NetApp SaaS Backup for Microsoft 365 documentation

SaaS Backup for Microsoft 365

NetApp
October 22, 2024

This PDF was generated from https://docs.netapp.com/us-en/saasbackupO365/index.html on October 22, 2024. Always check docs.netapp.com for the latest.

Table of Contents

NetApp SaaS Backup for Microsoft 365 documentation . . . 1
- Get started . . . 1
- Provide feedback, get help, or find more information . . . 1

Release notes . . . 2
- New features and updates . . . 2
- New features and updates - Archived . . . 5
- Known problems and limitations . . . 7

Concepts . . . 9
- NetApp SaaS Backup for Microsoft 365 Overview . . . 9
- Storage types you can use with SaaS Backup . . . 10

Get started . . . 11
- Workflow for getting started . . . 11
- Create a new Microsoft 365 service account . . . 13
- Configure Impersonation for Microsoft Exchange Online . . . 16
- Sign up for SaaS Backup for Microsoft 365 . . . 18
- Schedule your first backup . . . 20
- Perform an immediate backup of a specific backup policy . . . 20
- Data deletion . . . 21

Manage services . . . 22
- Activate a service . . . 22
- Deactivate a service . . . 22
- Activate support . . . 22
- Discover new mailboxes, sites, and groups . . . 23
- Purge a user, site collection, or Microsoft 365 group . . . 24
- Enable Modern Authentication . . . 24

Manage settings . . . 26
- Backup policies . . . 26
- Backup settings . . . 26
- Set notifications . . . 28
- Permissions . . . 29
- Role-based account access . . . 30

Manage users . . . 33
- Licenses . . . 33
- Rules . . . 34
- Security groups . . . 36

Manage backups . . . 38
- Schedule a backup or changing backup frequency . . . 38
- Perform an immediate backup of a service . . . 39
- Browse backups . . . 39
- Cancel a job . . . 40
- Update the backup retention period . . . 41
- Enable backups for OneNote . . . 42
- Templates and apps supported for backup in Microsoft SharePoint Online . . . 42

Manage restores . . . 45
About restores . . . 45
Perform a high-level service restore . . . 47
Perform a granular-level restore . . . 50
Restore from a previous backup . . . 62
Cancel a job . . . 64
Find restored files . . . 64
View data . . . 65
Create a user defined filter . . . 65
Perform a search . . . 66
Use Advanced Search for Microsoft Exchange Online . . . 67
View job history and activity log . . . 69
View a list of deprovisioned items . . . 70
View a list of purged data . . . 70
View deleted items . . . 71
Download logs . . . 71
Monitor user data . . . 72
Migrate data . . . 73
Provide feedback . . . 75
Where to get help and find more information . . . 76
Legal notices . . . 77
Copyright . . . 77
Trademarks . . . 77
Patents . . . 77
Privacy policy . . . 77
Open source . . . 77

NetApp SaaS Backup for Microsoft 365 documentation

NetApp SaaS Backup is a secure, web-based, software-as-a-service (SaaS) offering that backs up your Microsoft 365 data to Amazon S3 storage and Microsoft Azure Blob storage.

Get started

Get started with a paid subscription

Provide feedback, get help, or find more information

- Provide feedback
- Where to get help and find more information
- Product Page
- Solution Brief

Release notes

New features and updates

The following new features and updates have been added to this release of NetApp SaaS Backup for Microsoft 365.

October 2022

- Data migration is now possible in SaaS Backup for Microsoft 365. Account administrators can request data migration to tenant-owned Amazon S3 and Azure Blob storage destination buckets. Learn how to migrate data.
- The SaaS Backup Export Utility tool is now available and facilitates the export of your migrated data to Amazon S3 and Azure Blob storage destination buckets, or local storage. Sign in to the NetApp Support Tools page and search for the NetApp SaaS Backup Bulk Export Tool.

November 2021

Microsoft 365 targets October 2021 to deprecate Basic Authentication in Exchange Online. For more information, see Basic Authentication and Exchange Online - September 2021 Update. After deprecation, discovery failures can occur for Microsoft 365 groups, and Shared and Archive mailboxes. You can enable Modern Authentication at any time to avoid these failures.

If you are a new customer, Modern Authentication is enabled when you sign up. No action is needed.

If you are an existing customer and have not enabled Modern Authentication, you need to take action. See Enable Modern Authentication.

December 2020

If you deploy Microsoft Azure in the US, your data will not leave your Microsoft environment. During the sign-up process for SaaS Backup for Microsoft 365, you can use Azure Blob storage or your own storage.

Sign up for SaaS Backup from a paid subscription

November 2020

- Starting this month, you can monitor user data for all services. With this new functionality you can download an Excel file to monitor several user data types like email or url addresses, mailbox types, license use, discovery state, last discovery, backup status, backup tier, and more.

  Monitor user data

- Now you can restore your Microsoft Office 365 Groups to another group.

  Perform a high-level restore

- OneDrive for Business license holders can release licenses and purge users without restrictions.

  Release a user license
  Purge a user, site collection, or Microsoft 365 group

- When searching in the job history log, you can now filter by job completion status in addition to job type, service, start time, and end time.

  View job history

June 2020

- SaaS Backup for Microsoft 365 now supports advanced search capabilities for Exchange Online users. After **Advanced Search** is enabled, you can search for individual, shared, and archive mailbox items within the last six months of backup data.

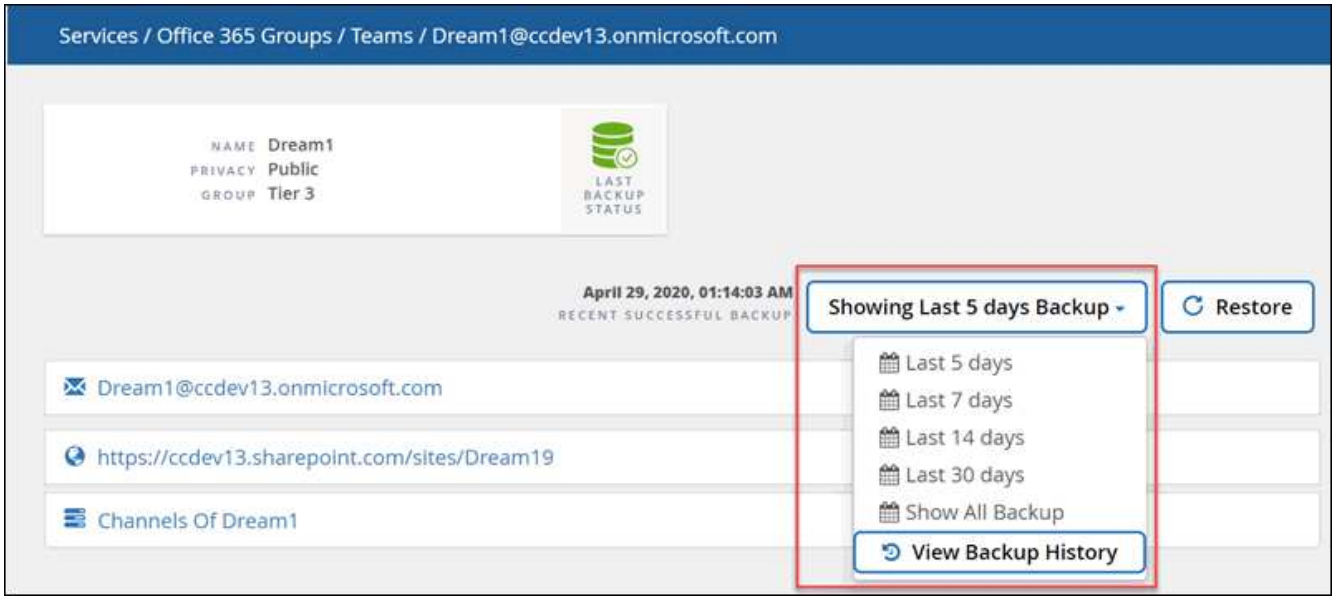
  Use Advanced Search

  To enable this feature, go to Support and submit a request.

