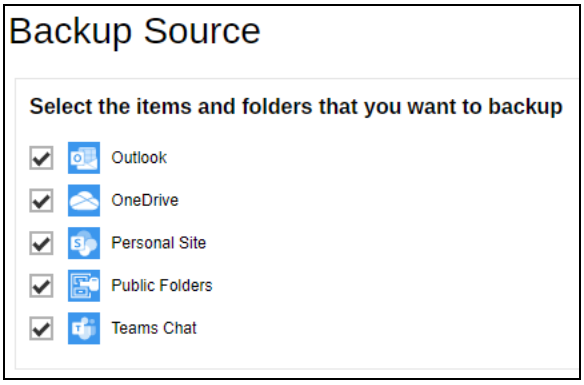
Backup Time	All Microsoft 365 user accounts will be backed up. This means the initial full backup job will take longer, any subsequent incremental backup will take longer.	Only selective Microsoft 365 user accounts will be backed up. This will mean the initial full backup job will be faster, any subsequent incremental backup will be faster.
Storage	As all Microsoft 365 user accounts are backed up, more storage will be required.	As only selective Microsoft 365 user accounts will be backed up, the backup set will require relatively less storage.
Data Synchronization Check	As all Microsoft 365 user accounts are selected for backup, regular DSC may not be required.	As only selective files and/or folders are selected for backup, DSC is highly recommended to synchronize de-selected files and/or folders in the backup source with the backup destination(s). To know more about the DSC, please refer to Appendix E: Example Scenario for Data Synchronization Check (DSC) with sample backup reports

- **Backup Source for AhsayACB**

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

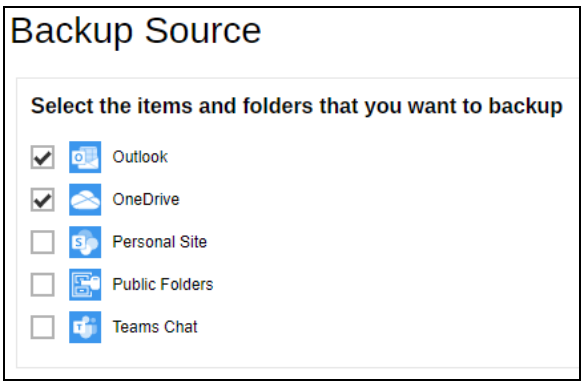
  - **All Items**

    Tick all the checkboxes, all of the items of the Microsoft 365 user account will automatically be selected.

  - **Selective Items**

    Tick selective items to backup, either Outlook, OneDrive, Personal Site or Public Folders. In our example, only Outlook and OneDrive are ticked.

  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.

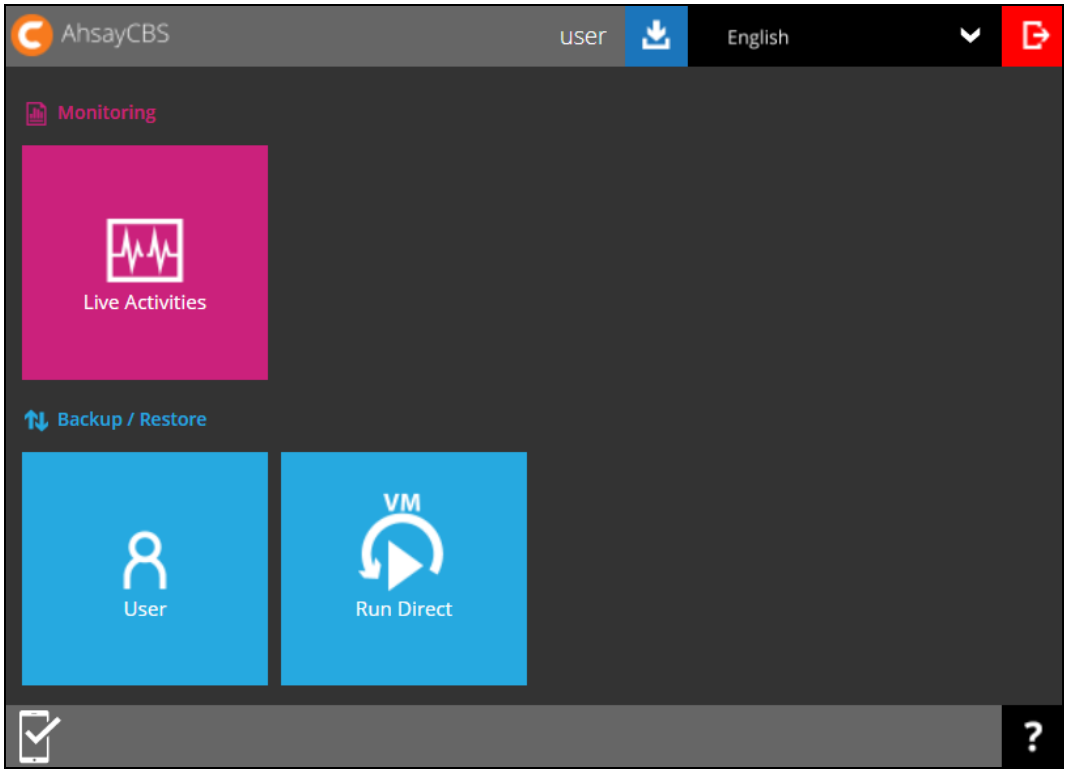
Backup Time	All Items of the Microsoft 365 user account will be backed up. This means the initial full backup job will take longer, any subsequent incremental backup will take longer.	Only selective Items of the Microsoft 365 user account will be backed up. This will mean the initial full backup job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

3 Creating a Microsoft 365 Backup Set

1. Log in to the User Web Console.

   For instructions on how to do this please refer to Chapter 2 of the AhsayCBS v9 User Guide.

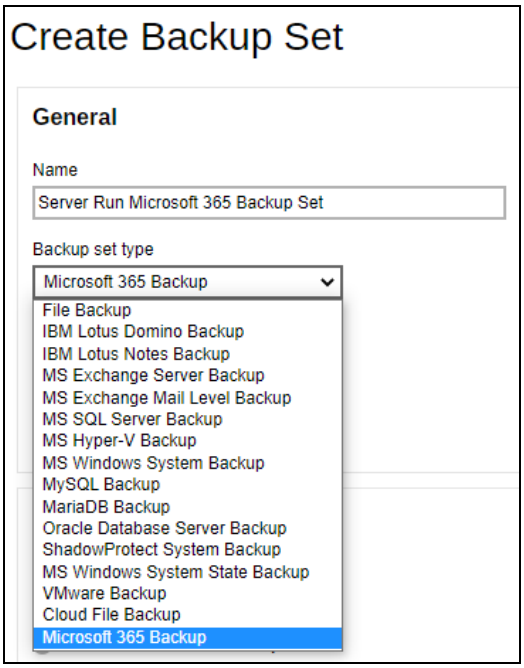
2. Click the **User** icon on the User Web Console landing page.



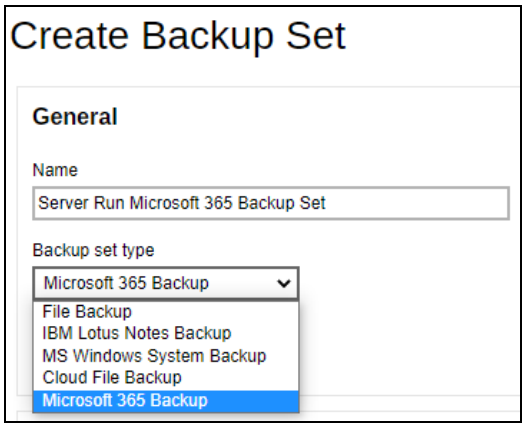
3. On the **Backup Set** menu, click the **+** icon to create a backup set.

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

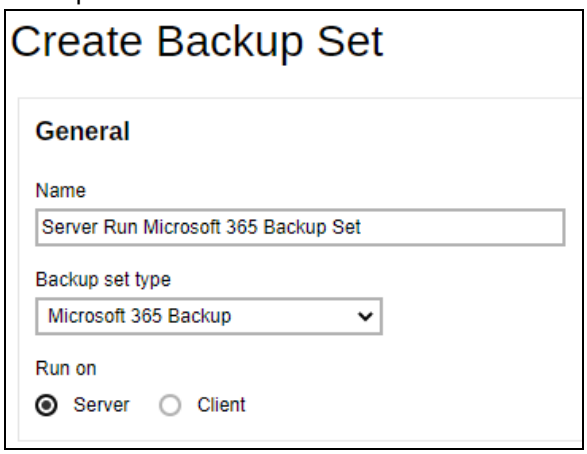
AhsayOBM



AhsayACB



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



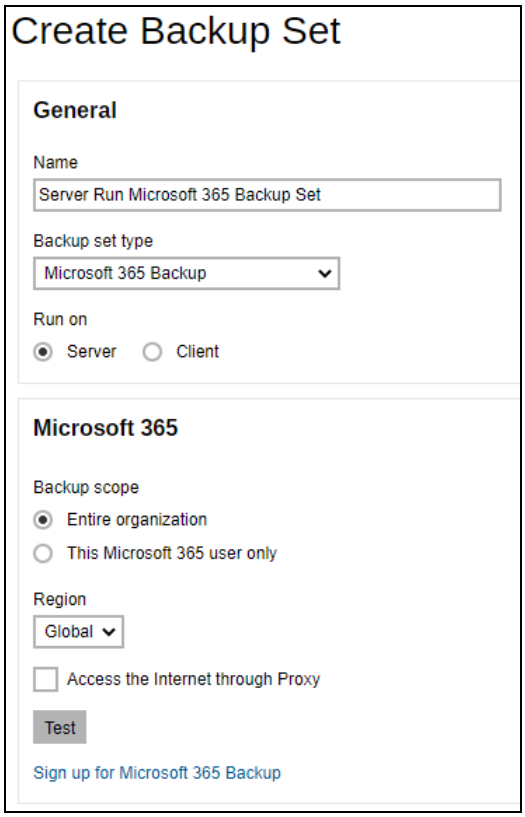
NOTES

- 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 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.

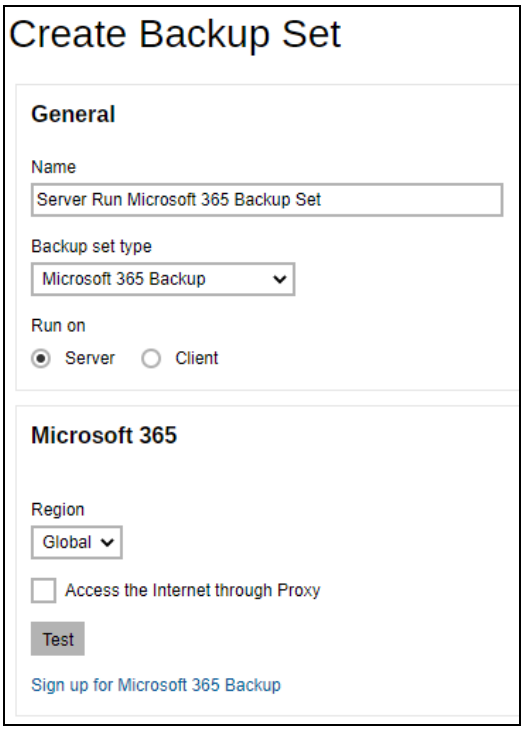
For AhsayOBM select the **Backup scope** and **Region** then click **Test**.

For AhsayACB select the **Region** then click **Test**.

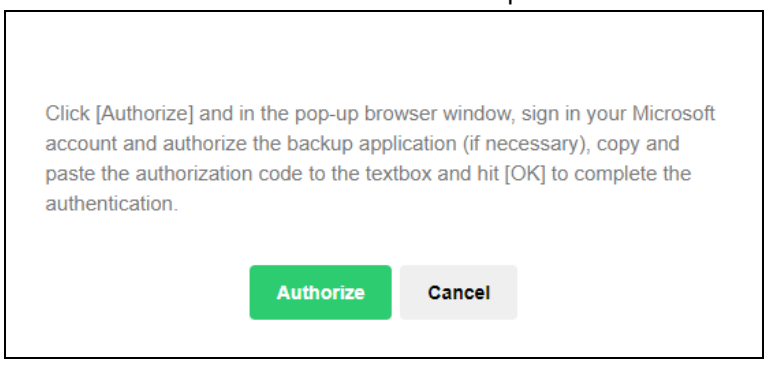
AhsayOBM



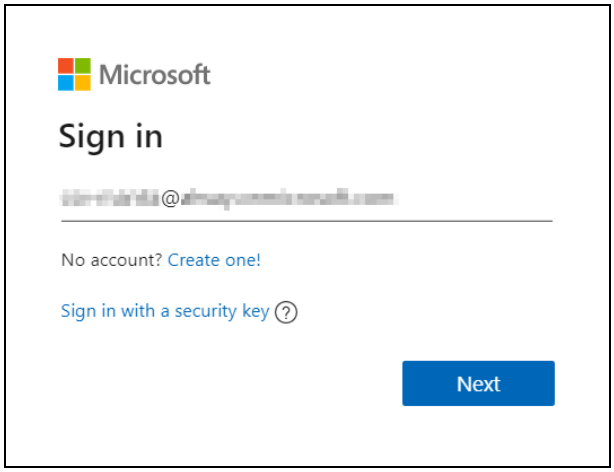
AhsayACB

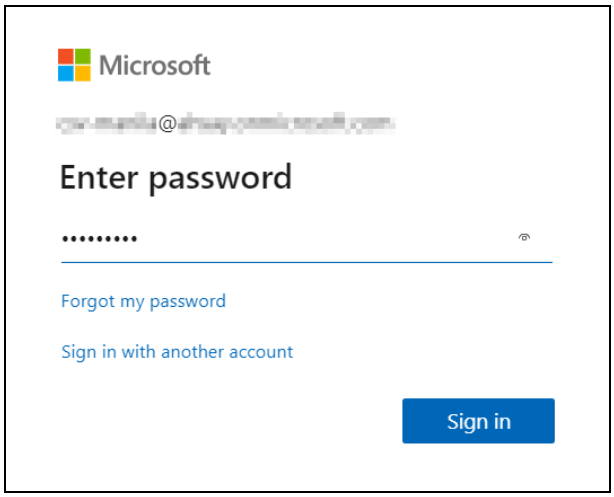


Click **Authorize** to start the authentication process.

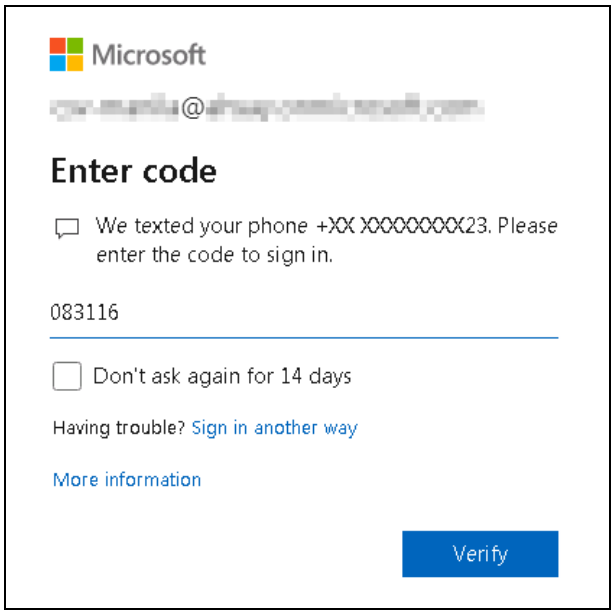


Sign in to your Microsoft account.





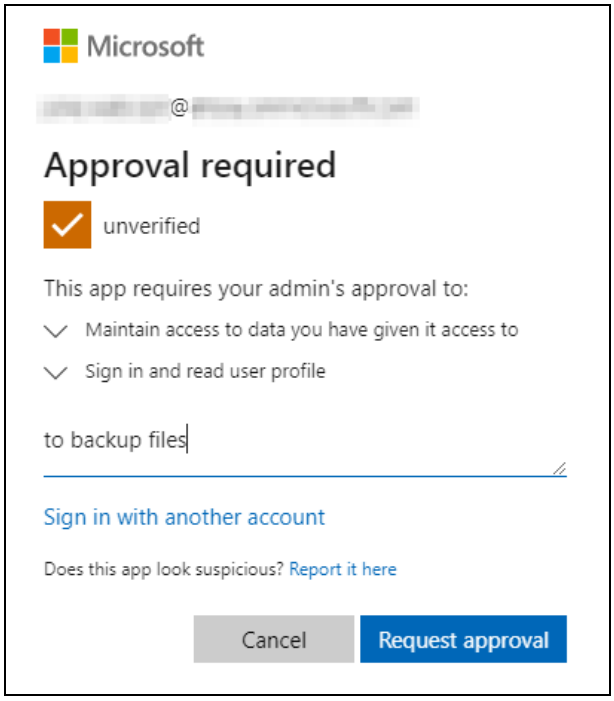
If MFA is enforced, enter the code and click **Verify**.



NOTE

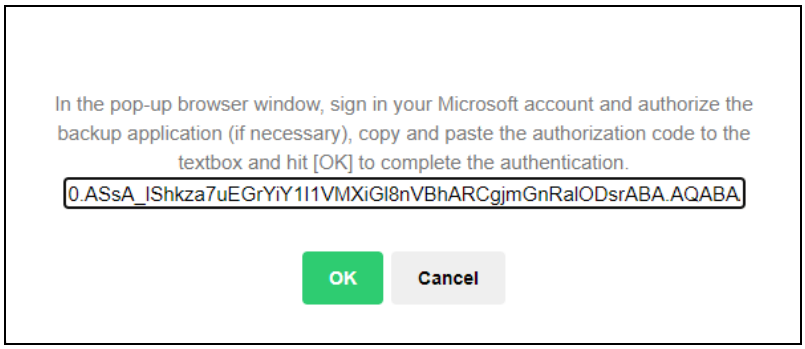
The verification code is only required if the MFA status of a Microsoft 365 account is enforced.

This will only be displayed if you login using an ordinary user account. Approval is required for ordinary users. Enter the reason for the request then click **Request approval**. Approval must be given by your administrator before an authorization code is issued.



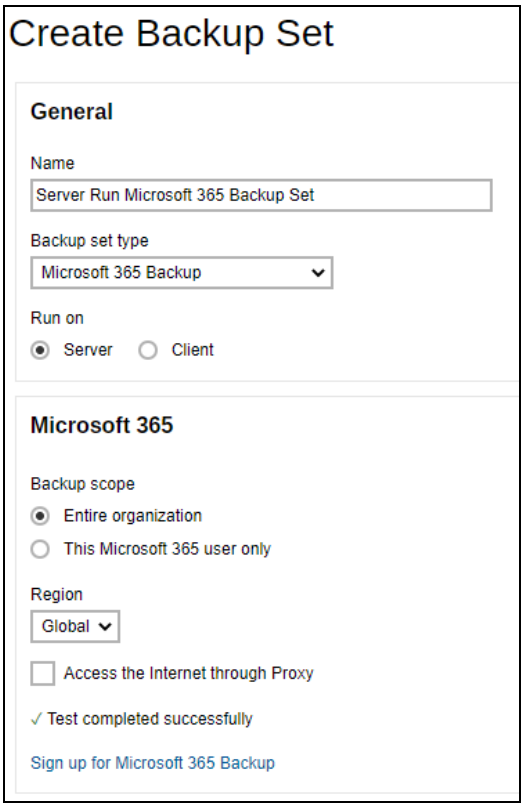
Copy the authorization code.

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

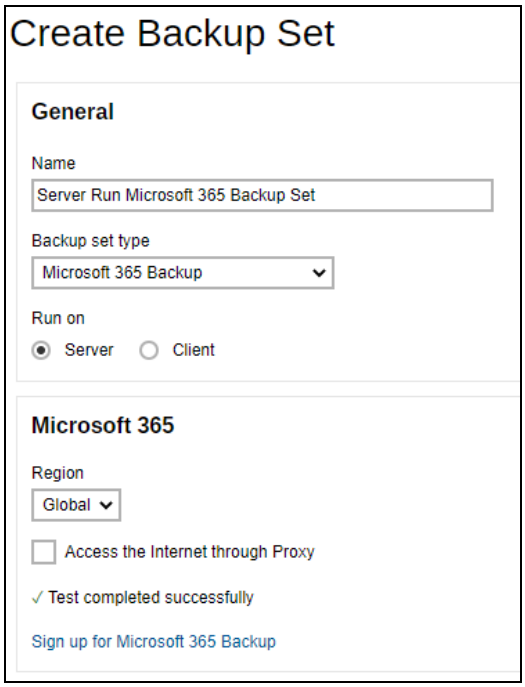


Test completed successfully will be displayed when the validation is successful. Click → to proceed.

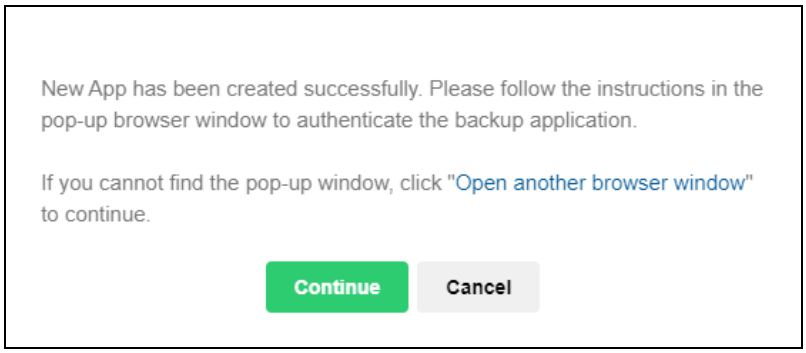
AhsayOBM



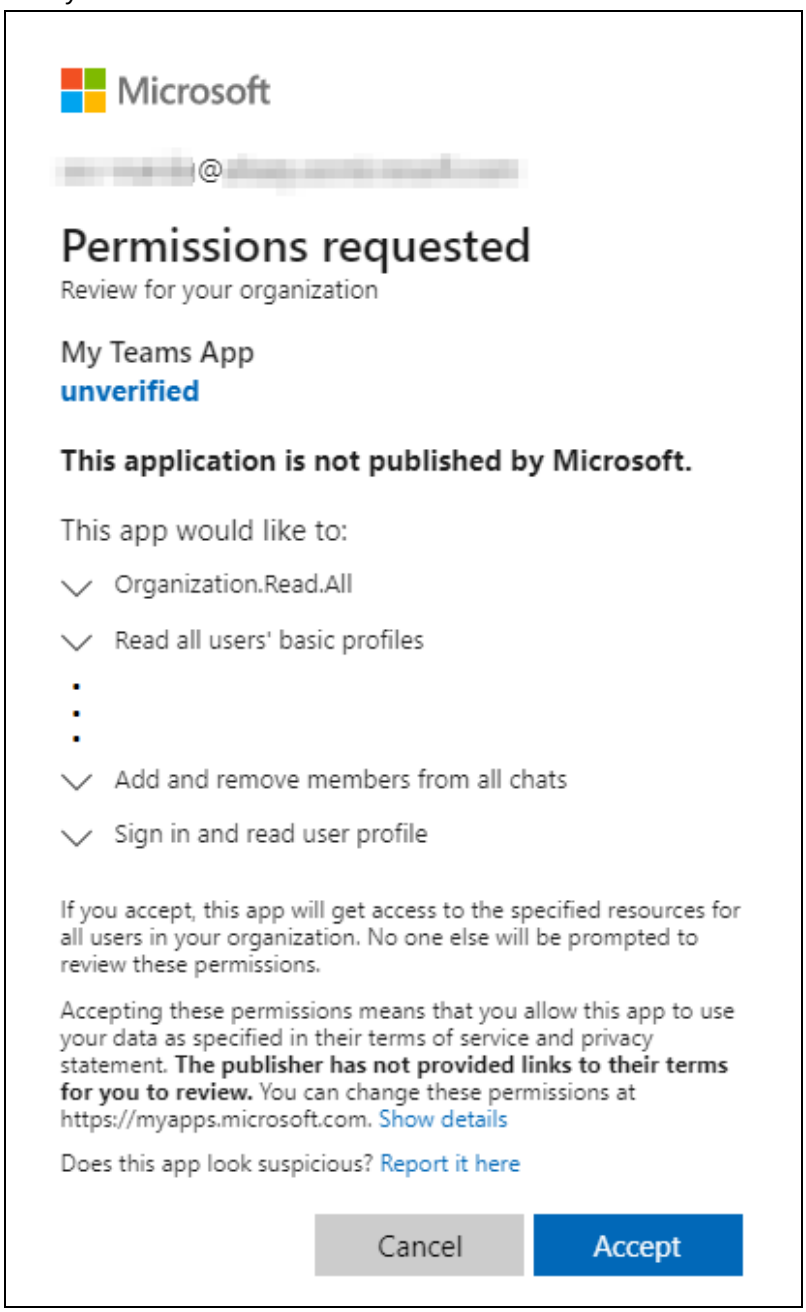
AhsayACB



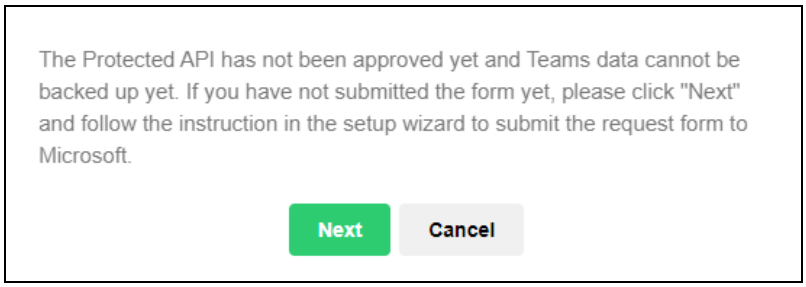
6. Click **Continue**.



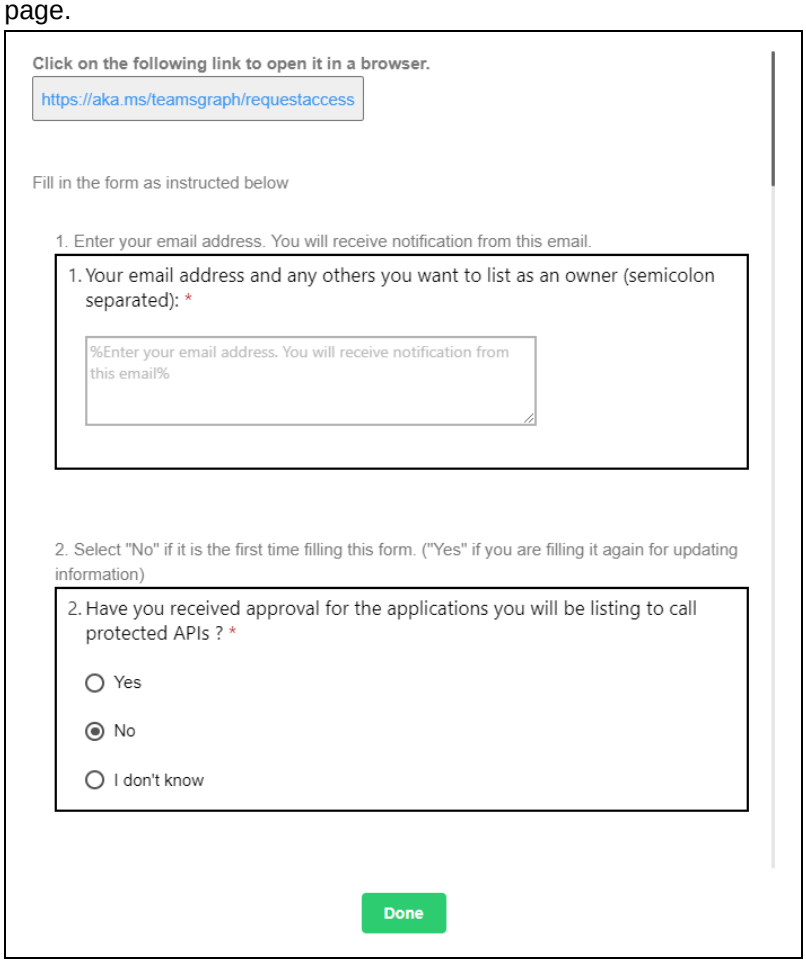
7. Sign into your Microsoft 365 account then accept the permission request. Go back to AhsayCBS and click **Continue**.



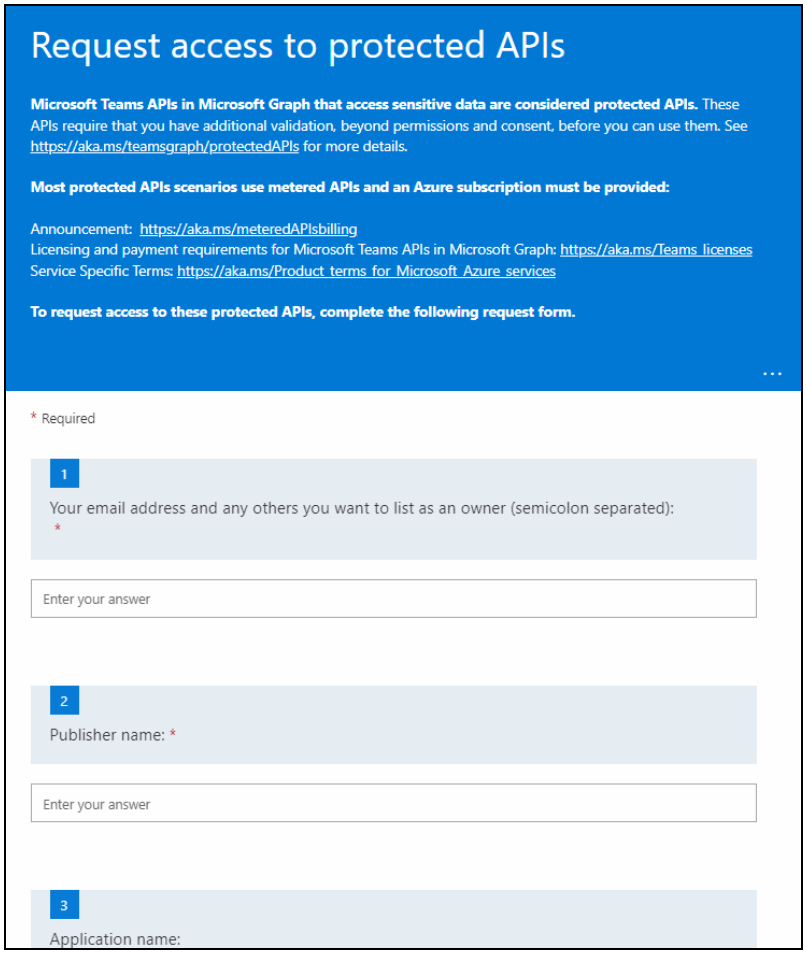
8. Click **Next**.



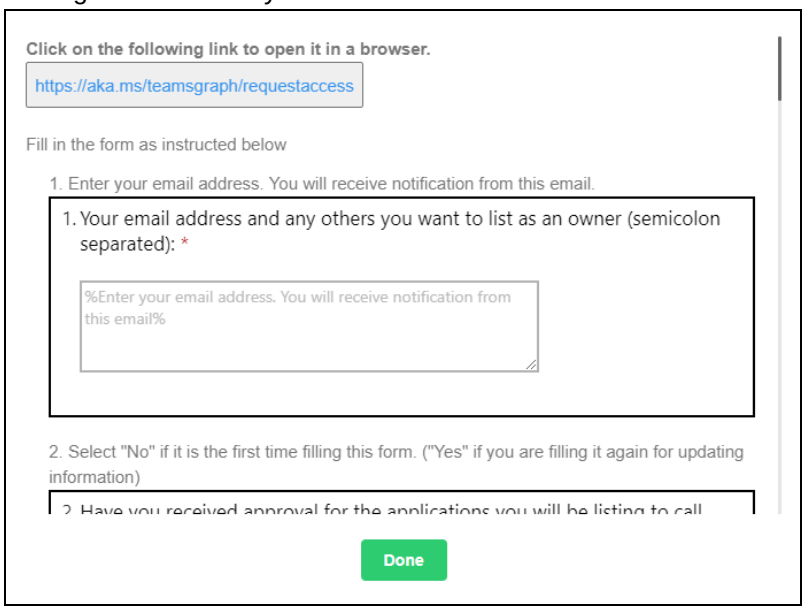
9. Click the link to fill up the form. For instructions on how to fill up the form scroll down this page.



Click **Submit** once done filling up the form and close the web browser.



Then go back to AhsayCBS and click **Done**.



NOTE

Requests for Permissions and Protected API access are only done once per user account.

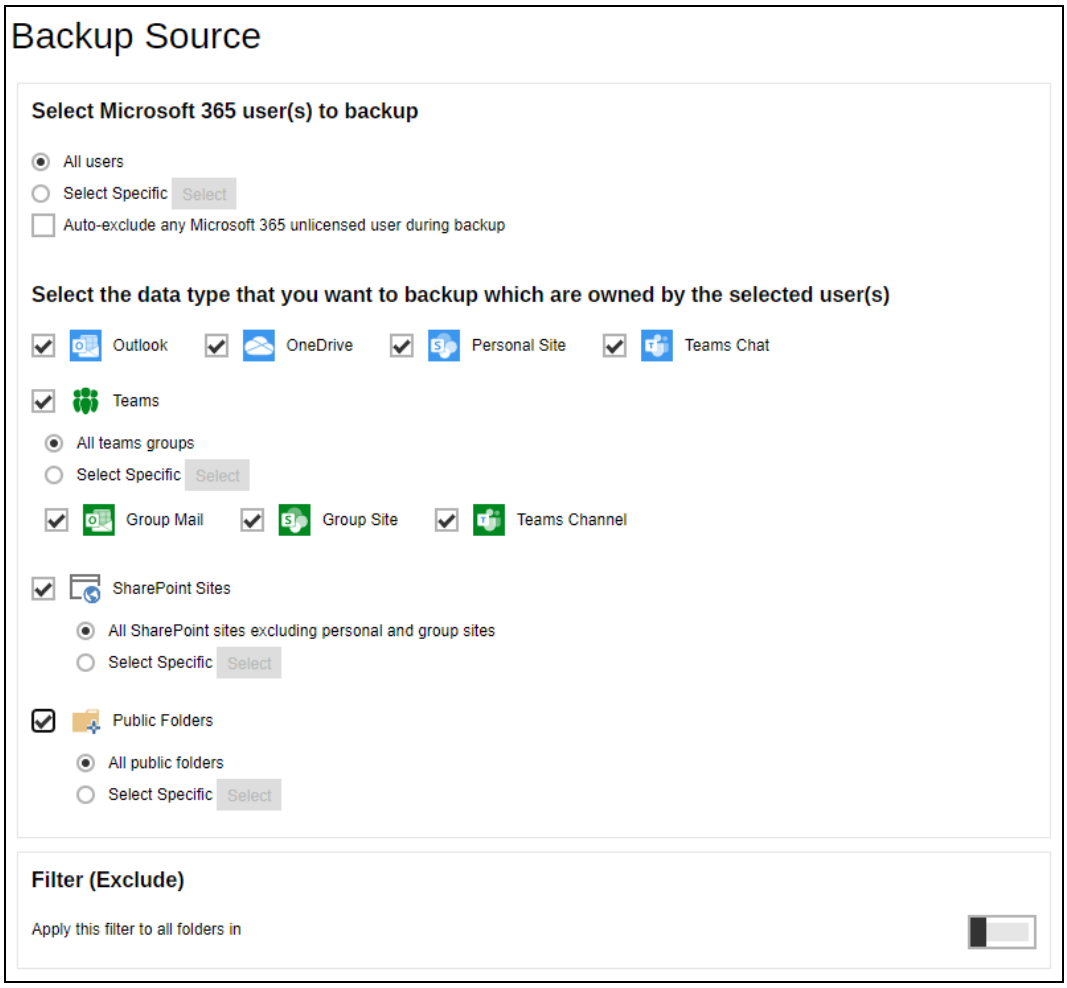
10. Select the users and the data type for backup.

    Backup Source window that will be displayed will be different for AhsayOBM and AhsayACB.

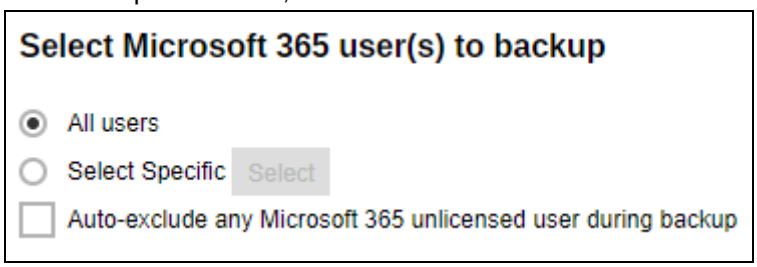
    AhsayOBM

    For AhsayOBM, the Backup Source window that will be displayed will depend on the backup scope selected. Either Entire organization or This Microsoft 365 user only.

    If Entire organization is selected this will be the screen displayed.

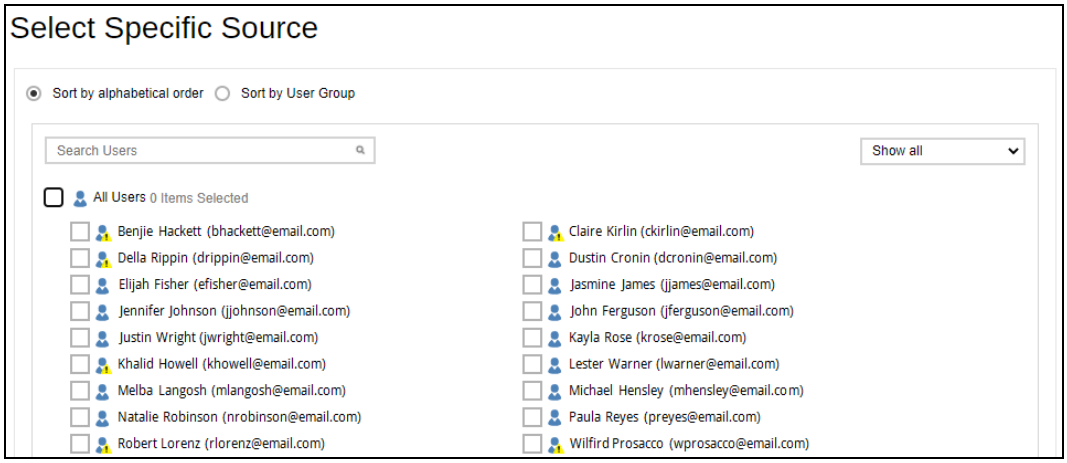


    To select specific users, click **Select**.

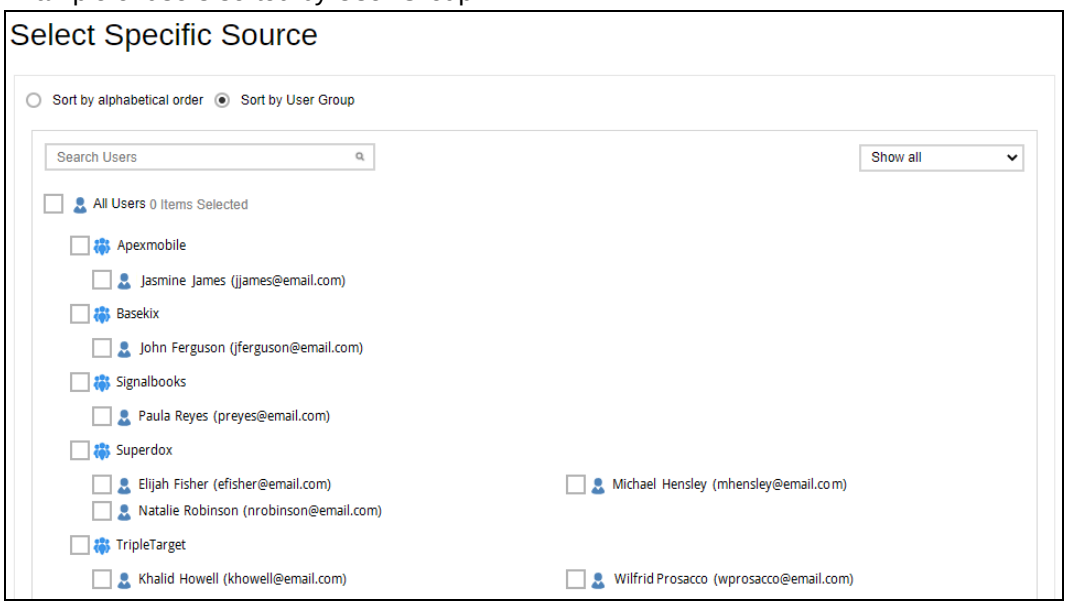


Users can be sorted alphabetically or by User Group.

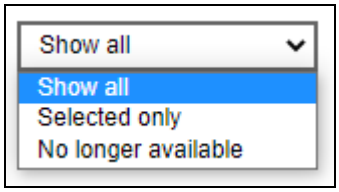
Example of users sorted alphabetically.



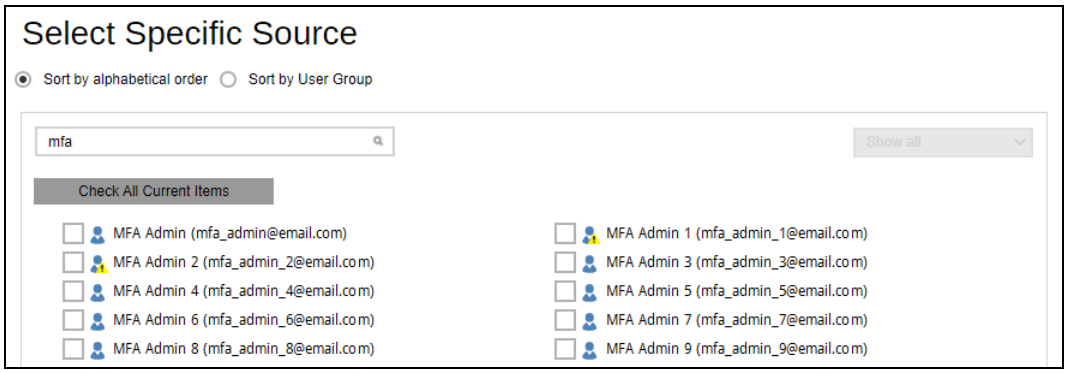
Example of users sorted by User Group.



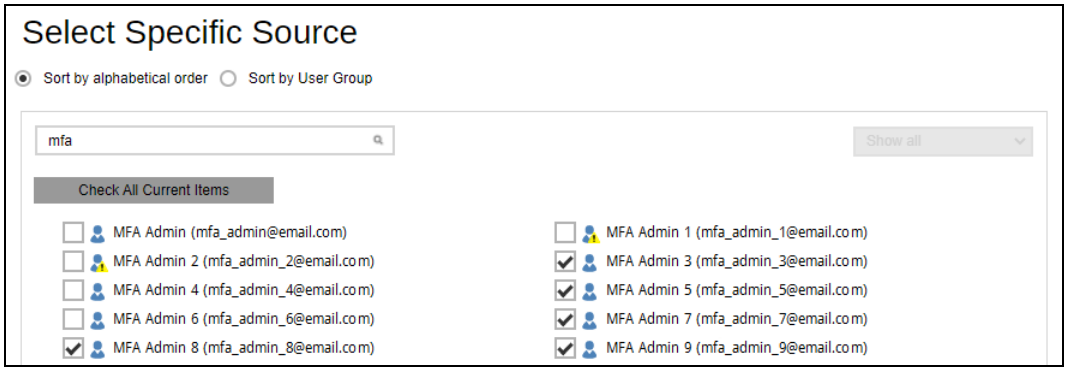
List of users can be displayed in three ways.



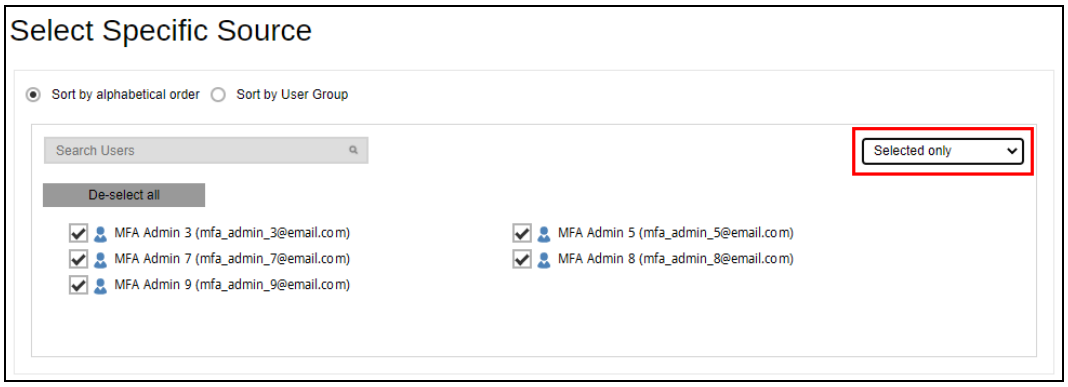
Searching for a particular user is possible by entering the name or email address then click . A list of names and email addresses will be displayed containing the search criteria. Click **Check All Current Items** to select all listed users.