  You can also email the SaaS Backup support team at saasbackupsupport@netapp.com.

March/April 2020

- Now you can select different time ranges to browse backups for Microsoft 365 Exchange, SharePoint, OneDrive for Business, and Groups for protected users.



  Browse backups

- SaaS Backup for Microsoft 365 now supports backup to Microsoft TeamsChat. With this new functionality, you can backup and restore your conversations, channels, tabs, attachments, members, and settings found in Microsoft TeamsChat.

  Perform an immediate backup of a service

  To enable this feature, go to Support and submit a request.

  You can also email the SaaS Backup support team at saasbackupsupport@netapp.com.

January 2020

- You can now view mailboxes, sites, mysites, groups, or accounts that have been deprovisioned.
  View deprovisioned items
- User licenses are now automatically release seven days after the accounts are purged. You can view a list of items scheduled to be purged within seven days and list of items that have already been purged.
  View a list of purged data
- Backup for Microsoft OneNote notebooks is now supported for Microsoft SharePoint Online and OneDrive for Business.
  Enable backups for OneNote

September 2019

- You can now activate support for paid subscriptions of SaaS Backup.
  Activating support enables you to access technical support over the phone, online chat, or web ticketing system.

  Activate Support

June 2019

- SaaS Backup for Microsoft 365 now supports the backup and restore of items created using the copy-to feature in Microsoft SharePoint Online and Microsoft OneDrive for Business.
- Enhancements have been made to include additional details in the restore statistics including restore size, restore location, and additional comments.

May 2019

- SaaS Backup now supports add-on licenses.

  Update subscription information

April 2019

- SaaS Backup for Microsoft 365 now supports deletion of security groups.

  Delete security groups

- Shared mailboxes no longer consume a user license.

March 2019

- SaaS Backup for Microsoft 365 now supports multiple backup locations in each supported region.

  You can now choose any of the available locations in your selected region as the site for your data backup. Choosing the location that is geographically closest to the location of your data is recommended. The location recommended by SaaS Backup is marked as **preferred** in the list of options.

- You can now release user licenses and make them available for other users.
  Release a user license

February 2019

- SaaS Backup for Microsoft 365 now supports the following:
  - Backup and restore of archive mailboxes.
  - Enhanced backup and restore statistics across Microsoft Office Exchange Online, SharePoint, and OneDrive for Business.

Archived

Click here for the archived list of new features

New features and updates - Archived

The following is an archived list of new features added to SaaS Backup for Microsoft 365.

December 2018

- SaaS Backup for Microsoft 365 can now be purchased through the AppDirect Marketplace and the CANCOM Marketplace.

August 2018

- The user interface has been redesigned for improved user experience and efficiency.
- Data retention polices have been updated to allow data to be retained for 3 years.
  Backup policies

May 2018

- NetApp Cloud Control has been renamed to NetApp SaaS Backup for Microsoft 365.
- You can now purge users, site collections, and Microsoft 365 groups, completely removing all associated data from SaaS Backup for Microsoft 365.
  Purge a user, site collection, or Microsoft 365 group
- SaaS Backup now discovers both public and private groups for Microsoft 365 groups.

April 2018

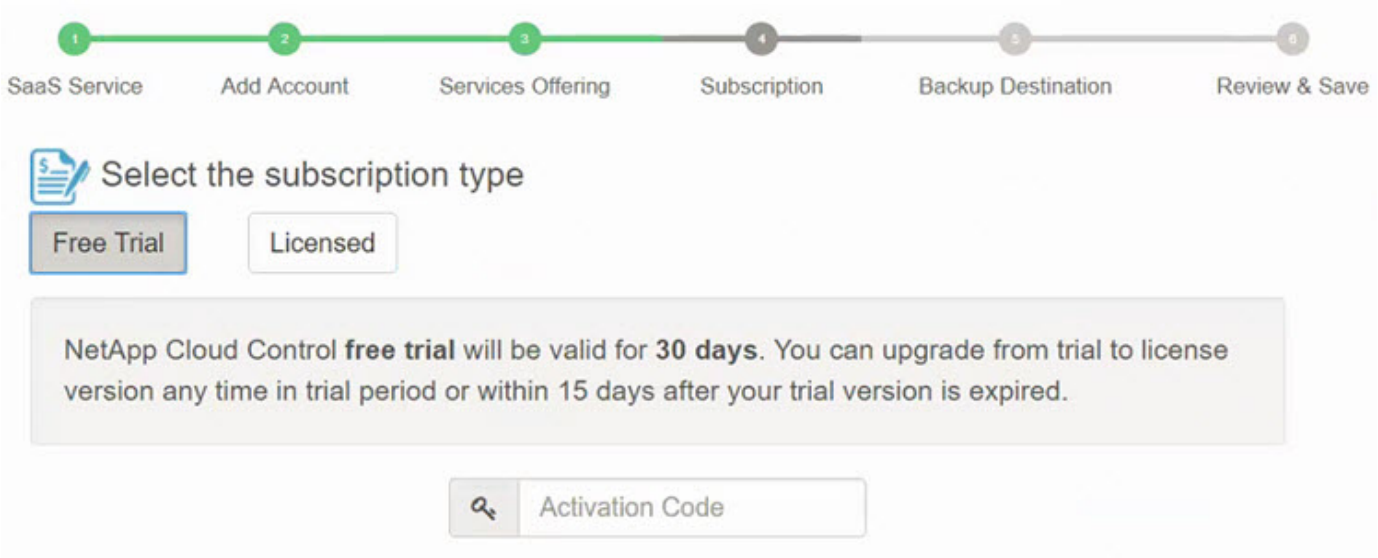
- SaaS Backup for Microsoft 365 now supports shared mailboxes for Microsoft Office Exchange Online.

  Shared mailboxes are discovered through the use of an automatically created service account. If you have not activated service for Microsoft Office Exchange Online prior to this update, the automatic service account for shared mailboxes is created by SaaS Backup when you activate Microsoft Office Exchange Online. If your service for Microsoft Office Exchange Online is already activated, you must grant SaaS Backup permission to create the automatic service account, so that your shared mailboxes can be discovered and backed up. Grant permissions to enable shared mailboxes

  After your automatic service account is created, your shared mailboxes will be automatically discovered during the next scheduled synchronization of your user account. If you want your shared mailboxes discovered immediately, you can discover your user accounts immediately.

March 2018

The location in which you enter an activation code for a free trial was moved to the Add a Service Provider wizard:



February 2018

- Filtering based on Template ID is now available for Microsoft SharePoint Online.
  Create a user defined filter
- You can now download the SaaS Backup for Microsoft 365 user account activity log to a .csv file.
  Download logs
- Synchronization of user accounts, sites, and groups between SaaS Backup for Microsoft 365 and your service is now enabled by default.
- Inclusion of backup version history is now enabled by default. The default number of versions is 20.
  Backup settings

January 2018

- The activity log now displays the name of the user ID associated with each action performed inside SaaS Backup for Microsoft 365.
- You can now manually synchronize your user permissions with Azure Active Directory from within SaaS Backup for Microsoft 365.
- Microsoft Exchange Online now supports export to PST for restore at the folder level.