Select specific users by ticking the checkbox beside the user.

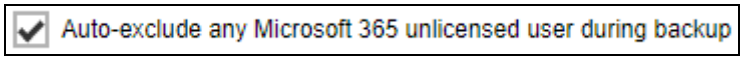


To display selected users only, select **Selected only**.

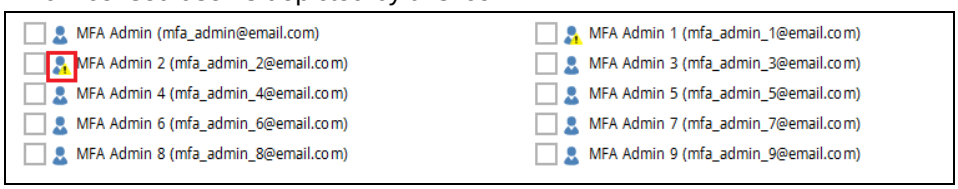


Click once done with the selection.

Tick the **Auto-exclude any unlicensed user during backup** checkbox if you do not want to include unlicensed users in your backup.



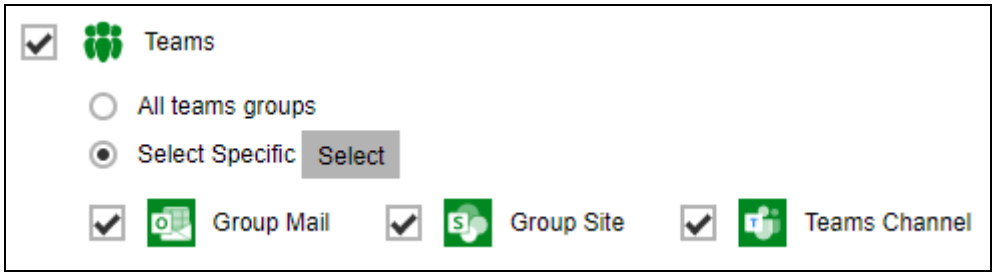
An unlicensed user is depicted by this icon .



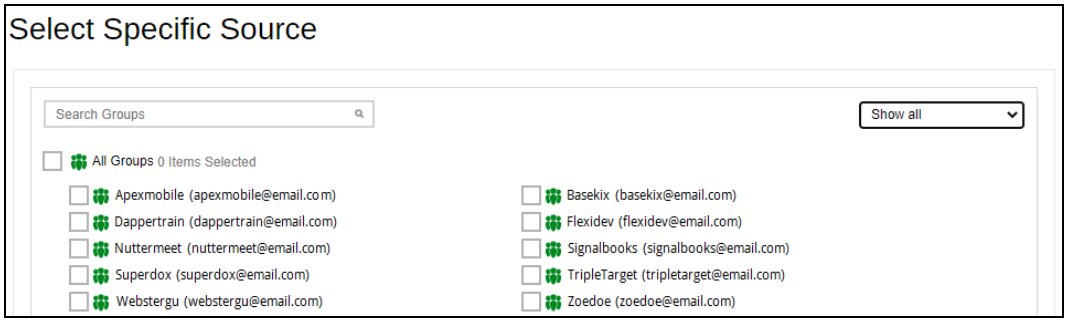
Select the data type that you want to be included in the backup. Select from Outlook, OneDrive, Personal Site and Teams Chat. Ticking the checkbox will backup all, i.e. ticking the Outlook checkbox will back up the mailboxes of the selected user(s). For Teams Chat, it is not necessary to select other user accounts involved in the chat to backup the conversation.

Select to backup Teams, SharePoint Sites and Public Folders.

To select a specific Group to backup in Teams, click **Select**.



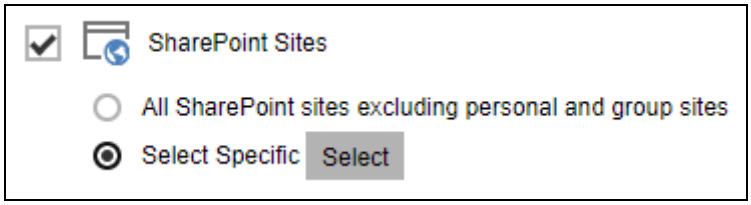
Searching for a particular group is also possible, enter the group name in the Search Groups field and click . List of groups can also be displayed in three ways: Show all, Selected only and No longer available. Click once done with the selection. Also select if Group Mail, Group Site and/or Teams Channel will be included in the backup.



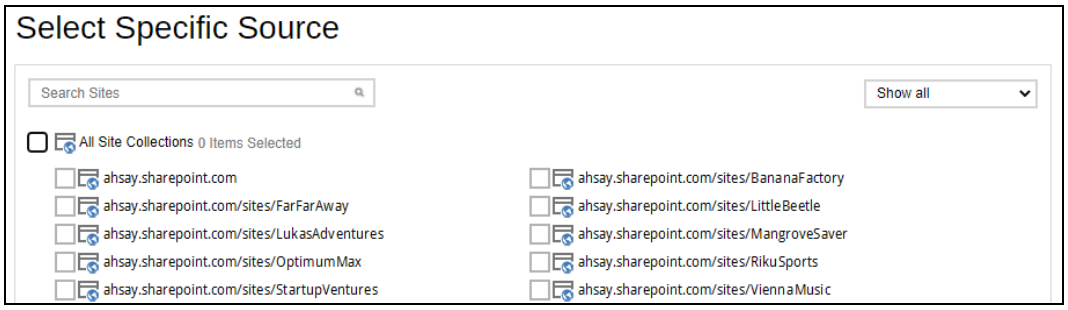
NOTE

In order to backup shared attachments for certain Teams Channel posts, OneDrive and Group Site must be selected as source.

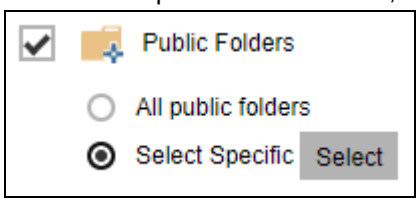
To select a specific Site to backup in SharePoint, click **Select**.



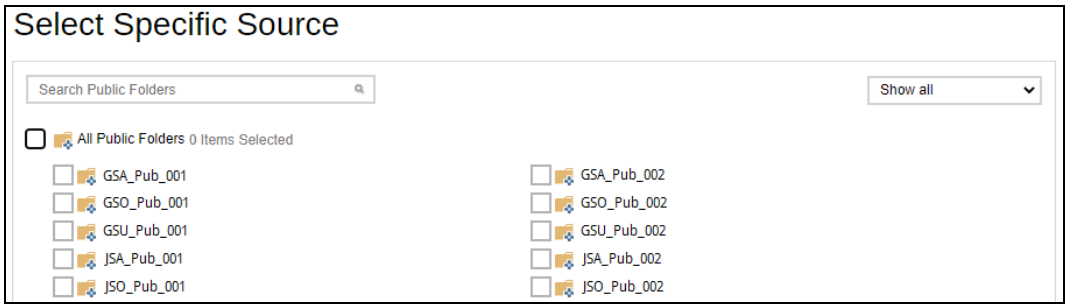
Searching and listing for Sites is the same process as discussed above.



To select a specific Public Foder, click **Select**.



Searching and listing for Public Folders is the same process as discussed above.

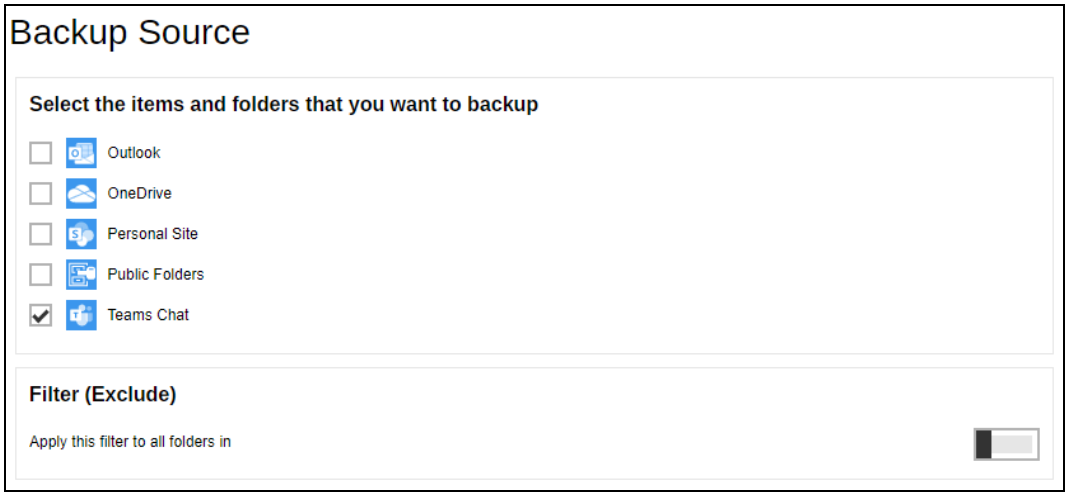


AhsayACB

This will be the window displayed if:

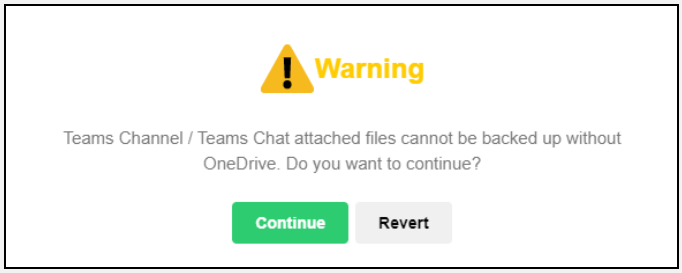
- This Microsoft 365 user only is selected in AhsayOBM
- AhsayACB

Select the items and folders for backup.



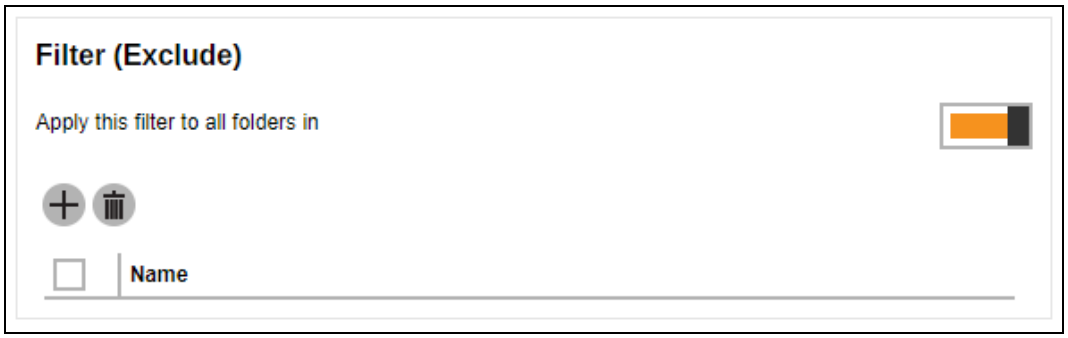
NOTE

This message will be displayed if OneDrive is not selected but Teams is selected for backup.



11. To exclude folders from your backup, use the exclude filter.

Enable the **Filter (Exclude)** by sliding the switch to the right. Click the + button to specify the criteria that will be used to exclude the folder.

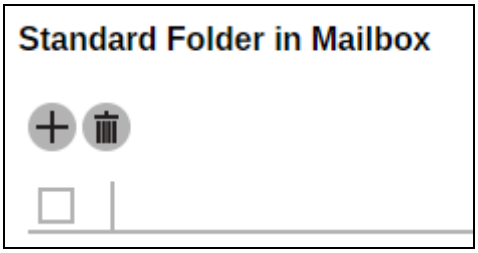


In the Filter window, enter a name for your filter.

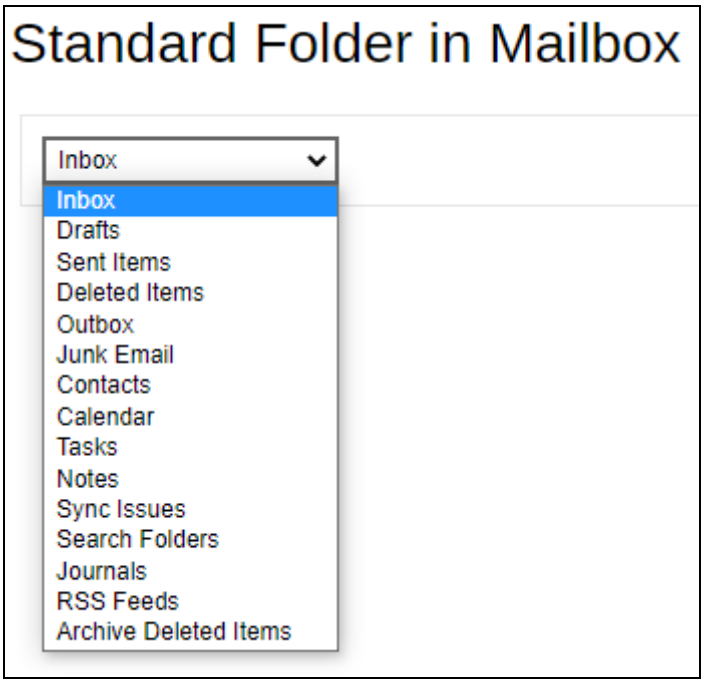
Select how the pattern will be compared, if by:

- **Simple comparison** – there are three choices:
  - **starts with**, folders that begins with the pattern will be selected
  - **ends with**, folders that ends with the pattern will be selected
  - **contain**, folders that contains the pattern will be selected

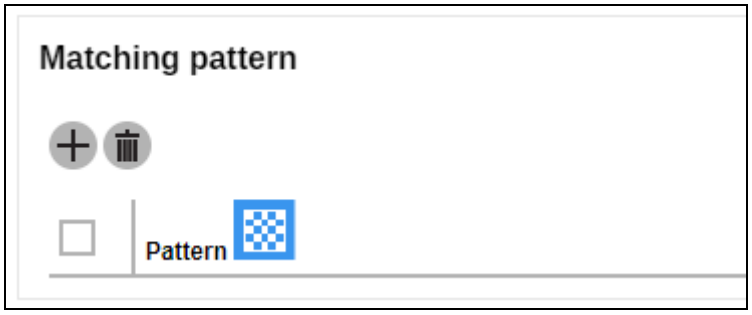
- **Regular expression (UNIX-style)** or
- **Standard Folder in Mailbox** – click the + button to select the folder.



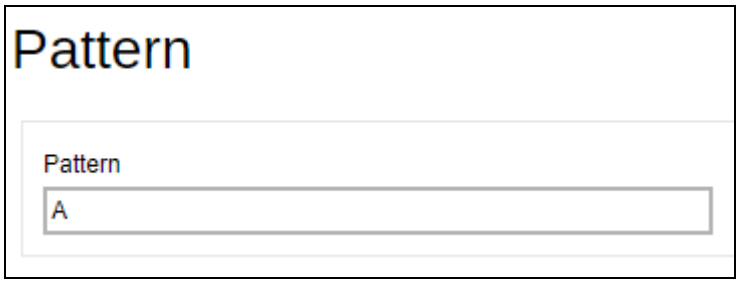
Select the folder from the drop down box then click to add. Repeat adding folders, until all the folders that you want to be excluded has been added to the filter.



Click the button to add the pattern.



Enter your pattern then click to add it. Repeat adding patterns, until all the patterns has been added to the filter.



NOTE

Matching pattern is only available for Simple comparison and Regular expression.

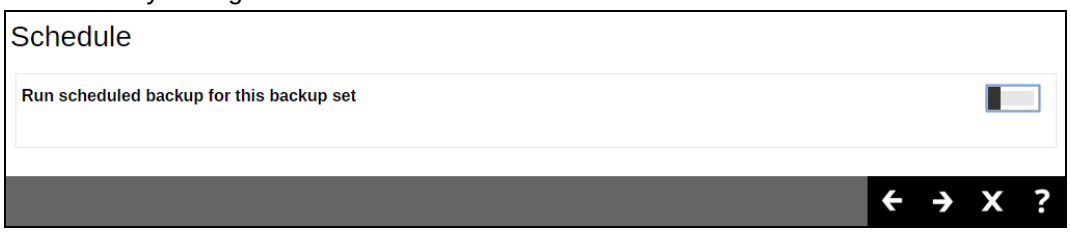
Click the **Browse** button to select where the filter will be applied.

Click **+** or **–** to expand or collapse the tree, then click the node where you want the filter to be applied. Click once done with the selection.

Click to add the filter.

Click to continue.

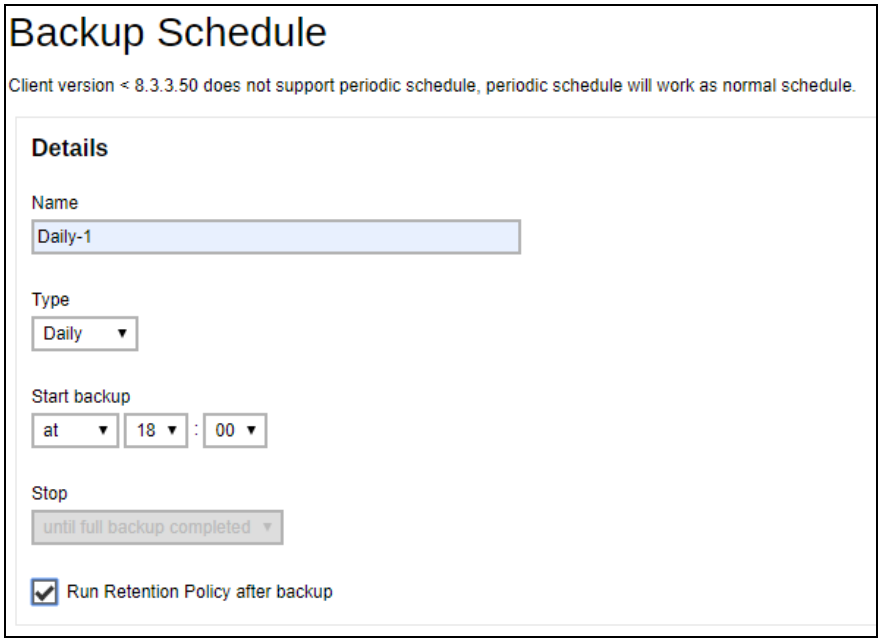
12. If you would like the backup set to run at a specified time interval of your choice, turn this feature on by sliding the on/off switch in the **Schedule** menu.



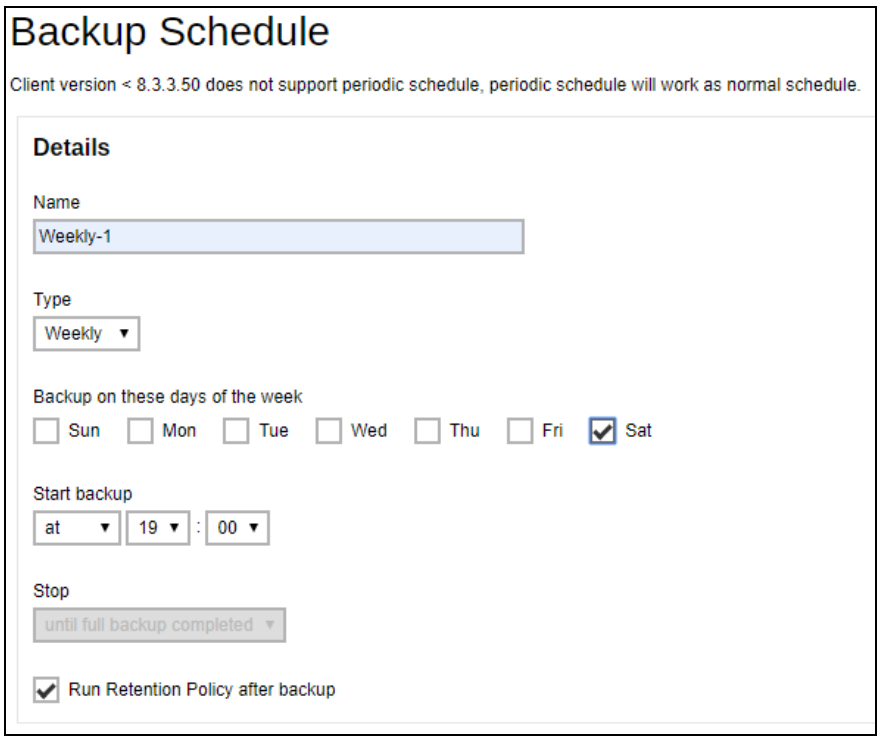
Click the button to add a schedule.

Configure the following backup schedule settings.

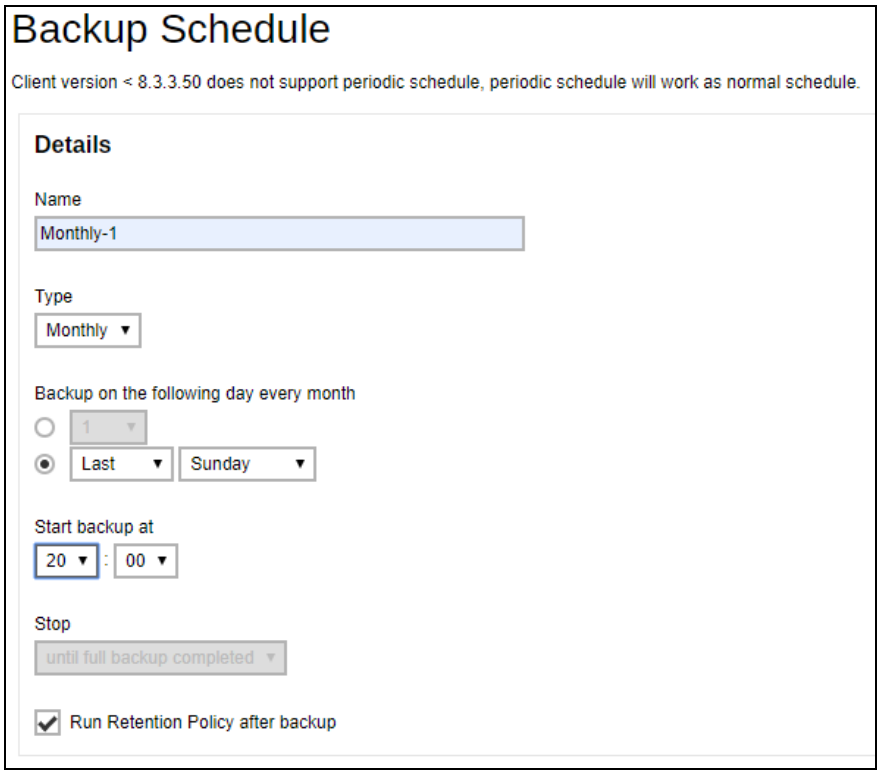
- **Name –** the name of the backup schedule.
- **Type –** the type of the backup schedule. There are four (4) different types of backup schedule: Daily, Weekly, Monthly and Custom.
  - **Daily –** the time of the day when the backup job will run.



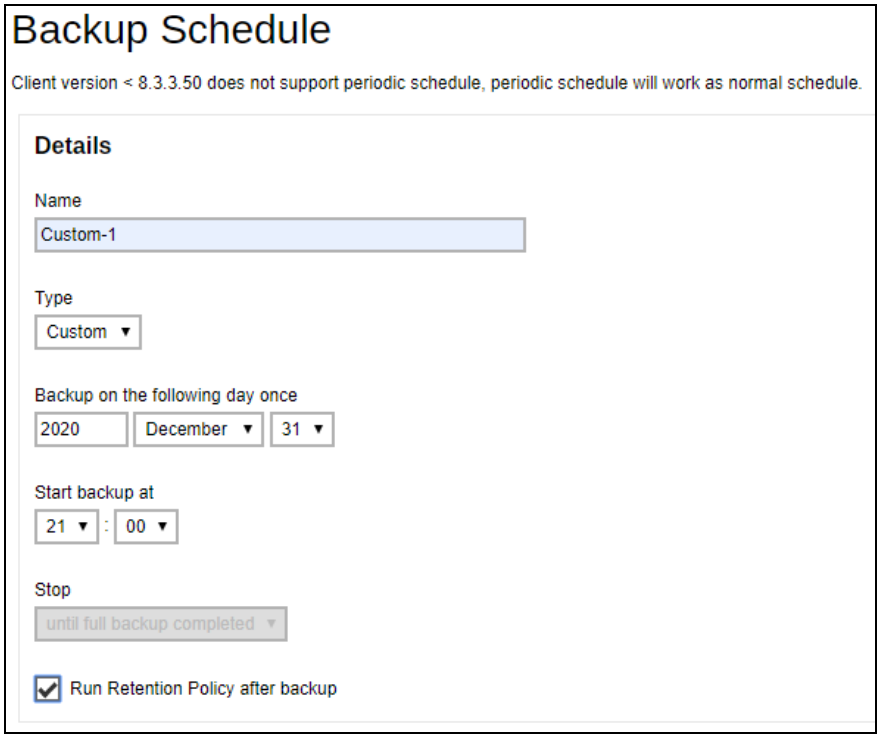
  - **Weekly –** the day of the week and the time of the day when the backup job will run.



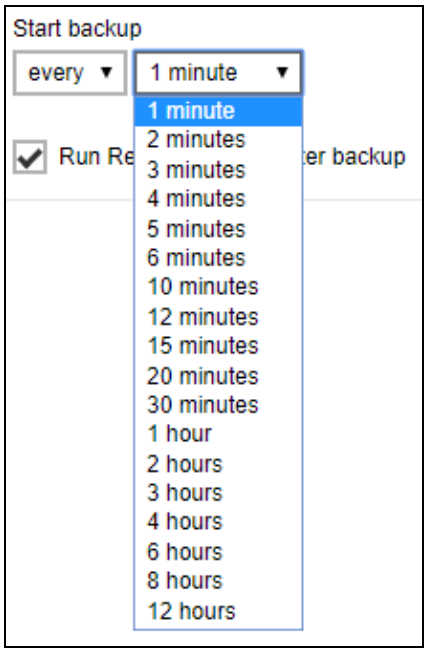
- **Monthly –** the day of the month and the time of the day when the backup job will run.



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



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



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

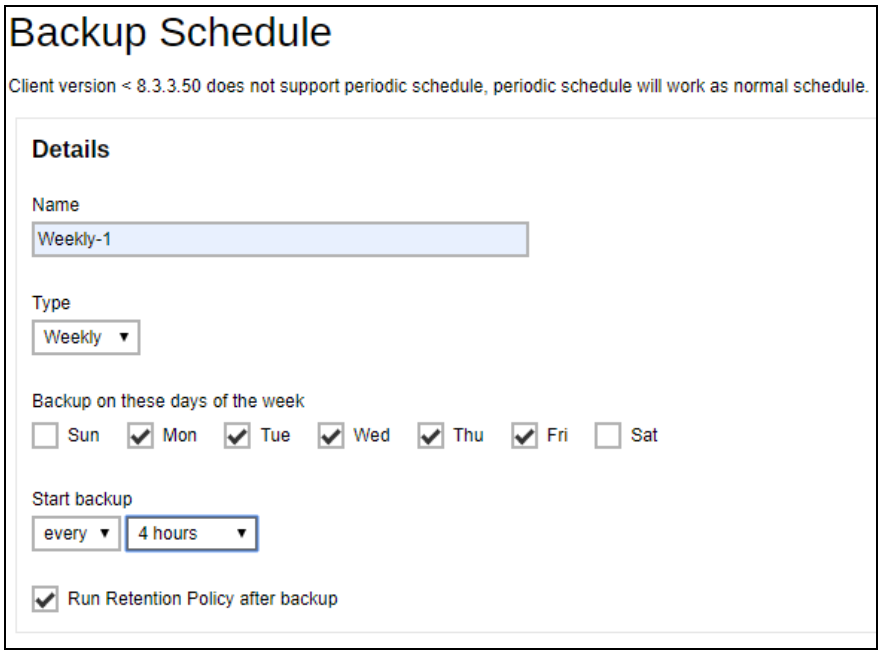


Figure 1.1 – Periodic schedule every 4 hours Monday - Friday during business hours

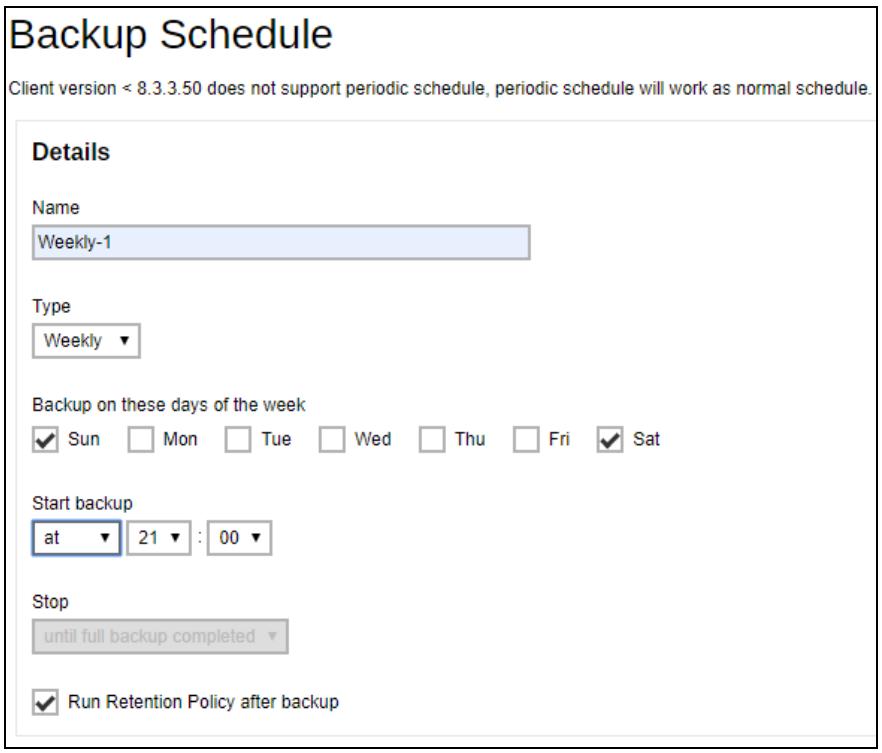


Figure 1.2 – Normal schedule runs at 21:00 or 9:00 PM on Saturday & Sunday during the weekend non-business hours

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

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

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

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

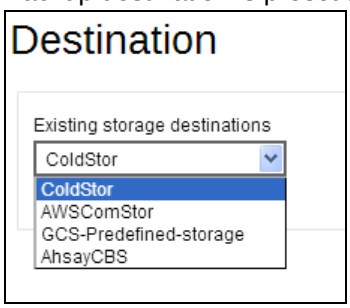
    As a general rule, it is recommended to review this setting regularly as the data size on the backup machine may grow over time.
- **Run Retention Policy after backup –** if enabled, retention policy job will run to remove files from the backup destination(s) which have exceeded the retention policy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

Click to save the configured backup schedule settings.

Click to proceed. Multiple backup schedules can be created.

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

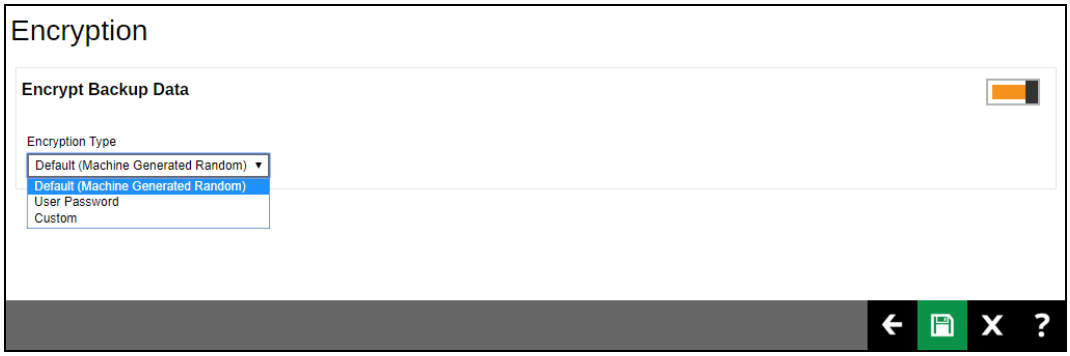
    Backup destination is preset to the AhsayCBS or Predefined Destination.



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

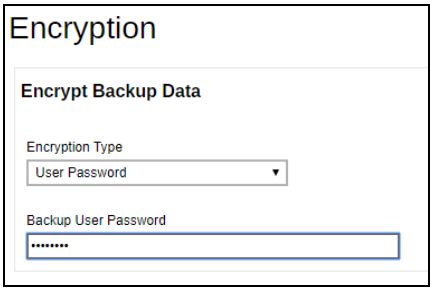
    Click at the bottom right corner to proceed when you are done with the setting.

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



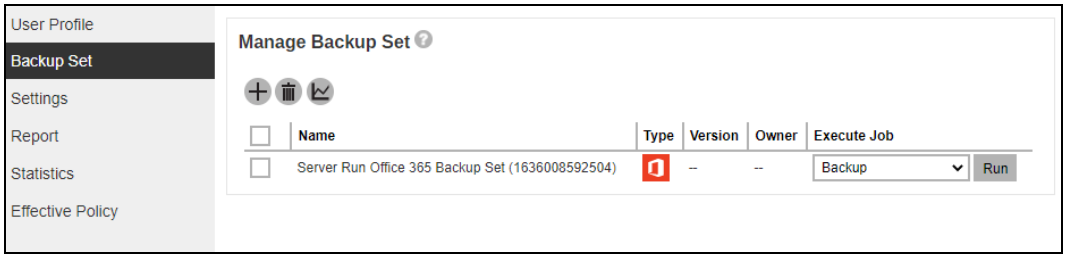
    You can choose from one of the following three Encryption Type options:

    - **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.

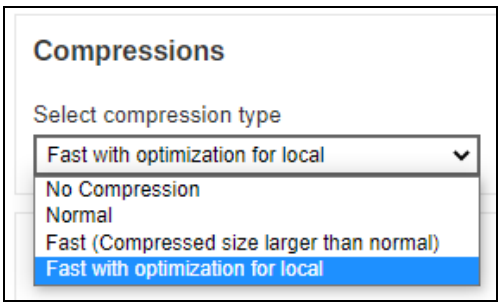
15. Click at the bottom right corner to confirm creating this backup set.



16. 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:

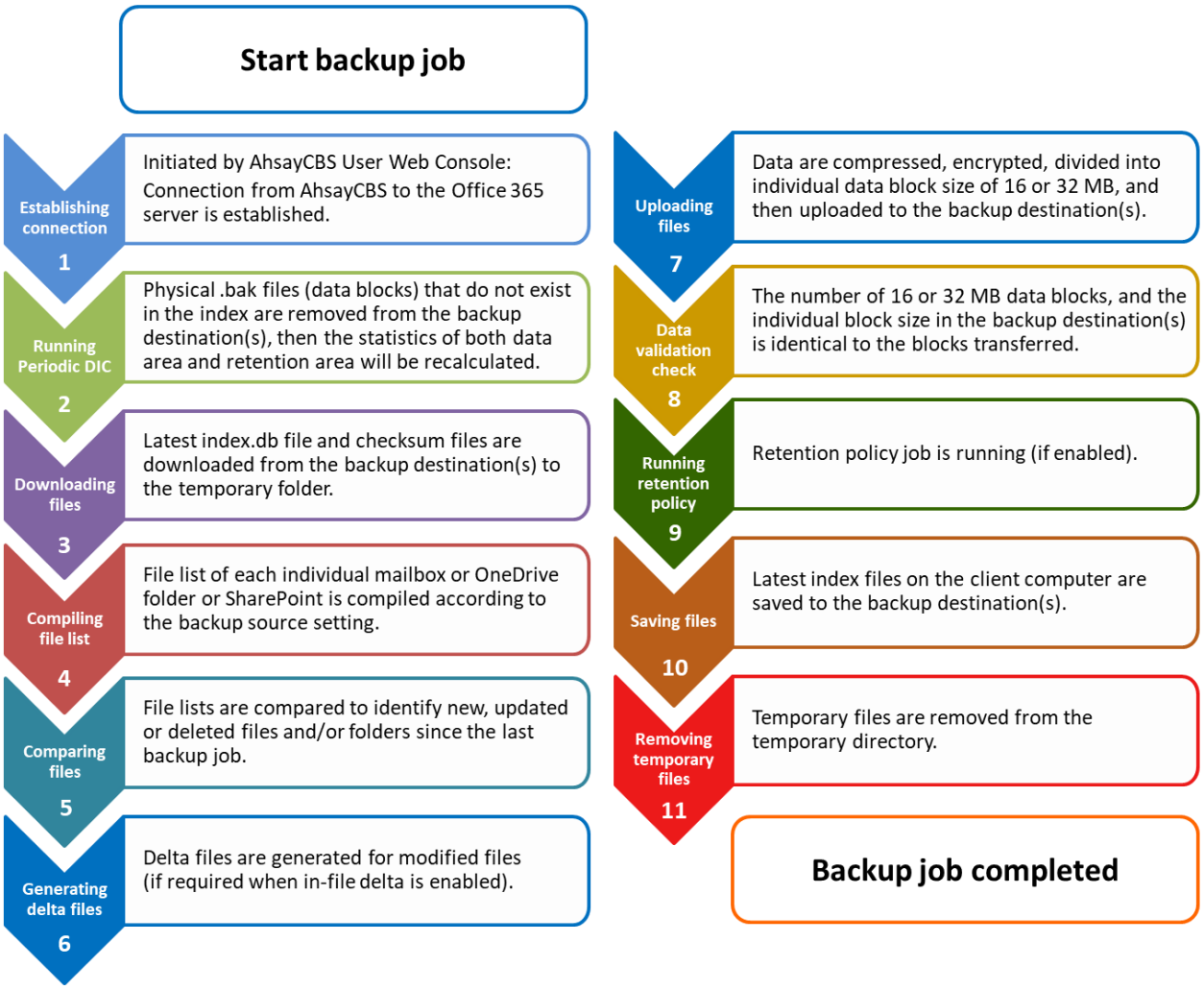
    - No Compression - file will not be compressed before backup.
    - Normal - compression is comparable to gzip Normal compression ratio.
    - Fast (Compressed size larger than normal) - compression will be faster but with less compression and lower CPU usage compared to Normal.
    - Fast with optimization for local - uses Snappy compression library when backing up to local destination only, otherwise setting will default to gzip if backing up to other destinations. Has the lowest CPU usage, very high speed and reasonable compression but compressed file size may be larger than Fast.



4 Overview of Microsoft 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)**



4.1 Periodic Data Integrity Check (PDIC) Process

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:

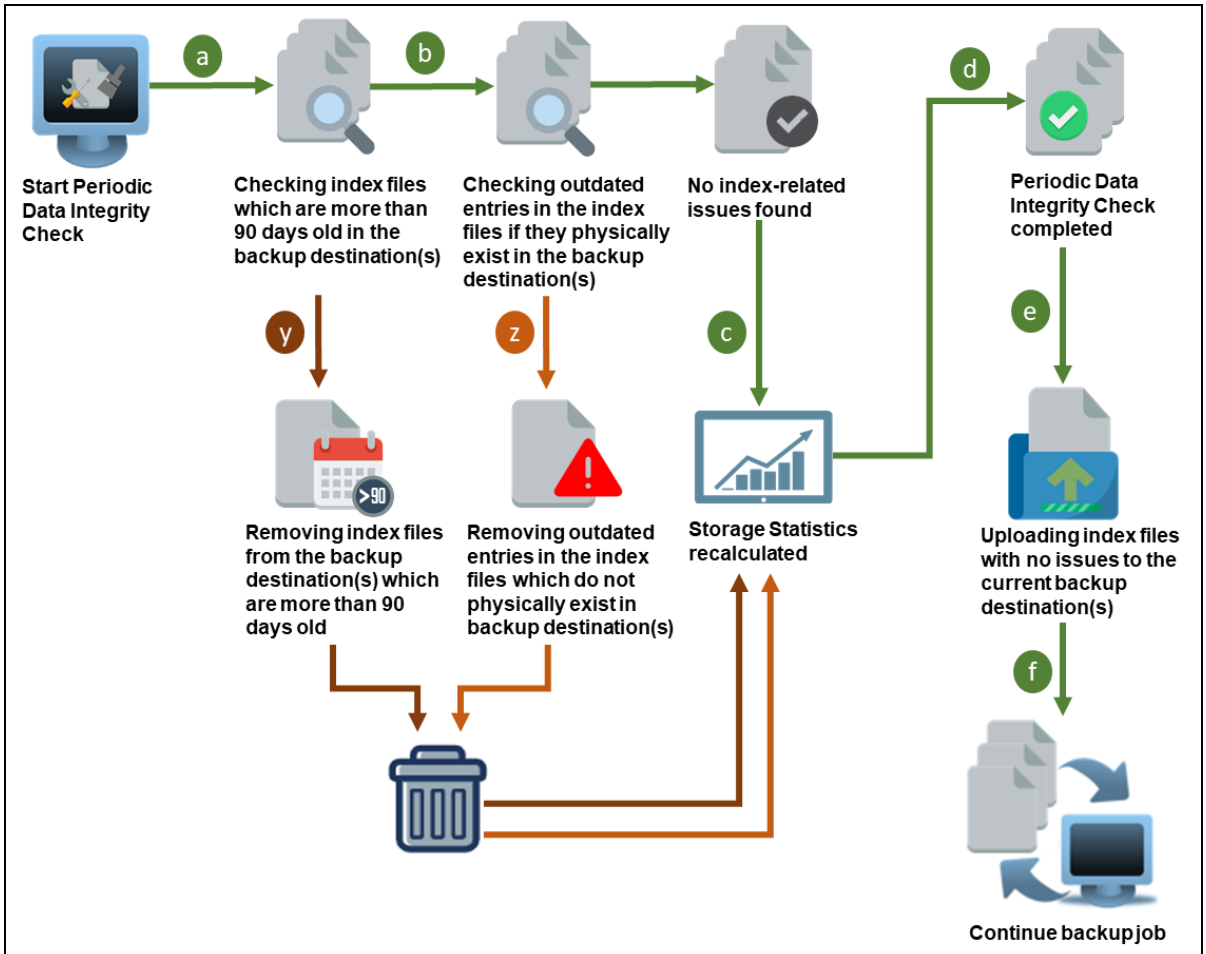
- the PDIC will run on the first backup job that falls on Wednesday; or
- if there is no active backup job(s) running from Monday to Friday, then the PDIC will run on the next available backup job.

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 v9 (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.



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

➔ If **YES**, proceed to y

➔ If **NO**, proceed to b

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

➔ If **YES**, proceed to c

➔ If **NO**, proceed to z

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

d Periodic Data Integrity check is completed.

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

f The backup job process will continue.

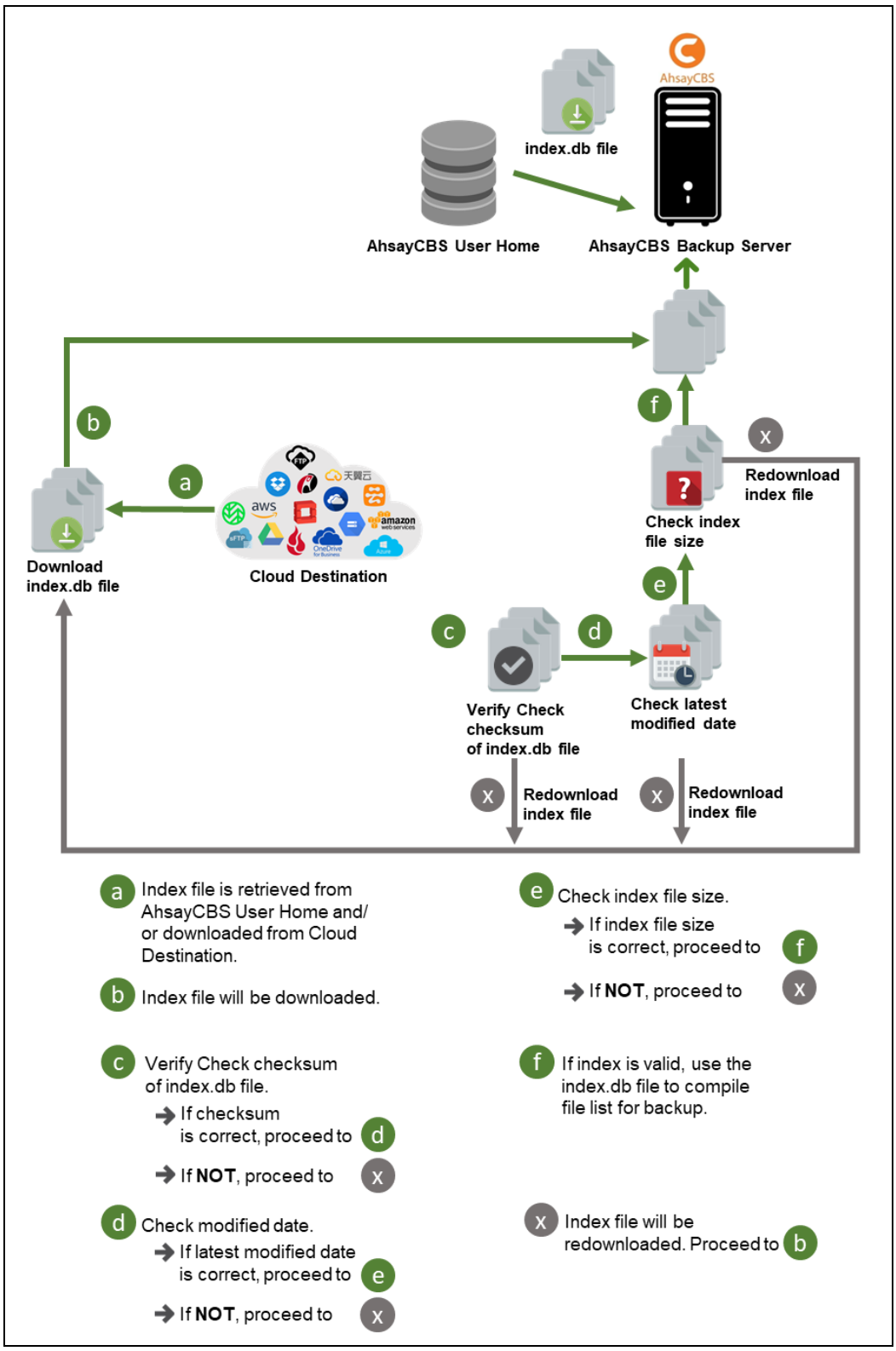
y Index files which are more than 90 days old will be removed from the backup destination(s).

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

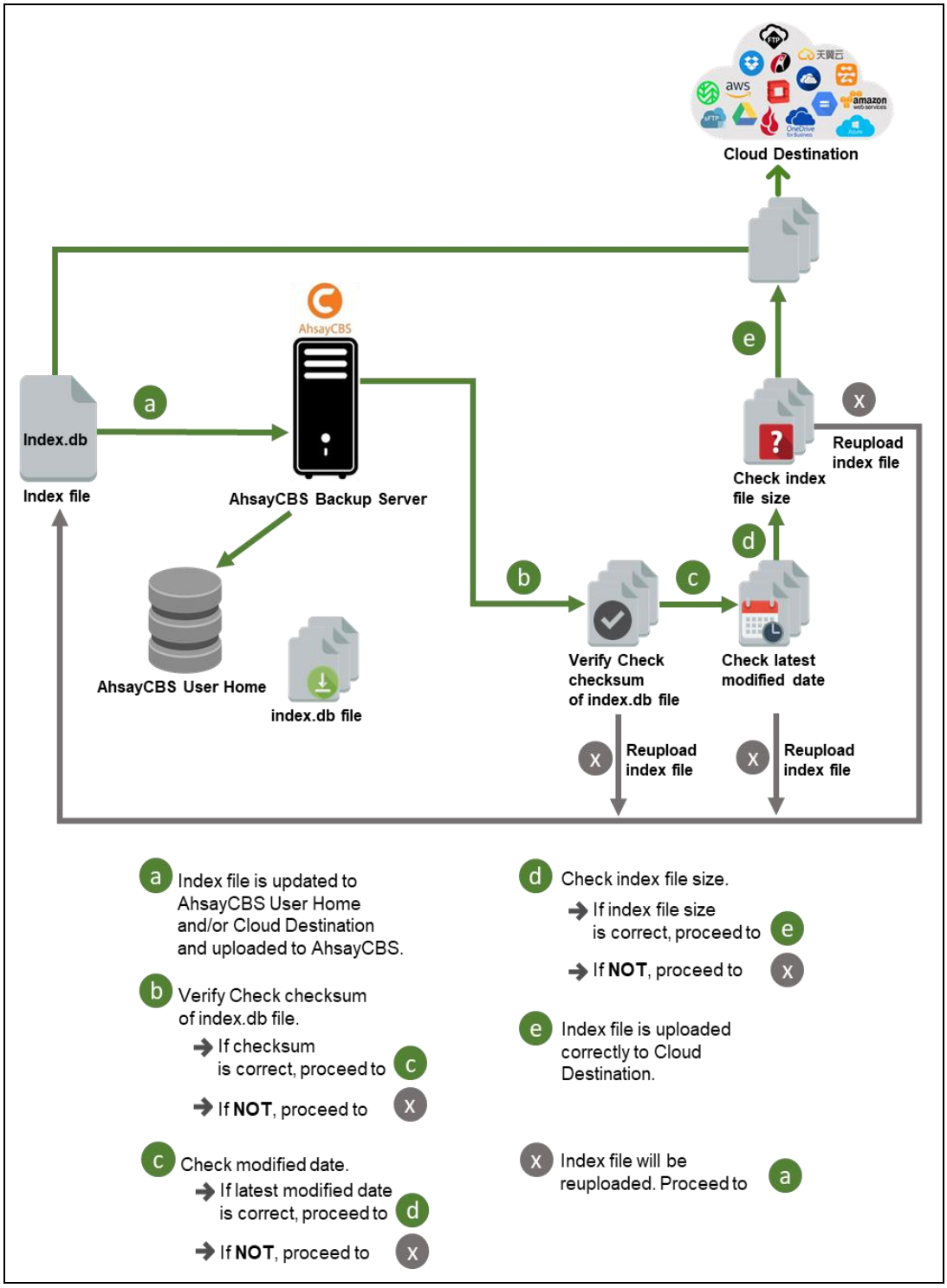
4.2 Backup Set Index Handling Process

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.

4.2.1 Start Backup Job

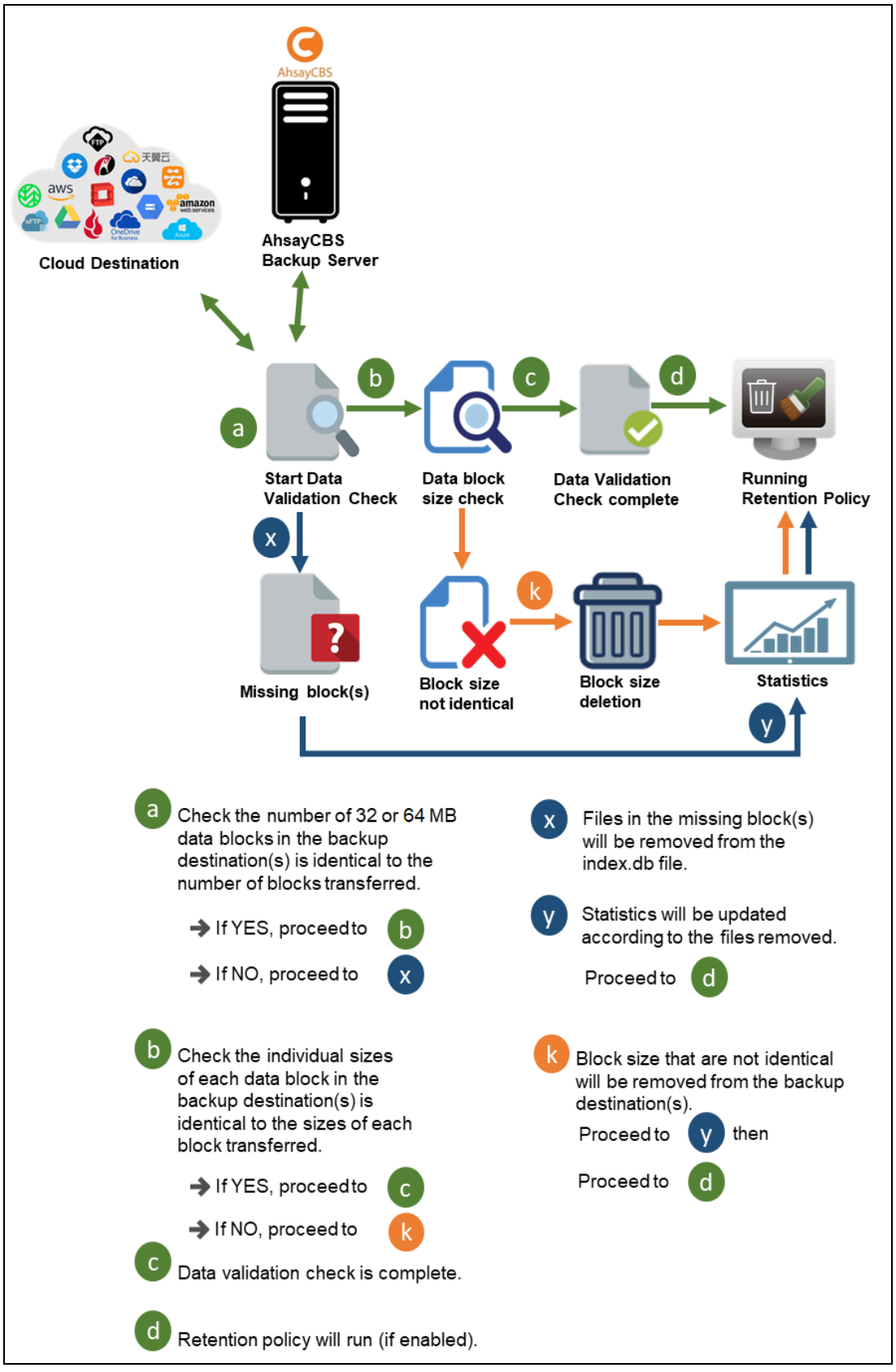


4.2.2 Completed Backup Job



4.3 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 32 or 64 MB data block files and the size of each block file are checked again after the files are transferred.

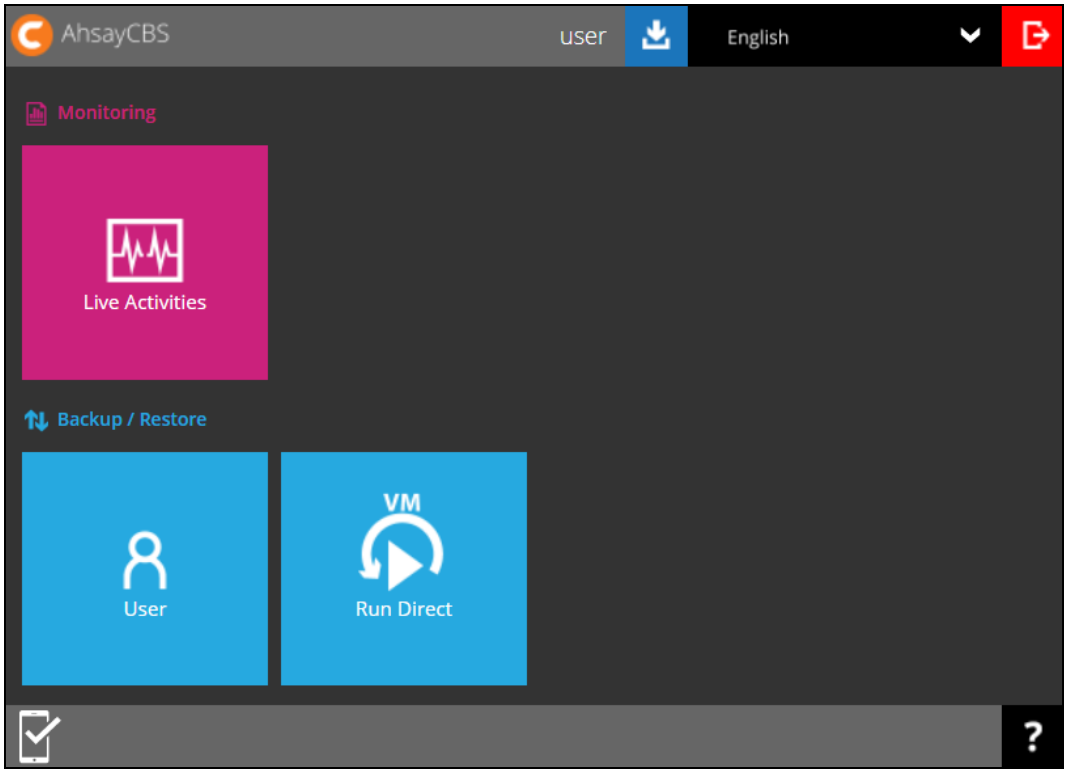


5 Running Backup Job

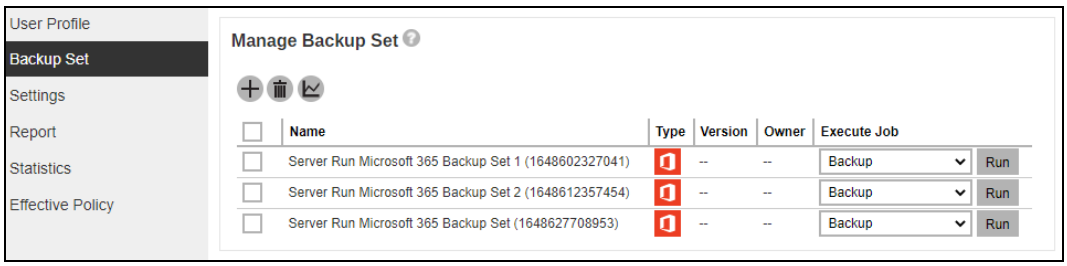
1. Log in to the User Web Console.

   For instructions on how to do this please refer to Chapter 2 of the AhsayCBS v9 User Guide.

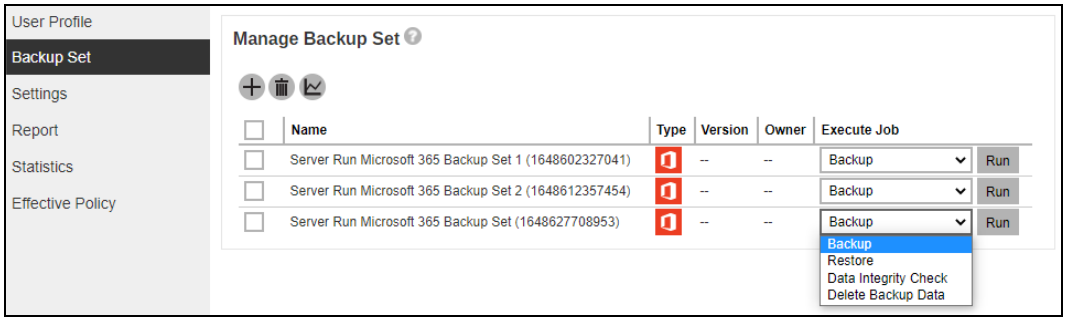
2. Click on the **User** icon.



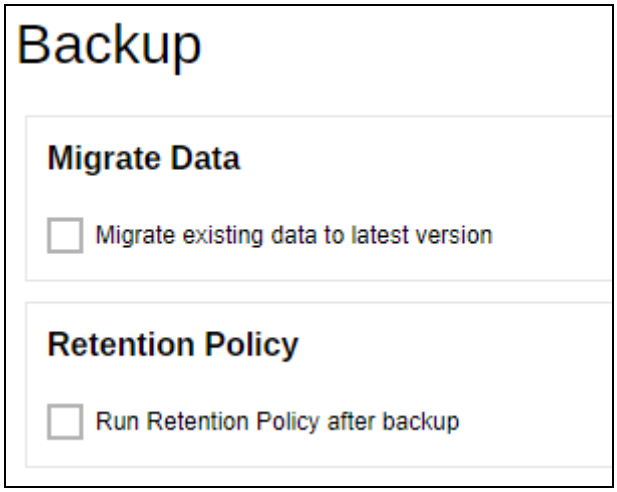
3. Under the **Backup Set** > **Manage Backup Set** menu, you should see the backup set you have created.



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**.



5. Check the **Migrate Data** and **Retention Policy** settings if necessary.



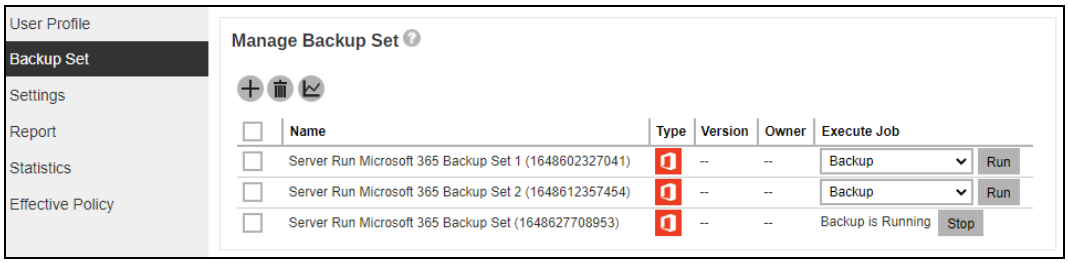
NOTE

Migrate Data will only be available if Deduplication is enabled for the backup set. Deduplication settings may be modified in Backup / Restore > User > Backup Set > %Backup Set Name% > Deduplication.

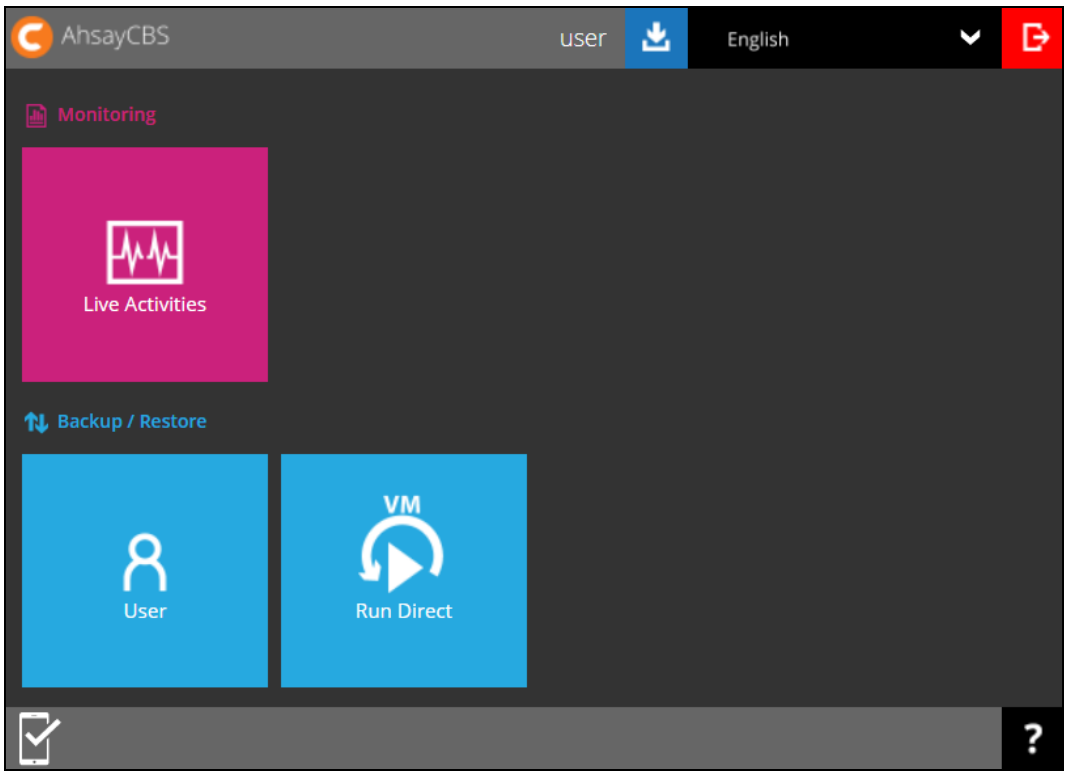
When the Migrate Data option is enabled, the existing data will be migrated to the latest version during a backup job. Backup job(s) for backup sets with Migrate Data enabled may take longer to finish. For more information about this feature, refer to AhsayCBS v9 New Features Supplemental document.

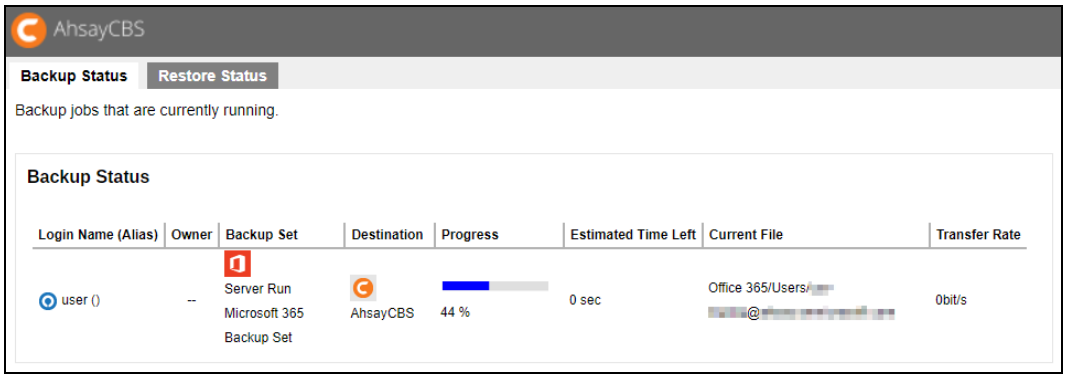
6. Click to start the backup.

7. You will see the status showing **Backup is Running** when the backup is in progress.



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



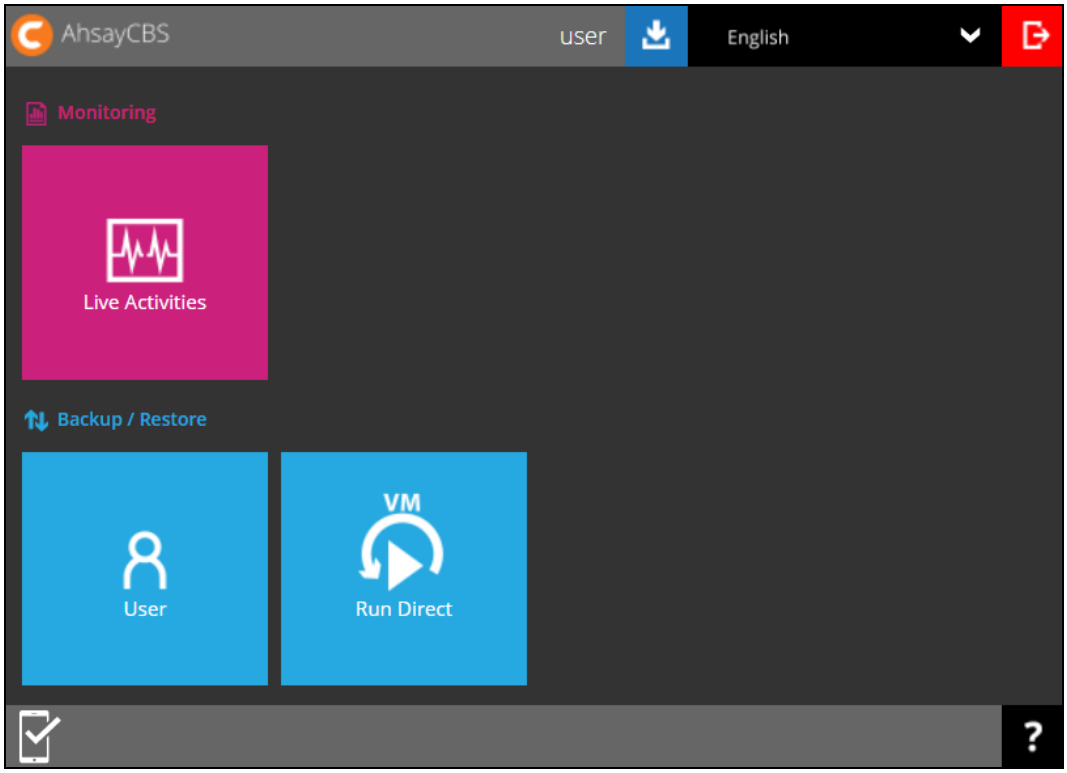


6 Restoring Microsoft 365 Backup Set

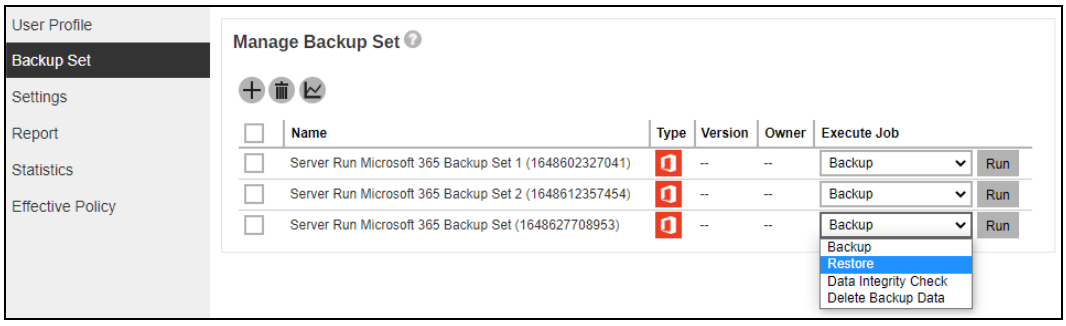
1. Log in to the User Web Console.

   For instructions on how to do this please refer to Chapter 2 of the AhsayCBS v9 User Guide.

2. Click on the **User** icon.

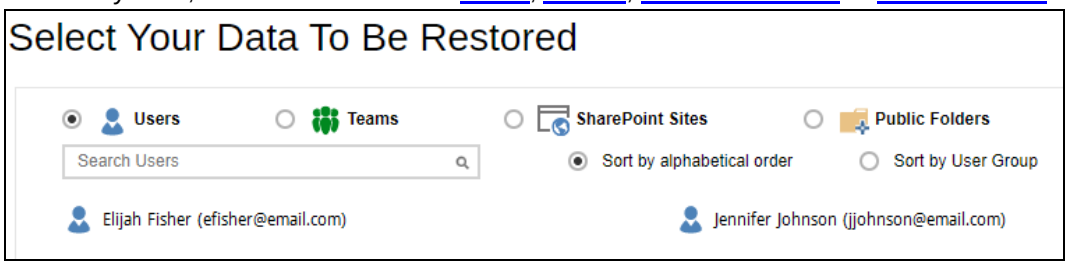


3. You should see the backup set you would like to restore under **Backup Set** > **Manage Backup Set**. Click on the drop-down menu on the backup set you would like to restore, then select **Restore** and click **Run**.

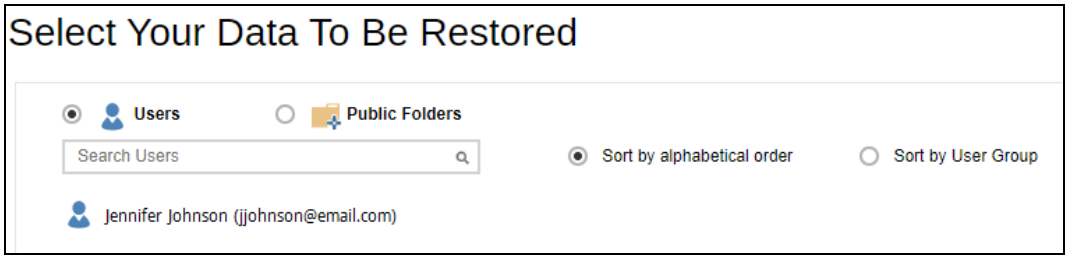


4. Choose data to be restored.

   For AhsayOBM, select to restore from Users, Teams, SharePoint Sites or Public Folders.



While for AhsayACB, select to restore from Users or Public Folders.



NOTE

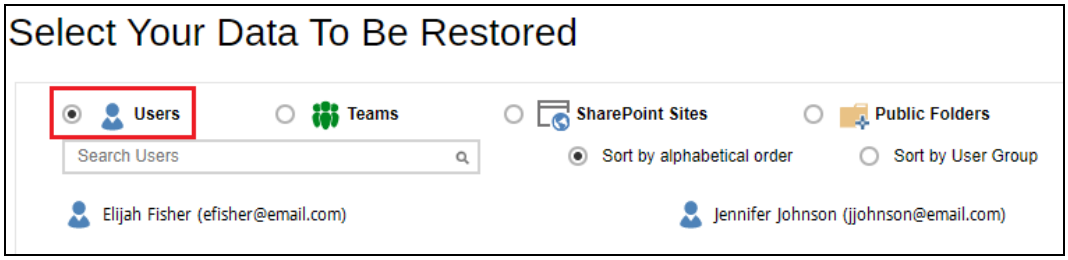
Choices for data to be restored will depend on the data that was backed up. Only one type of data can be restored at a time, e.g. if you choose to restore Users and Teams you can restore Users first then after the restore process, do the restore for Teams next.

From Users

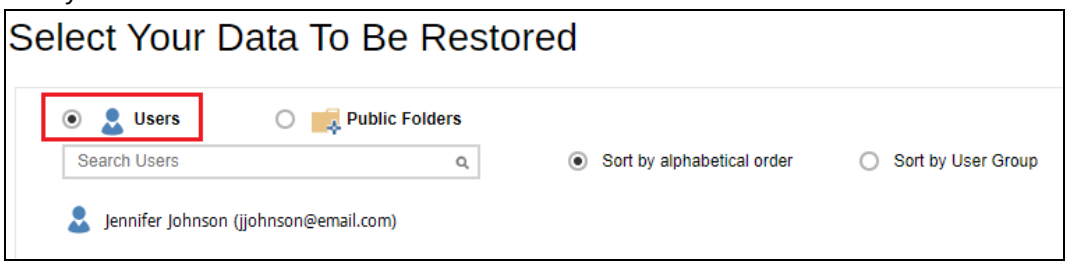
Users can be sorted alphabetically or by User Group. There is also a search function if there are many Users listed. Click on the user that will be restored.

Here are sample screenshots for:

AhsayOBM

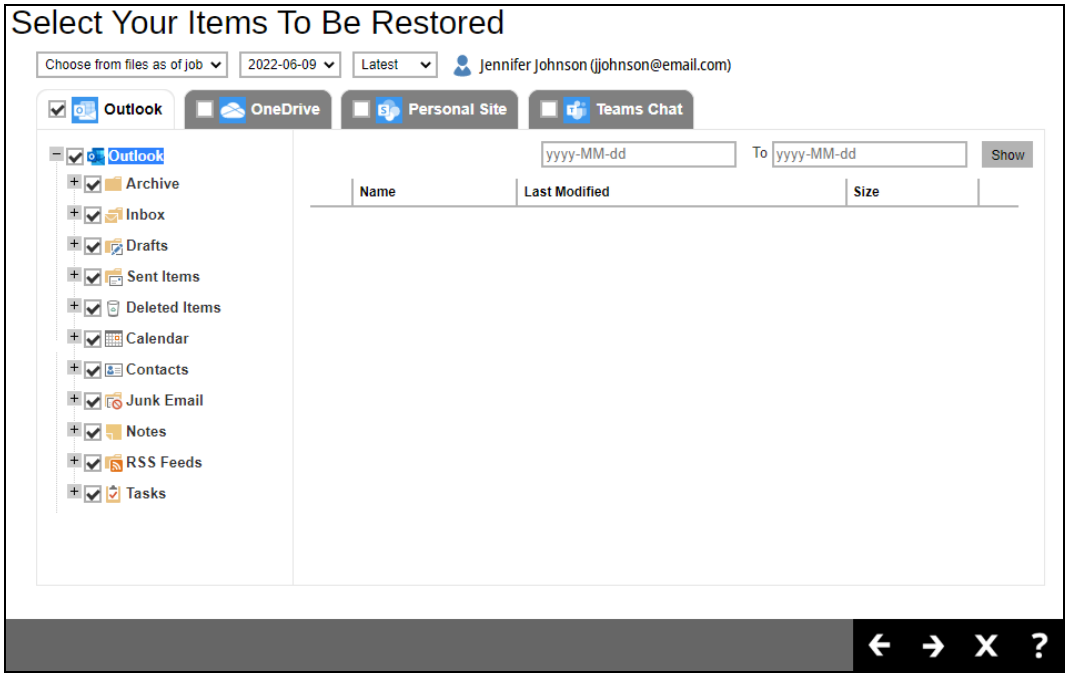


AhsayACB

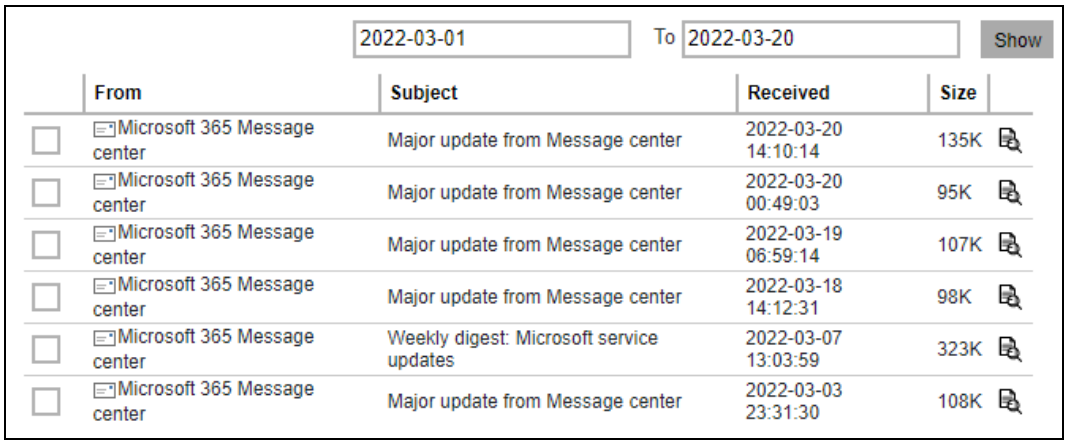


Select the item(s) you would like to restore. You can also choose to restore backed up file from a specific backup job of your choice using the drop-down menu at the top.

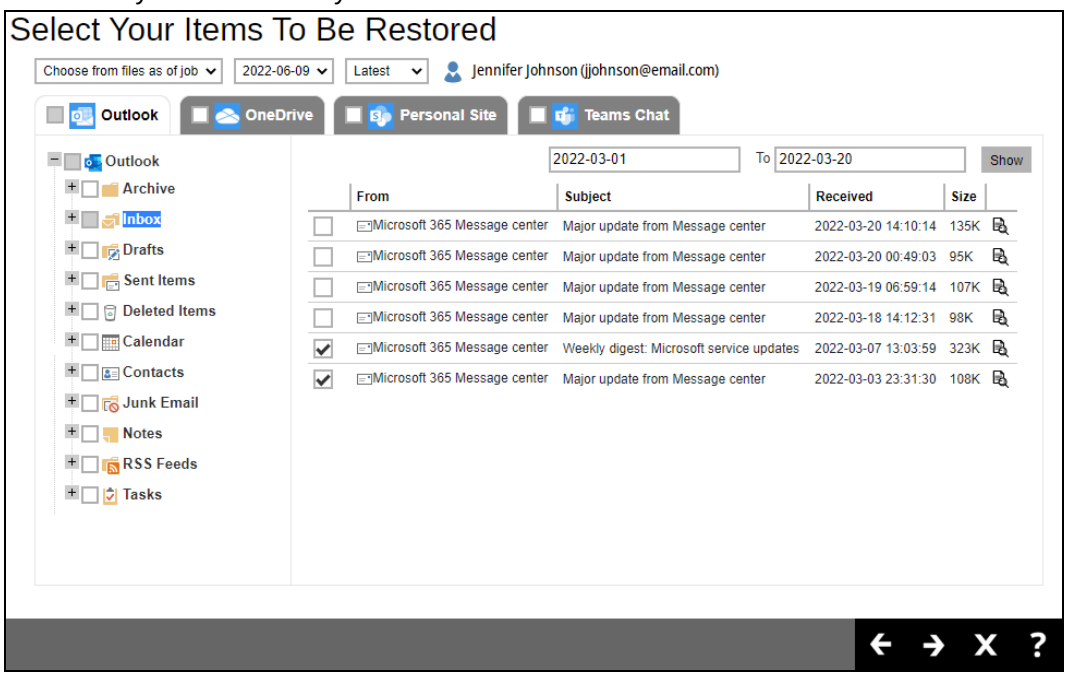
If the checkbox beside Outlook is ticked, then all the items under Outlook will be restored.



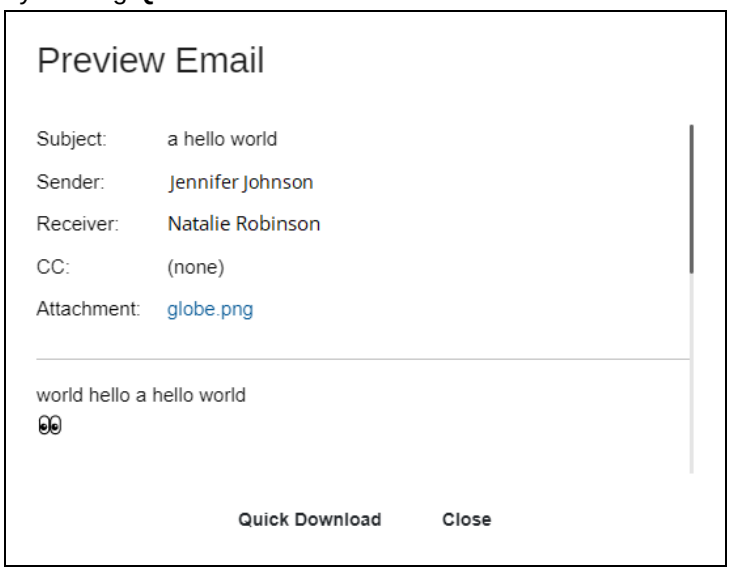
Items can also be filtered according to the received date. Set the From and To dates of the items then click **Show**.

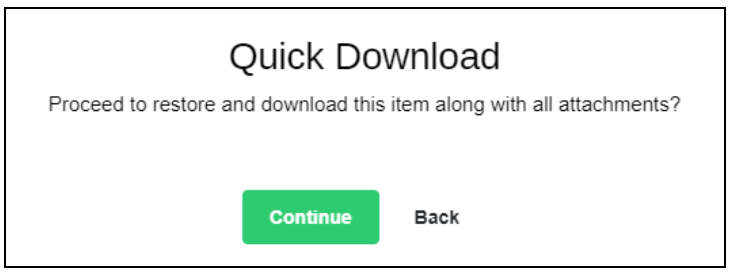


Specific items can also be selected. There is a preview function that will let you see the content so you can check if you want to restore it.

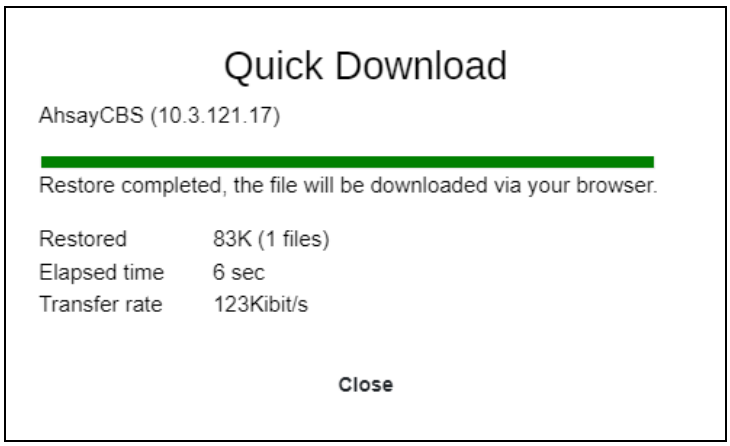


To do this click . In the Preview Email window you can restore and download the email by clicking **Quick Download** then **Continue**.

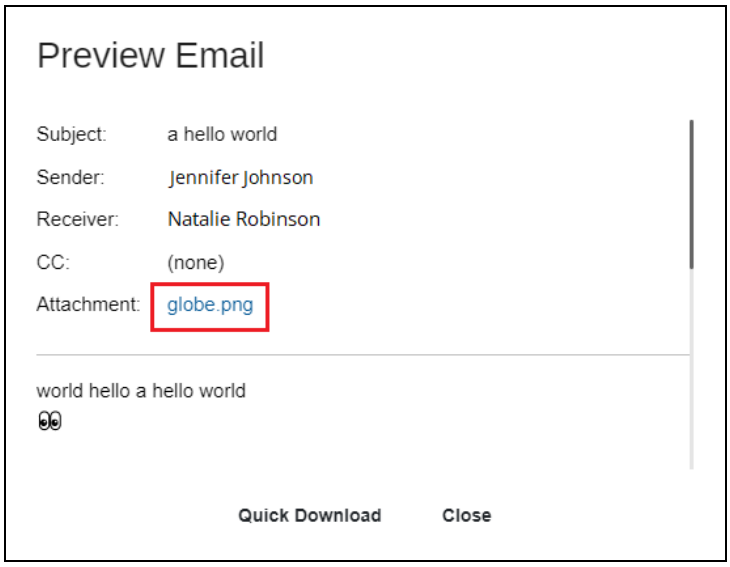




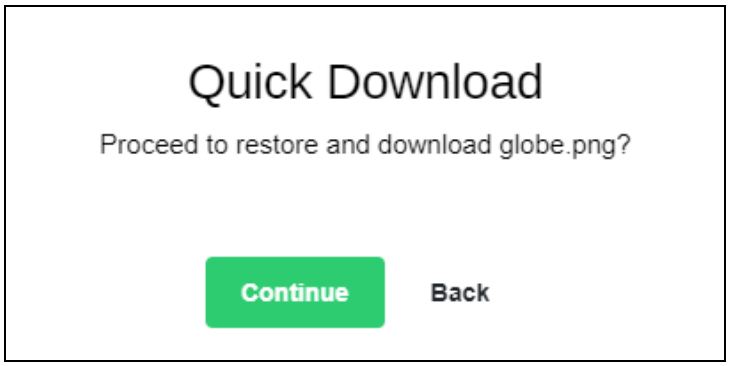
After the download is complete, a zip file will be created that contains the file. Click **Close** once done.



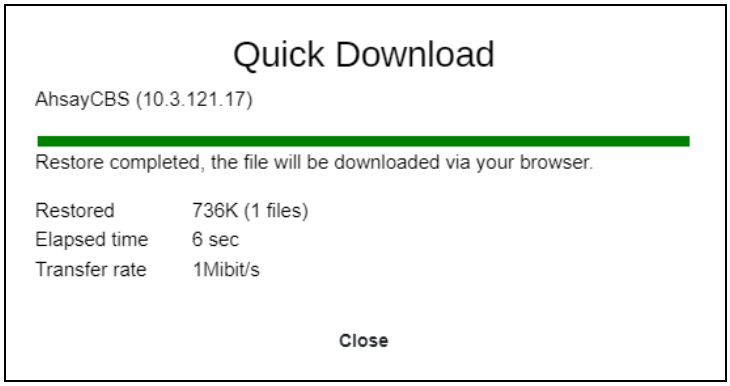
You can also download just the attachment by clicking on the attachment itself.



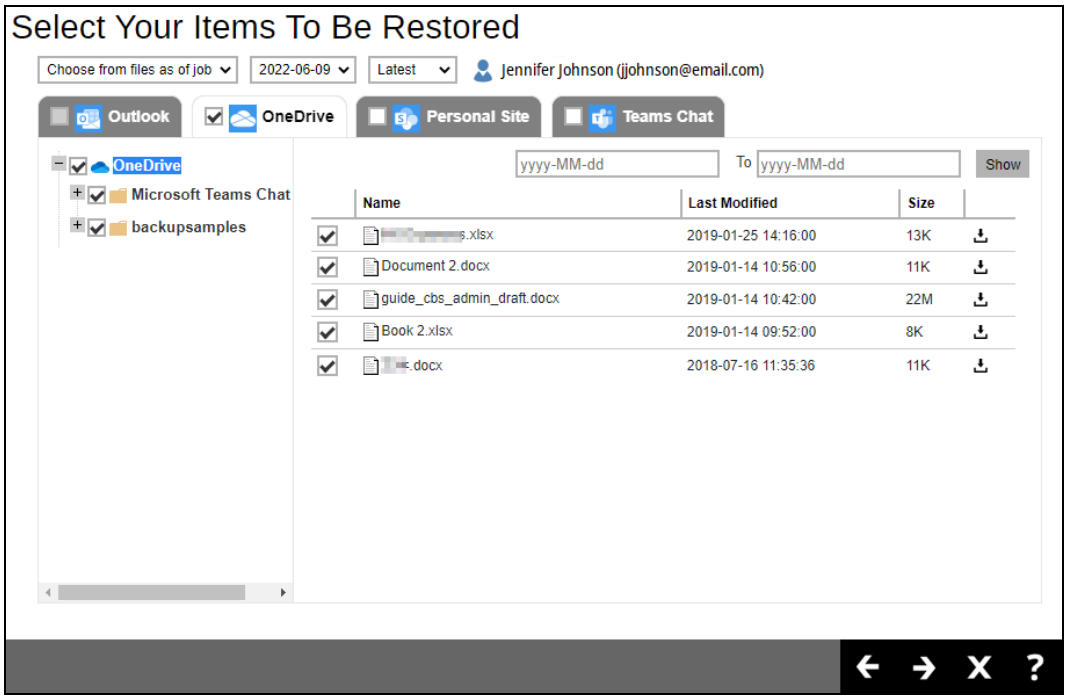
Click **Continue** to proceed.