November 2017

- SaaS Backup for Microsoft 365 now supports Azure Blob as an option for SaaS Backup provided storage.
- SaaS Backup for Microsoft 365 now supports Microsoft 365 Groups for backup and restore.
  Microsoft Exchange Online or Microsoft SharePoint Online must be activated before you can activate Microsoft 365 Groups. Microsoft 365 Groups can only be protected by the tier 3 backup policy.
- Microsoft Exchange Online now supports export to PST for restore at the mailbox level.

October 2017

- Rules can be created that allow you to automatically move users to a preselected backup tier based on predefined criteria.
  You can create rules for Microsoft Exchange Online and Microsoft OneDrive for Business. You cannot create rules for Microsoft SharePoint Online.
  Create new rules

Known problems and limitations

The following are known limitations identified at the application level for SaaS Backup for Microsoft 365.

For SharePoint Online

SaaS Backup does not support backups of archived SharePoint sites.

For OneDrive for Business

Newly added drives are not detected until you manually complete a sync for the service.

For Exchange Online

- SaaS Backup does not support backups for public folders.
- **Advanced Search** is only available for Exchange Online. The setting is disabled by default. A customer must request to enable this feature. After the **Enable Advanced Search** setting is enabled, administrators must manually enable the search feature for individual users.

For Teams

- Channel configuration is restored but content and conversations are not.
- Due to API limitations, SaaS Backup cannot differentiate between public and private channels in SaaS Backup.
- High-level restore restores Mailbox & SharePoint data only, not conversations.
- Backup or restore for emojis and gifs is not supported in Teams Chat.
- Team chat conversations only export option is Export to HTML.
  Attachment links posted in conversations are not visible in the html document.

For OneNote

- Export to data is not available.
- Incremental backup job might fail with the following error message:
  `Partial Failure. Failed to back up few OneNote Sections.`
- OneDrive backups include the backup of .onebak files.
- Restore statistics are not available for download.
- Data export and data purge are not supported.

Other problems and limitations

The following known problems and limitations are not specific to one application.

For all users who sign up with a Microsoft 365 service account:

- SaaS Backup supports Basic Authentication only.

For free trial users:

- A maximum of 10 restores per service are allowed in a 24-hour period.

For licensed users:

- A maximum of 10 export data restores per service are allowed in a 24-hour period. All other restore options have no limitations.

For restores of site collection groups:

- If an entire site collection group is deleted, the restore of private groups in the collection fails, resulting in a restore job status of “partially failed.” If this happens, the site is not accessible from the GUI.

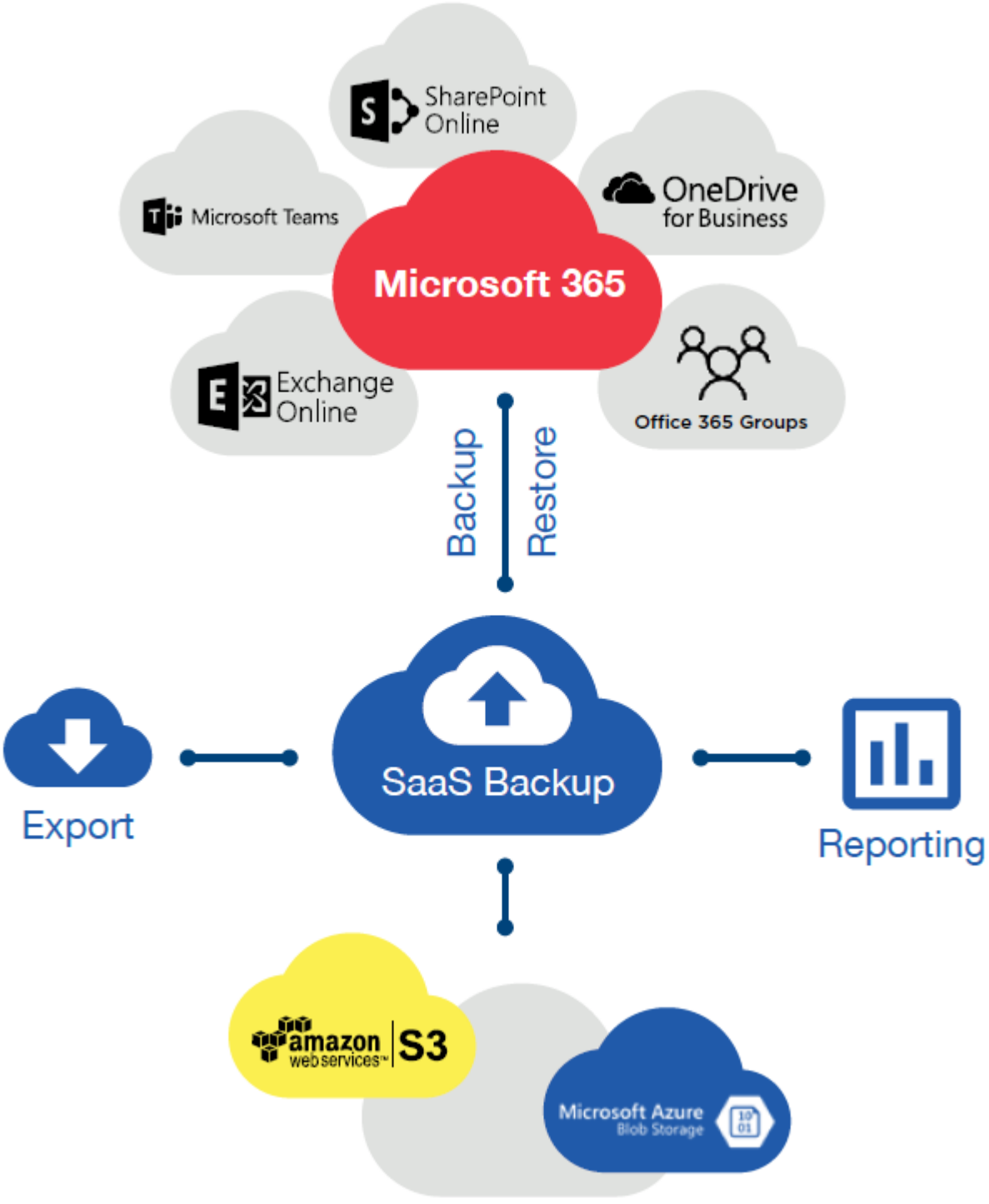
For **Advanced Search**:

- A maximum of 10 search jobs are allowed in a 24-hour period.

Concepts

NetApp SaaS Backup for Microsoft 365 Overview

NetApp SaaS Backup for Microsoft 365 is a secure, web-based, software-as-a-service (SaaS) offering that backs up your Microsoft 365 data to Amazon S3 storage or Microsoft Azure Blob storage. SaaS Backup provides encryption for data at rest and in flight.