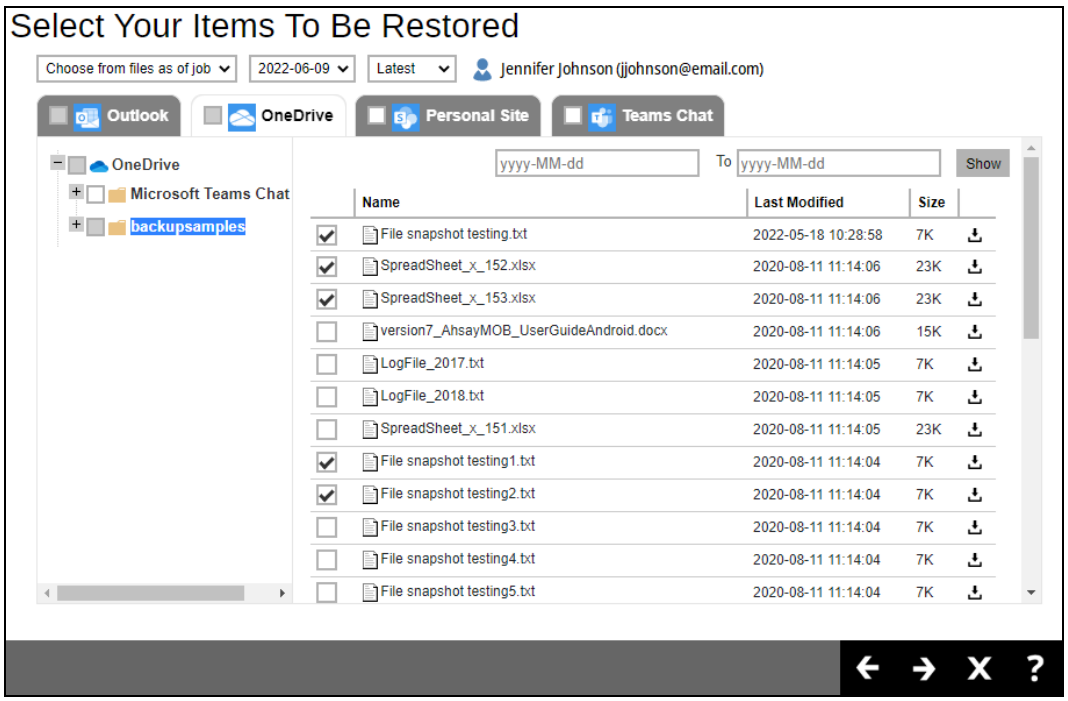
Click **Close** once done.



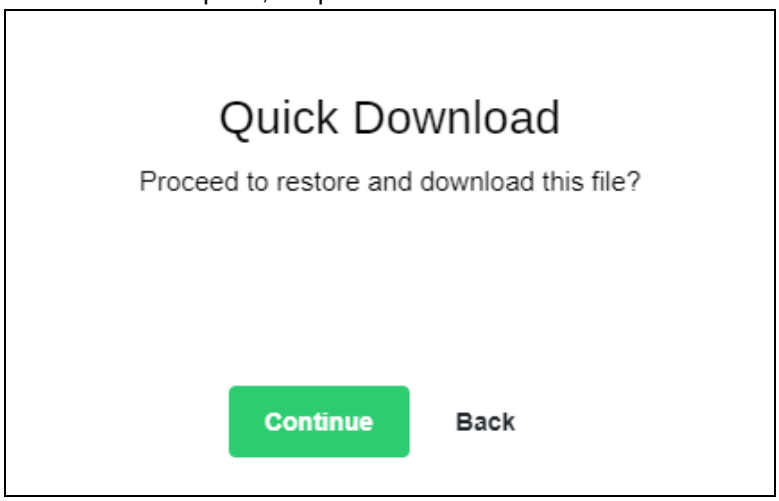
If the checkbox beside OneDrive is ticked, then all the items under OneDrive will be restored.

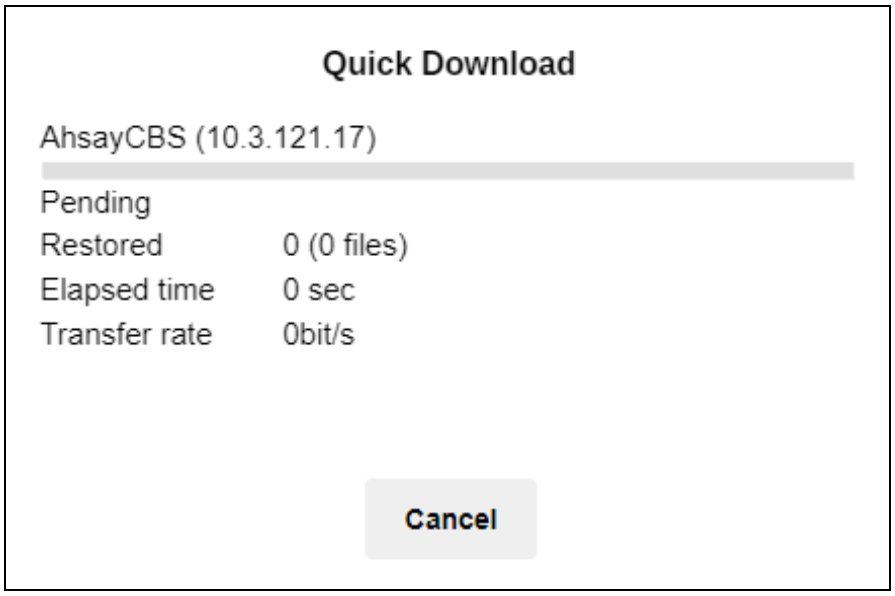


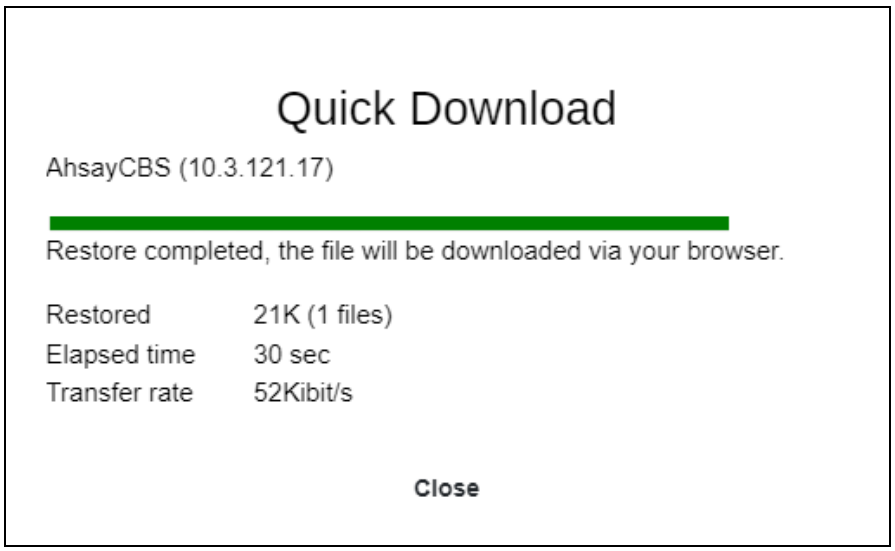
Specific items can also be selected. There is a download function that will let you download the item.



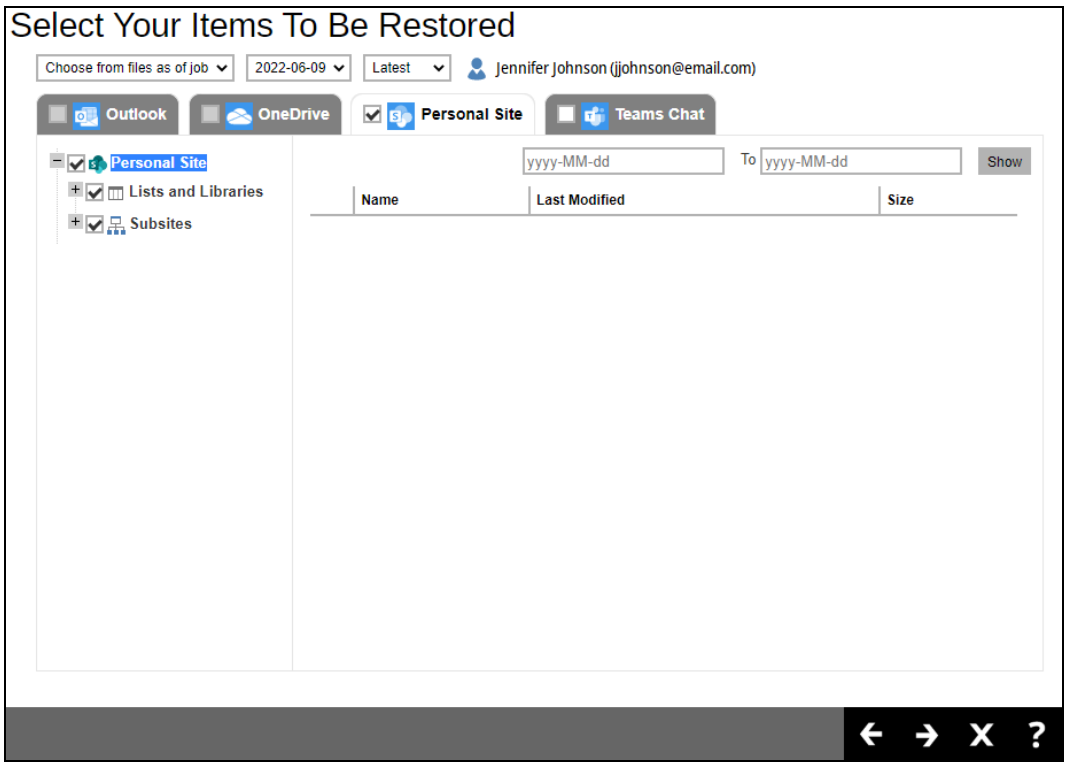
Click to download the item. Click **Continue** to start the download and restore. After the download is complete, a zip file will be created that contains the file.



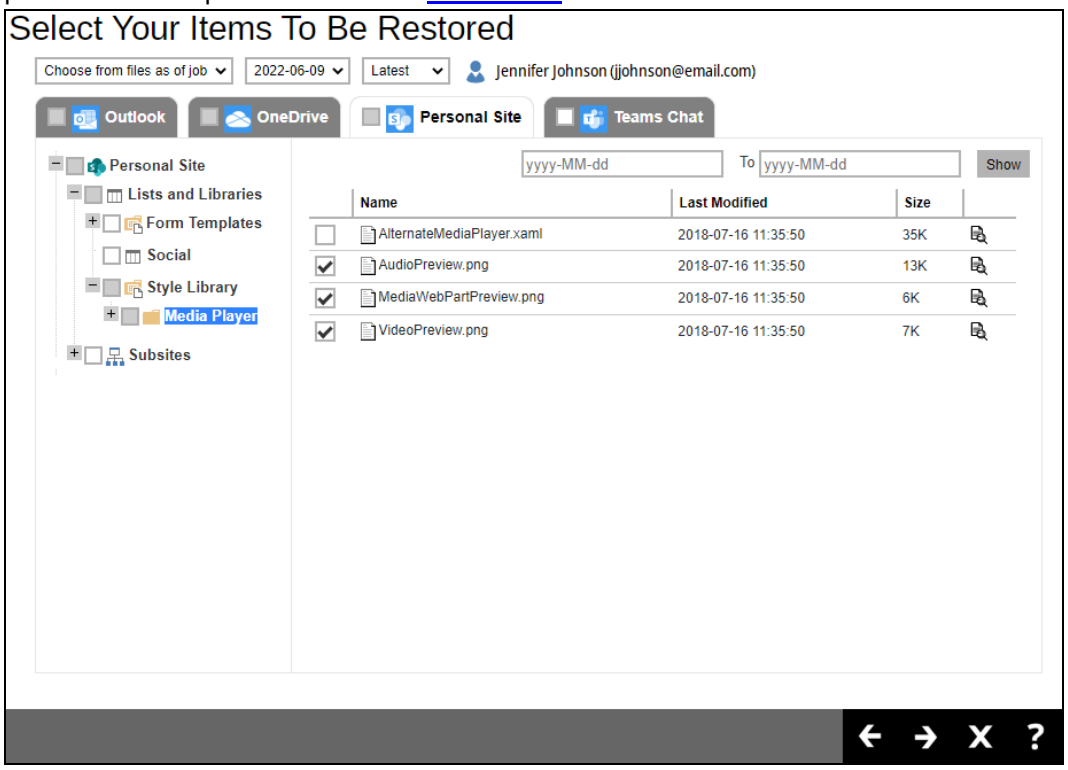

Quick Download
AhsayCBS (10.3.121.17)
Pending
Restored 0 (0 files)
Elapsed time 0 sec
Transfer rate 0bit/s
Cancel


Quick Download
AhsayCBS (10.3.121.17)
Restore completed, the file will be downloaded via your browser.
Restored 21K (1 files)
Elapsed time 30 sec
Transfer rate 52Kibit/s
Close

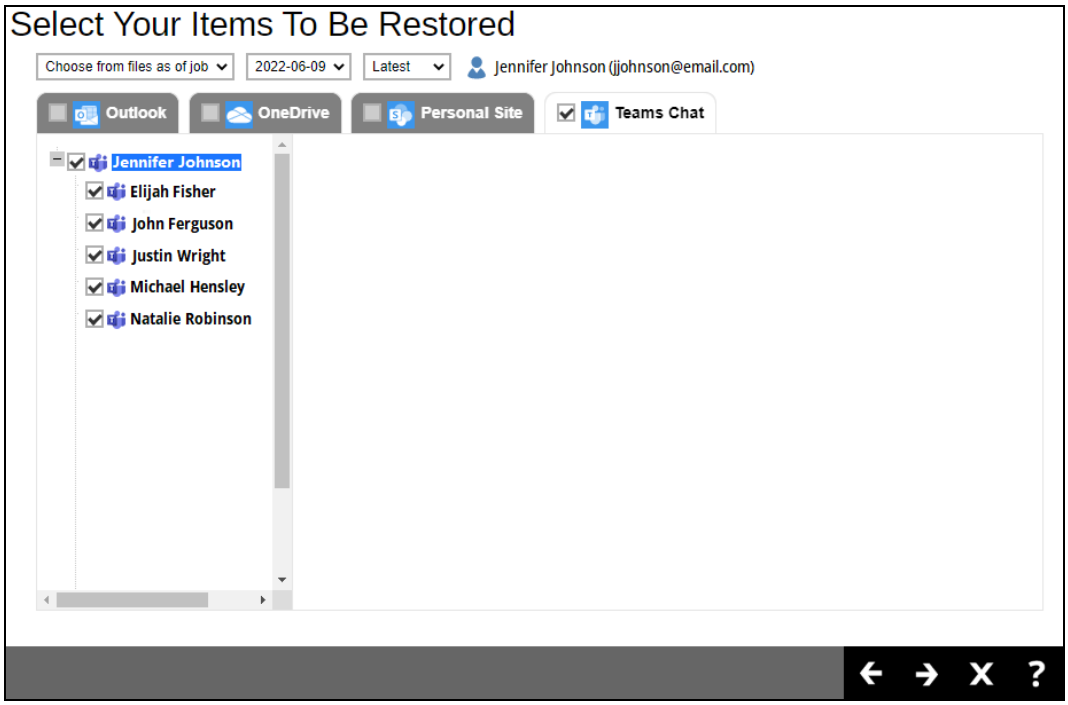
If the checkbox beside Personal Site is ticked, then all the items under Personal Site will be restored.



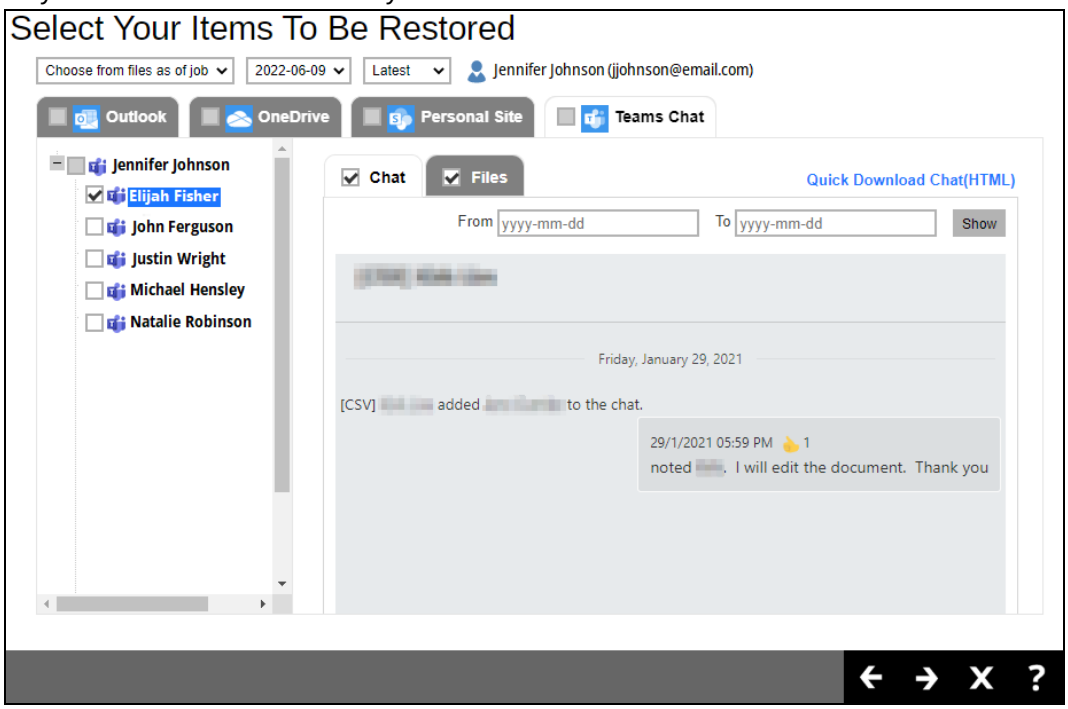
Specific items can also be selected. There is a preview function that will let you see the content so you can check if you want to restore it. For instructions on how to use the preview function please refer to the instructions discussed above.



If the checkbox beside Teams Chat is ticked, then all the items under Teams Chat will be restored.



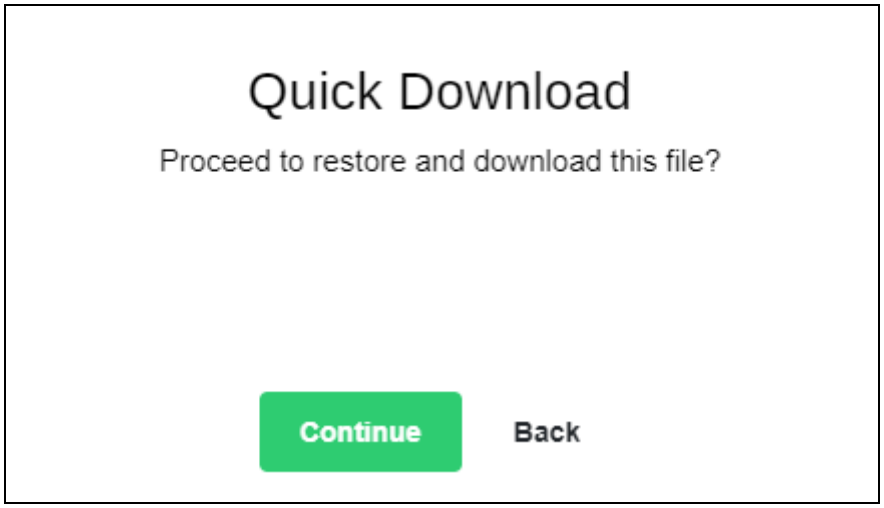
Specific items can also be selected to be restored. There is a download function that will let you download the chat directly. Click the Quick Download Chat(HTML) link.

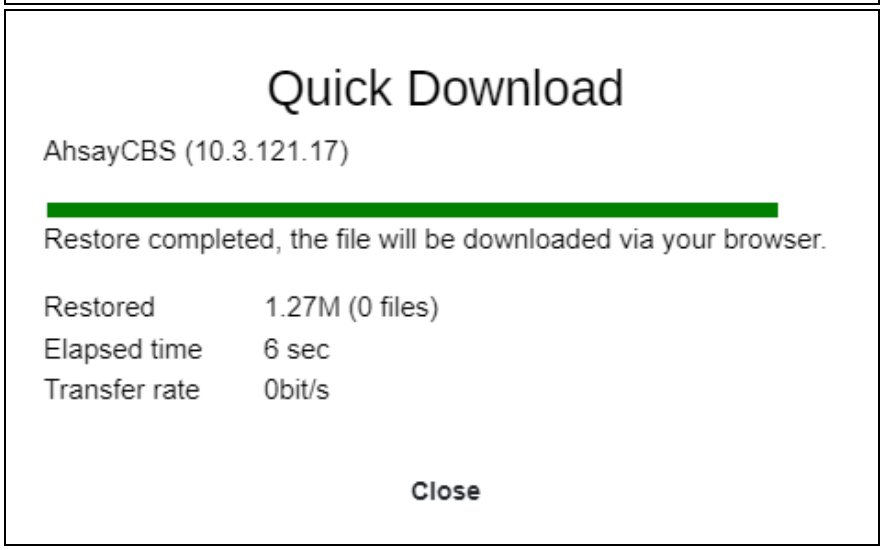


NOTE

Teams chat will not be restored to the original thread. Instead, it will only be restored as data export in HTML format stored in the local machine or OneDrive.

Click **Continue** to start the download and restore. Click **Close** once done.

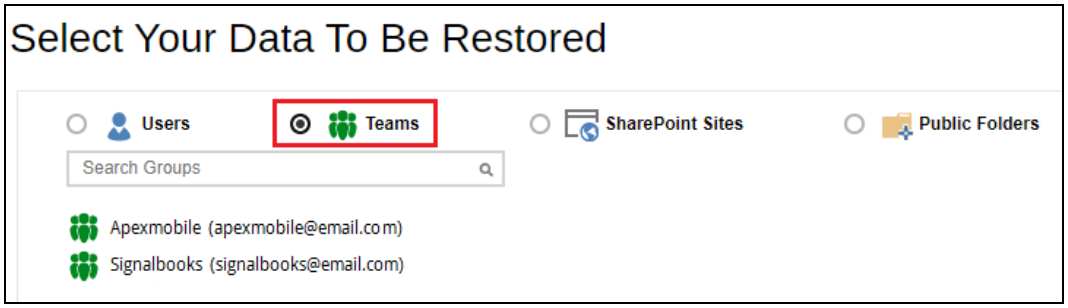




Click to proceed.

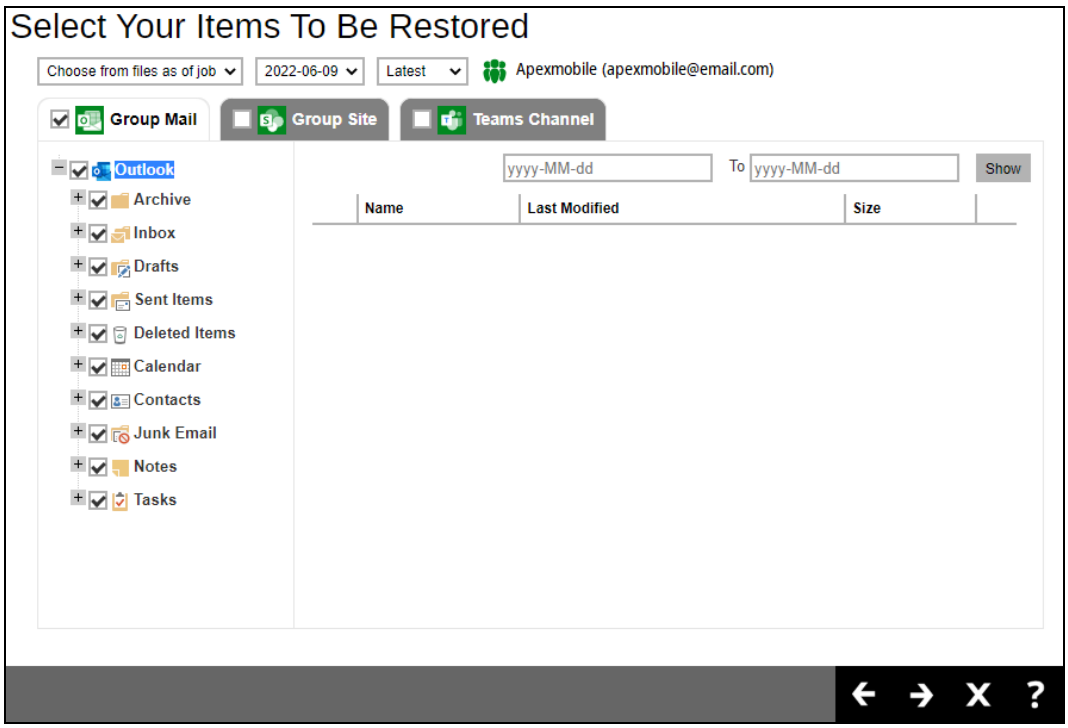
From Teams

Click on the Group that will be restored. There is also a search function if there are many Groups listed.

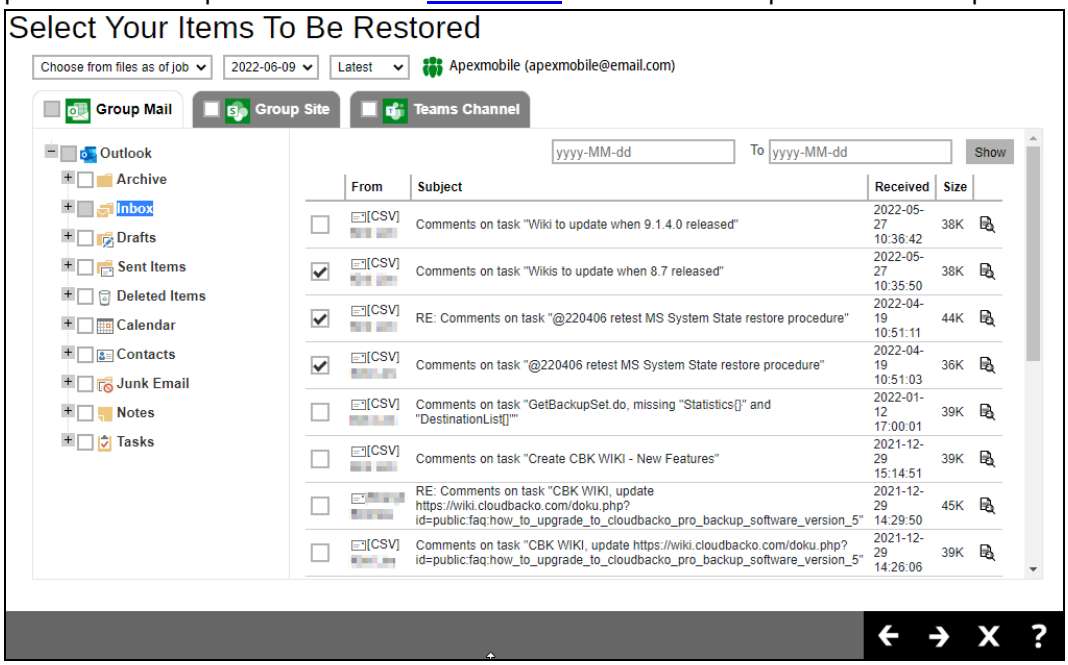


Select the item(s) you would like to restore. You can also choose to restore backed up file from a specific backup job of your choice using the drop-down menu at the top.

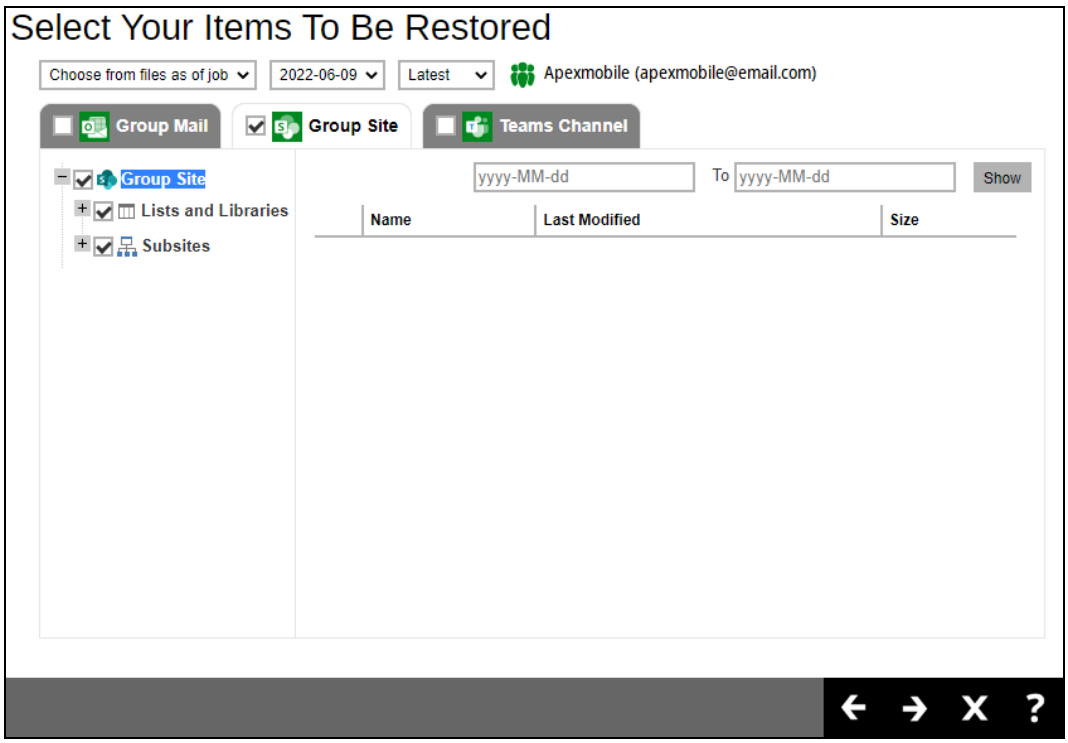
If the checkbox beside Group Mail is ticked, then all the items under Group Mail will be restored.



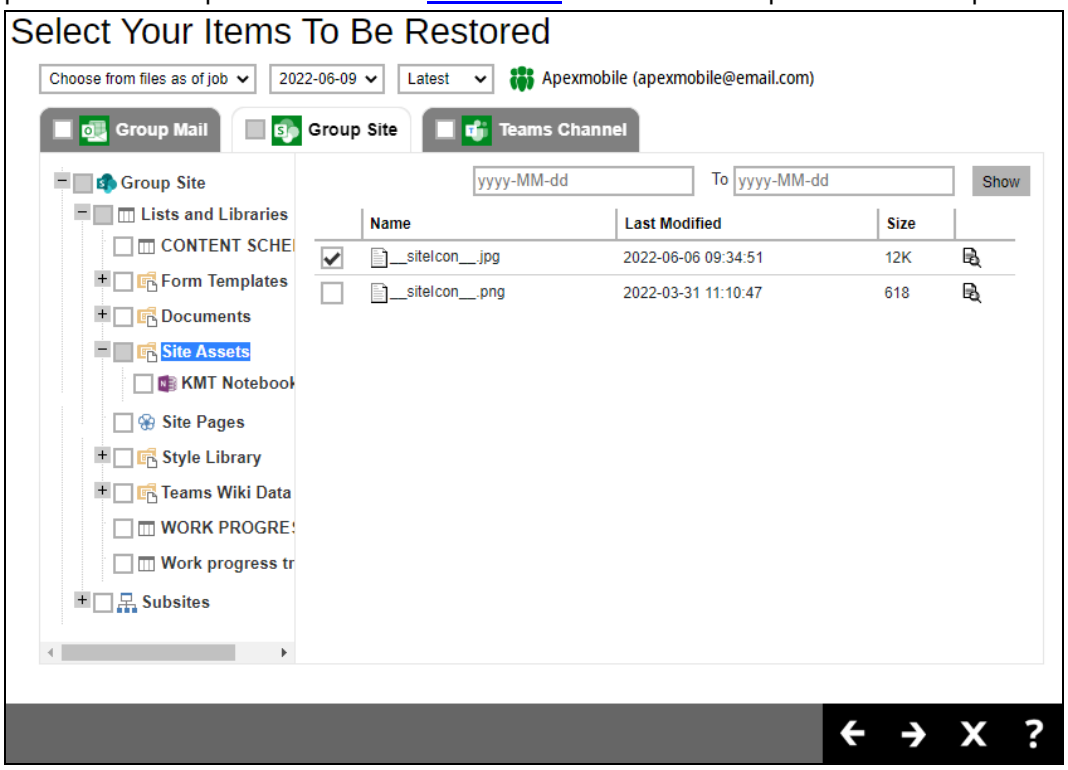
Specific items can also be selected. There is a preview function that will let you see the content so you can check if you want to restore it. For instructions on how to use the preview function please refer to the instructions discussed in the previous sub-chapter.



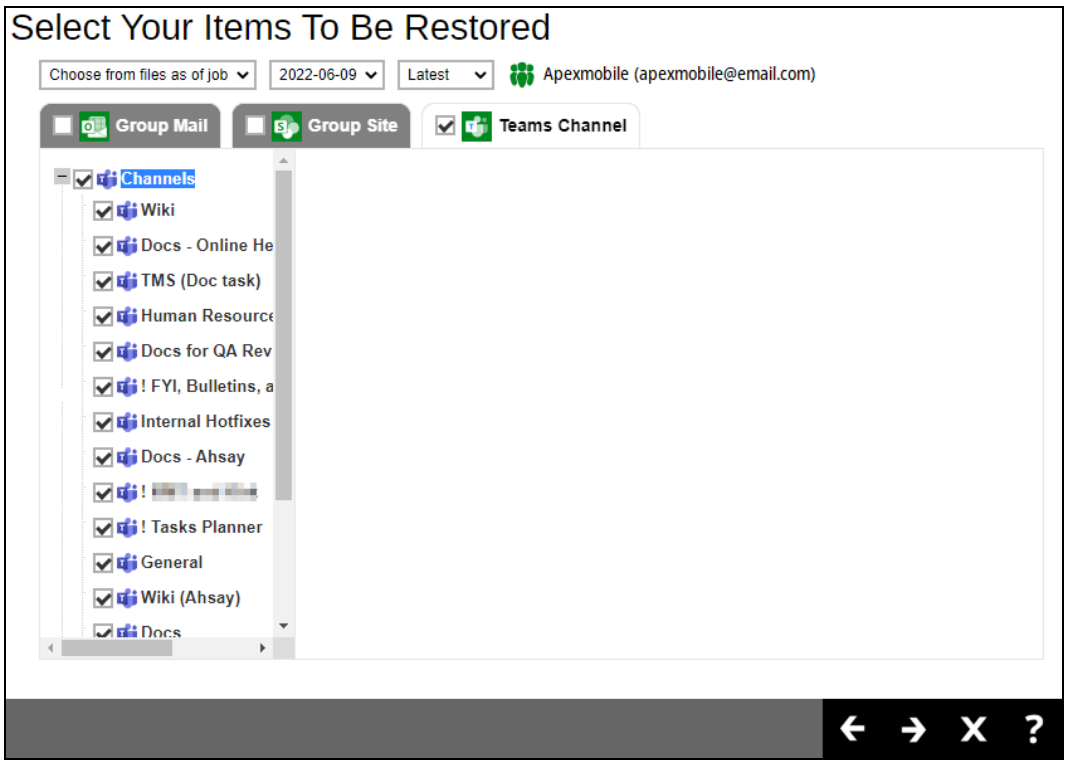
If the checkbox beside Group Site is ticked, then all the items under Group Site will be restored.



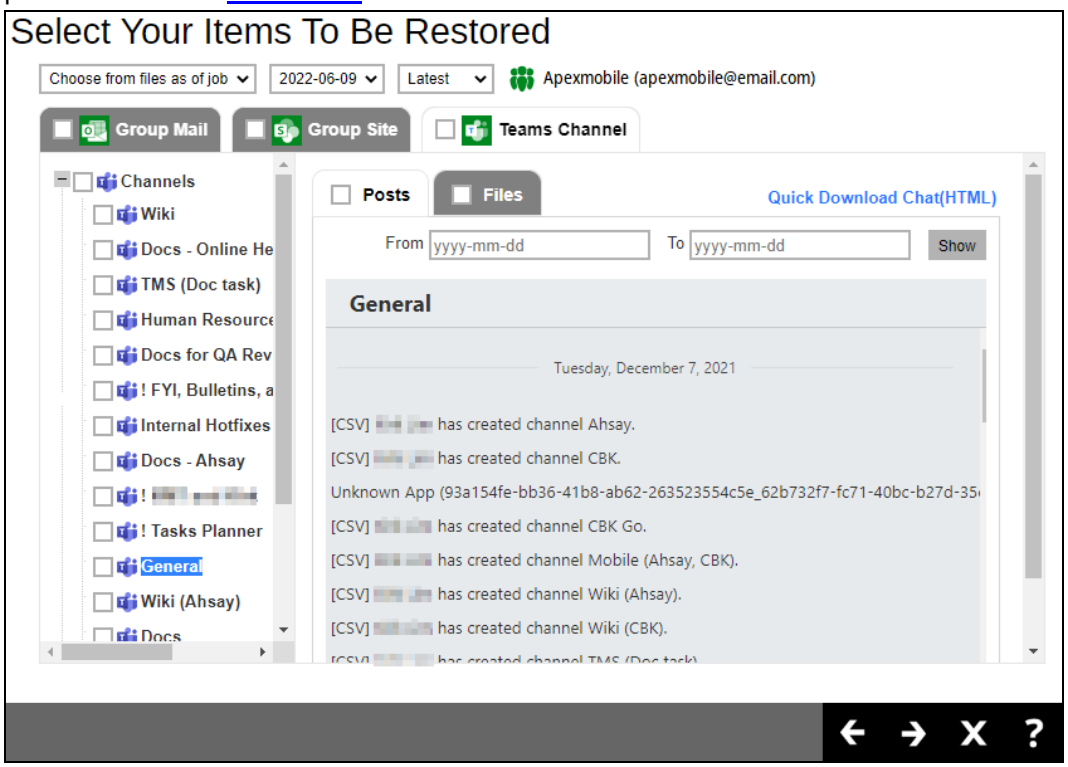
Specific items can also be selected. There is a preview function that will let you see the content so you can check if you want to restore it. For instructions on how to use the preview function please refer to the instructions discussed in the previous sub-chapter.



If the checkbox beside Teams Channel is ticked, then all the items under Teams Channel will be restored.



Specific items can also be selected to be restored. There is a download function that will let you download the item directly. For instructions on how to use the download function please refer to the instructions discussed above.

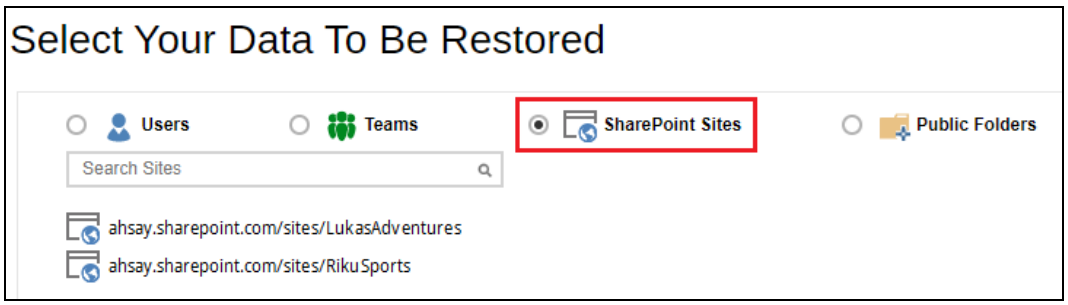


NOTE

Posts in Teams Channel will not be restored to the original thread. Instead, it will only be restored as data export in HTML format stored in the local machine or OneDrive.

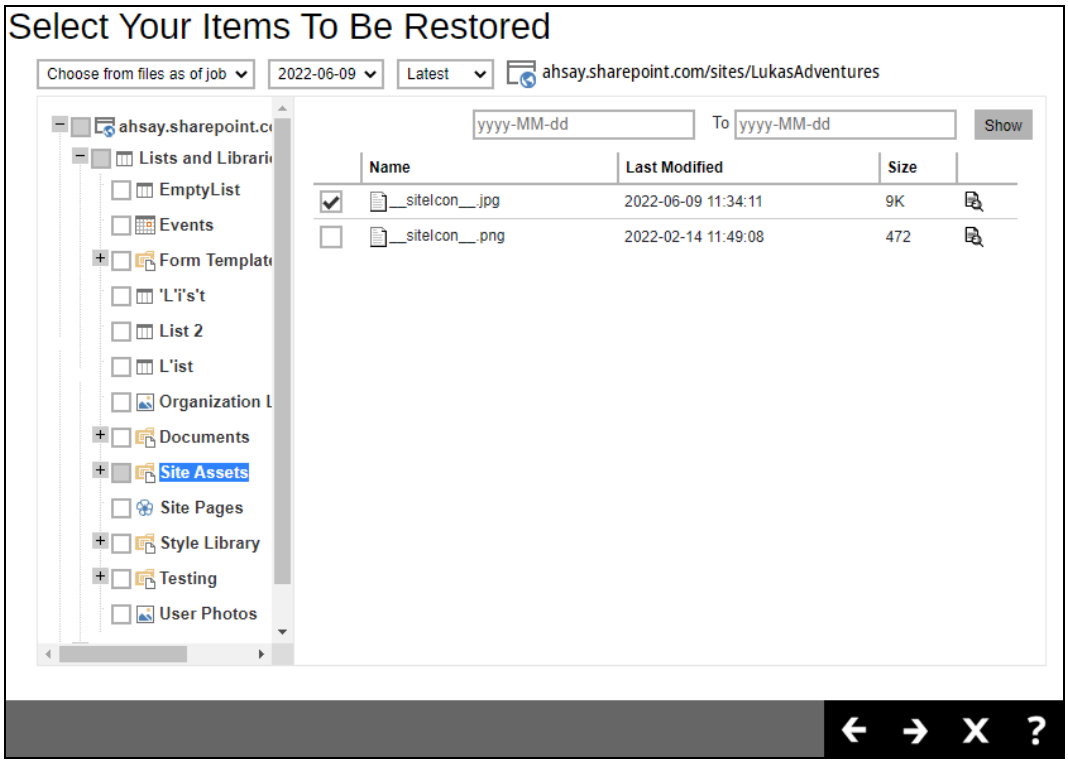
From SharePoint Sites

Click on the Sites that will be restored. There is also a search function if there are many Sites listed.



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 drop-down menu at the top.

There is a preview function that will let you see the content so you can check if you want to restore it. For instructions on how to use the preview function please refer to the instructions discussed in the previous sub-chapter.

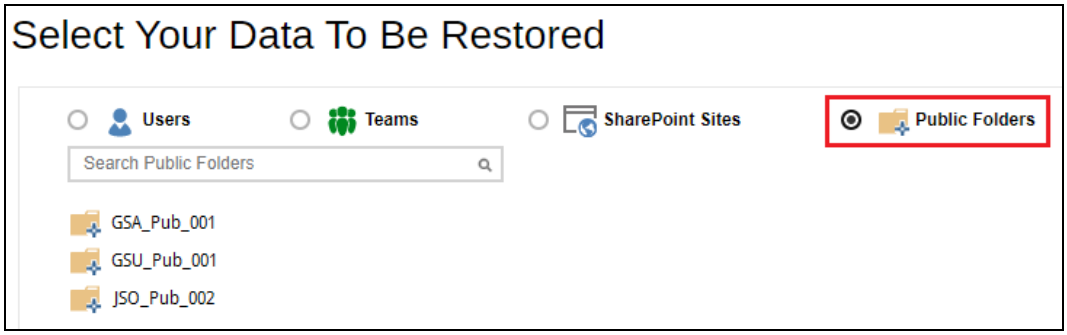


From Public Folders

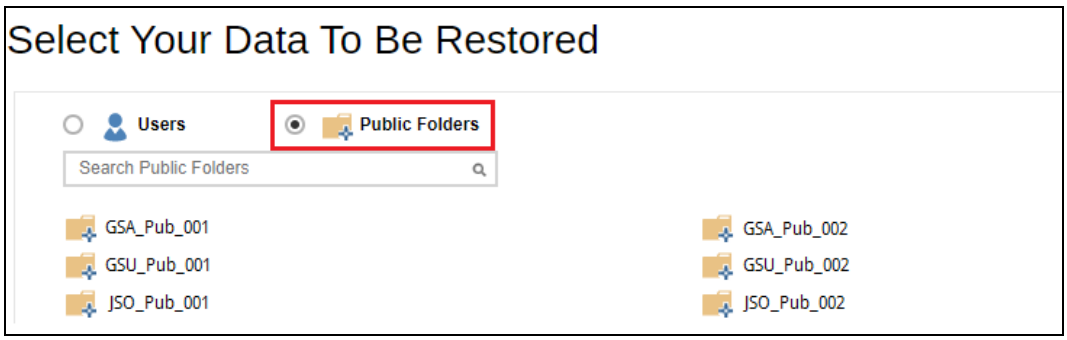
Click on the Public Folder that will be restored. There is also a search function if there are many Public Folders listed.

Here are sample screenshots for:

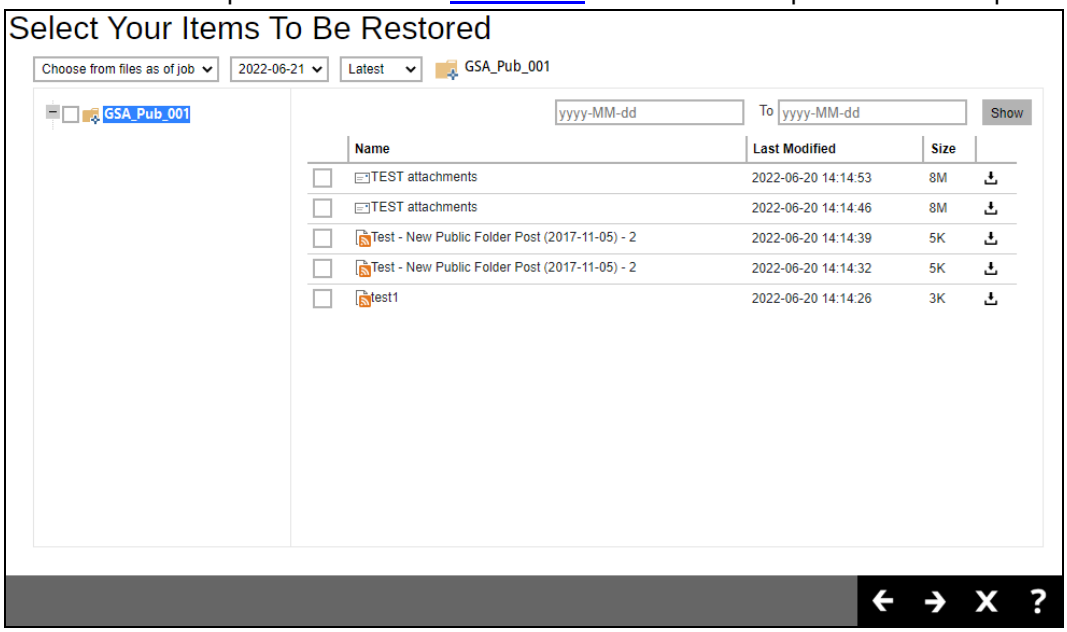
AhsayOBM



AhsayACB

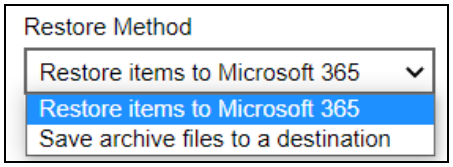


Select the item(s) you would like to restore. You can also choose to restore backed up file from a specific backup job of your choice using the drop-down menu at the top. There is a download function that will let you download the item. For instructions on how to use the download function please refer to the instructions discussed in the previous sub-chapter



5. Select the location where the data will be restored.

   The choices for the restore location that will be displayed depends on the data and restore method selected. There are two restore methods available: Restore items to Microsoft 365 and Save archive files to a destination.



   If Restore items to Microsoft 365 is selected, there are three options for the restore location:

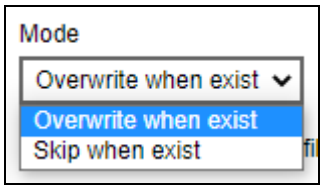
   - Original
   - Alternate
   - Alternate Microsoft 365 organization

   - **Original**

     To restore to Original, select **Original**.

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

     - **Mode**



       There are two choices for the mode:

       - **Overwrite when exist**

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

       - **Skip when exist**

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

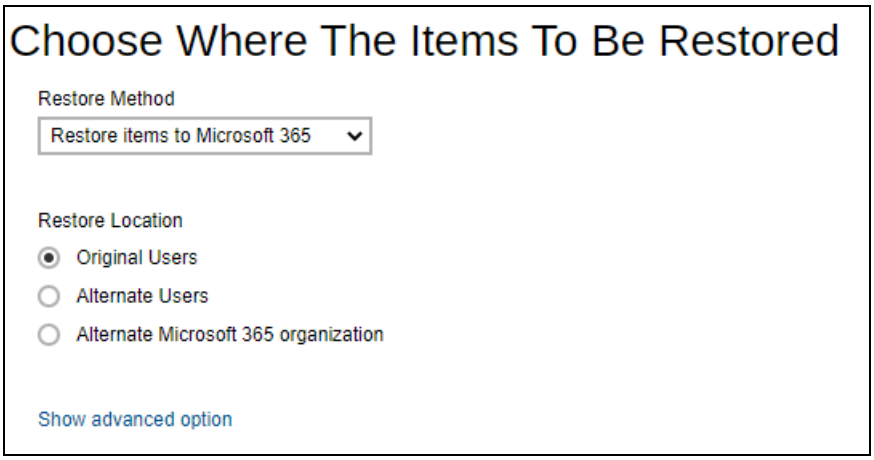
     - **Verify checksum of in-file delta files during restore**

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

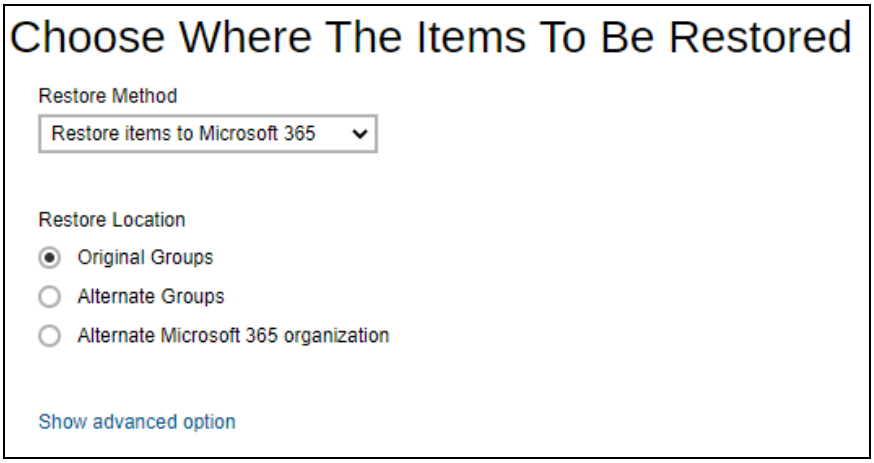
   Click to start the restoration.

Here are examples for the different data types:

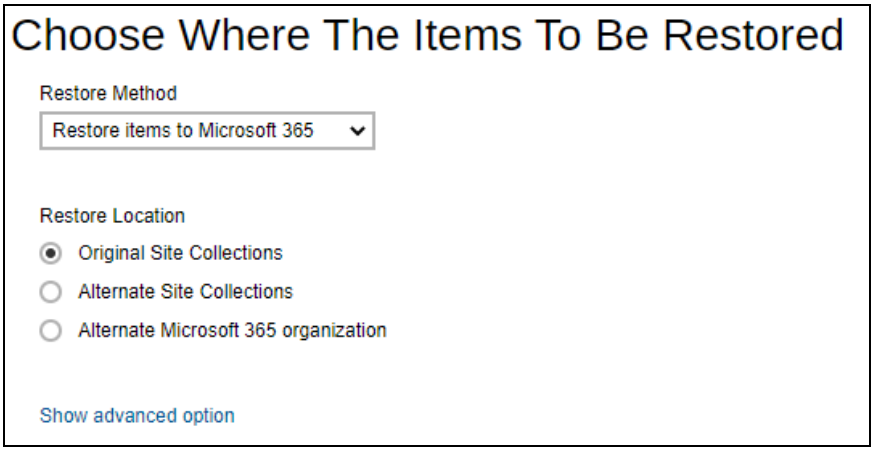
Users



Teams



Sharepoint Sites



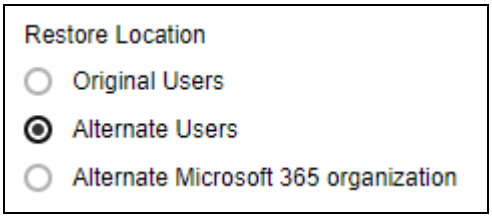
Public Folders

- **Alternate**

To restore to alternate user/group/site/public folder, select **Alternate**.

To configure other restore settings please refer to the instructions discussed above.

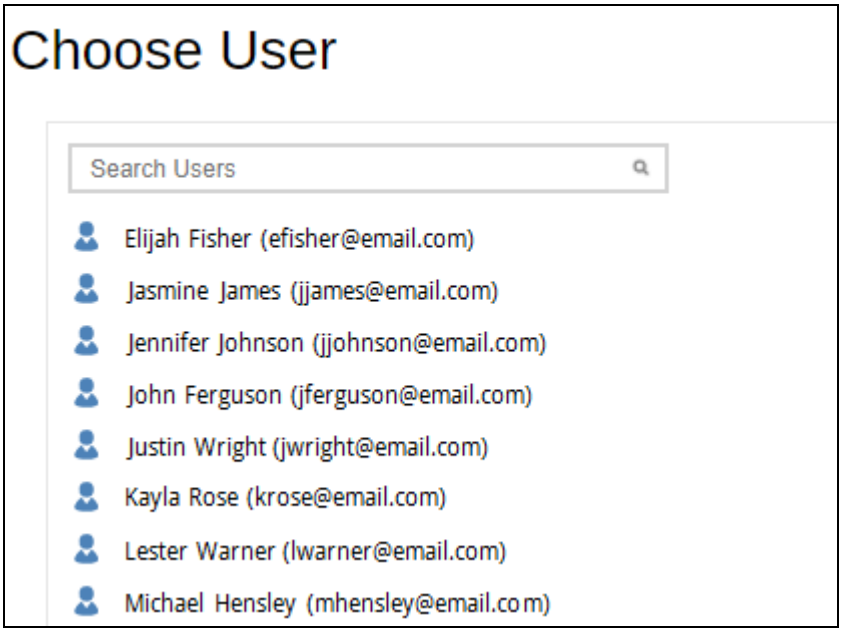
Click to proceed.



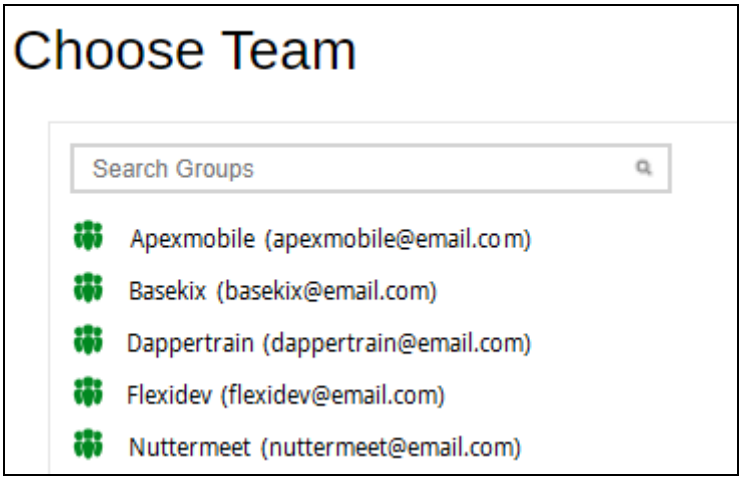
Select the alternate user/group/site then click to start the restoration.

Here are examples for the different data types:

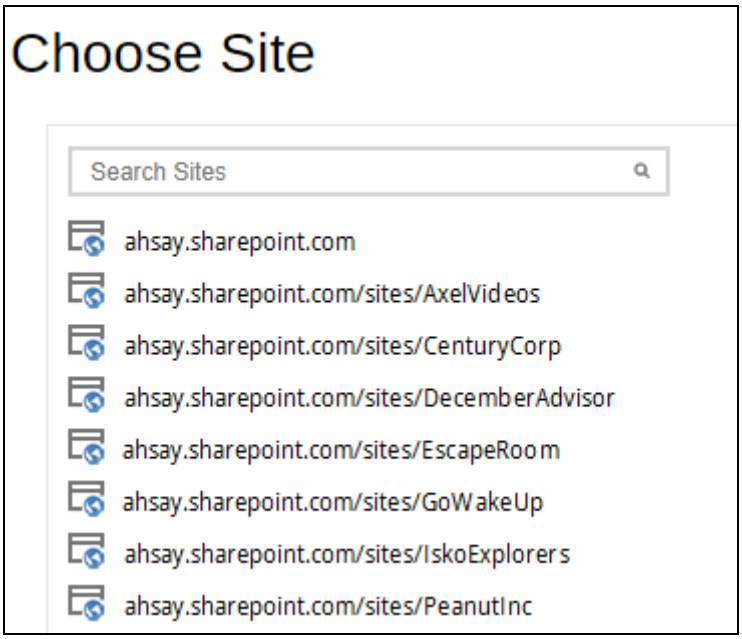
Users



Teams



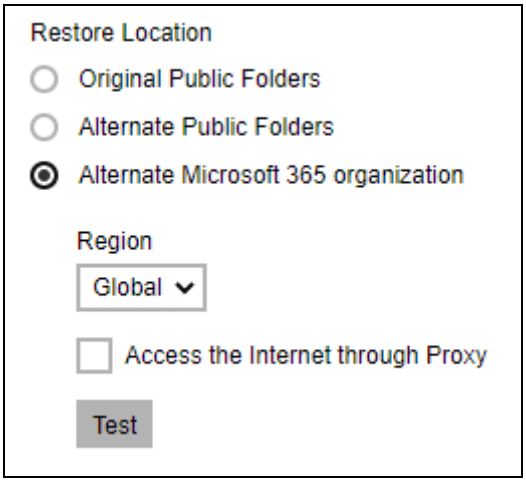
SharePoint Sites



Public Folders

- **Alternate Microsoft 365 organization**

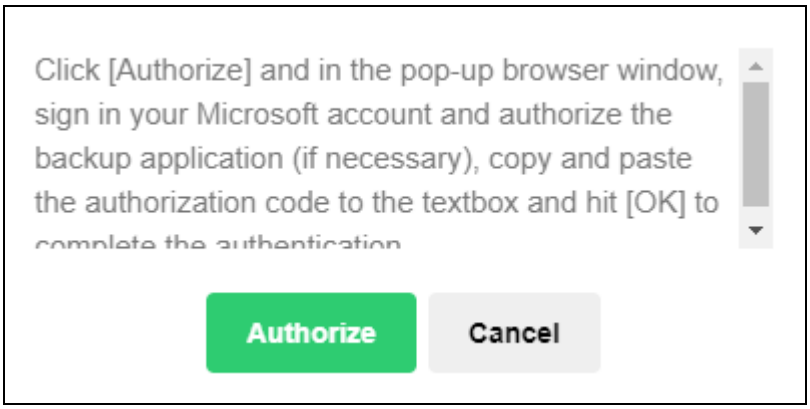
  To restore to an alternate Microsoft 365 organization, select **Alternate Microsoft 365 organization**. Then select the **Region**.



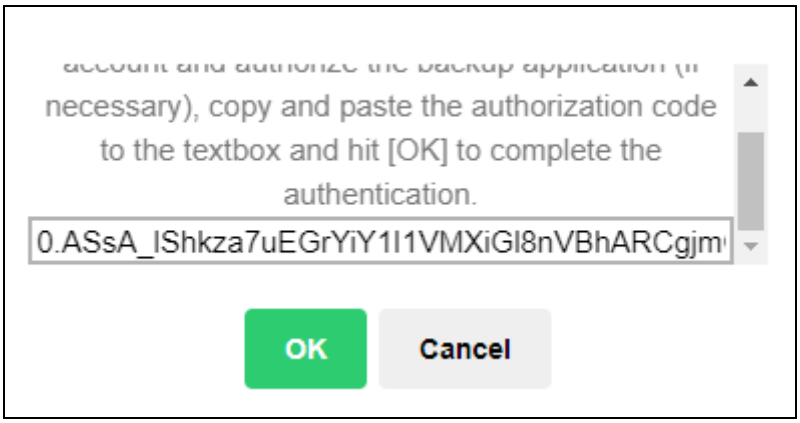
  To configure other restore settings please refer to the instructions discussed above.

  Click **Test**.

  Click **Authorize**.



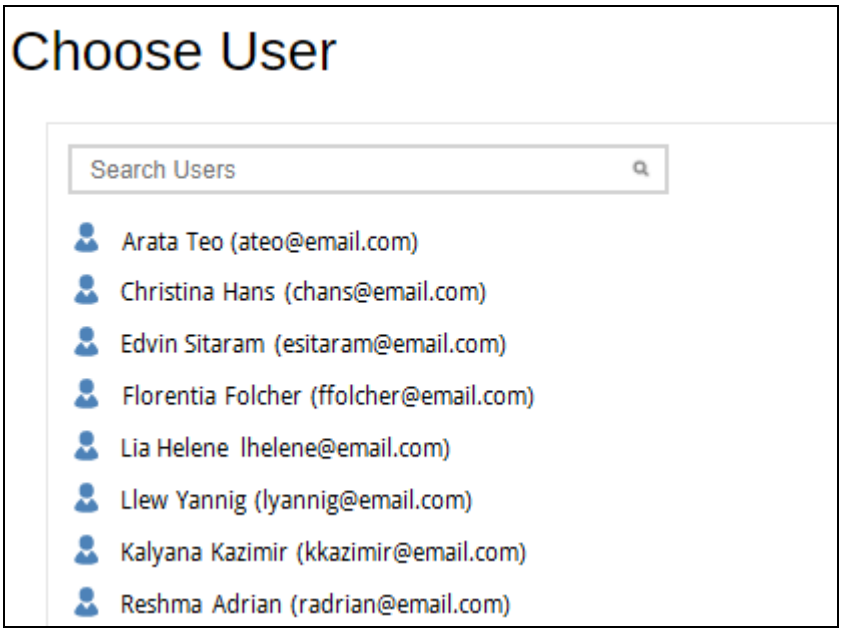
  Login to your Microsoft 365 account then copy and paste the authorization code then click **OK**. Click to proceed.



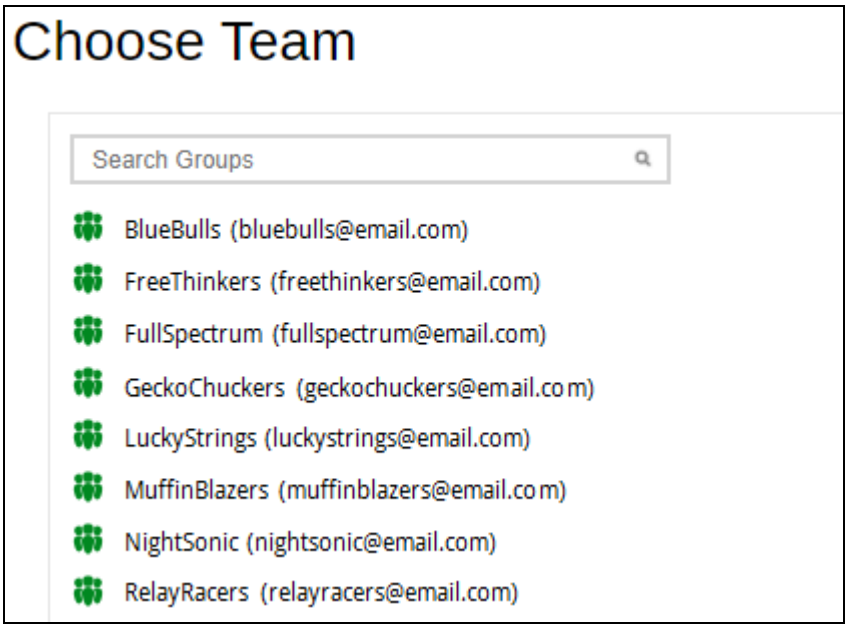
  Select the alternate user/team/site/public folder then click to start the restoration.

Here are examples for the different data types:

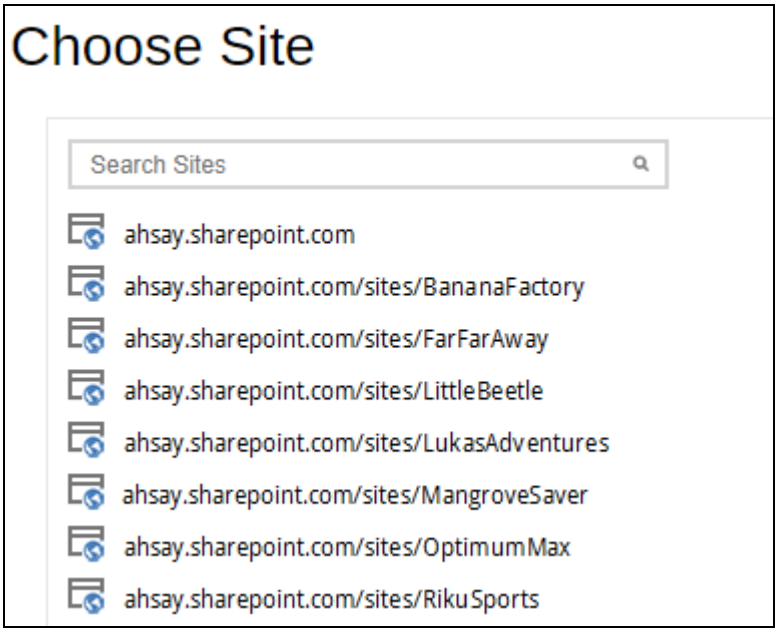
Users



Teams



SharePoint Sites



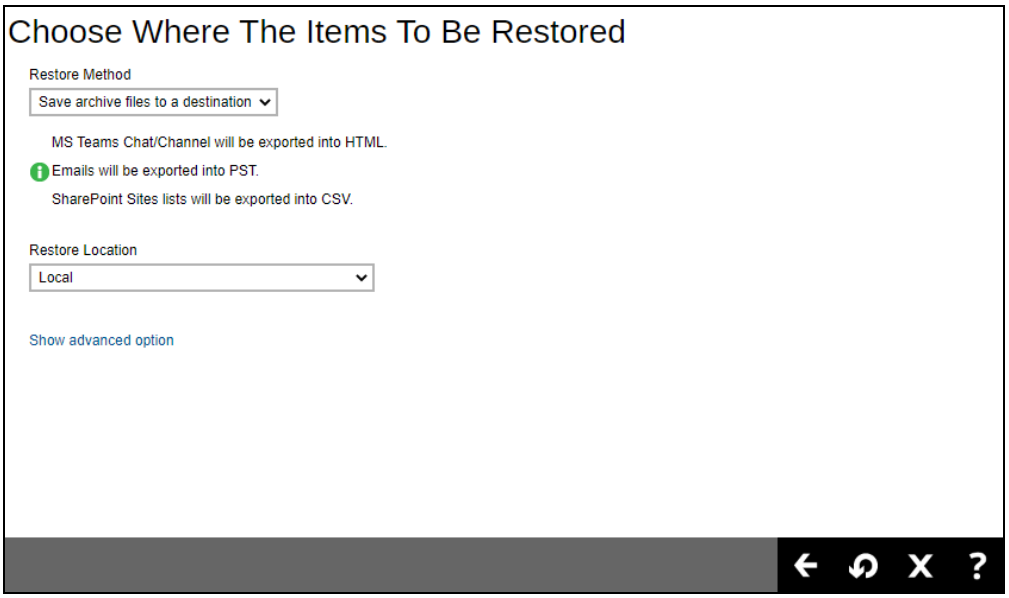
Public Folders

If Save archive files to a destination is selected, there are three options for the restore location:

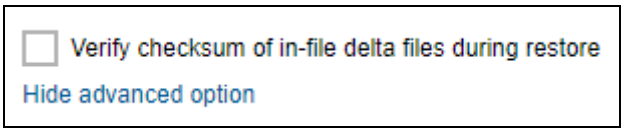
- Local
- OneDrive of Original Microsoft 365 organization
- OneDrive of Alternate Microsoft 365 organization

- **Local**

Restore to Local is available for all data types. To restore to Local, select **Local**.



To configure other restore settings click **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.

Click to start the restoration.

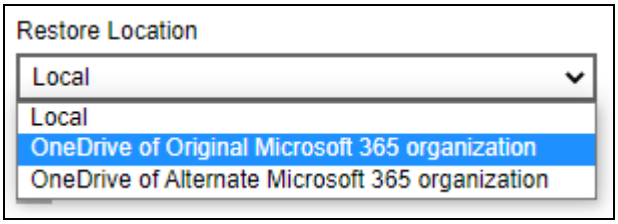
NOTE

For AhsayACB, restore location that will be available is only Local.

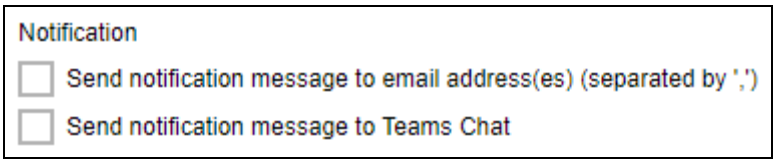
OneDrive of Original Microsoft 365 organization

Restore to OneDrive of original Microsoft 365 organization is only available for the following data types: Users and Teams.

Select **OneDrive of Original Microsoft 365 organization** from the dropdown menu.

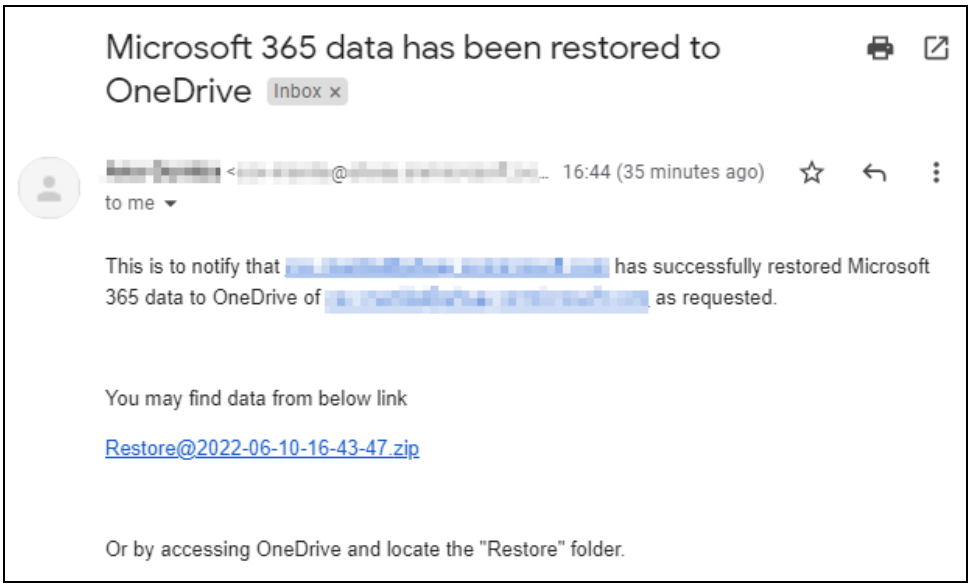


Users can be notified if an item is restored to their OneDrive. You can opt to send the notification message by email and/or to Teams Chat.



If you prefer to send the notification by email, provide the email address where it will be sent. You can provide several email address(es) by separating it with a comma.

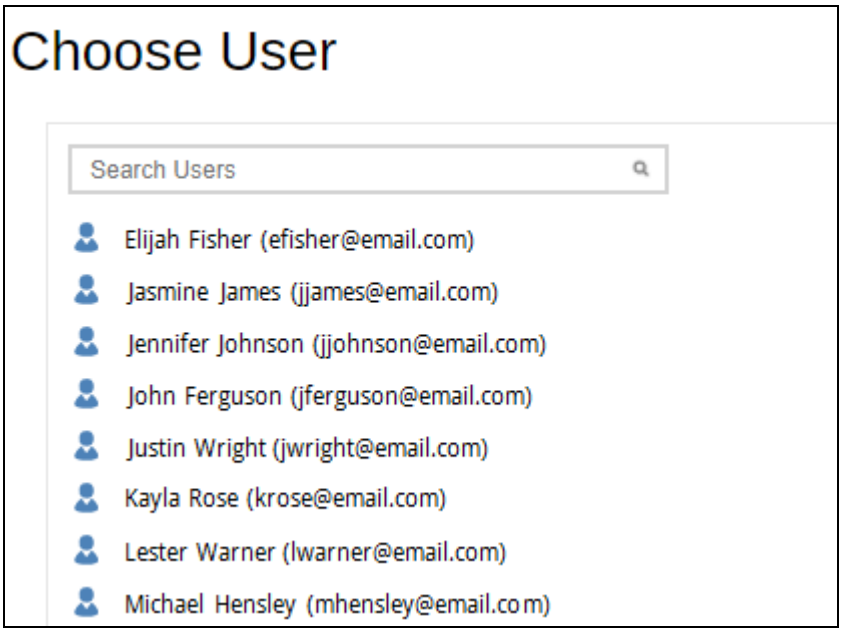
Here is a sample of the email notification that will be sent.



To configure other restore settings please refer to the instructions above.

Click to proceed.

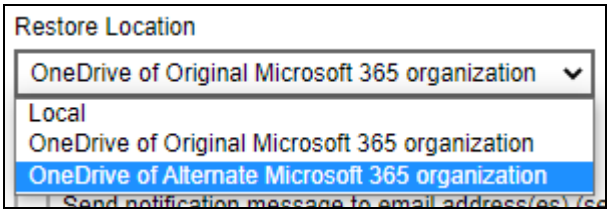
Select the user. Then click to start the restoration.



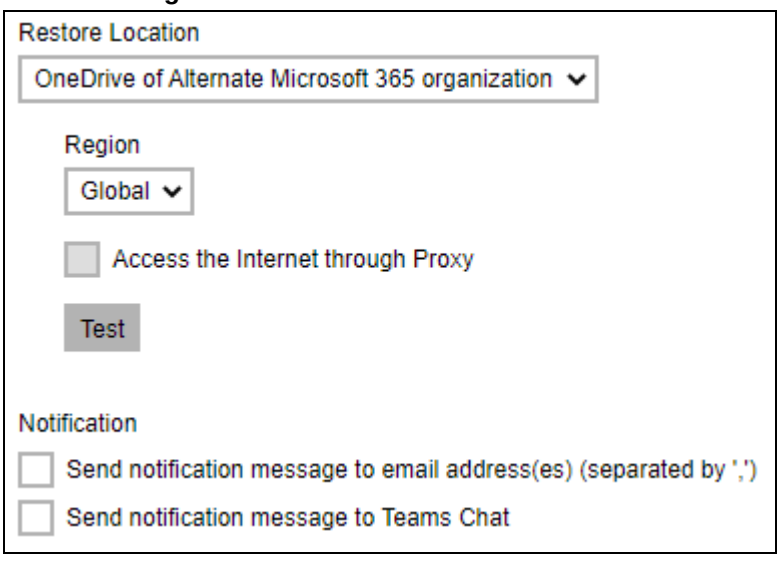
- **OneDrive of Alternate Microsoft 365 organization**

Restore to OneDrive of alternate Microsoft 365 organization is only available for the following data types: Users and Teams.

Select **OneDrive of Alternate Microsoft 365 organization** from the dropdown menu.



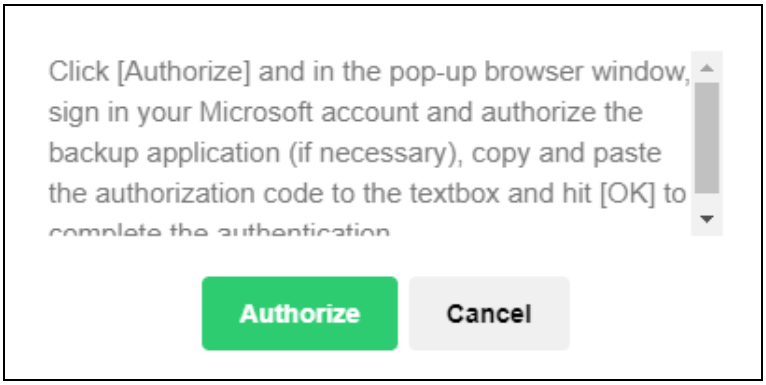
Select the **Region**.



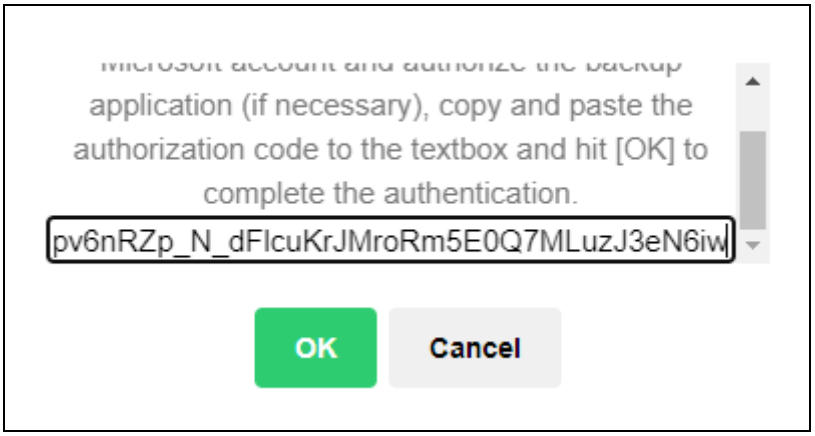
To configure notification settings please see instructions above.

Click **Test**.

Click **Authorize**.

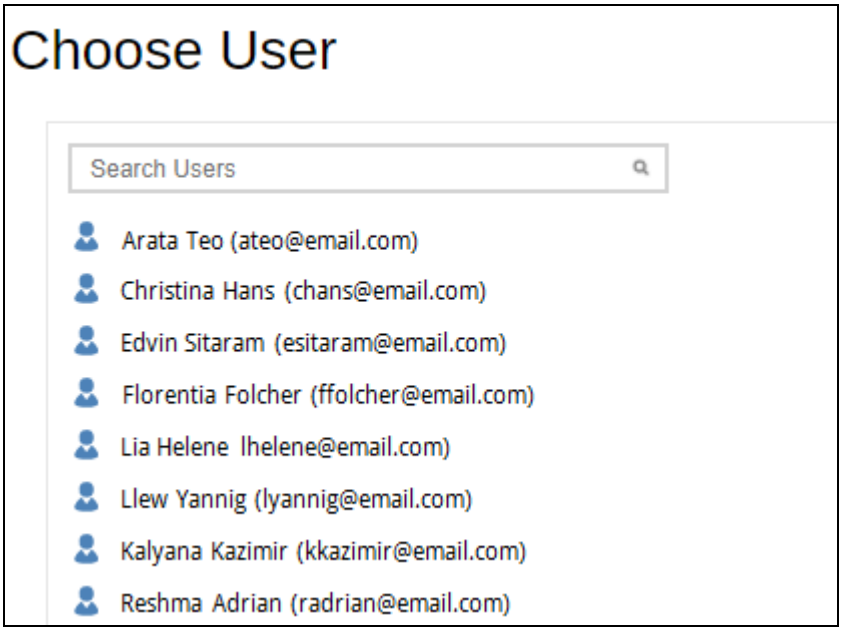


Login to your Microsoft 365 account then copy and paste the authorization code then click **OK.**

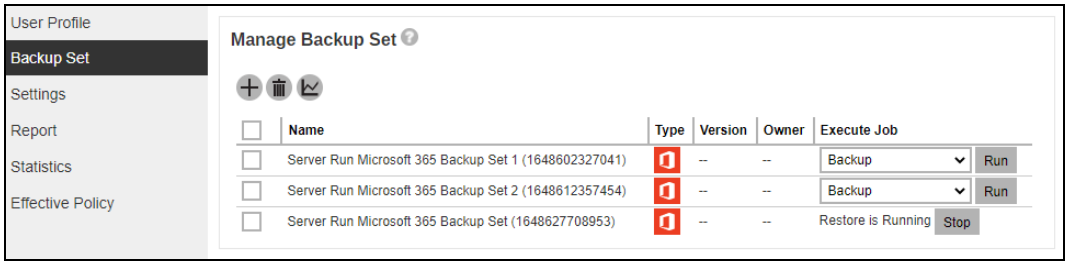


Click to proceed.

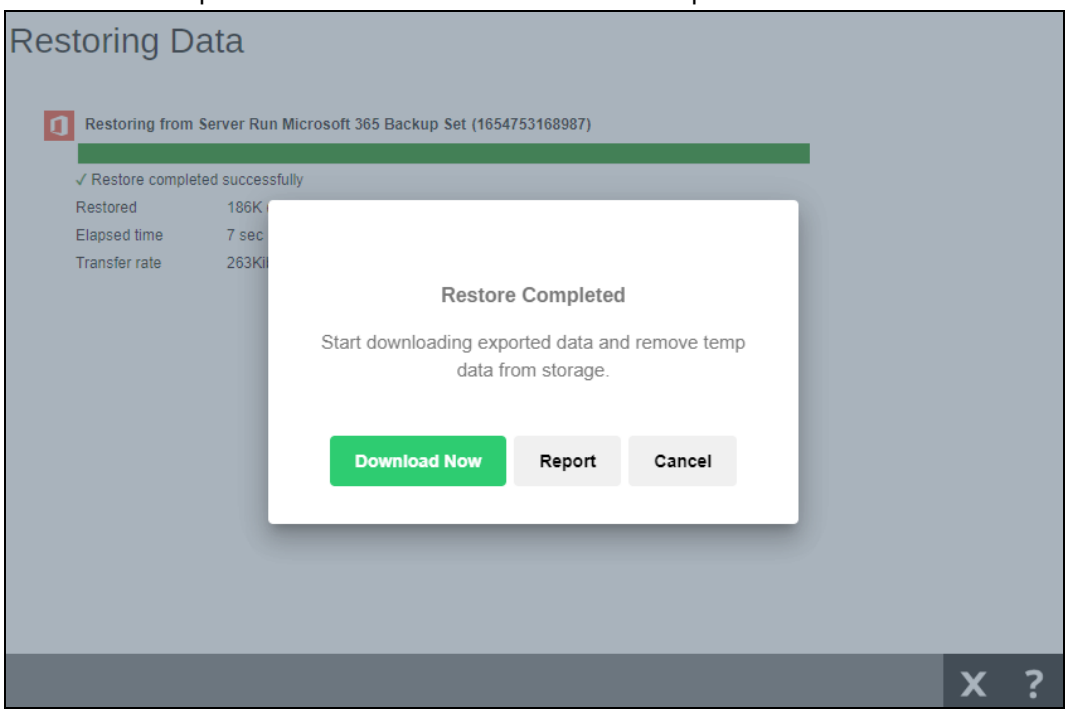
Select the user. Then click to start the restoration.



6. Click to go back to the Manage Backup Set screen and you will see the status showing **Restore is Running** when the restore is in progress.

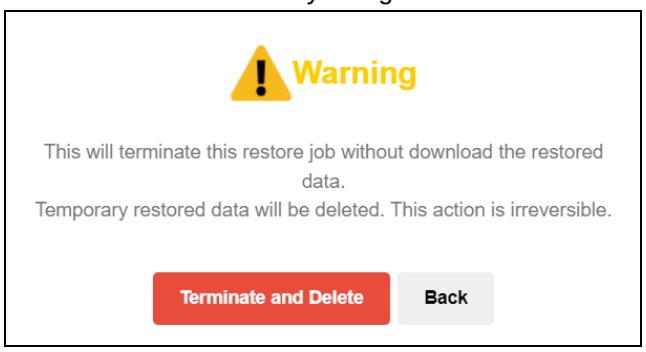


This step will **only** be displayed when **Save archive files to a destination** is selected as the restore method. Once restore is completed, click **Download Now** if you want to download the exported data. The data will be saved in a zip file.

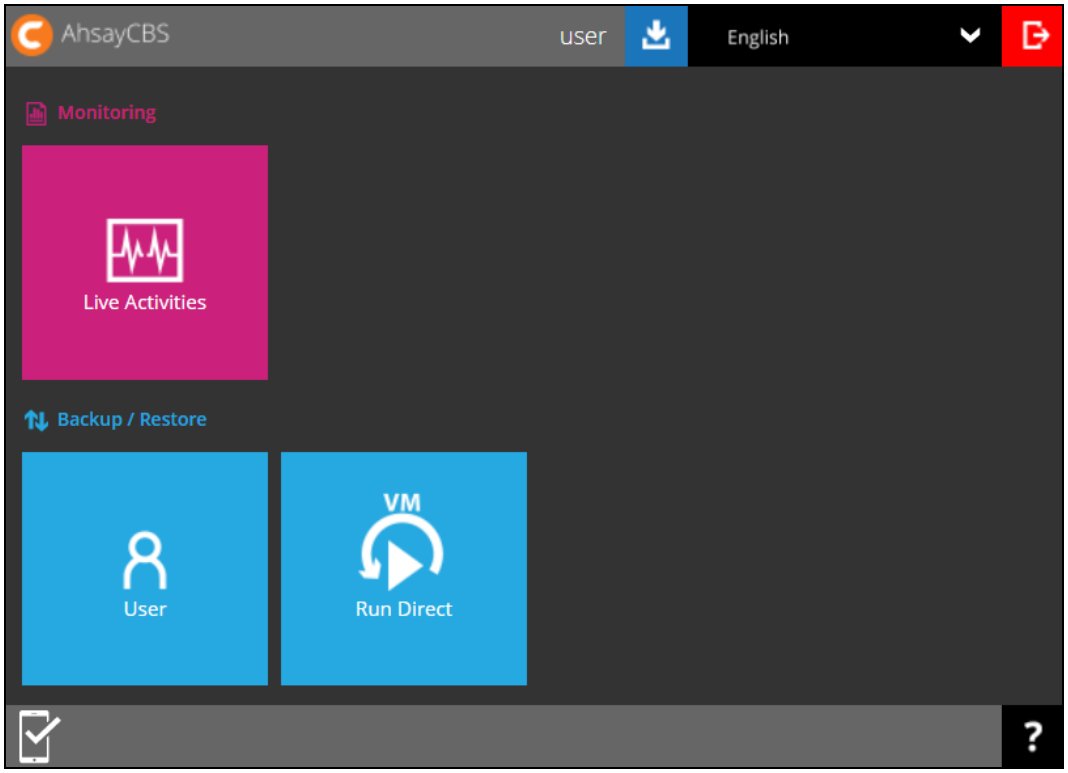


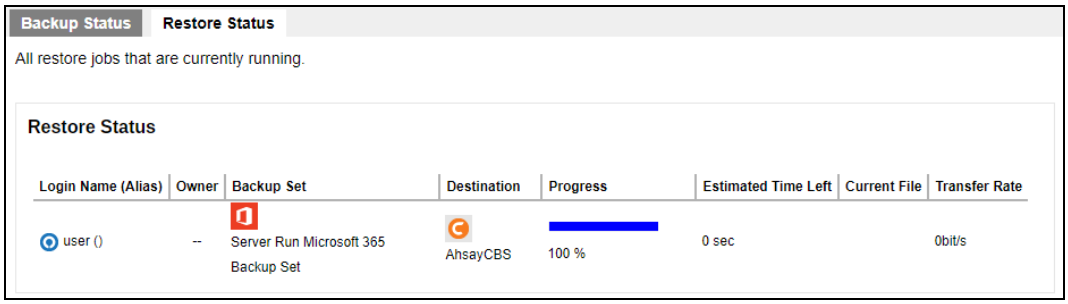
Click **Report** if you want to view the report, the report will be generated in pdf format.