Storage types you can use with SaaS Backup

SaaS Backup provided storage

SaaS Backup offers the following storage options:

- Amazon S3
- Azure Blob

Get started

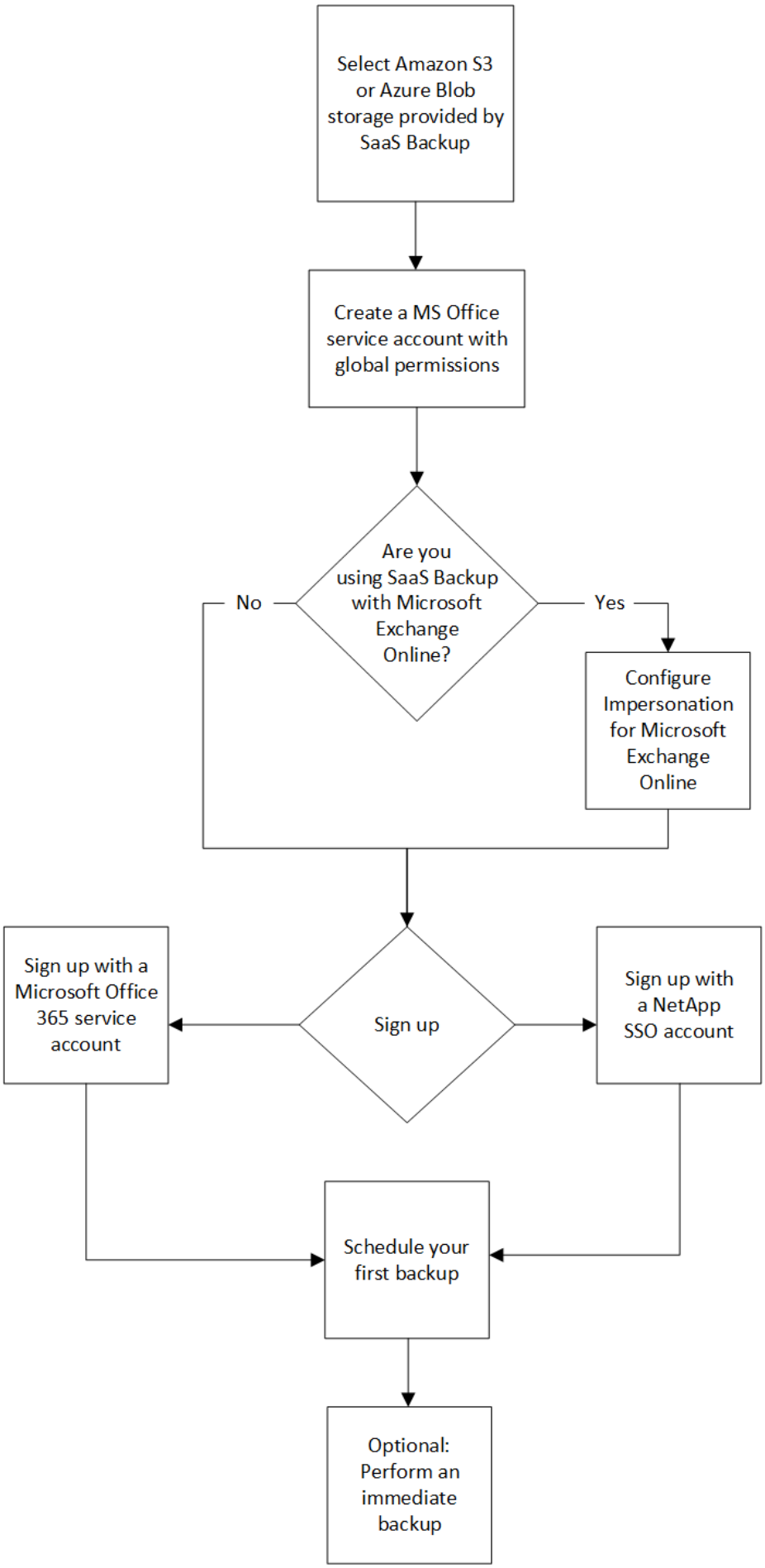
Workflow for getting started

To get started with SaaS Backup for Microsoft 365, you must do the following:

1. Decide if you will use Amazon S3 or Azure Blob storage provided by SaaS Backup.

   Storage types you can use with SaaS Backup.

2. Create a MS Office service account with global permissions.
3. If needed, configure Impersonation for Microsoft Exchange Online.
4. Sign up for SaaS Backup for Microsoft 365 using your Microsoft 365 account or your NetApp SSO account.
5. Schedule your first backup
6. Optional: Immediately back up your data

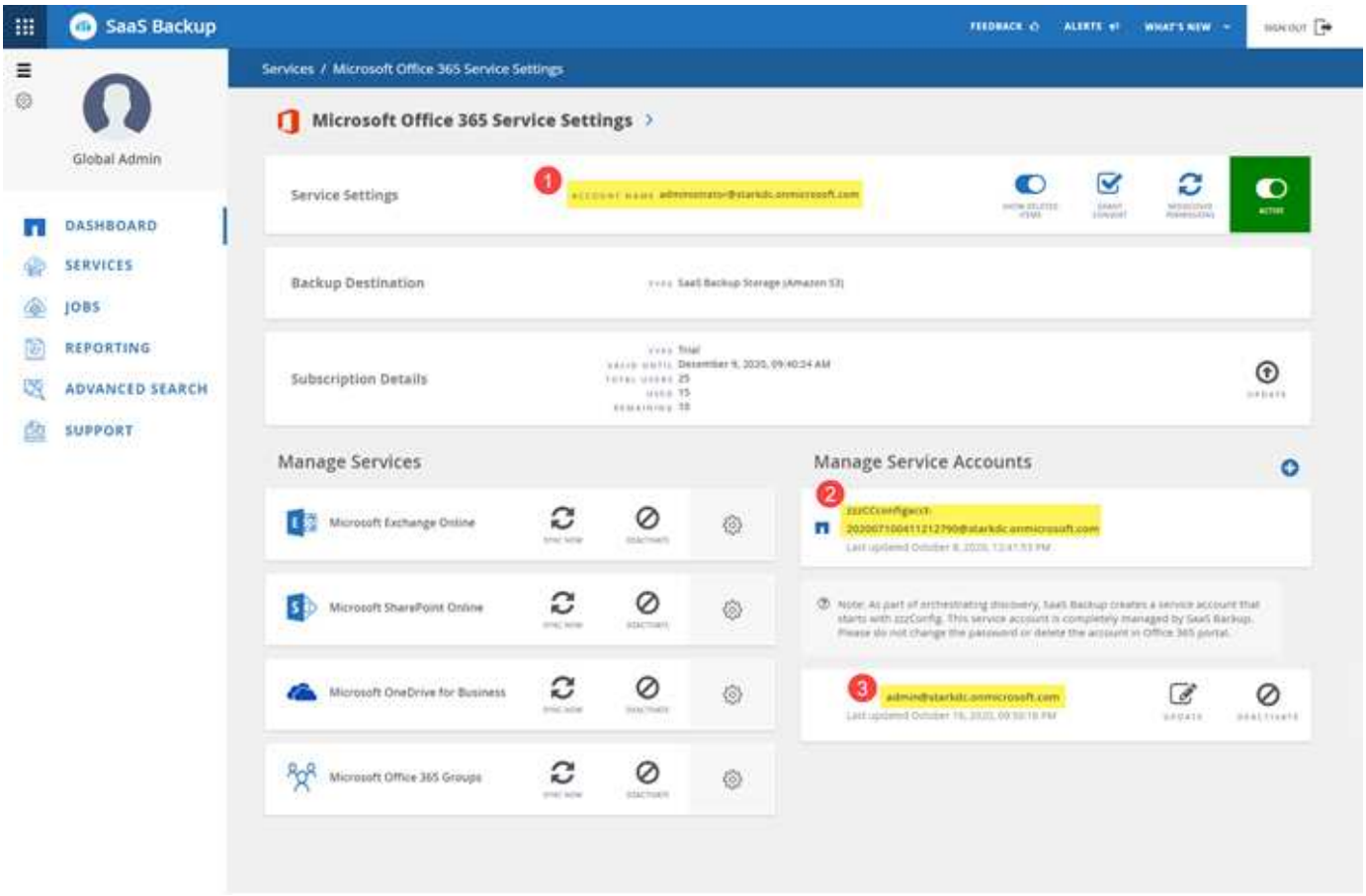

Select Amazon S3 or Azure Blob storage provided by SaaS Backup
Create a MS Office service account with global permissions
Are you using SaaS Backup with Microsoft Exchange Online?
No
Yes
Configure Impersonation for Microsoft Exchange Online
Sign up with a Microsoft Office 365 service account
Sign up
Sign up with a NetApp SSO account
Schedule your first backup
Optional: Perform an immediate backup

Create a new Microsoft 365 service account

When you create your new Microsoft 365 account, this account must have global administration permissions with a valid and assigned Microsoft Office 365 license.

This is not the only service account used to manage SaaS Backup for Microsoft 365. The following image points out the different service account types with descriptions below.

Service account descriptions



1 The account used to sign up for SaaS Backup; it requires global administration permissions with a valid Microsoft 365 license during signup. It can be used for backup and restore operations.

2 A **zzzCCconfigacct** is automatically created as a service account to discover Microsoft 365 Groups. When Modern Authentication is enabled, you do not have a ZZZ Config service account.

3 An additional service account can be added to enhance performance of backup and restore operations.

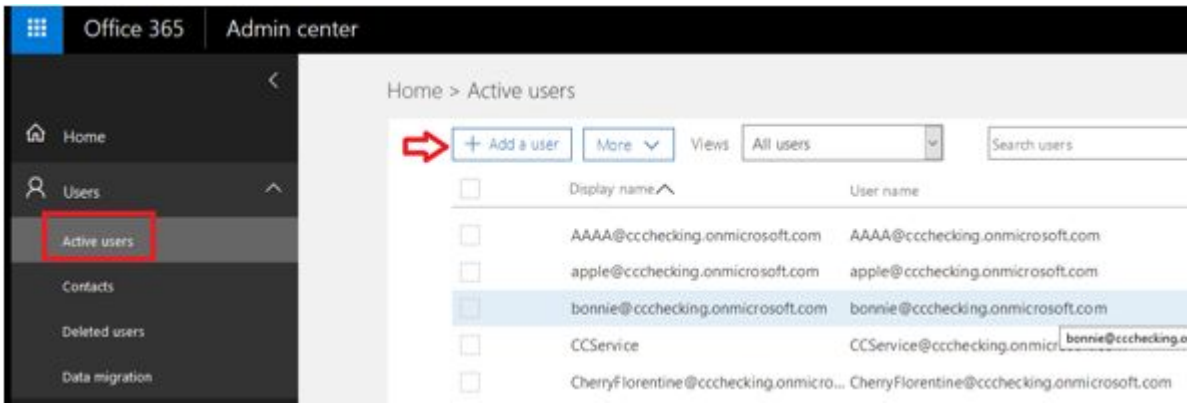
Create a new MS 365 service account with global administrator permissions

During signup, create an account with global permissions and a valid Microsoft 365 license. You can remove the global administration permissions and the license from this account after you complete signup.

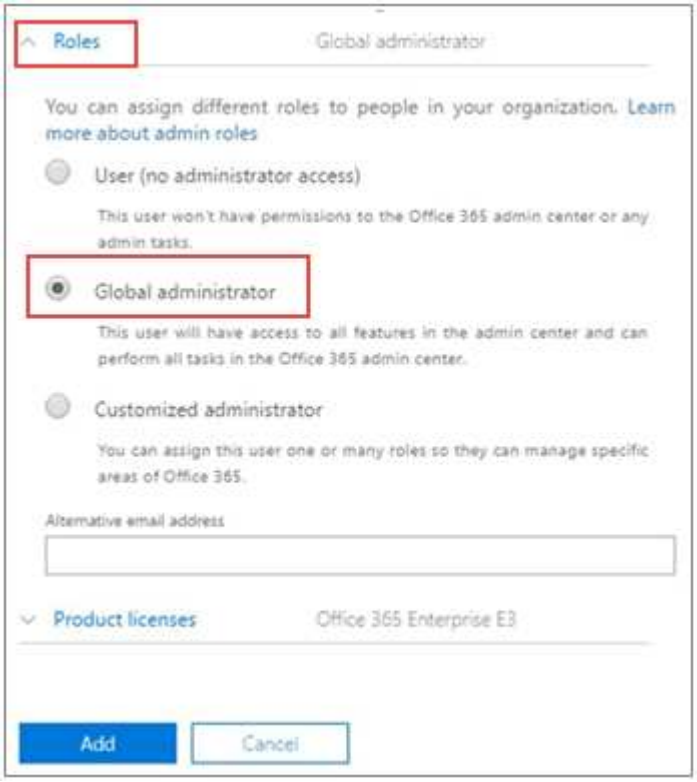
Steps

1. Log in to your Microsoft 365 Management portal using an account with administrative privileges.
2. Click **Users**.

3. Select **Active users**, and then click **Add a user**.



4. Enter the details of the new service account.
   - First name
   - Last name
   - Display name
   - User name
     The user name is the name of the service account.
5. Expand **Roles**, select **Global administrator** as the role, and then click **Add**.



The service account details are sent to the administrator.

6. Log in to your Microsoft 365 Management Portal with the new account to activate it.
7. After signup, ensure this service account maintains three permissions:
   - Exchange Administrator
   - SharePoint Administrator
   - Application Impersonation Role

   This is especially important if you restrict the individual licenses for the Global administrator role.

ZZZ Config service account

ZZZ Config service account is an auto-created account used for discovering Shared/Archive mailboxes and private groups if you use Basic Authentication. It should have Exchange and SharePoint permissions (customized administrator in M365). It is recommended that you exclude this account from MFA policies. To avoid any discovery or backup failures, leave the account as is.

If you enable Modern Authentication, the ZZZ Config service account is removed.

New customers do not have a ZZZ Config service account.

Create additional service accounts

Service Accounts can be added in SaaS Backup for Microsoft 365 to improve the backup performance for a customer. A service account is a Microsoft 365 user account without a license; it is used for backup and restore operations.

This type of account requires 3 permissions:

- Exchange administrator
- SharePoint administrator
- Application impersonation role

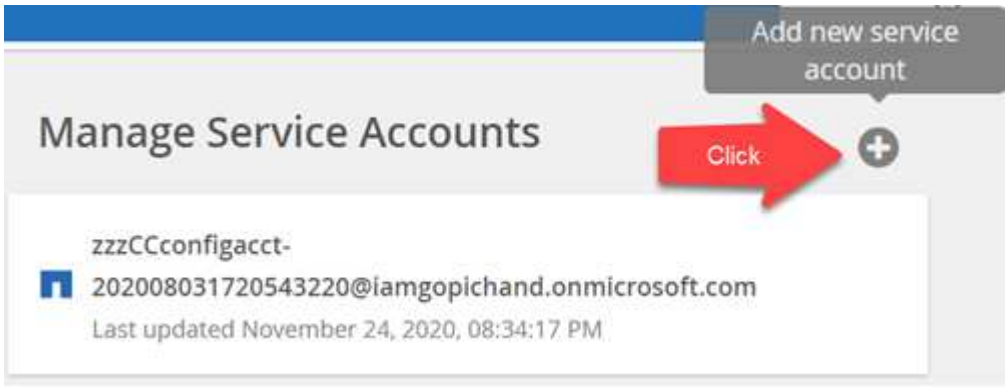
To add an additional service account, the service account must already exist in your Microsoft 365 environment. If you do not have an existing account, then create one.

To optimize performance, it is recommended that you have 1 service account added per 1000 users in Office 365.