Otherwise click **Cancel**, To stop the restore job and delete temporary restored data, click **Terminate and Delete**. By doing so the restore will not finish.



Another way to monitor the restore status is from the **Live Activities**.





7 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 report of the result cannot be reviewed. It will only be available upon request from your backup service provider.

  Please contact your backup service provider for more information.

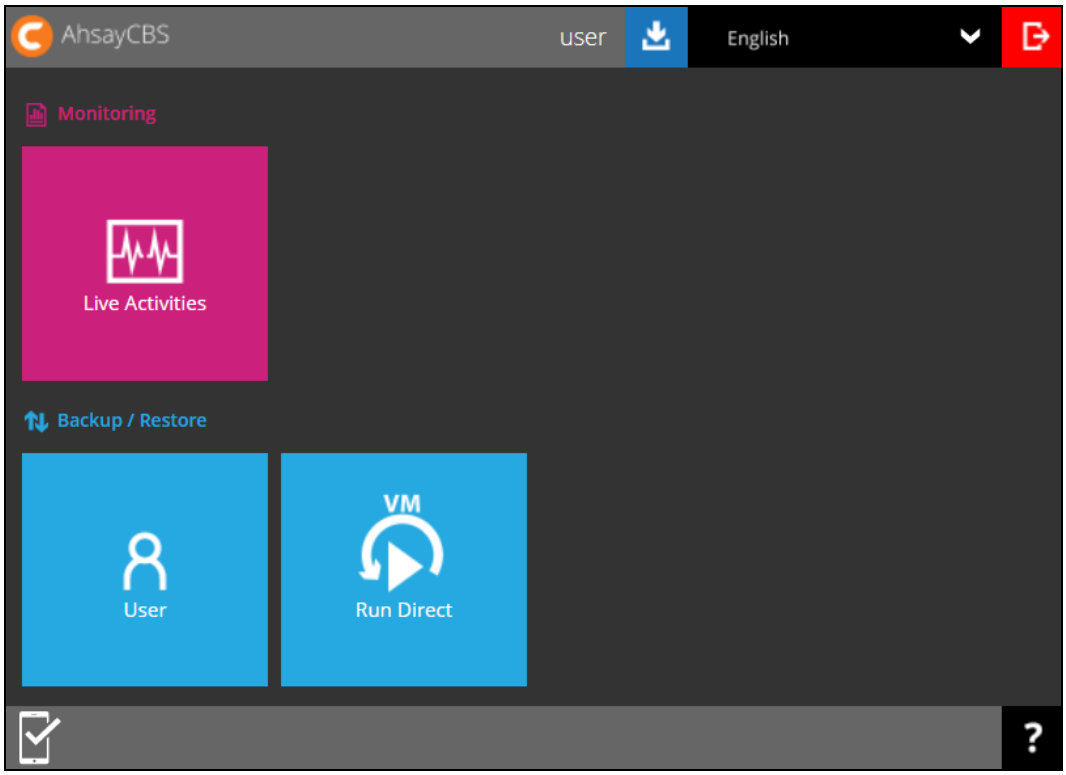
- **Backup Service Provider**

  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.

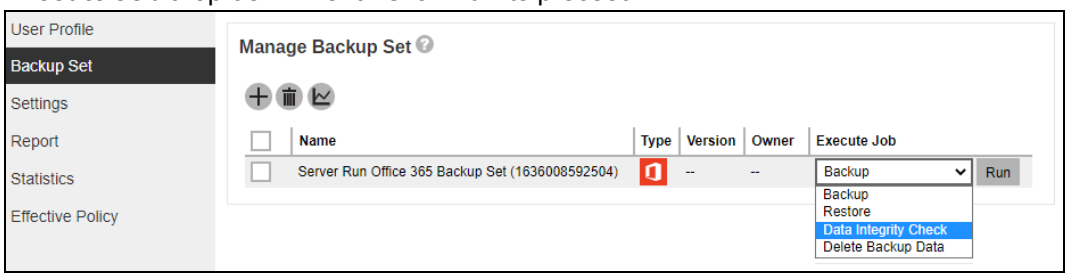
1. Log in to the User Web Console.

   For instructions on how to do this please refer to Chapter 2 of the AhsayCBS v9 User Guide.

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.

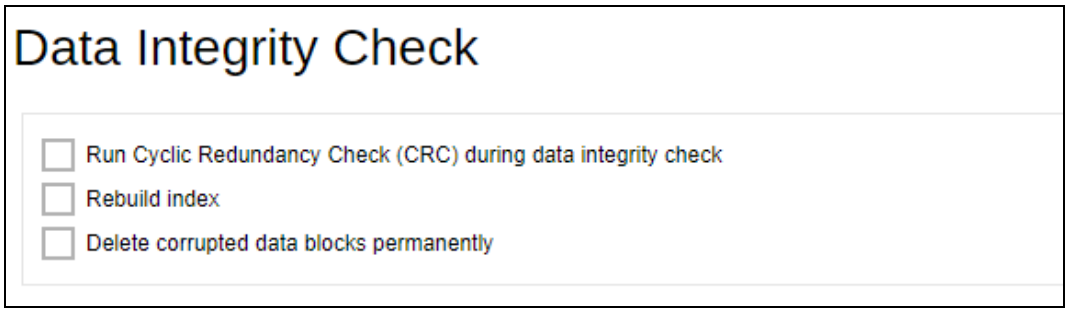
However, if the corrupted files are in the retention area, they will not be backed up again as the source file has already been deleted from the backup server.

Rebuild index

This option is disabled by default. When this option is enabled, the Data Integrity Check will start rebuilding corrupted index and/or broken data blocks if there are any.

Delete corrupted data blocks permanently

This option is disabled by default. When this option is enabled, the Data Integrity Check will delete the corrupted data blocks permanently instead of moving it to the Recycle Bin.



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

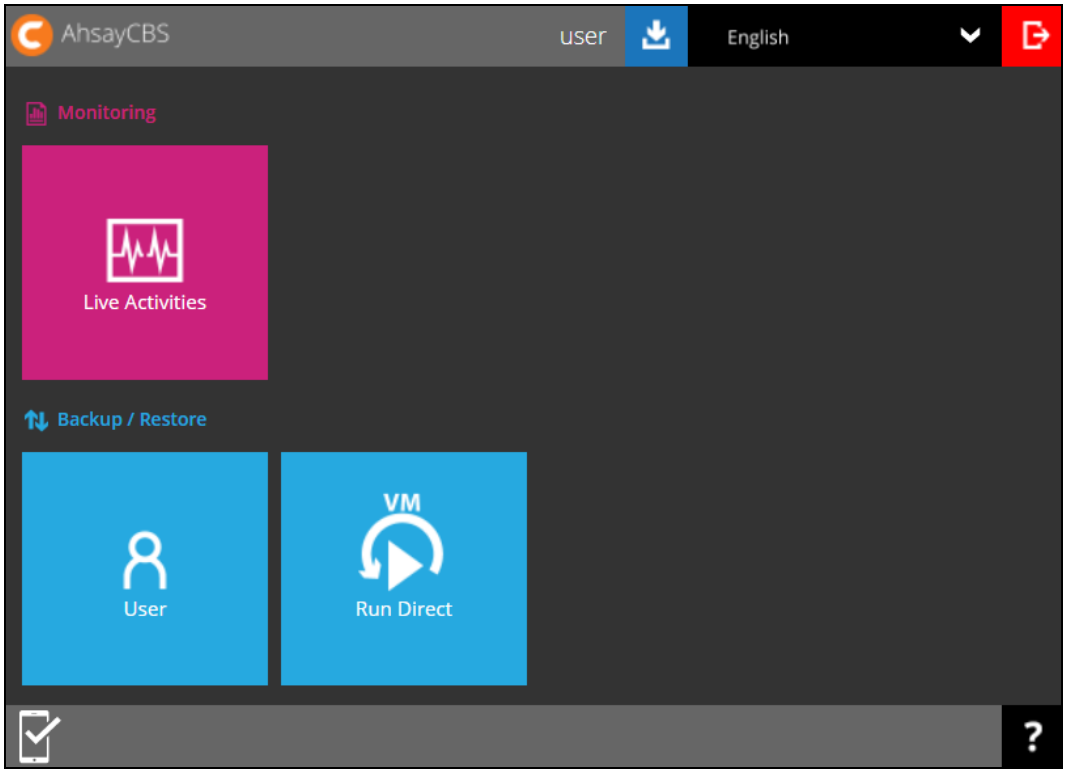
During a backup job, a Periodic Data Integrity Check (PDIC) will be performed as part of the backup process. This feature provides an additional regular data integrity check of the backup data.

8 Deleting Backup Data

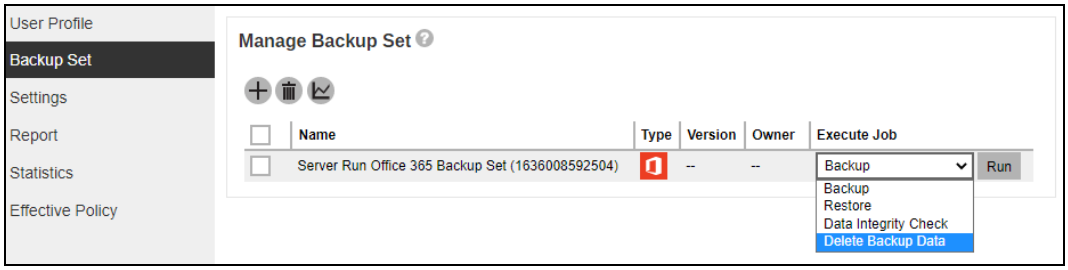
1. Log in to the User Web Console.

   For instructions on how to do this please refer to Chapter 2 of the AhsayCBS v9 User Guide.

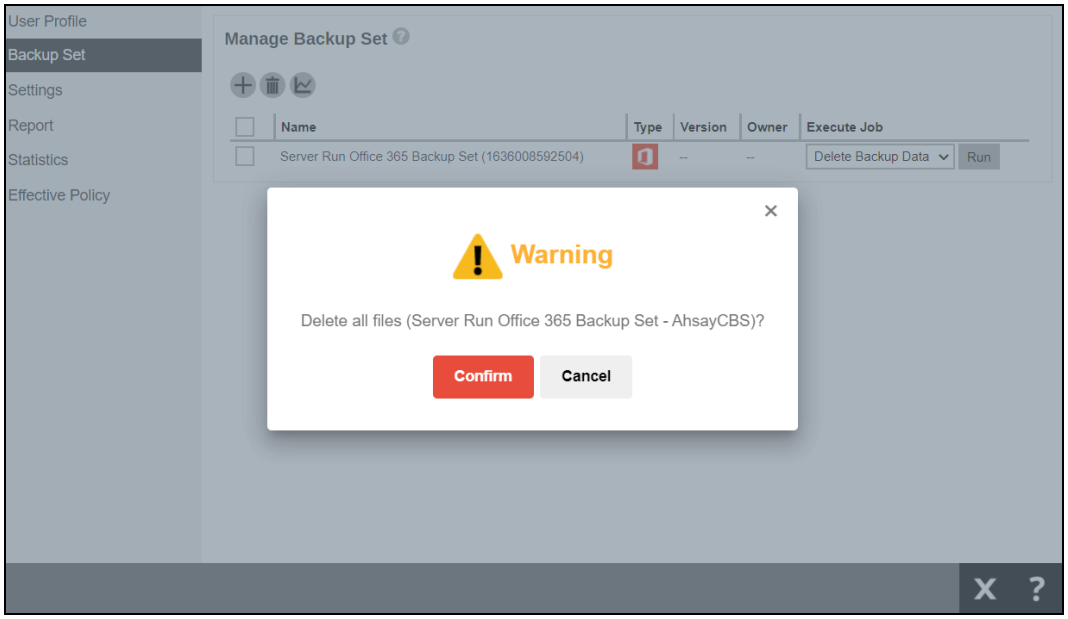
2. Click on the **User** icon.

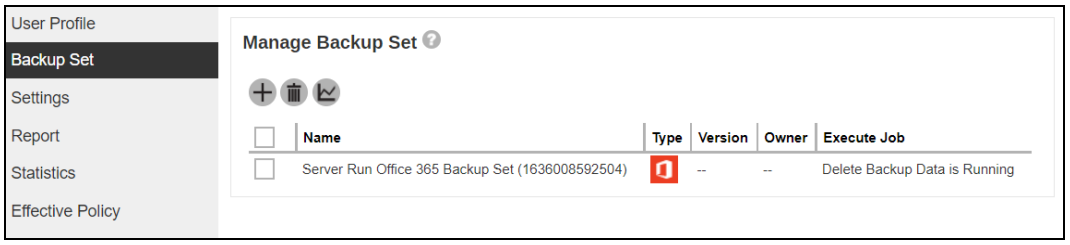


3. Select **Backup Set** from the left panel, then select **Delete Backup Data** under the **Execute Job** drop-down menu. Click **Run** to proceed.



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





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.

9 Contact Ahsay

9.1 Technical Assistance

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

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

9.2 Documentation

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

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 Microsoft 365 License Requirement and Usage

Scenario No. 1: Backing up Microsoft 365 user account in multiple backup sets.

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

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

Backup Set Name	Microsoft 365 User Account
Backup Set A	user01@company-Microsoft365.com
Backup Set B	user01@company-Microsoft365.com
Backup Set C	user01@company-Microsoft365.com

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

Backup Set Name	Microsoft 365 User Account
Backup Set A	user01@company-Microsoft365.com
	user02@company-Microsoft365.com
Backup Set B	user01@company-Microsoft365.com
Backup Set C	user02@company-Microsoft365.com

Example No. 3: To back up three (3) Microsoft 365 user accounts on multiple backup sets, three (3) Ahsay Microsoft 365 licenses are needed.

Backup Set Name	Microsoft 365 User Account
Backup Set A	user01@company-Microsoft365.com
	user02@company-Microsoft365.com
	user03@company-Microsoft365.com
Backup Set B	user01@company-Microsoft365.com
	user02@company-Microsoft365.com
Backup Set C	user03@company-Microsoft365.com

Scenario No. 2: Backing up SharePoint Sites (not Personal Sites) under Site collections in multiple backup sets.

The required Microsoft 365 license is zero, but a minimum of one (1) Microsoft 365 add-on module license is needed to start the backup.

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

Backup Set Name	SharePoint Site
Backup Set A	companyMicrosoft365.sharepoint.com/Finance
Backup Set B	companyMicrosoft365.sharepoint.com/Finance
Backup Set C	companyMicrosoft365.sharepoint.com/Finance

Example No. 2: To back up any number of SharePoint sites under Site Collection, one (1) Ahsay Microsoft 365 license is needed.

Backup Set Name	SharePoint Site
Backup Set A	companyMicrosoft365.sharepoint.com/sites//Finance
	companyMicrosoft365.sharepoint.com/sites/SupportTeam
	companyMicrosoft365.sharepoint.com/sites/Engineering
Backup Set B	companyMicrosoft365.sharepoint.com/sites/Finance
Backup Set C	companyMicrosoft365.sharepoint.com/sites/Finance
	companyMicrosoft365.sharepoint.com/sites/SupportTeam
	companyMicrosoft365.sharepoint.com/sites/Engineering

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

The required Microsoft 365 license is zero, but a minimum of one (1) Microsoft 365 add-on module license is needed to start the backup.

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

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

Scenario No. 4: Backing up Microsoft 365 User Accounts, files and/or folders under Public Folder, and SharePoint sites under Site Collections in multiple backup sets.

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

Example No. 1: To back up three (3) Microsoft 365 user account, files and/or folders under Public Folder, and SharePoint sites under Site Collections on multiple backup sets, three (3) Ahsay Microsoft 365 licenses are needed.

Backup Set Name	Microsoft 365 User Account, SharePoint Site, and Files and/or Folders
Backup Set A	user01@company-Microsoft365.com
Backup Set B	user01@company-Microsoft365.com
	user02@company-Microsoft365.com
	companyMicrosoft365.sharepoint.com/sites/Finance
	companyMicrosoft365.sharepoint.com/sites/SupportTeam
Backup Set C	user01@company-Microsoft365.com
	user02@company-Microsoft365.com
	Folder01 ○ microsoftword01.docx ○ powerpointpresentation01.pptx ○ spreadsheet01.xls ○ notepad01.txt ○ picture01.jpg ○ picture02.jpg
Backup Set D	user01@company-Microsoft365.com
	user02@company-Microsoft365.com
	user03@company-Microsoft365.com
	Folder01 ○ microsoftword01.docx ○ powerpointpresentation01.pptx ○ spreadsheet01.xls ○ notepad01.txt ○ picture01.jpg ○ picture02.jpg
	companyMicrosoft365.sharepoint.com/sites/Finance
	companyMicrosoft365.sharepoint.com/sites/SupportTeam

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

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

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

Backup Set Name	Microsoft 365 User Account and Shared Mailbox Accounts
Backup Set A	user01@company-Microsoft365.com
	user02@company-Microsoft365.com
	user03@company-Microsoft365.com
	sharedmailbox01@test-Microsoft365.com
	sharedmailbox02@test-Microsoft365.com
	sharedmailbox03@test-Microsoft365.com

Microsoft 365 license usage in backup

The number of Microsoft 365 licenses used in a backup can be checked from the backup log. The logs will first display the number of licenses that can be used which is labeled as “Quota (E-mail Account)”. Then it will display the actual number of licenses used “Quota (E-mail account) used in this backup set”. Lastly, it will list the e-mail accounts that was used.

Here is a sample of how it is listed in the log:

```
[2022/06/15 11:53:58] [info] [-] Quota (E-mail Account): 400
[2022/06/15 11:53:58] [cbs] [-] info,Quota (E-mail Account): 400,0,0,0,,,
[2022/06/15 11:53:58] [info] [-] Quota (E-mail Account) used in this backup set: 12
[2022/06/15 11:53:58] [cbs] [-] info,Quota (E-mail Account) used in this backup set: 12,0,0,0,,,
[2022/06/15 11:53:58] [info] [-] 1. Abacussam@example.com
[2022/06/15 11:53:58] [info] [-] 2. BasicZexo@example.com
[2022/06/15 11:53:58] [info] [-] 3. Dave555@example.com
[2022/06/15 11:53:58] [info] [-] 4. alphabetZack@example.com
[2022/06/15 11:53:58] [info] [-] 5. carolinarib@example.com
[2022/06/15 11:53:58] [info] [-] 6. evanmcevan@example.com
[2022/06/15 11:53:58] [info] [-] 7. fredisred@example.com
[2022/06/15 11:53:58] [info] [-] 8. hellohello@example.com
[2022/06/15 11:53:58] [info] [-] 9. mitchellwinner@example.com
[2022/06/15 11:53:58] [info] [-] 10. nonna@example.com
[2022/06/15 11:53:58] [info] [-] 11. quagmire@example.com
[2022/06/15 11:53:58] [info] [-] 12. russlabc@example.com
```

Run on Server backup log can be found in the path:

%User Home%\%backup username%\db\ClientLogs\Ahsay Cloud Backup Suite\log\%backupset ID%\Backup

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

Example: 10,000 Microsoft 365 users needed to be backup. Since the maximum number of Microsoft 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 Microsoft 365 Users
- Option 2 - 10 Backup Sets, each has 1,000 Microsoft 365 Users

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

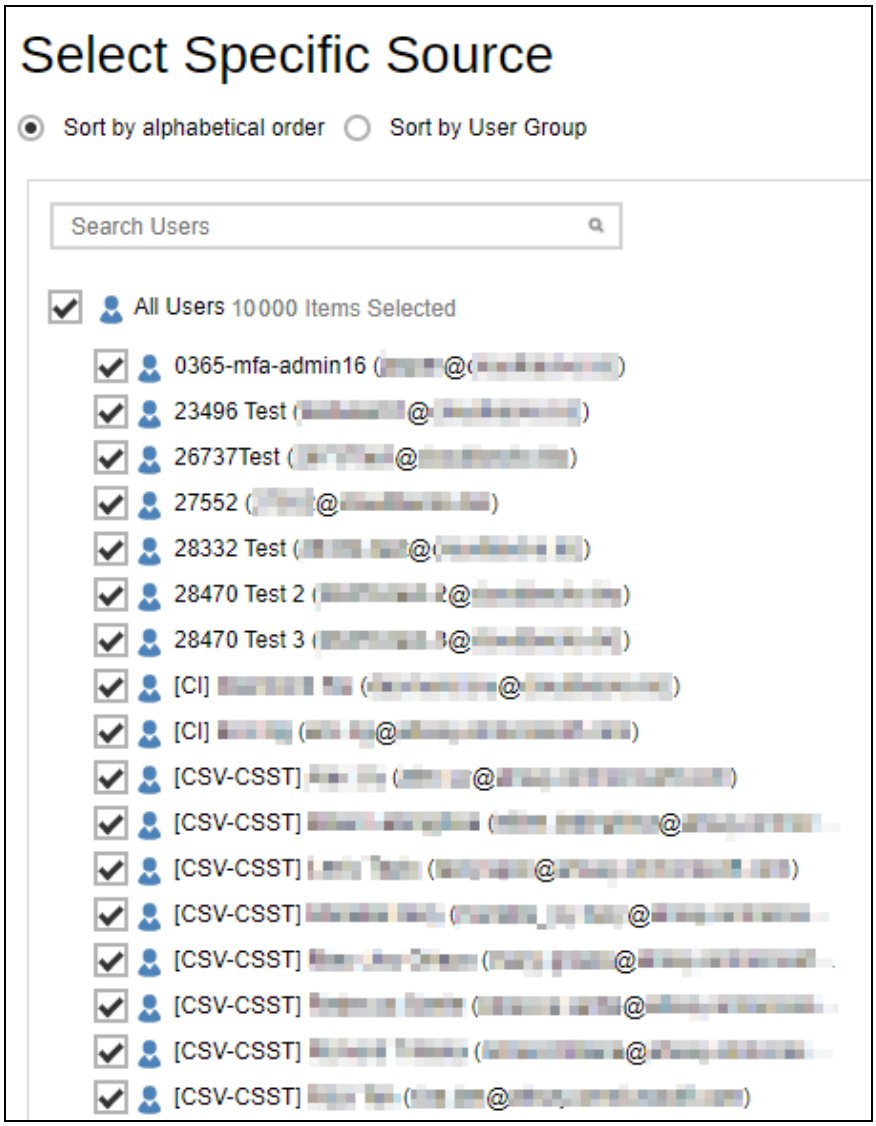
Backup Set Name	User Number
Backup -Set-1	No.1 – 2000
Backup -Set-2	No.2001 – 4000
Backup -Set-3	No. 4001 – 6000
Backup -Set-4	No. 6001 – 8000
Backup -Set-5	No. 8001 – 10000

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

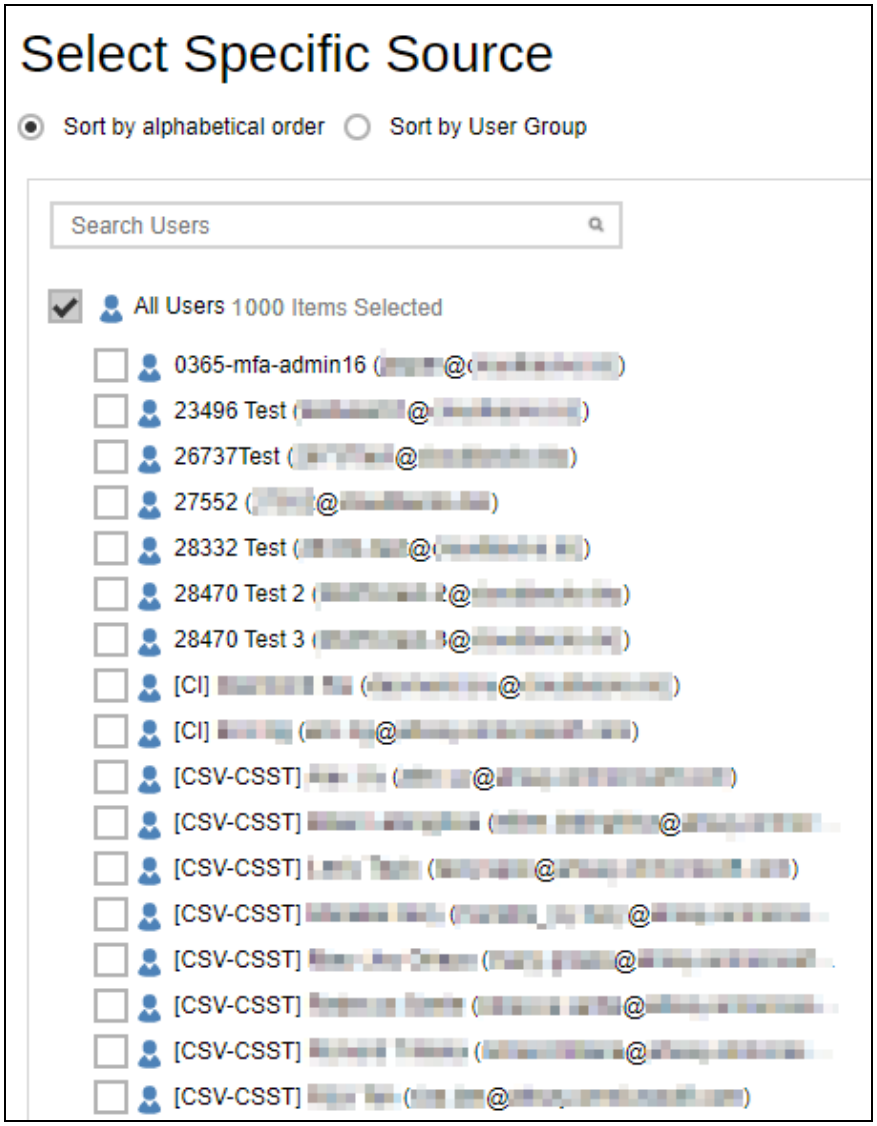
Backup Set Name	User Number
Backup -Set-1	No.1 – 1000
Backup -Set-2	No.1001 – 2000
Backup -Set-3	No. 2001 – 3000
Backup -Set-4	No. 3001 – 4000
Backup -Set-5	No. 4001 – 5000
Backup -Set-6	No. 5001 – 6000
Backup -Set-7	No. 6001 – 7000
Backup -Set-8	No. 7001 – 8000
Backup -Set-9	No. 8001 – 9000
Backup -Set-10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

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



2. Deselect the first 9,000 Microsoft 365 users.

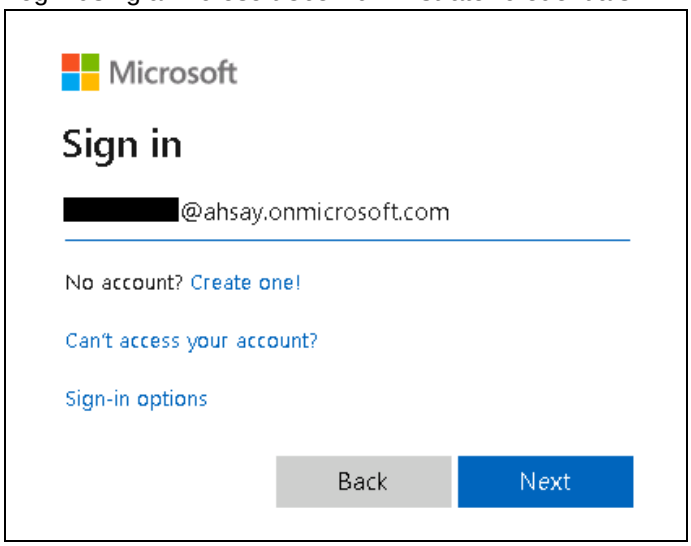


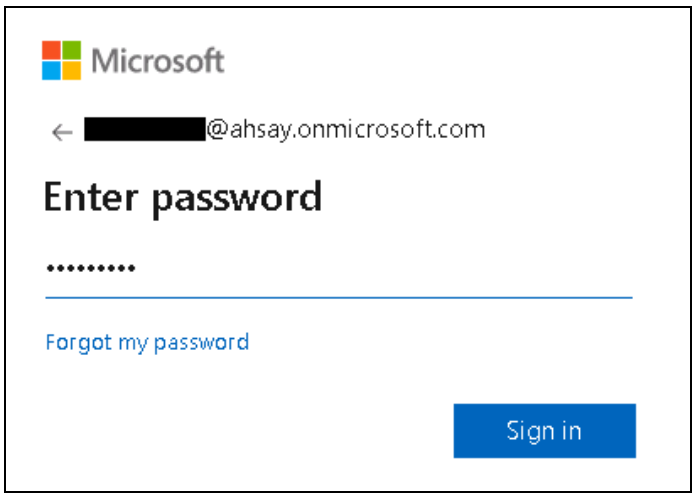
Appendix C: Setting Multi-Factor Authentication (MFA) in Microsoft 365 Admin Center

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 evidence or proof of personal information or identification. It also adds a second layer of security to users upon logging in.

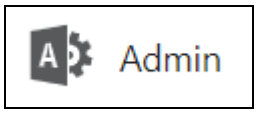
To enable MFA of any Microsoft 365 user accounts, follow the steps below:

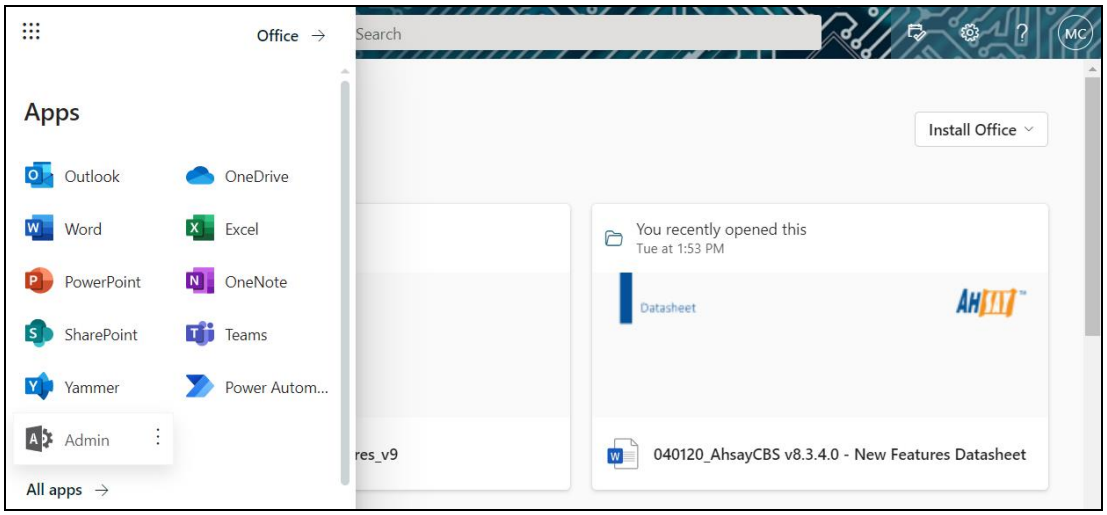
1. Login using a Microsoft 365 Administrator credentials.



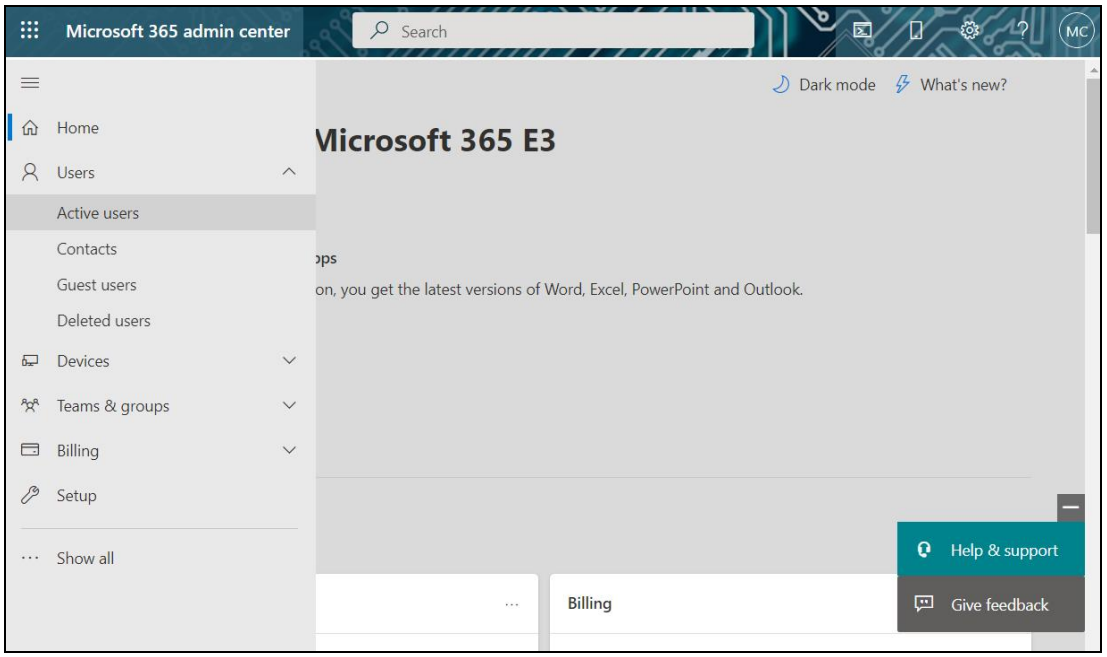


2. Click the **Admin Center** icon.

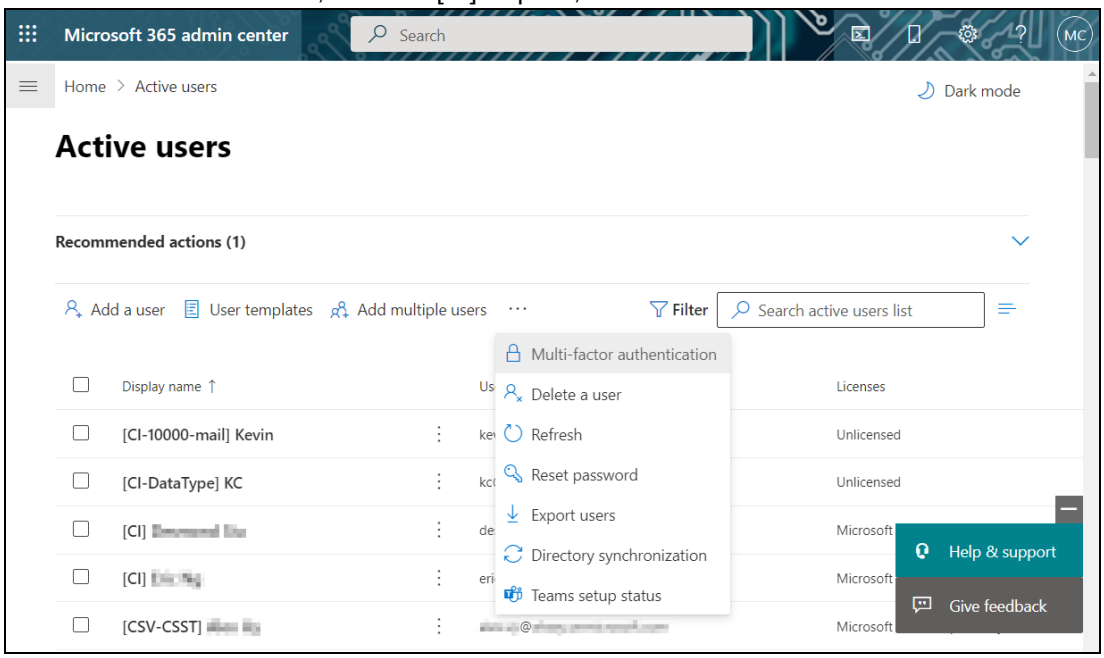




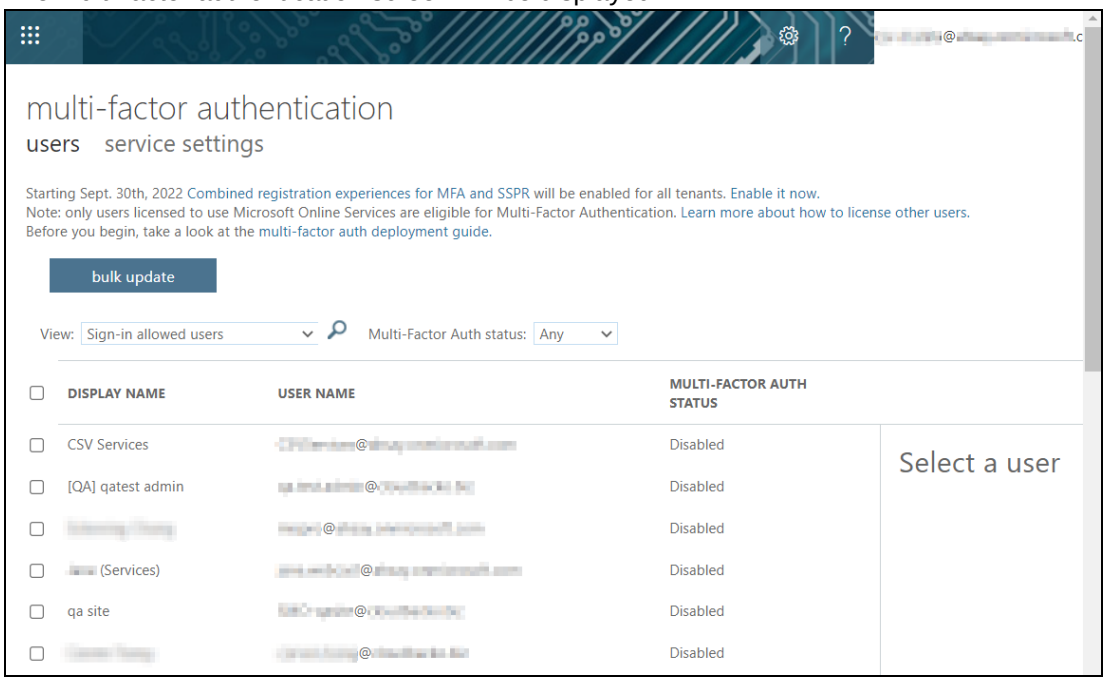
3. Go to **Users** and select the **Active users** from the list.



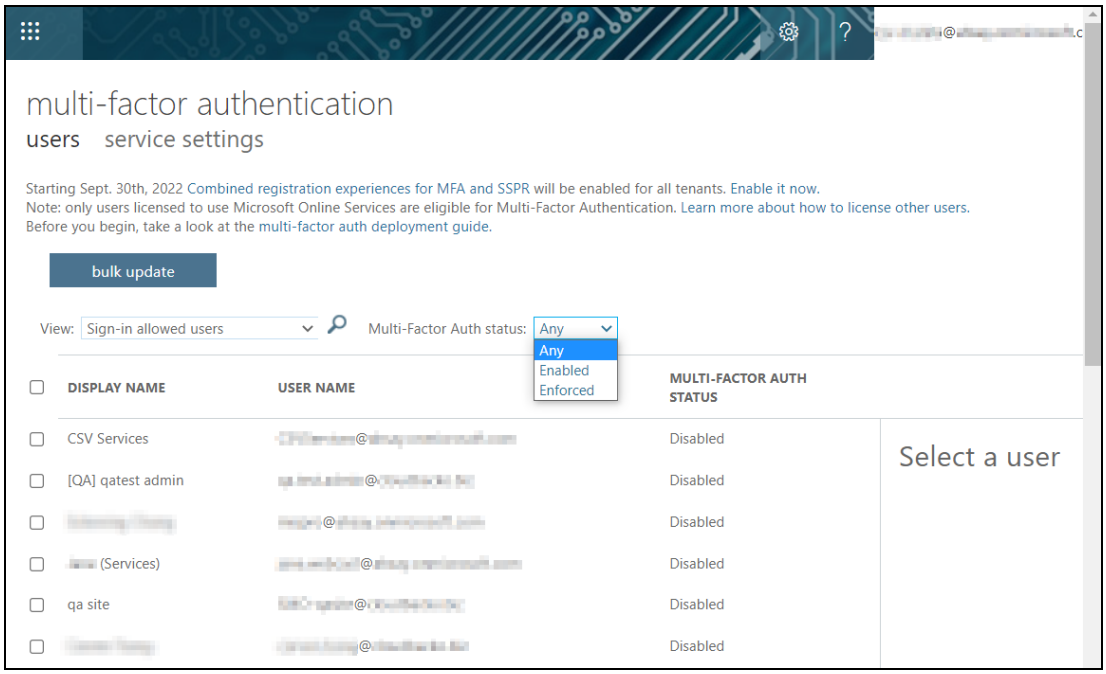
4. In the Active user's screen, click the [...] ellipses, then click Multi-factor authentication.



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

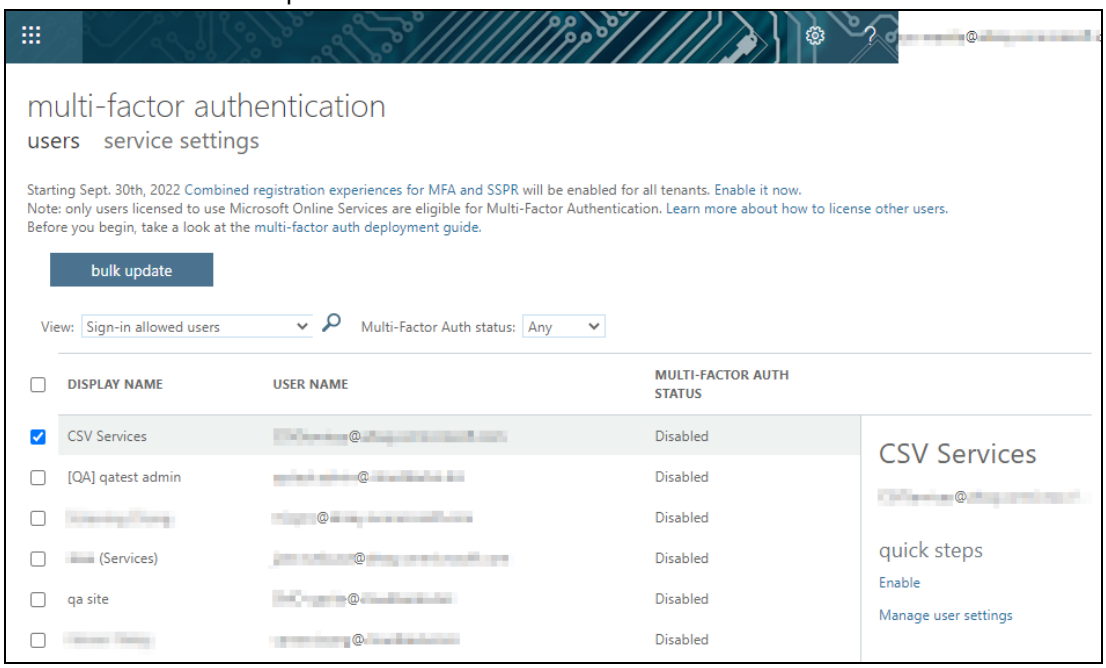


6. You can search and select one or more Microsoft 365 user accounts. There is also a drop-down list available for multi-factor authentication status namely, **Disabled, Enabled**, and **Enforced**.