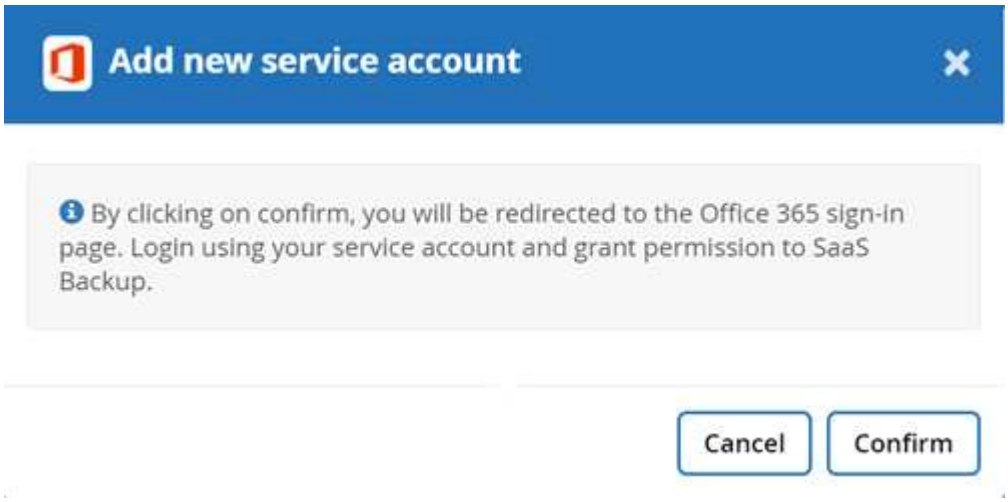
Steps

1. Log in to SaaS Backup for Microsoft 365.
2. Click  .
3. Click **Service Settings**.

4. To add a service account, click  under **Manage service accounts**.



A confirmation message pops up.



5. Click **Confirm**.
6. On the Microsoft 365 sign-in page, provide the credentials of the above mentioned service account to add it to SaaS Backup.

Configure Impersonation for Microsoft Exchange Online

If you plan to use SaaS Backup with Microsoft Exchange Online, you must configure impersonation. Impersonation allows your Microsoft 365 service account to impersonate

user accounts and access associated permissions.

Automatically configure impersonation

To automatically configure impersonation, run MSDN PowerShell Commands.

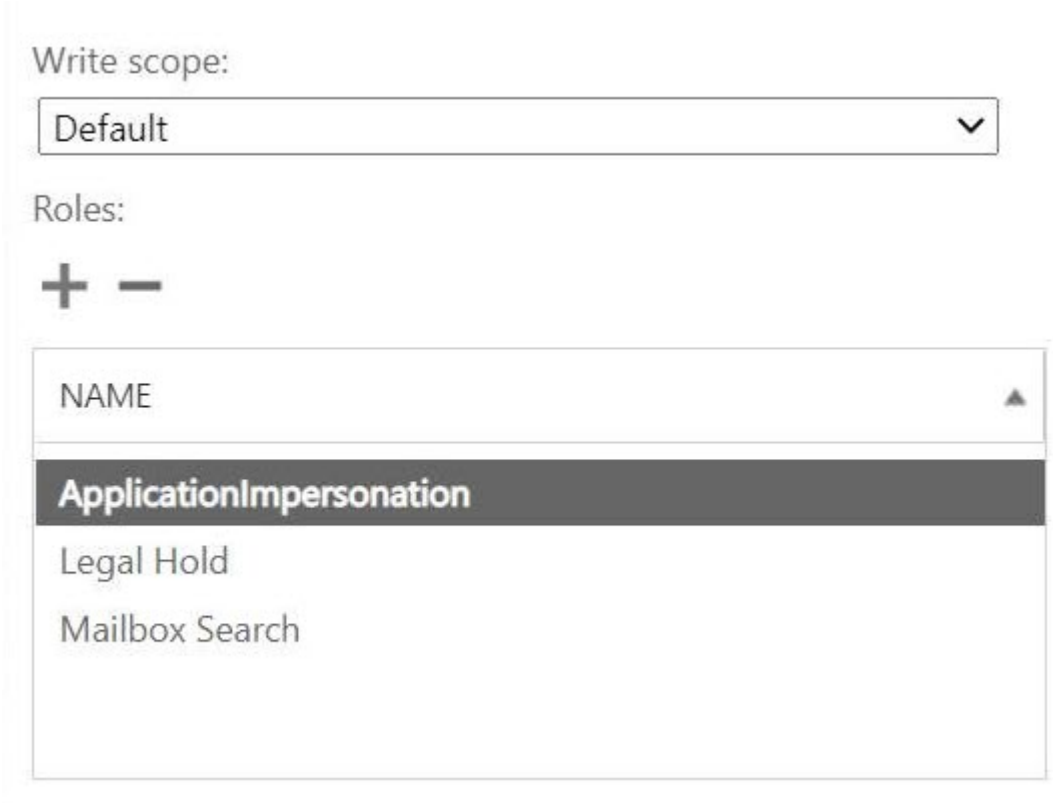
Manually configure impersonation

You can manually configure impersonation with your Microsoft 365 administrator account as well as with added Microsoft 365 service accounts in SaaS Backup. For more information about Microsoft 365 service accounts, go to creating a Microsoft 365 service account with global permissions.

To manually configure impersonation do the following:

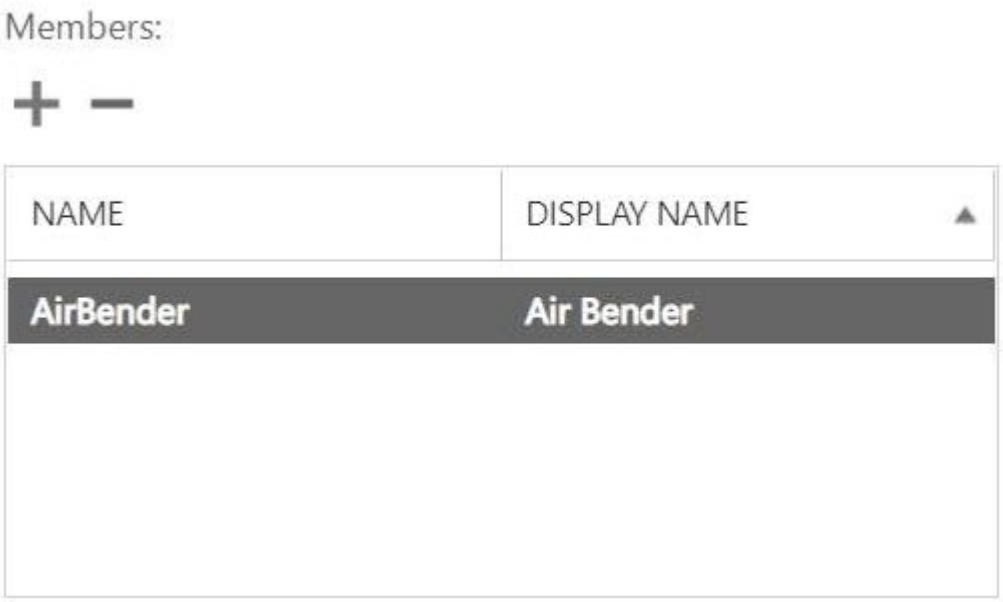
Steps

1. Log in to your Microsoft 365 service account.
2. Select the **Exchange** tab.
3. On the left, under Dashboard, select **Permissions**.
4. Click **Admin roles**.
5. Double-click in the right pane to select **Discovery management**.
6. Under **Roles**, click the **+** symbol.



7. Select **ApplicationImpersonation** from the drop-down menu.
8. Click **Add**.
9. Click **OK**.

10. Verify that **ApplicationImpersonation** was added under **Roles**.
11. Under Members, click the **+** symbol.



A new window appears

12. Choose the user name.
13. Click **Add**.
14. Click **OK**.
15. Verify that the user name appears in the **Members** section.
16. Click **Save**.

Sign up for SaaS Backup for Microsoft 365

You can sign up for SaaS Backup for Microsoft 365 with your Microsoft 365 service account or with your NetApp SSO account.

Sign up with a Microsoft 365 service account

Steps

1. Enter the SaaS Backup for Microsoft 365 URL into your web browser:
   https://saasbackup.netapp.com
2. Select your region.
   Your tenancy is created in the selected region. Your data will be stored in that datacenter location and cannot be changed later.
3. Click **Sign up** at the bottom of the landing page.
4. Accept the End-User License Agreement.
5. Click **Sign Up with Office 365**.

6. Enter the email address and password for your Microsoft 365 global administrator service account, and

then click **Sign in**.
A list of the permissions requested by SaaS Backup for Microsoft 365 is displayed.

7. Click **Accept**.
8. Enter the requested user information.
9. Click **Sign up**.
Your user name and a list of permissions given to SaaS Backup for Microsoft 365 is displayed.
10. Click **Next**.
A list of the available Microsoft 365 services is displayed.
11. Select the Microsoft 365 services that you want to activate.
12. Click **Next**.
13. If you purchased your license through NetApp, your subscription types are displayed
Click here for additional steps.
14. If you purchased your license through a Cloud Marketplace, such as AWS, your license information is displayed.
Click here for additional steps.

Sign up with a NetApp SSO account

Before you begin

To validate your subscription, you must have a NetApp SSO user ID and password. If you do not have a NetApp SSO account, go to https://mysupport.netapp.com/eservice/public/now.do to register for one. After your request has been processed, you will receive an email notification containing your NetApp SSO credentials. It will take approximately 24 hours to process the request and send the notification email.

Steps

1. Enter the SaaS Backup for Microsoft 365 URL into your web browser:
https://saasbackup.netapp.com
2. Click Sign up at the bottom of the landing page.
3. Accept the End-User License Agreement.
4. Click **Sign Up with NetApp SSO**.


5. Enter your NetApp SSO and password, and then click **LOGIN**.
6. Enter the requested user information, and then click **Sign Up**.
7. Click the **Services**  icon.
8. Click the Microsoft 365  icon to select the SaaS service.
9. Click **Add Microsoft Office 365 Account**.
10. Enter the email address and password for your Microsoft 365 global administrator service account, and then click **Sign in**.
A list of the permissions requested by SaaS Backup for Microsoft 365 is displayed.
11. Click **Accept**.
12. Click **Next**.
A list of the available Microsoft 365 services is displayed.

13. Select the Microsoft 365 services that you want to activate.
14. Click **Next**.
15. Select **Licensed** for the subscription type.
16. Enter the requested information, and then validate the subscription.
17. Click **Next**.
18. Select your backup storage option.
    a. Click **SaaS Backup Provided Storage**.
    b. Select the **Amazon S3** or **Azure Blob** storage option.
    c. Select the **AWS S3** or **Azure Blob** region for your backup.
    You should select the region that is the closest to the physical location of the data you are backing up.
    d. Click **Next**.
    e. Review your configuration, and then click **Save**.

Schedule your first backup

When you set up SaaS Backup for Microsoft 365, by default, your data is unprotected. You must move your data from the unprotected tier to one of the protected tiers to so that your data will be backed up during the next scheduled back up of the selected tier.

Steps

1. From the Dashboard, select the service containing the unprotected data.
2. Click **view** next to the number of unprotected mailboxes, MySites, sites or groups.
3. Select the items that you want to protect.
4. Click the **Groups** menu.


5. Select the **tier** for the backup policy that you want to assign.
See Backup Policies for a description of the backup policy tiers.
6. Click **Apply**.

Perform an immediate backup of a specific backup policy

When you set up SaaS Backup for Microsoft 365, by default, all of your data is unprotected. After you move your data to a protected tier, you can perform an immediate backup of the tier to which you moved your data. This prevents your data from being at risk until the first scheduled backup occurs. If you can wait for the first scheduled backup, performing an immediate backup is not necessary.

You can perform an immediate backup any time you deem necessary for data protection. If you are running a trial version of SaaS Backup for Microsoft 365, you can only perform three immediate backups per day, per service.

Steps

1. From the Dashboard, select the service for which you want to perform an immediate backup.
2. Under **Backup Policies**, click the tier that you want to back up.
3. Click Backup Now.

   A message is displayed indicating that the services under the selected tier will be placed in the job queue for immediate backup.

4. Click **Confirm**.
   A message is displayed indicating that the backup job was created.
5. Click **View the job progress** to monitor the progress of the backup.

Data deletion

If you do not renew your licensed version of SaaS Backup for Microsoft 365, the data used during your subscription is deleted as follows:

If your SaaS Backup paid subscription is…	Number of days after paid subscription ends	Your data is…
Expired	1-30 days	Available: The administrator has normal access and can perform manual backups and restores. SaaS Backup continues to display alerts and send out notifications.
Disabled	31-60 days	Deactivated: The administrator does not have access to the SaaS Backup portal. If subscription is renewed during this period, data can be reactivated.
Deprovisioned	61 or more days	Deleted: All data is deleted and your tenant account is removed.

Manage services

Activate a service

If needed, you can activate one or more SaaS Backup for Microsoft 365 services. Microsoft Exchange Online or Microsoft SharePoint Online must be activated before you can activate Microsoft 365 Groups.

Steps

1. Click 

from the left navigation pane.
2. Click the Microsoft 365 link.

3. Click **Activate** next to the service that you want to activate.
4. Click **Confirm**.

Deactivate a service

If needed, you can deactivate one or more of your SaaS Backup for Microsoft 365 services. If you deactivate a service, all of the schedules associated with that service are removed and no further backup is performed. You can still view the last backup that occurred before deactivation and you can still perform restores.

Steps

1. Click 

from the left navigation pane.
2. Click the Microsoft 365 link.

3. Click 

next to the service that you want to deactivate.
4. Click **Confirm**.

Activate support

If you purchased SaaS Backup through NetApp, support is activated by default. If you purchased SaaS Backup through a Cloud Marketplace such as AWS, you must activate support. Activating support enables you to access technical support over the phone, online chat, or web ticketing system.

If you are upgrading from a trial version of SaaS Backup, you can activate support either before or after you complete the upgrade process.

Before you begin

In order to activate support, you must have a NetApp SSO user ID and password. If you do not have a NetApp SSO account, go to http://register.netapp.com to register for one. After your request has been processed, you will receive an email notification containing your NetApp SSO credentials. It will take approximately 24 hours to process the request and send the notification email.

Steps

1. Click 

from the left navigation pane.
2. Click the settings icon  .
3. In the **Activate Support** box, click **Activate**.
4. Enter your NetApp SSO username and password.
5. Click **Activate**.

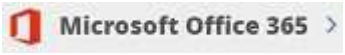
The support status is now **Active**.

Discover new mailboxes, sites, and groups

A synchronization must occur between SaaS Backup and your Microsoft 365 account for new mailboxes (including shared and archive mailboxes), sites, groups, and teams to be discovered by SaaS Backup. By default, synchronization automatically occurs once every 24 hours. However, if you make changes and you want discovery to occur before the next scheduled **Auto Sync**, you can initiate an immediate synchronization.

Steps

1. Click 

from the left navigation pane.
2. Click the Microsoft 365 settings icon.


3. Click **Sync Now** next to the service that you want to synchronize.


New users, shared mailboxes, and archive mailboxes are discovered and added in an unprotected state. If you want newly discovered users, shared mailboxes, or archive mailboxes to be backed up, you must change the backup policy of the users from unprotected to one of the predefined tier groups.
4. Click **Confirm**.
5. Click **View the job progress** to monitor the progress.
When the job is complete, you can click the job under **Recent Completed Jobs** to view the number of users that were added or removed during the synchronization. Changes to user accounts are indicated as follows:
   - **Rediscovered** users indicates the number of unchanged user accounts.
   - **Deactivated** users indicates the number of deleted user accounts.
   - **Newly added** users indicates the number of new user accounts.