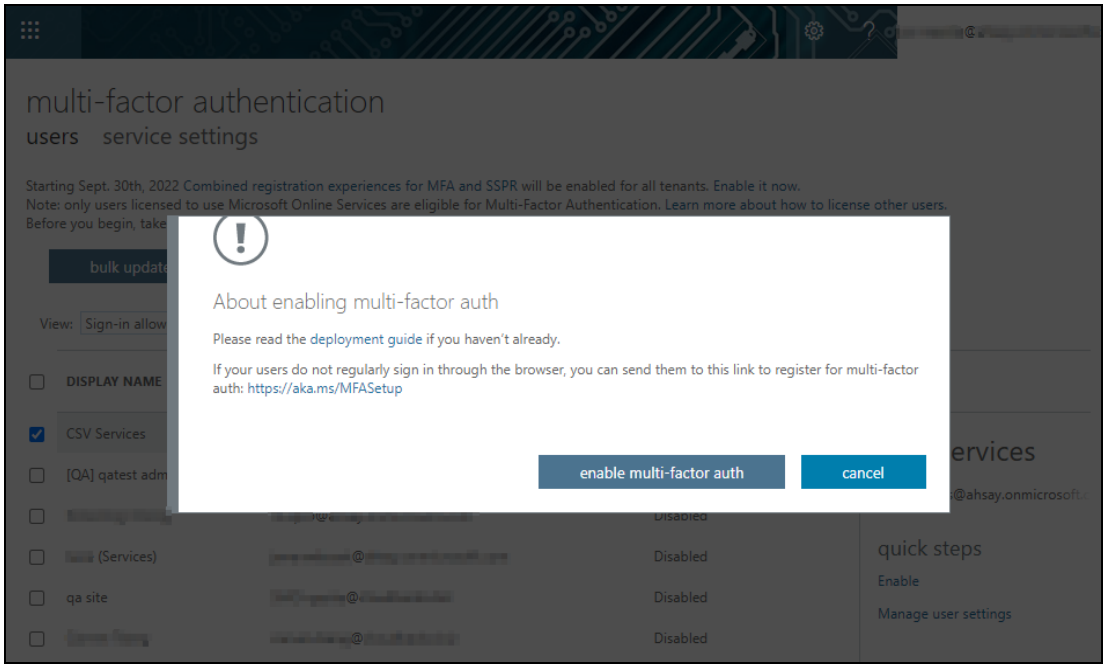


- Disabled – This status refers to the users who are not yet enrolled in the MFA. This is the default status.
- Enabled – This status refers to the users who are enrolled in the MFA, but changes have not yet taken effect.
- Enforced – This status refers to the users who are enrolled in the MFA has completed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

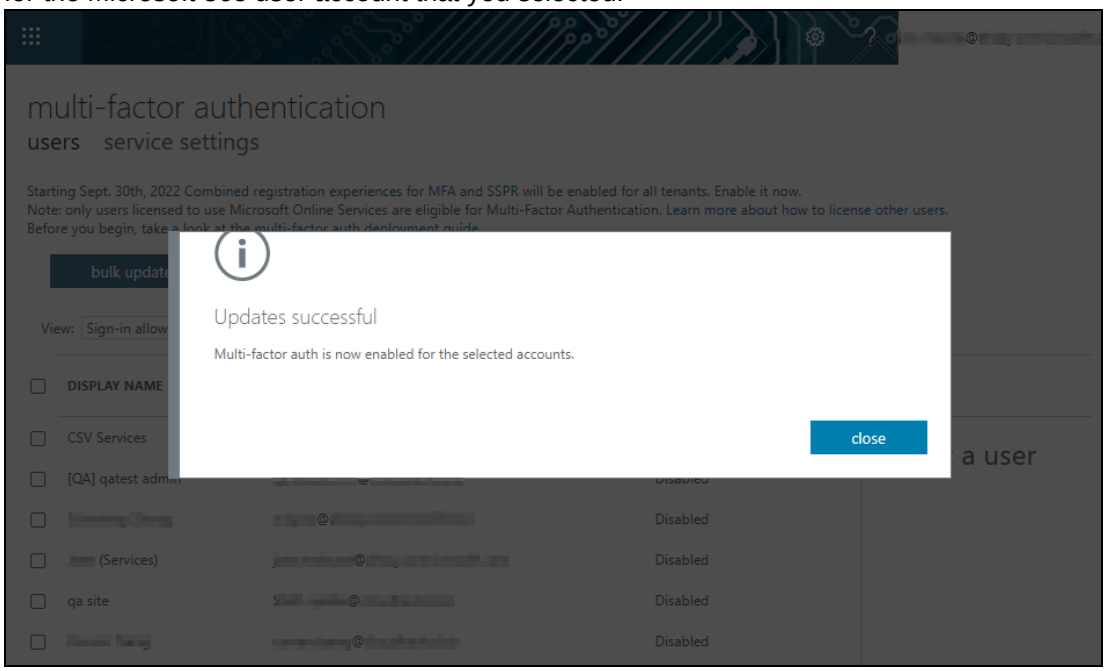
7. Upon selecting a user, on the right side of the screen it will show you a link to enable the MFA. Click the **Enable** link to proceed.



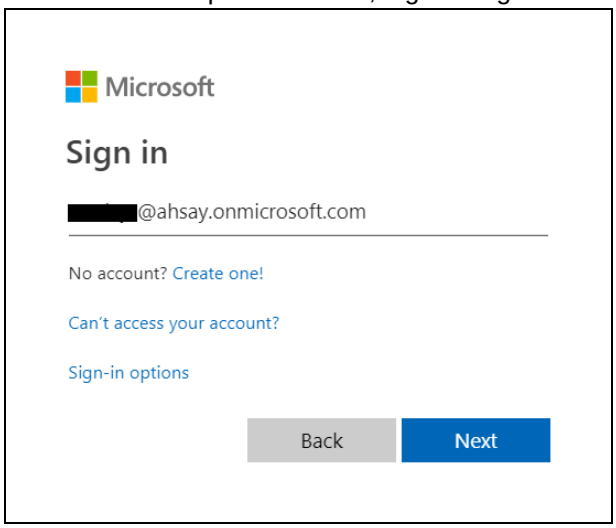
8. A warning message will be displayed. Click the **enable multi-factor auth** button to proceed. Otherwise, click the **cancel** button to abort.

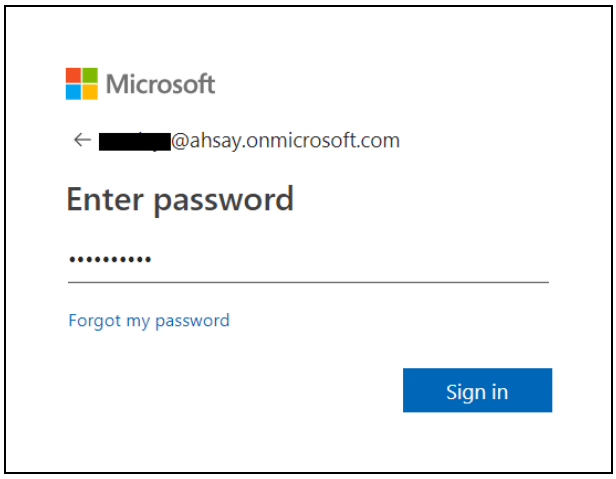


9. If you select enable multi-factor auth, the screen below shows the successful enabling of MFA for the Microsoft 365 user account that you selected.

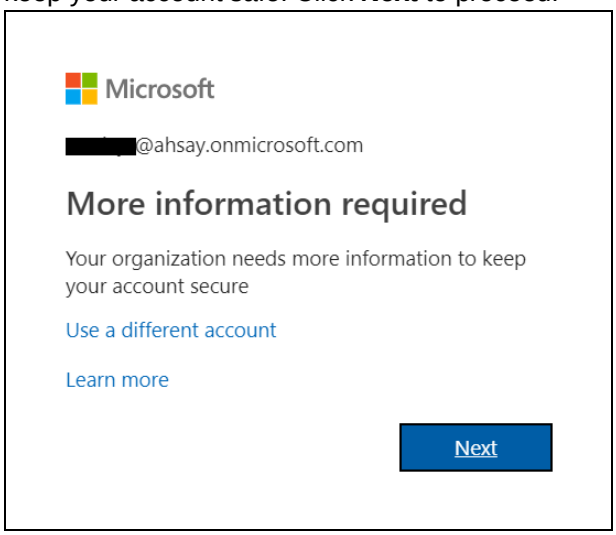


10. To finish the setup for the MFA, login using the MFA enabled Microsoft 365 user account.

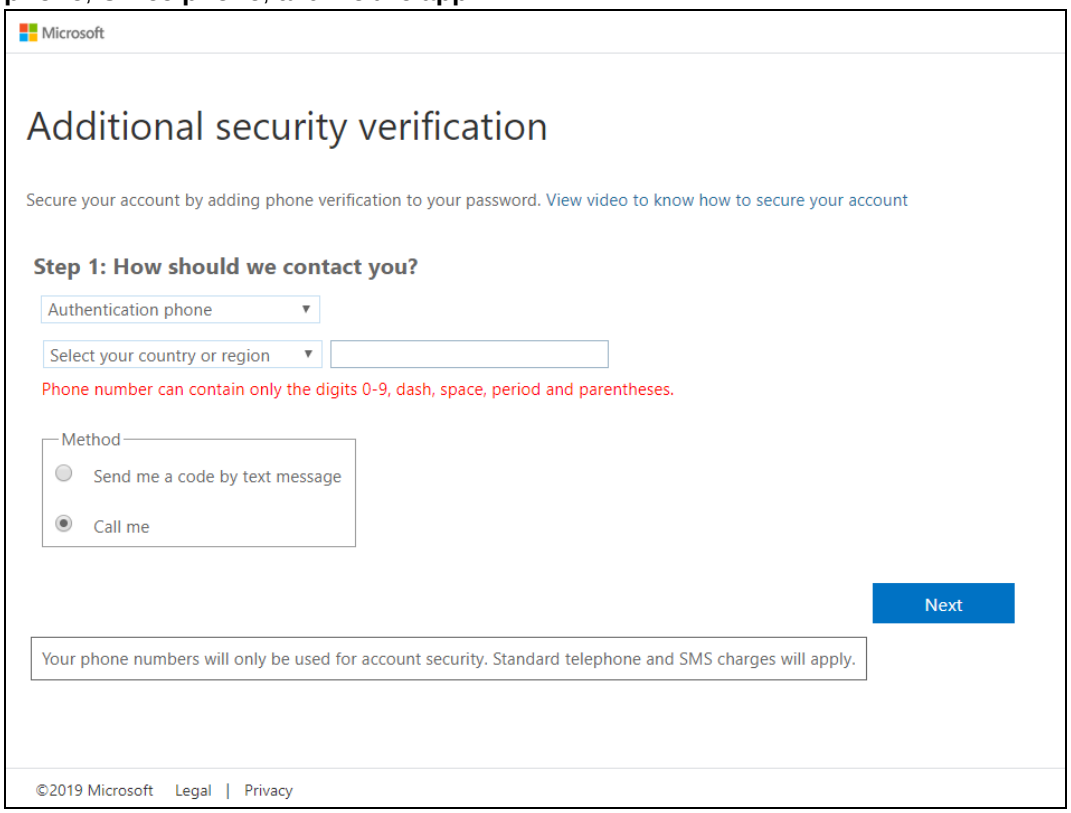




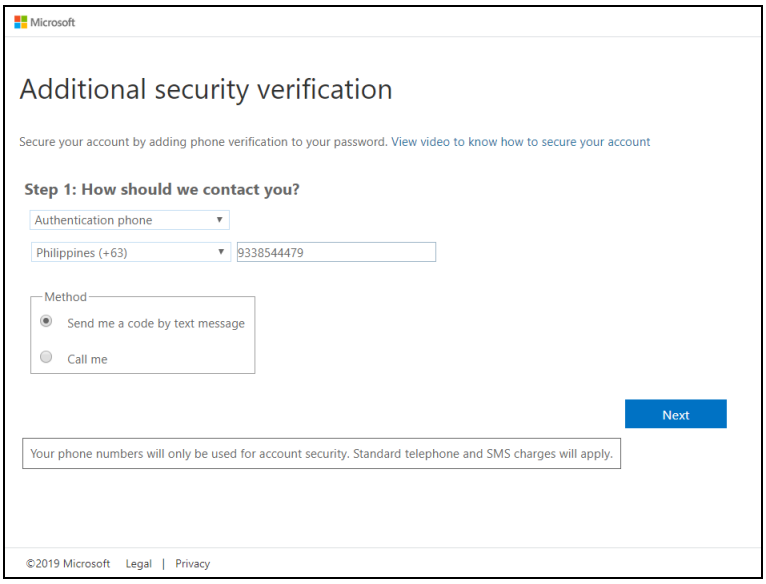
11. Upon logging in, there will be a message that will require you to provide more information to keep your account safe. Click **Next** to proceed.



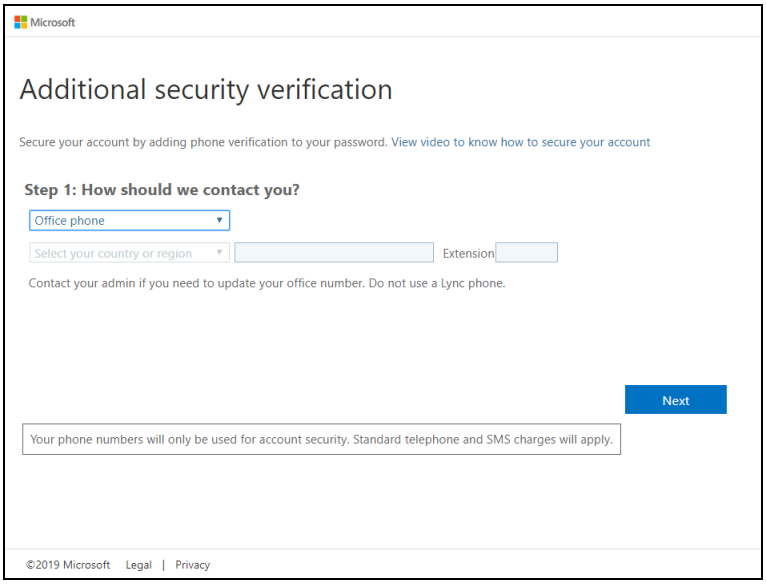
12. The **Additional security verification** screen will be displayed. Select one (1) option you want for the security of your account. You can choose from the three (3) options, **Authentication phone**, **Office phone**, and **Mobile app**.



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

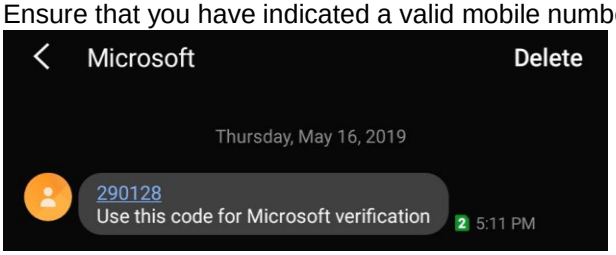


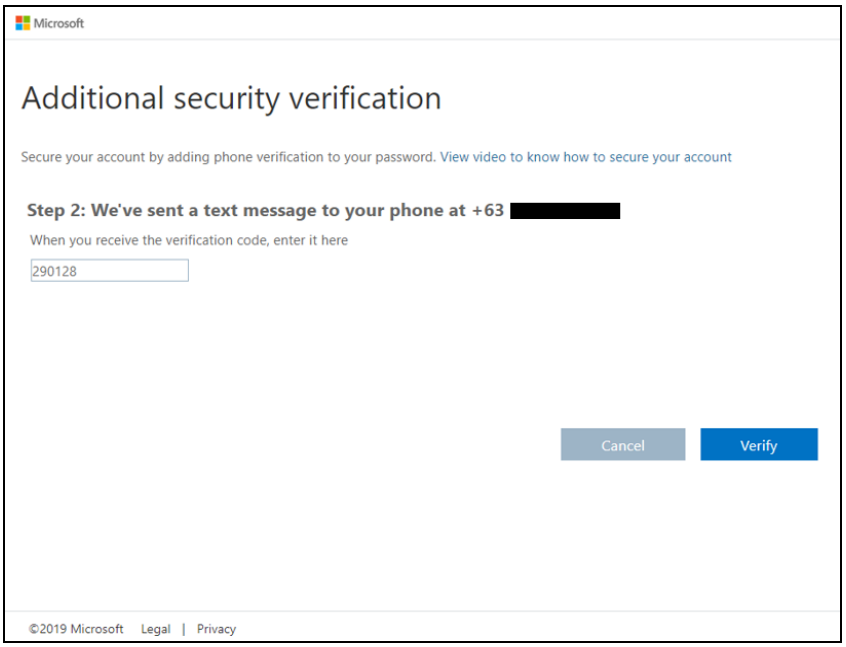
- Office phone – This option is disabled. Please ask your administrator if you need to update your office phone number.

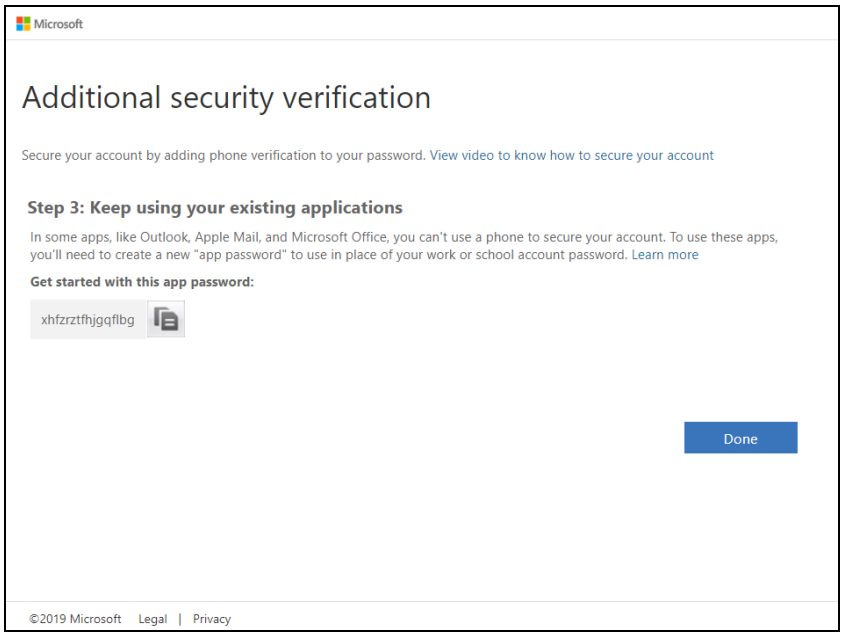


- Mobile app
  - Select which option you like upon using the mobile app
    - Receive notifications for verification
    - Use verification code

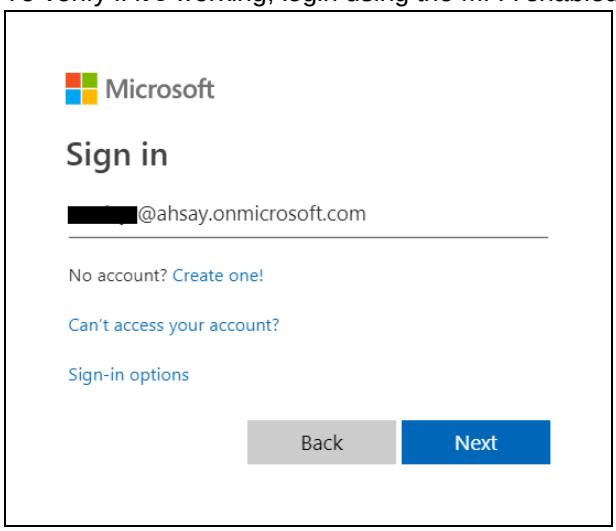
13. If you have selected the first option which is the **Authentication phone** with a method of **Send me a code by text,** you will receive a text message containing the verification code. Ensure that you have indicated a valid mobile number.



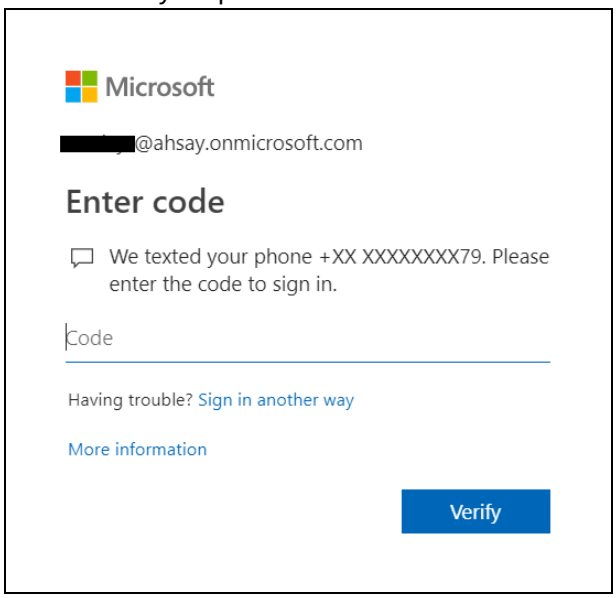


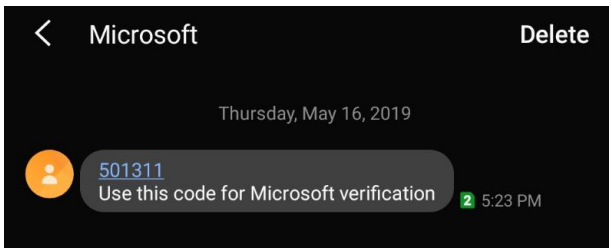


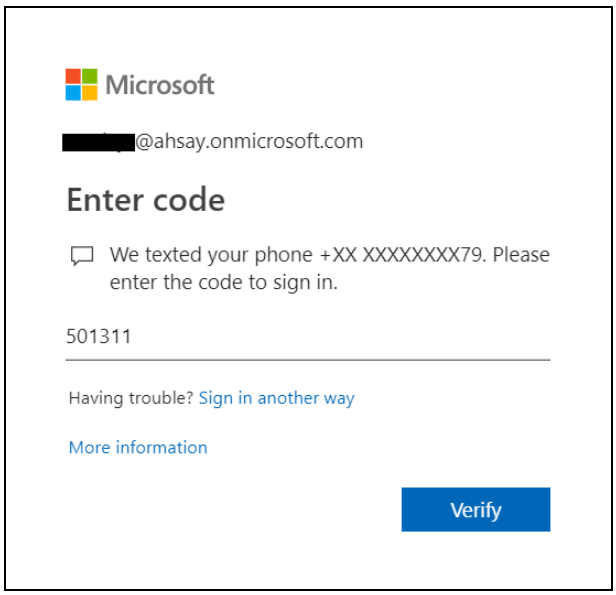
14. To verify if it's working, login using the MFA enabled Microsoft 365 user account.



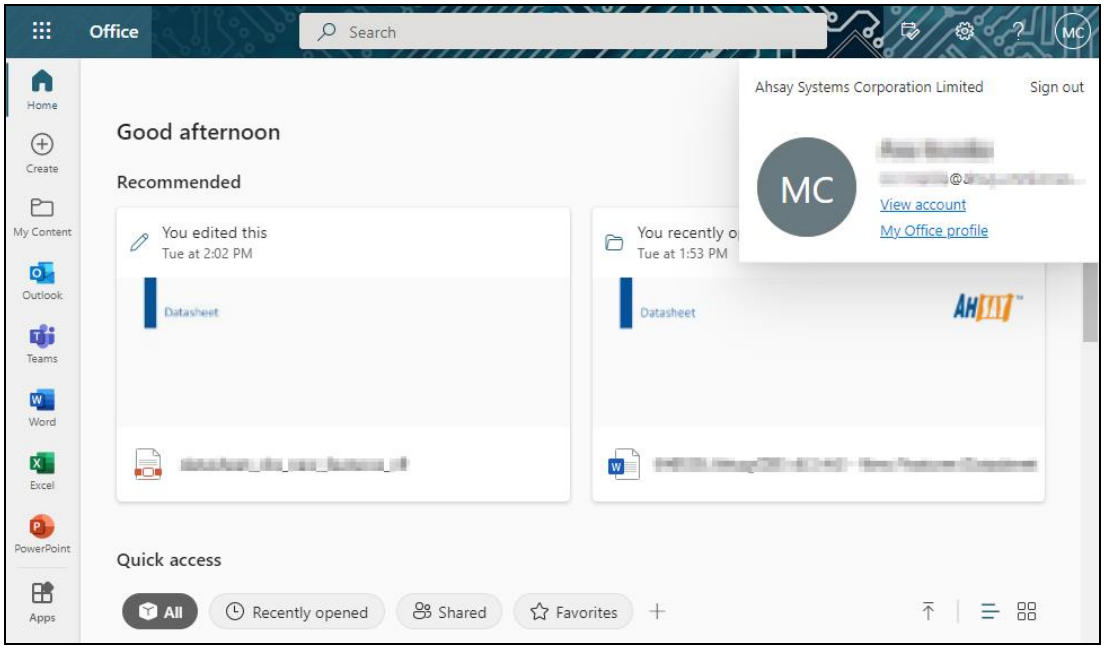
15. Upon logging in, there will be a message that will require you to provide the code that have been sent to your personal mobile number. Click **Verify** to proceed.







16. After the verification process, the screen will be automatically redirected to the Microsoft 365 Main screen.

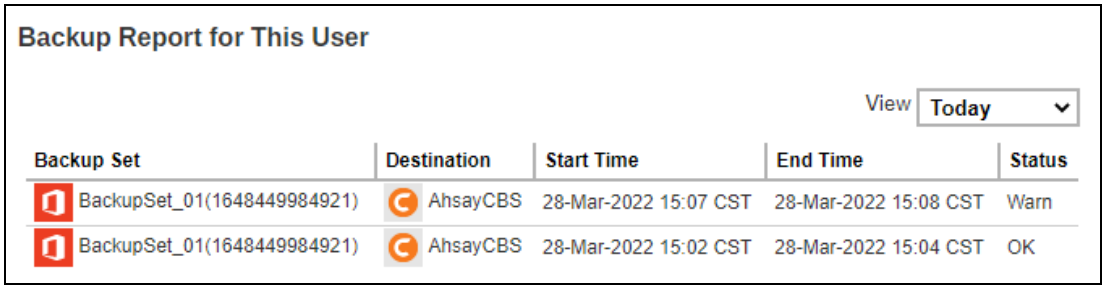


Appendix D: Example Scenario for Backup Set Maintenance

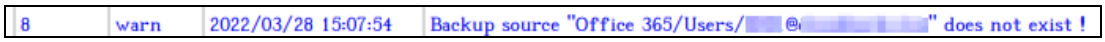
Scenario: Microsoft 365 user account does not exist warning message

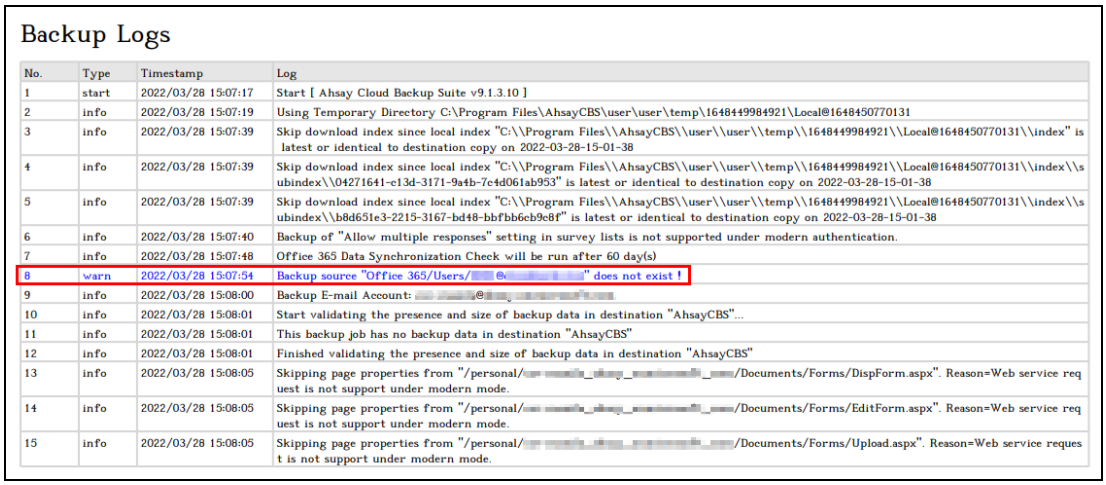
This is the sample warning message if the user does not exist. If a user is removed from the domain and the Admin did not manually unselected the user from the backup source, then during backup job there will be a warning that the user does not exist. The warning will appear on the backup log.

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



Backup report contains a warning message.



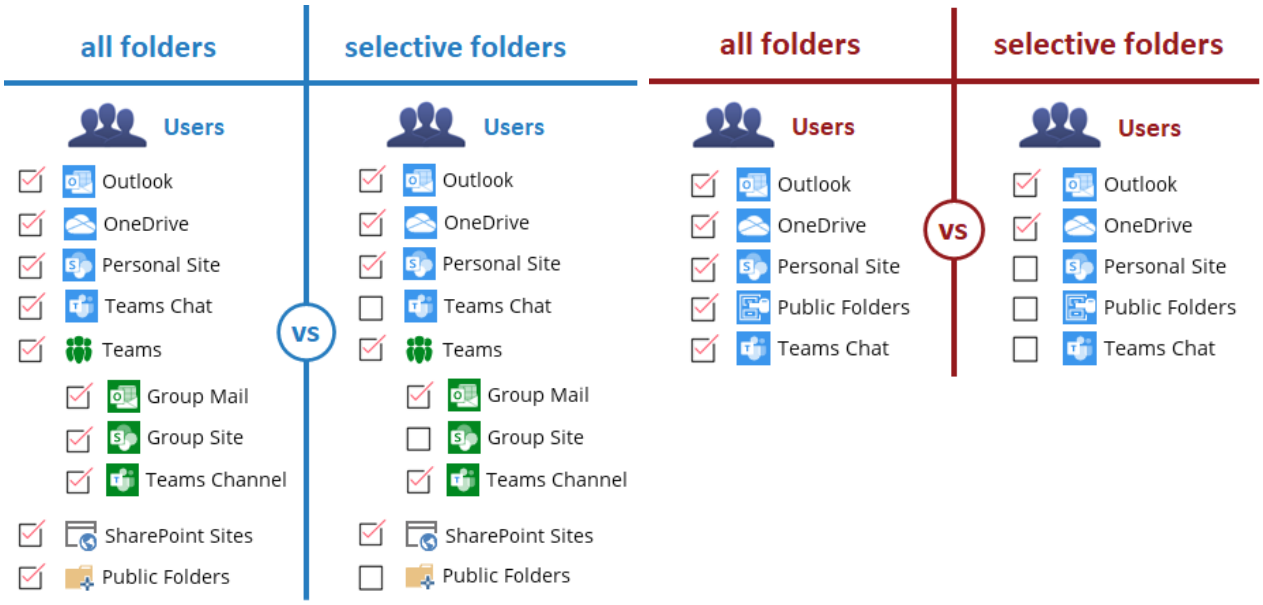


Backup Logs

No.	Type	Timestamp	Log
1	start	2022/03/28 15:07:17	Start [Ahsay Cloud Backup Suite v9.1.3.10]
2	info	2022/03/28 15:07:19	Using Temporary Directory C:\Program Files\AhsayCBS\user\user\temp\1648449984921\Local@1648450770131
3	info	2022/03/28 15:07:39	Skip download index since local index "C:\\Program Files\\AhsayCBS\\user\\user\\temp\\1648449984921\\Local@1648450770131\\index" is latest or identical to destination copy on 2022-03-28-15-01-38
4	info	2022/03/28 15:07:39	Skip download index since local index "C:\\Program Files\\AhsayCBS\\user\\user\\temp\\1648449984921\\Local@1648450770131\\index\\subindex\\04271641-c13d-3171-9a4b-7c4d061ab953" is latest or identical to destination copy on 2022-03-28-15-01-38
5	info	2022/03/28 15:07:39	Skip download index since local index "C:\\Program Files\\AhsayCBS\\user\\user\\temp\\1648449984921\\Local@1648450770131\\index\\subindex\\b8d651e3-2215-3167-bd48-bbfbb6cb9c8f" is latest or identical to destination copy on 2022-03-28-15-01-38
6	info	2022/03/28 15:07:40	Backup of "Allow multiple responses" setting in survey lists is not supported under modern authentication.
7	info	2022/03/28 15:07:48	Office 365 Data Synchronization Check will be run after 60 day(s)
8	warn	2022/03/28 15:07:54	Backup source "Office 365/Users/ does not exist !
9	info	2022/03/28 15:08:00	Backup E-mail Account:
10	info	2022/03/28 15:08:01	Start validating the presence and size of backup data in destination "AhsayCBS"...
11	info	2022/03/28 15:08:01	This backup job has no backup data in destination "AhsayCBS"
12	info	2022/03/28 15:08:01	Finished validating the presence and size of backup data in destination "AhsayCBS"
13	info	2022/03/28 15:08:05	Skipping page properties from "/personal/ /Documents/Forms/DispForm.aspx". Reason=Web service request is not support under modern mode.
14	info	2022/03/28 15:08:05	Skipping page properties from "/personal/ /Documents/Forms/EditForm.aspx". Reason=Web service request is not support under modern mode.
15	info	2022/03/28 15:08:05	Skipping page properties from "/personal/ /Documents/Forms/Upload.aspx". Reason=Web service request is not support under modern mode.

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

Selection of all folders vs selective folders



AhsayOBM AhsayACB

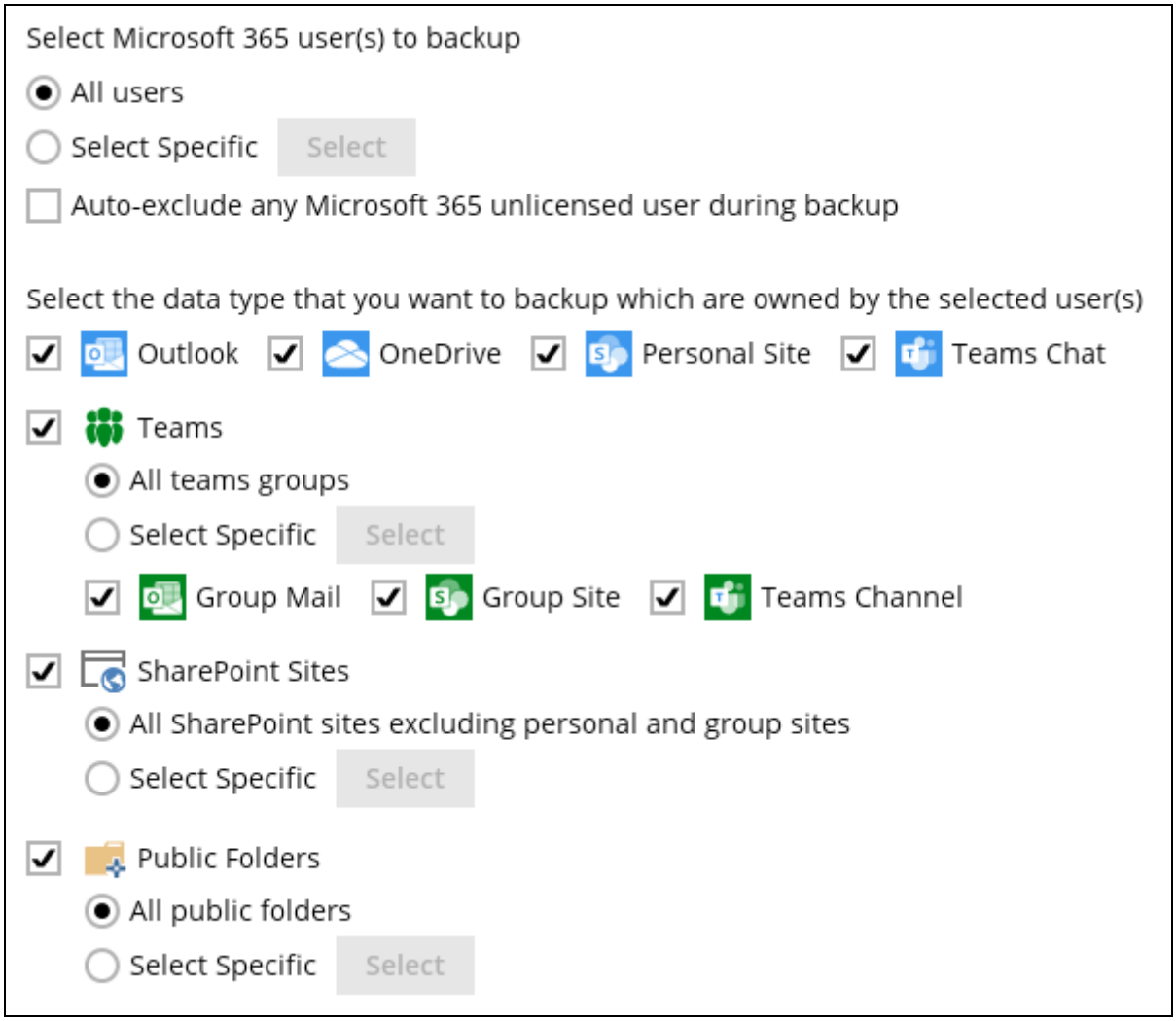
All folders selection

Selecting all folders automatically selects all the files and/or folders under Outlook, OneDrive and Personal Site of the selected Microsoft 365 user account. And all the files and/or folders under Teams, SharePoint Sites and Public Folders of the Microsoft 365 organization for AhsayOBM; only Public Folders for AhsayACB.

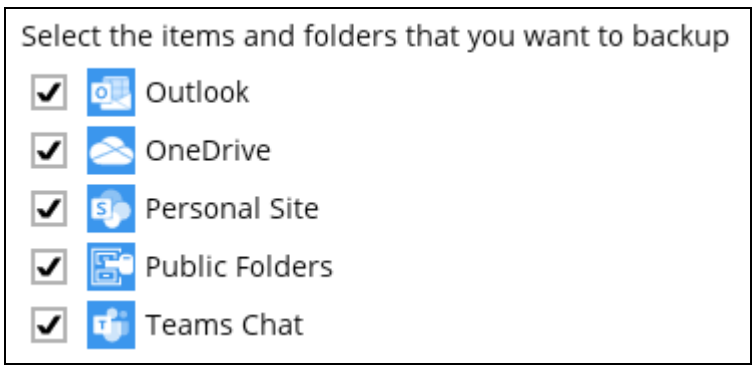
DSC is not required when all the folders are selected for back up. As during a backup job any deleted files in the backup source will be automatically moved to retention area.

Below are the sample screenshot of the backup source with all folders selected.

AhsayOBM



AhsayACB



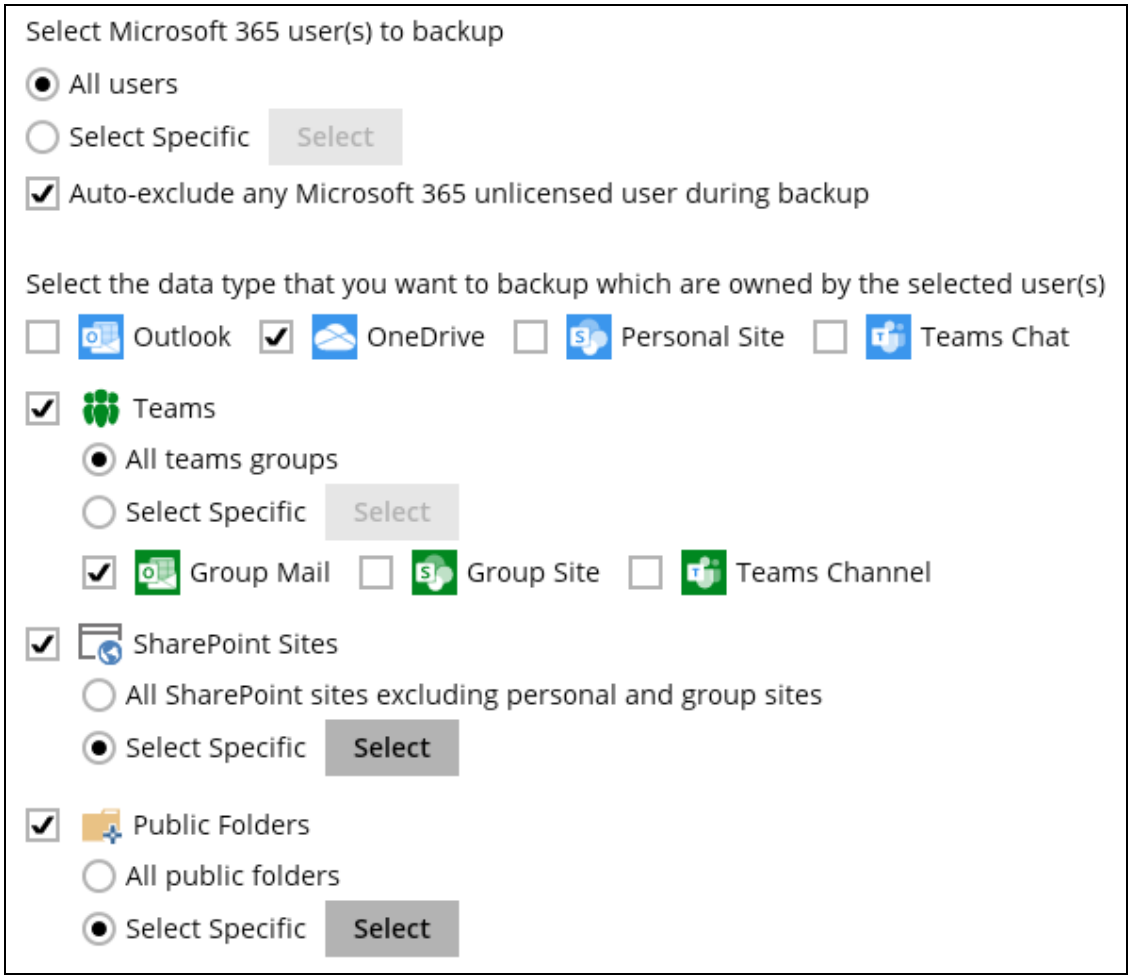
Selective folders

When not all folders are selected for backup and folders are subsequently un-selected from the backup source. The backup job will not pick up the changes of the de-selected folders, they will not be moved to 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 destination.

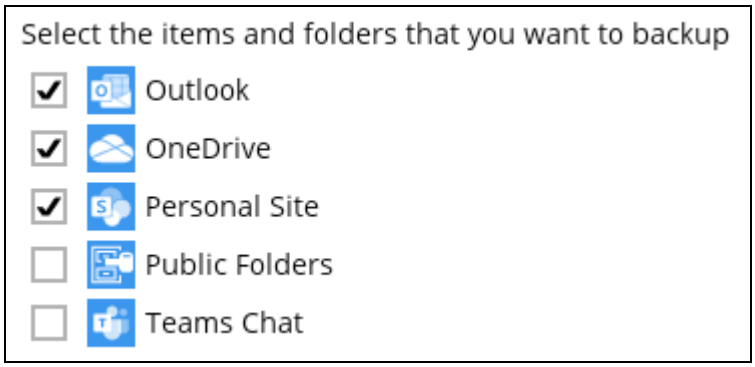
DSC is highly recommended to synchronize de-selected folders in the backup source with the backup destination. This will ensure that there will be no data build up on the backup destination.

Below is the sample screenshot of the backup source with selective folders.

AhsayOBM



AhsayACB



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

Backup Report

Backup Logs

No.	Type	Timestamp	Log
1	start	2022/03/28 15:01:59	Start [Ahsay Cloud Backup Suite v9.1.3.10]
2	info	2022/03/28 15:02:02	Using Temporary Directory C:\Program Files\AhsayCBS\user\user\temp\1648449984921\Local@1648450770131
3	info	2022/03/28 15:02:27	Backup of "Allow multiple responses" setting in survey lists is not supported under modern authentication.
4	info	2022/03/28 15:02:35	Run Office 365 Data Synchronization Check (1st time)
5	info	2022/03/28 15:02:41	Skip backing up E-mail Account "[redacted]", Reason = ""
6	info	2022/03/28 15:02:48	Backup E-mail Account: [redacted]
7	info	2022/03/28 15:02:48	Skipping page properties from "/personal/[redacted]/Documents/Forms/DispForm.aspx". Reason=Web service request is not support under modern mode.
8	info	2022/03/28 15:02:48	Skipping page properties from "/personal/[redacted]/Documents/Forms/EditForm.aspx". Reason=Web service request is not support under modern mode.
9	info	2022/03/28 15:02:48	Skipping page properties from "/personal/[redacted]/Documents/Forms/Upload.aspx". Reason=Web service request is not support under modern mode.
10	info	2022/03/28 15:02:48	Skipping site managed features from "https://ahsay-my.sharepoint.com/personal/[redacted]". Reason=Web service request is not support under modern mode.
11	info	2022/03/28 15:02:48	Skipping web managed features from "https://ahsay-my.sharepoint.com/personal/[redacted]". Reason=Web service request is not support under modern mode.
12	info	2022/03/28 15:02:48	Start validating the presence and size of backup data in destination "AhsayCBS"...
13	info	2022/03/28 15:02:48	This backup job has no backup data in destination "AhsayCBS"
14	info	2022/03/28 15:02:48	Finished validating the presence and size of backup data in destination "AhsayCBS"
15	info	2022/03/28 15:03:25	Deduplication Info: File="Office 365/Site Collections/D901_ahsay-my.sharepoint.com%2fpersonal%2f[redacted]/D001_All Files/D903_Documents/D903_Microsoft Teams Chat Files/F01_guide_cbs_admin_v8_11022021.doc", 0.0% of file size saved by deduplication, number of deduplicated blocks=0, total number of blocks=58, deduplicated size=0, total size=75,529,728

On the sample backup report, it shows the countdown until the next DSC which is in sixty (60) days.

Backup Report

Backup Logs

No.	Type	Timestamp	Log
1	start	2022/03/28 15:32:01	Start [Ahsay Cloud Backup Suite v9.1.3.10]
2	info	2022/03/28 15:32:03	Using Temporary Directory C:\Program Files\AhsayCBS\user\user\temp\1648449984921\Local@1648450770131
3	info	2022/03/28 15:32:25	Skip download index since local index "C:\\Program Files\\AhsayCBS\\user\\user\\temp\\1648449984921\\Local@1648450770131\\index" is latest or identical to destination copy on 2022-03-28-15-07-05
4	info	2022/03/28 15:32:25	Skip download index since local index "C:\\Program Files\\AhsayCBS\\user\\user\\temp\\1648449984921\\Local@1648450770131\\index\\subindex\\04271641-e13d-3171-9a4b-7e4d061ab953" is latest or identical to destination copy on 2022-03-28-15-07-05
5	info	2022/03/28 15:32:25	Download valid index files from backup job "2022-03-28-15-07-05" to "C:\\Program Files\\AhsayCBS\\user\\user\\temp\\1648449984921\\Local@1648450770131\\index\\subindex\\2b51a316-0a7e-375d-bb91-041688da39a5".
6	info	2022/03/28 15:32:25	Skip download index since local index "C:\\Program Files\\AhsayCBS\\user\\user\\temp\\1648449984921\\Local@1648450770131\\index\\subindex\\b8d651e3-2215-3167-bd48-bbfbb6cb9c8f" is latest or identical to destination copy on 2022-03-28-15-07-05
7	info	2022/03/28 15:32:26	Backup of "Allow multiple responses" setting in survey lists is not supported under modern authentication.
8	info	2022/03/28 15:32:34	Office 365 Data Synchronization Check will be run after 60 day(s)
9	info	2022/03/28 15:32:39	Skip backing up E-mail Account "[redacted]", Reason = ""
10	info	2022/03/28 15:32:46	Backup E-mail Account: [redacted]
11	info	2022/03/28 15:32:47	Start validating the presence and size of backup data in destination "AhsayCBS"...
12	info	2022/03/28 15:32:47	This backup job has no backup data in destination "AhsayCBS"
13	info	2022/03/28 15:32:47	Finished validating the presence and size of backup data in destination "AhsayCBS"
14	info	2022/03/28 15:32:52	Skipping site managed features from "https://ahsay-my.sharepoint.com/personal/[redacted]". Reason=Web service request is not support under modern mode.
15	info	2022/03/28 15:32:52	Skipping web managed features from "https://ahsay-my.sharepoint.com/personal/[redacted]". Reason=Web service request is not support under modern mode.
16	info	2022/03/28 15:32:53	Start validating the presence and size of backup data in destination "AhsayCBS"...

On the sample backup report, it shows the countdown is done and DSC is running.

Backup Report

Backup Logs

No.	Type	Timestamp	Log
1	start	2022/03/28 15:01:59	Start [Ahsay Cloud Backup Suite v9.1.3.10]
2	info	2022/03/28 15:02:02	Using Temporary Directory C:\Program Files\AhsayCBS\user\user\temp\1648449984921\Local@1648450770131
3	info	2022/03/28 15:02:27	Backup of "Allow multiple responses" setting in survey lists is not supported under modern authentication.
4	info	2022/03/28 15:02:35	Run Office 365 Data Synchronization Check
5	info	2022/03/28 15:02:41	Skip backing up E-mail Account "[redacted]", Reason = ""
6	info	2022/03/28 15:02:48	Backup E-mail Account: [redacted]
7	info	2022/03/28 15:02:48	Skipping page properties from "/personal/[redacted]/Documents/Forms/DispForm.aspx". Reason=Web service request is not support under modern mode.
8	info	2022/03/28 15:02:48	Skipping page properties from "/personal/[redacted]/Documents/Forms/EditForm.aspx". Reason=Web service request is not support under modern mode.
9	info	2022/03/28 15:02:48	Skipping page properties from "/personal/[redacted]/Documents/Forms/Upload.aspx". Reason=Web service request is not support under modern mode.
10	info	2022/03/28 15:02:48	Skipping site managed features from "https://ahsay-my.sharepoint.com/personal/[redacted]". Reason=Web service request is not support under modern mode.
11	info	2022/03/28 15:02:48	Skipping web managed features from "https://ahsay-my.sharepoint.com/personal/[redacted]". Reason=Web service request is not support under modern mode.
12	info	2022/03/28 15:02:48	Start validating the presence and size of backup data in destination "AhsayCBS"...
13	info	2022/03/28 15:02:48	This backup job has no backup data in destination "AhsayCBS"
14	info	2022/03/28 15:02:48	Finished validating the presence and size of backup data in destination "AhsayCBS"
15	info	2022/03/28 15:03:25	Deduplication Info: File="Office 365/Site Collections/D901_ahsay-my.sharepoint.com%2fpersonal%2f[redacted]/D001_All Files/D903_Documents/D903_Microsoft Teams Chat Files/F01_guide_cbs_admin_v8_11022021.doc", 0.0% of file size saved by deduplication, number of deduplicated blocks=0, total number of blocks=58, deduplicated size=0, total size=75,529,728

On the sample backup report, it shows that DSC is disabled.

Backup Report

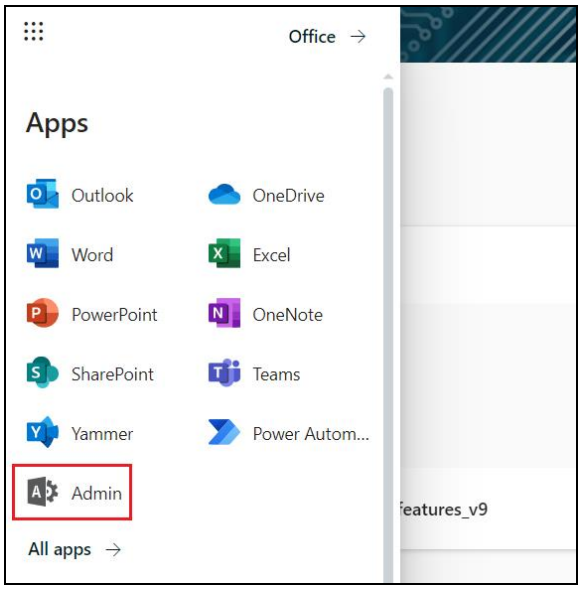
Backup Logs

No.	Type	Timestamp	Log
1	start	2022/03/30 12:00:05	Start [Ahsay Cloud Backup Suite v9.1.3.18]
2	info	2022/03/30 12:00:08	Using Temporary Directory C:\Program Files\AhsayCBS\user\user\temp\1648612357454\Local@1648612503906
3	info	2022/03/30 12:00:31	Index file does not exist in the destination backup job folder "null"
4	info	2022/03/30 12:00:31	Create new index since no valid index exist on both local and destination
5	info	2022/03/30 12:00:33	Backup of "Allow multiple responses" setting in survey lists is not supported under modern authentication.
6	info	2022/03/30 12:00:41	Office 365 Data Synchronization Check is disabled (Debug option - Office365.DSCInterval = -1)
7	info	2022/03/30 12:00:46	[List] 100% (0/0) Listing items from: ([redacted])
8	info	2022/03/30 12:00:47	[List] 100% (22/22) Listing items from: Top of Information Store ([redacted])
9	info	2022/03/30 12:00:48	Index file does not exist in the destination backup job folder "null/b8d651e3-2215-3167-bd48-bbfbb6cb9c8f"
10	info	2022/03/30 12:00:48	Create new index since no valid index exist on both local and destination
11	info	2022/03/30 12:00:53	Backup E-mail Account: csv-manila@ahsay.onmicrosoft.com
12	info	2022/03/30 12:00:53	[List] 100% (0/0) Listing items from: Archive ([redacted])
13	info	2022/03/30 12:00:53	[List] 100% (1/1) Listing items from: Calendar ([redacted])
14	info	2022/03/30 12:00:53	[List] 100% (2/2) Listing items from: Calendar ([redacted])
15	info	2022/03/30 12:00:53	[List] 100% (0/0) Listing items from: Calendar/Birthdays ([redacted])
16	info	2022/03/30 12:00:54	[List] 100% (97/97) Listing items from: Calendar/United Kingdom holidays ([redacted])
17	info	2022/03/30 12:00:54	[List] 100% (0/0) Listing items from: Contacts ([redacted])
18	info	2022/03/30 12:00:54	[List] 100% (7/7) Listing items from: Contacts ([redacted])
19	info	2022/03/30 12:00:54	[List] 100% (0/0) Listing items from: Deleted Items ([redacted])
20	info	2022/03/30 12:00:54	[List] 100% (0/0) Listing items from: Drafts ([redacted])
21	info	2022/03/30 12:01:08	[List] 80% (512/635) Listing items from: Inbox ([redacted])

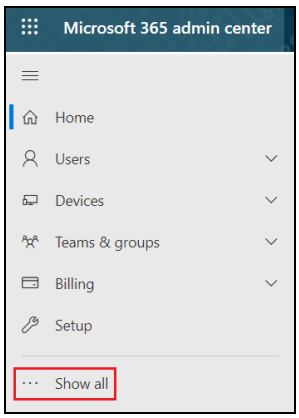
Appendix F: How to view Item count and Storage used in Microsoft 365 Admin Center

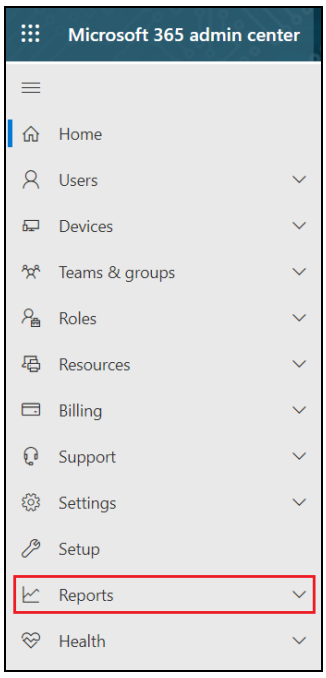
To view the item count and storage size of Microsoft 365 user account based on the usage for Exchange (Outlook), OneDrive, and SharePoint, follow the instructions below:

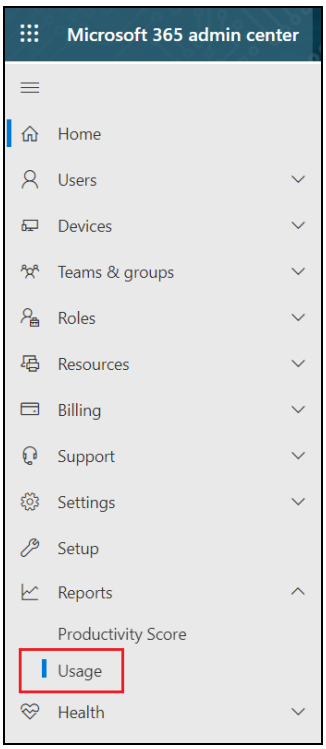
1. Login to the Microsoft 365 (https://login.microsoft.com).
2. Go to Microsoft 365 admin center.



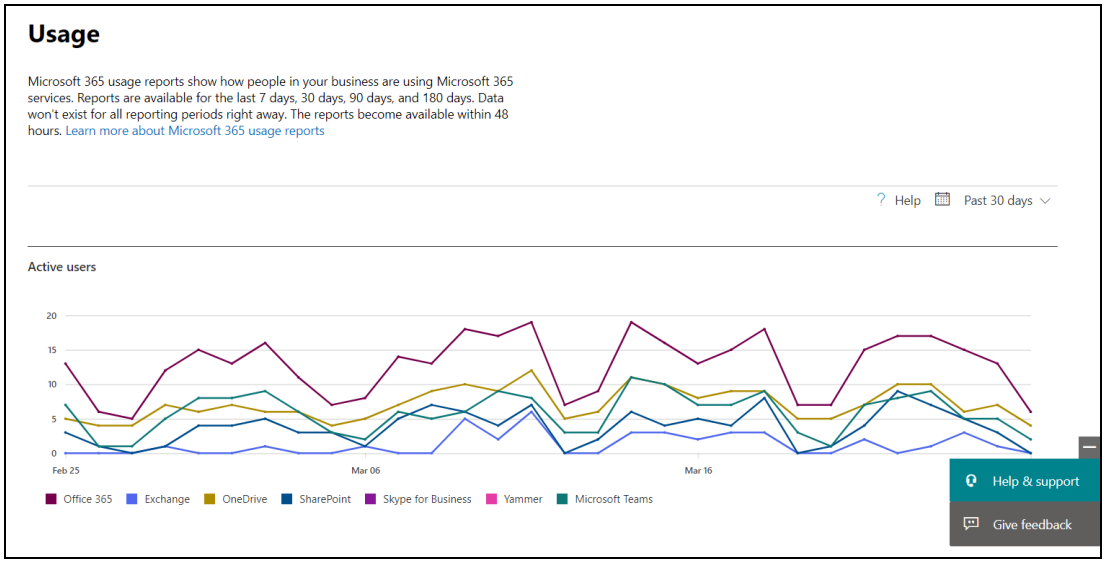
3. On the Microsoft 365 admin center, click **Show all** then click the dropdown arrow for the **Reports** and select **Usage**.

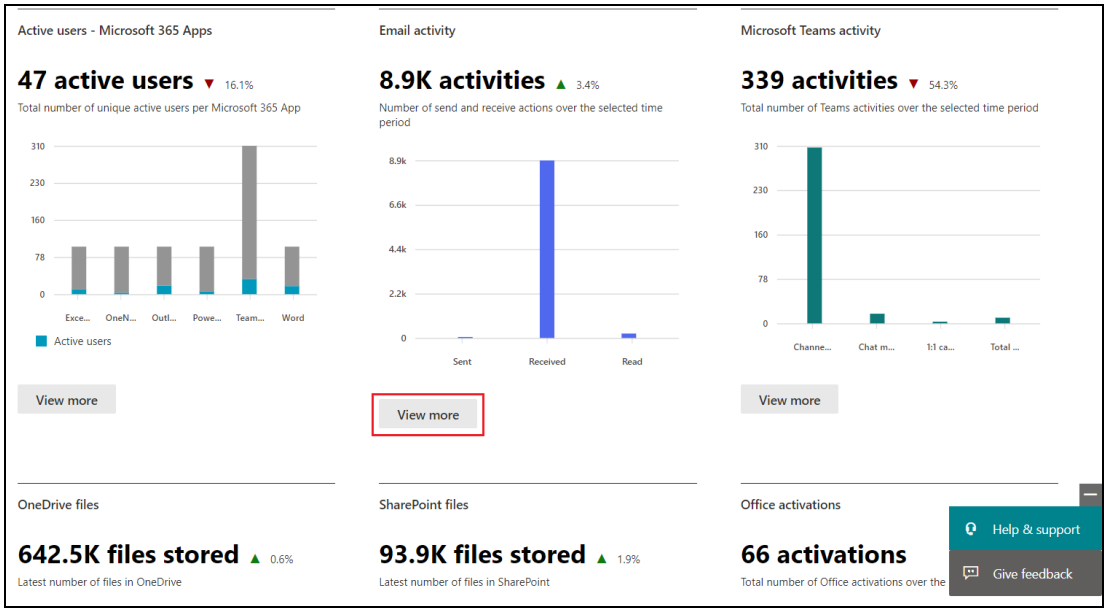




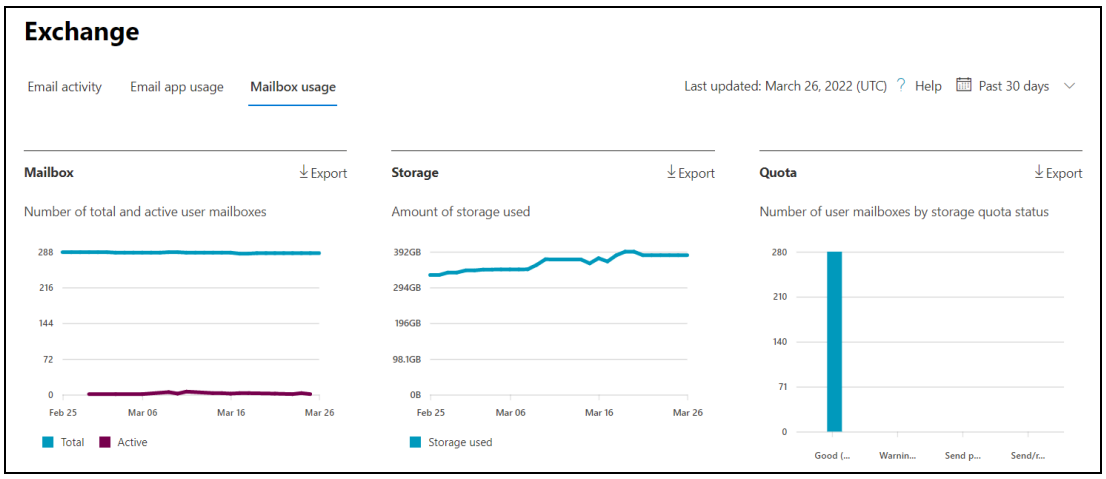


4. On the Usage screen, scroll down and click the **View more** button of the usage report that you want to view.



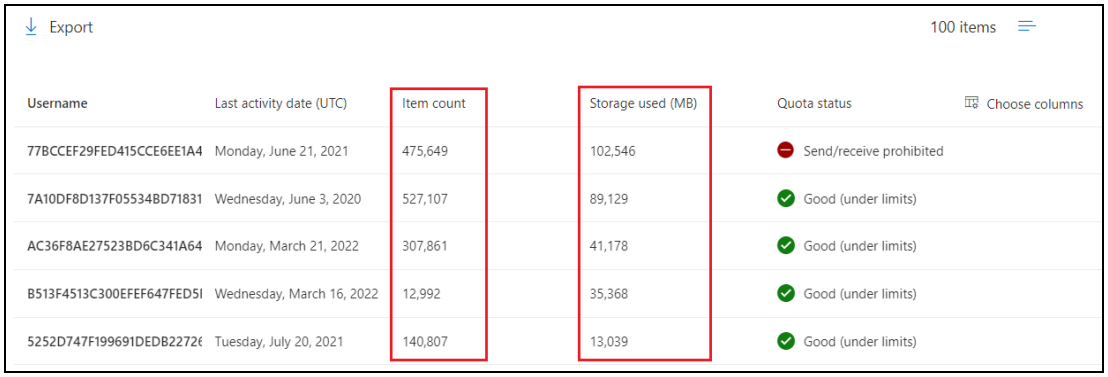


5. For **Exchange**, click the **View More** button under Email activity, then go to **Mailbox usage**.

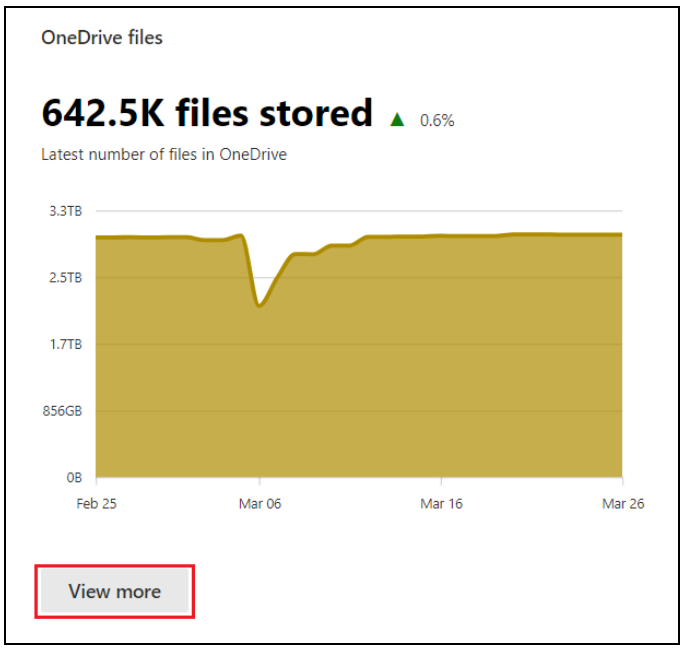


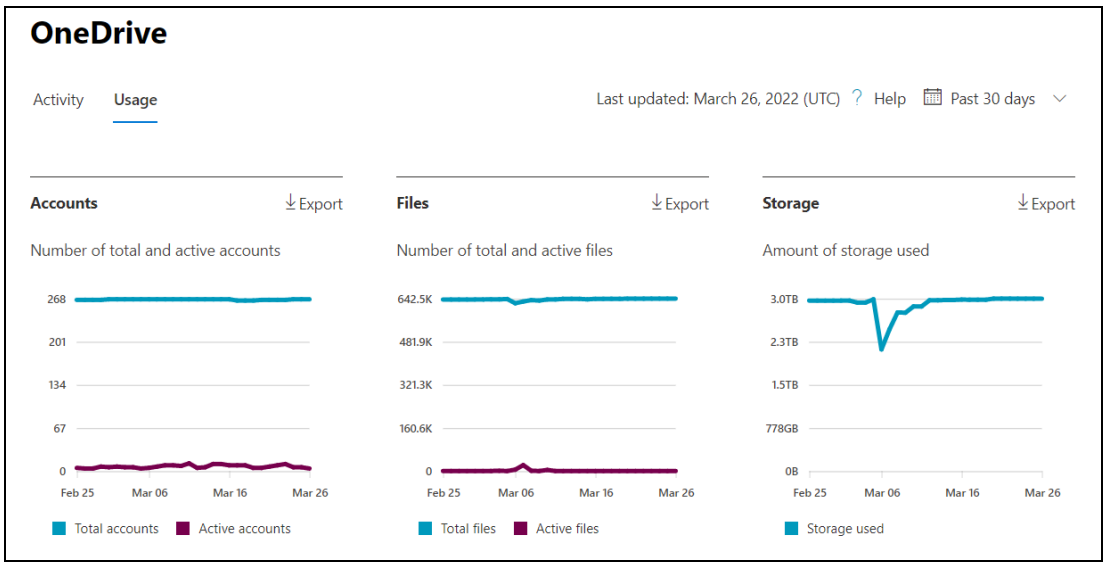
Highlighted columns are, Item count and Storage used (MB).

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



6. For **OneDrive**, click the **View More** button under OneDrive files.



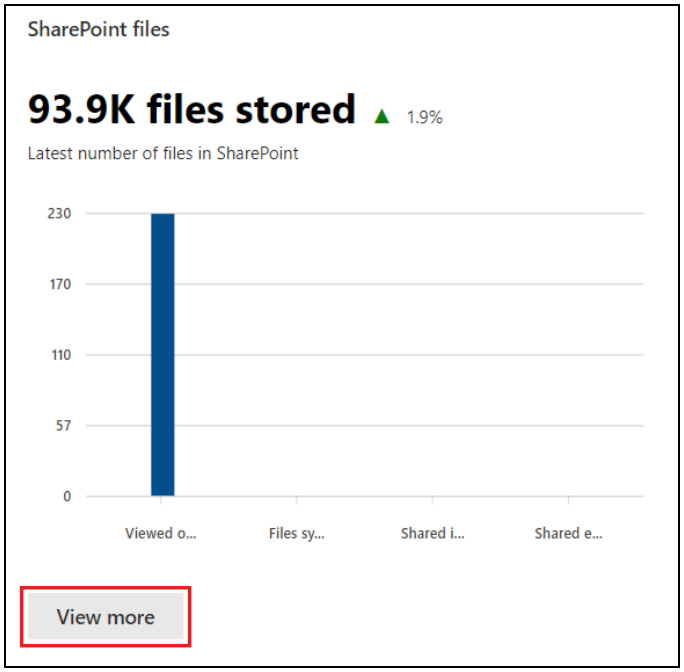


Highlighted columns are, Files and Storage used (MB).

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

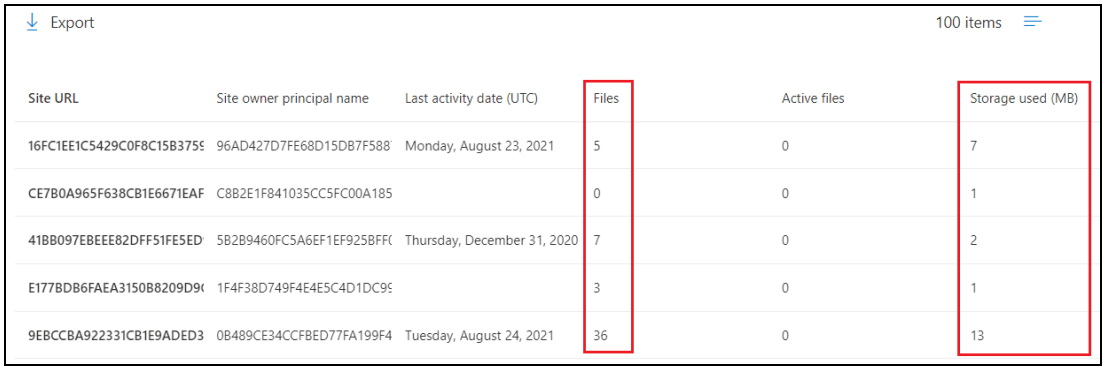
URL	Owner principal name	Last activity date (UTC)	Files	Active files	Storage used (MB)
85020A16D191961B6FF5F9F9(	EF2D97C6B7E96131AB26327C		0	0	2
133C6F634EDAED8B325F34A	87BACCAFAFB7D267C6F7609:	Tuesday, March 22, 2022	5	1	150
F1814962EA16EFFDDC1DED21	E3CFB36D2C508888C216EF8B		0	0	2
B83A4C6013BFA395AAB499E	A6520A6D09563C27BDFBEAD	Wednesday, March 3, 2021	15	0	6
3450D92B766F9ABDFD6CA6(	047D65F02E3C4F1EDE4B5753	Thursday, September 2, 2021	79	0	273

7. For **SharePoint**, click the **View More** button under SharePoint files then go to **Site usage**.



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

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



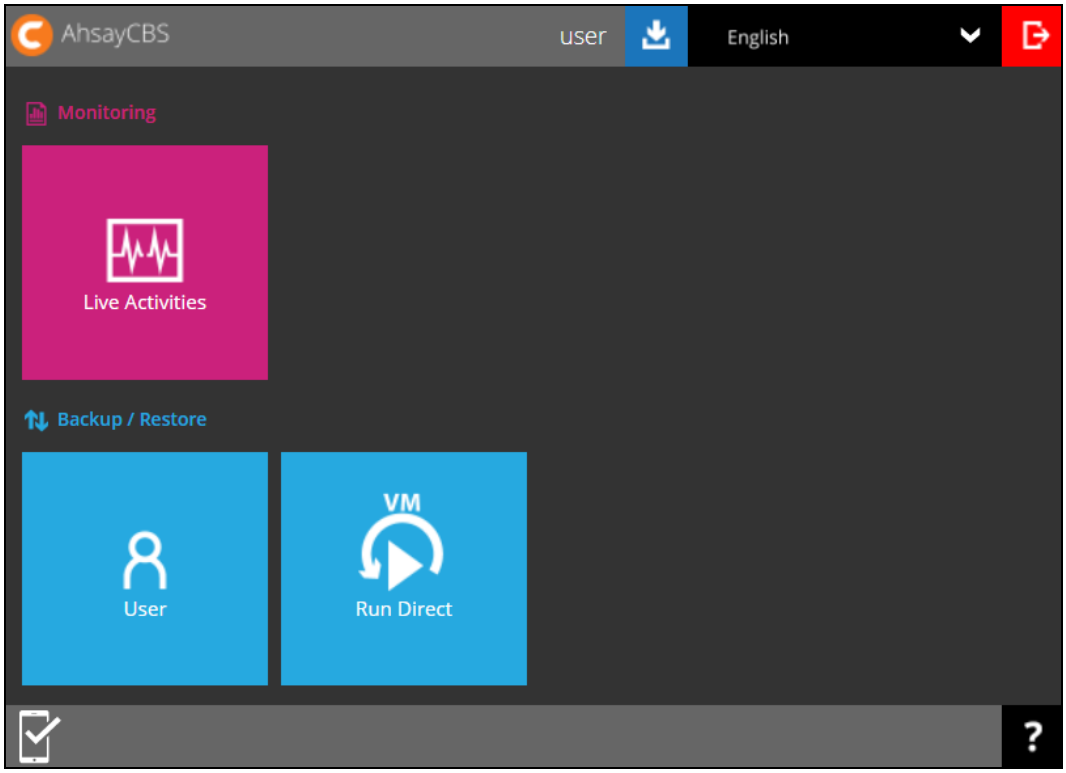
Appendix G: Re-Authentication of Microsoft 365 Backup Set

After upgrading to AhsayCBS v9 or above, Microsoft 365 backup settings of existing backup sets must be updated. 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 backup set.

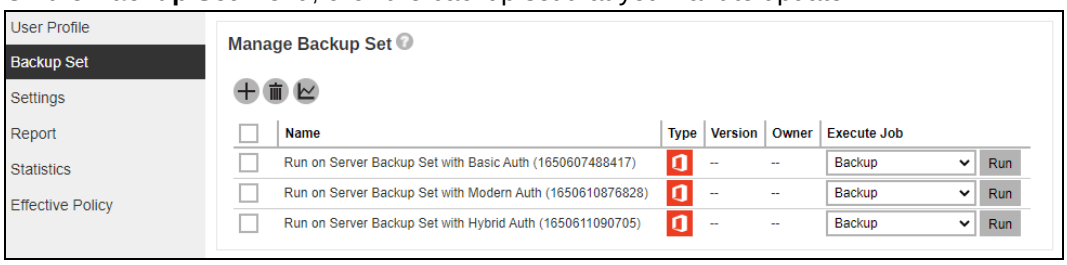
To update the backup settings, follow the instructions below:

1. Log out all Microsoft 365 account on the default browser before starting the update of backup set.
2. Log in to the User Web Console.

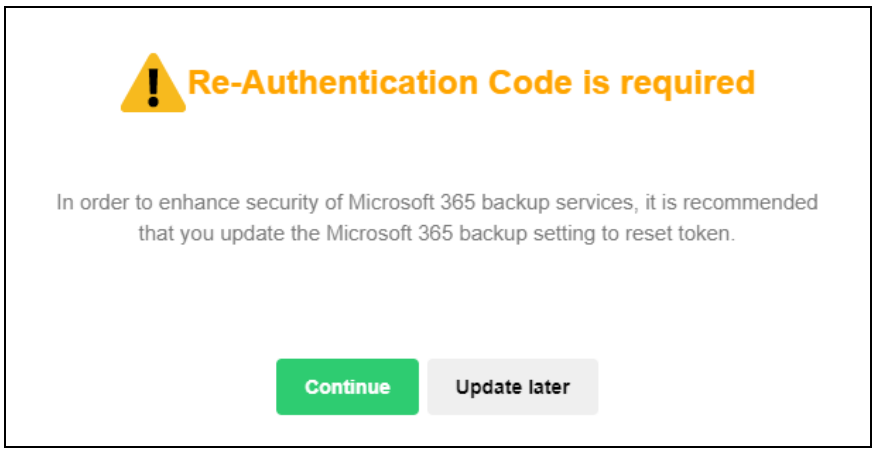
   For instructions on how to do this please refer to Chapter 2 of the AhsayCBS v9 User Guide.
3. Click the **User** icon on the User Web Console landing page.



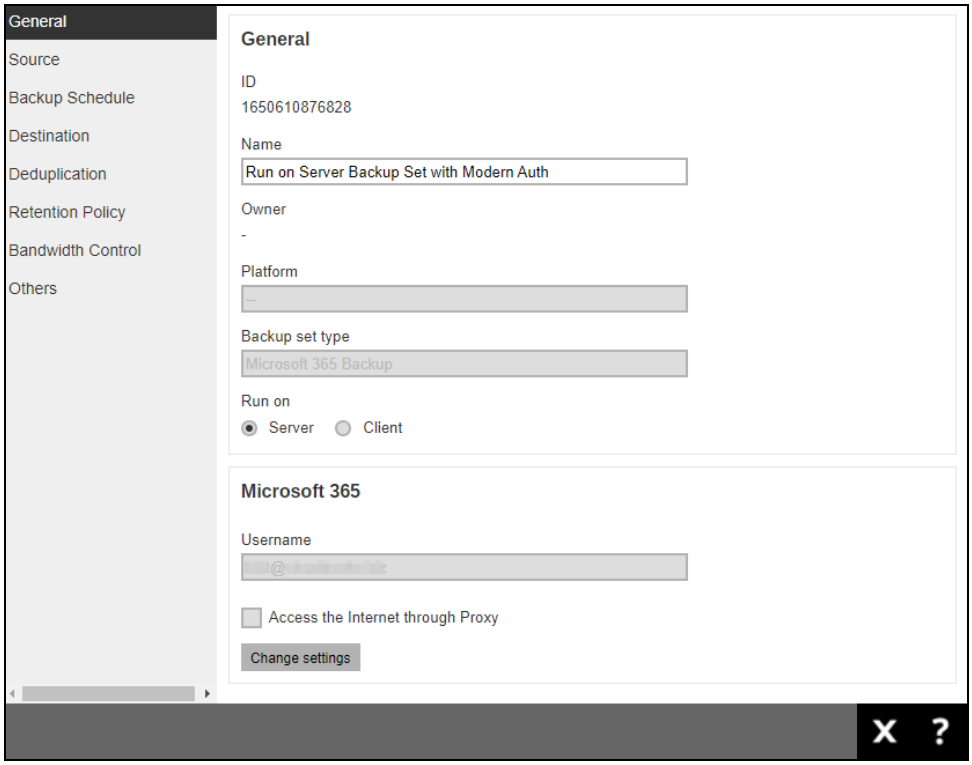
4. On the **Backup Set** menu, click the backup set that you want to update.



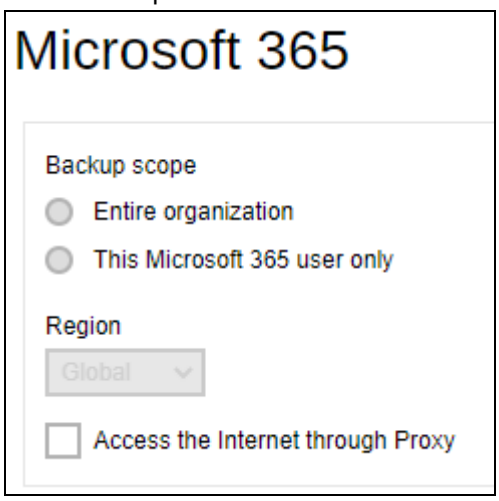
5. If the backup set is using Basic Authentication, this pop up message will be displayed. Click **Continue**.



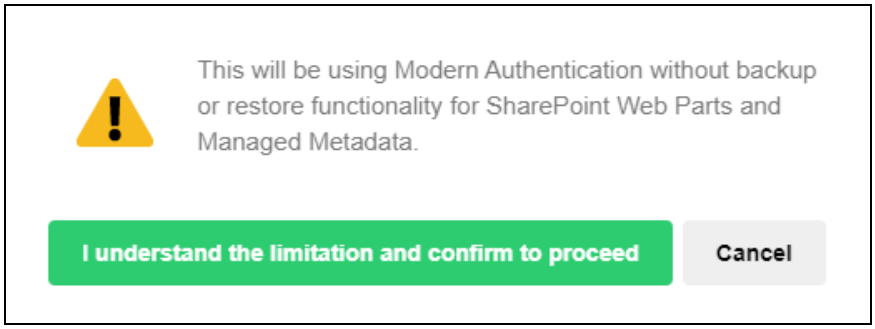
If the backup set is using Modern or Hybrid Authentication, click **Change settings**.



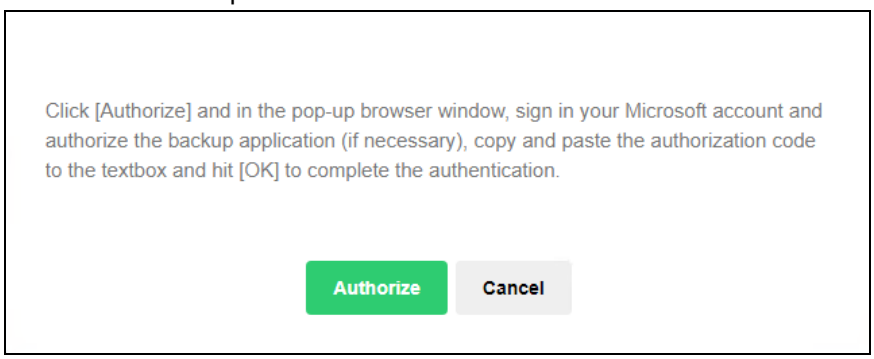
6. Click to proceed with the authentication process.



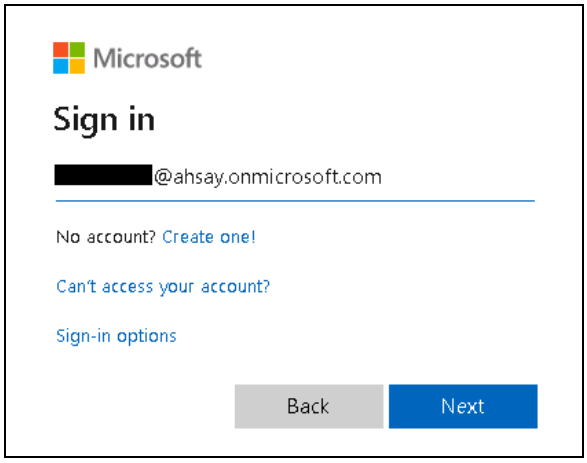
7. Click **I understand the limitation and confirm to proceed**.

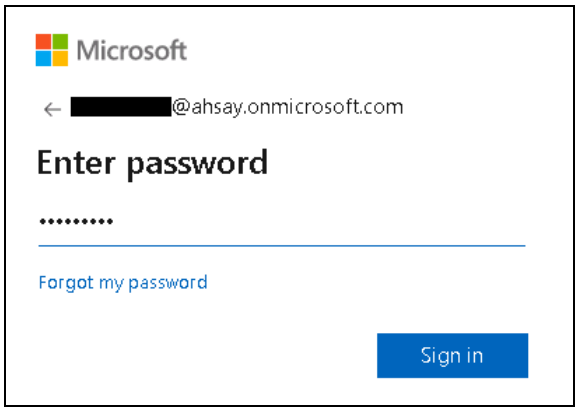


8. Click **Authorize** to proceed with the authentication.



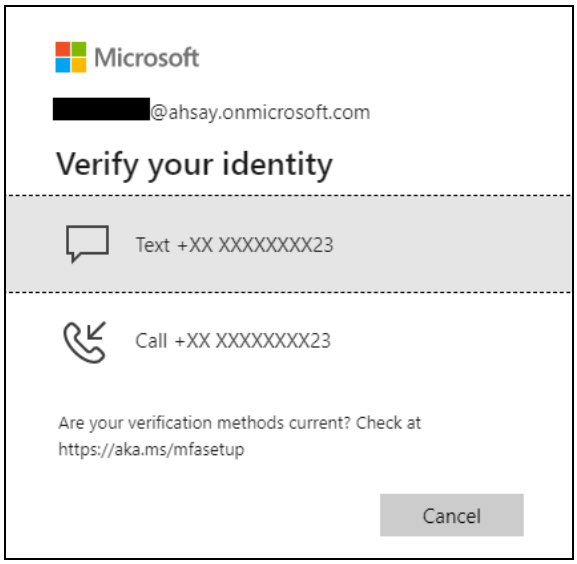
9. Sign in to your Microsoft 365 account.



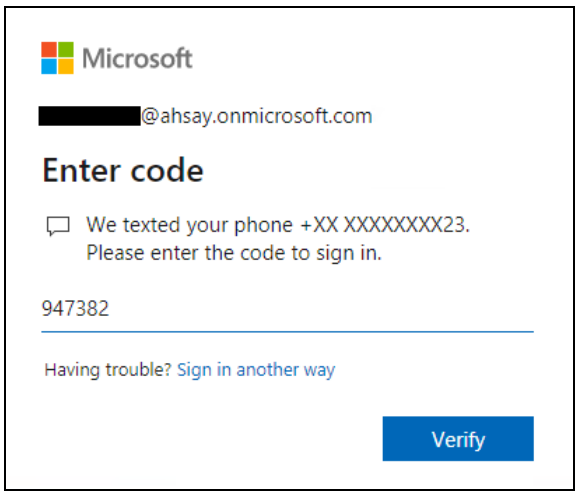


If MFA is enforced, select from Text or Call to verify your identity.

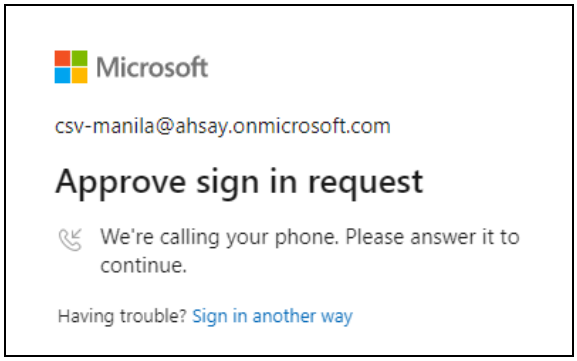
Otherwise proceed to the next step.



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



If Call is selected, answer the call and follow the instructions given to verify the account.

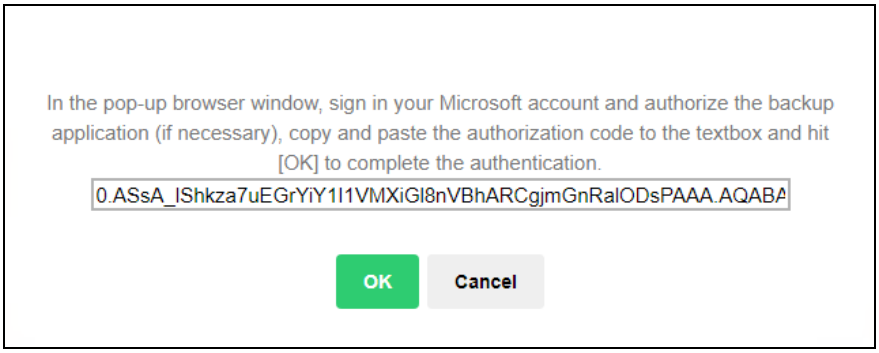
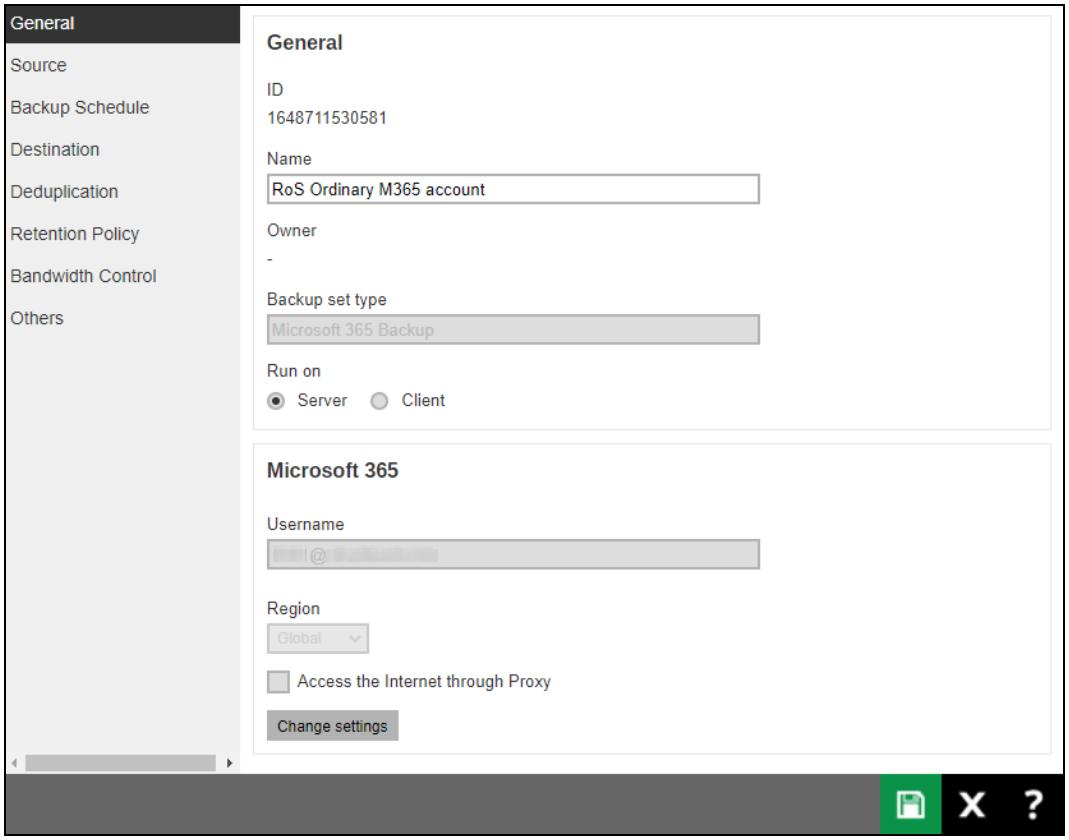


NOTE

The verification code will only be required if the MFA status of a Microsoft 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 update.