Purge a user, site collection, or Microsoft 365 group

You can completely remove all the data associated with a user, site collection, or Microsoft 365 group. Purged data is recoverable for seven days. After seven days, the data is permanently deleted and the user license is automatically released.

Steps

1. Click the configuration icon  next to your SaaS Backup user id in the top left corner.
2. Select **ACCOUNT SETTINGS**.
3. Click **RETAIN AND PURGE**.
4. Under **Purge Data**, select the **Type of Service** (Exchange, OneDrive, or SharePoint) from the dropdown menu.
5. Search for the user, site collection, or Microsoft 365 group that you want to purge.
   For Microsoft Exchange Online or OneDrive for Business, enter the user or Microsoft 365 group name. For SharePoint Online, enter the site collection name.

   NOTE: If the user has an archive mailbox, the username of the archive mailbox is prefixed by "In-Place Archive".
6. When the search result returns, click the  to select the user, site collection, or Microsoft 365 group.
7. Click **Save**.
8. Click **Yes** to confirm that you want purge the data.

Enable Modern Authentication

Microsoft 365 targets October 2021 to deprecate Basic Authentication in Exchange Online. After deprecation, discovery failures can occur for Microsoft 365 groups, and Shared and Archive mailboxes.

You can enable Modern Authentication at any time.

New customers don’t need to take any action. Modern Authentication is enabled when you sign up.

Existing customers need to take action. Follow the instructions below to enable Modern Authentication.

To enable Modern Authentication, log in with your tenant account credentials; the account name can be found in Microsoft 365 Service Settings (see **Option 2 steps** below). Make sure the Global Administrator role is assigned to this account. After Modern Authentication is successfully enabled, you can remove the Global Administrator role from the admin user.

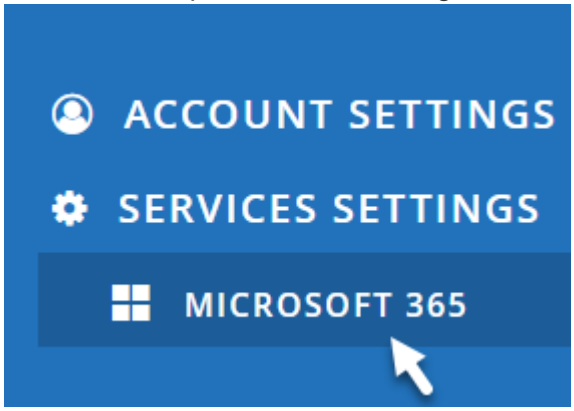
Option 1 steps

1. Sign in to SaaS Backup for Microsoft 365.
   The following message pops up.
2. Select **Confirm** to enable Modern Authentication.
3. Accept all permissions.

Modern Authentication is now enabled.
The ZZZ config service account has been removed.

Option 2 steps

1. In SaaS Backup for Microsoft 365, go to Settings > Service settings > Microsoft 365 service settings.



2. Select **Enable Modern Authentication**.

3. Accept all permissions.
Modern Authentication is now enabled.
The ZZZ config service account has been removed.

If you receive a failure notification, you can retry to enable Modern Authentication.

For support, email saasbackupsupport@netapp.com.

For more information, see Basic Authentication and Exchange Online - September 2021 Update.

Manage settings

Backup policies

SaaS Backup for Microsoft 365 has three predefined tiers of backup policies. These policy tiers vary in backup frequency and data retention period, depending upon whether you are using SaaS Backup provided storage or BYOS.

You can move data between the three policies, but you cannot create new policies or change the parameters of the predefined tiers.

Backup policies for SaaS Backup provided storage

Backup policy	Backup frequency	Default data retention period
Tier 1	Once every 12 hours	3 years
Tier 2	Once every 18 hours	3 years
Tier 3	Once every 24 hours	3 years

As an administrator, you can change the data retention period for SaaS Backup provided storage up to an unlimited period of time. SaaS Backup retains the backup data for the retention period if the subscription is active.

Backup policies for BYOS

BYOS is for existing customers only.

Backup policy	Backup frequency	Default data retention period
Tier 1	Once every 12 hours	Unlimited
Tier 2	Once every 18 hours	Unlimited
Tier 3	Once every 24 hours	Unlimited

Backup settings

You can update your backup settings to control various backup options. Available backup settings vary based on service.

Backup settings per service

Backup setting	Description	Enabled	Available in…
Auto Sync	Enables the automatic scheduled synchronization of newly added or deleted users, OneDrives, or site collections once every 24 hours.	By default	• Microsoft Exchange Online • Microsoft SharePoint Online • Microsoft OneDrive for Business • Microsoft 365 Groups
Enable OneNote Backup	Enables the backup of OneNote notebooks.	Manually	• Microsoft SharePoint Online • Microsoft OneDrive for Business
Enable Restore of Recoverable Items	Enables the user to restore Microsoft Exchange recoverable items.	Manually	• Microsoft Exchange Online
Enable Backup of Recoverable Items	Enables the backup of Microsoft Exchange recoverable items. Only the tier 1 backup policy allows for the backup of recoverable items.	Manually	• Microsoft Exchange Online
Include Workflows	Includes workflows in the backup.	Manually	• Microsoft SharePoint Online • Microsoft 365 Groups
Include List Views	Includes list views in backup.	Manually	• Microsoft SharePoint Online • Microsoft 365 Groups

Backup setting	Description	Enabled	Available in…
Include Version History	Enables maintenance of multiple file versions in the backup. This setting only applies to individual files. It does not apply to entire folders, tiers, or services.	By default	• Microsoft SharePoint Online • Microsoft OneDrive for Business • Microsoft 365 Groups
Number of Versions	Sets the number of backup file versions to maintain. By default, the latest version is automatically backed up, even if this setting is not enabled.	Set to 20 by default	• Microsoft SharePoint Online • Microsoft OneDrive for Business • Microsoft 365 Groups

Update backup settings

Steps

1. Click **Services** from the left navigation pane.

2. Click Microsoft 365.

3. Under **Manage Services**, click the backup settings icon next to the service that you need to update. A list of your backup settings available for the selected service is displayed.
4. Select the desired backup settings.
5. Click **Confirm**.

Set notifications

You can add users to account notifications and then select the specific notifications you want each user to receive. For example, you can select to have a user receive an email notification each time there is a restore failure.

Steps

1. Click **ACCOUNT SETTINGS**.

2. Click **NOTIFICATION MANAGEMENT**.
3. Enter the email address of the account you want to receive notifications.
4. Click **Add Notifications**.
   The user is added under the list of accounts for notifications.
5. Select the specific notifications you want the user to receive.
6. Click **Save**.

Permissions

Add additional service accounts

If needed, you can add additional service accounts to improve backup performance. Service accounts are used to perform concurrent backups efficiently.

Steps

1. Log in to the Microsoft 365 Management Portal using an account with administrative privileges.
2. Click on the app launcher icon and then click **Admin**.
3. On the left, click **Users** and then **Active Users**.
4. Click **Add a User** to create a new account.
5. Fill in the form following the instructions below.
   - Use **Let me create the password**.
   - Deselect **Make this user change their password when they first sign in** option.
   - Select the role **Customized Administrator**.
   - Select **Exchange administrator** and **SharePoint administrator**.
   - Select **Create user without product License**.
6. For Exchange backups to run with newly created service accounts, assign the Exchange impersonation rights to these newly created service accounts.
   Configuring impersonations

SaaS backup automatically assigns the permissions on OneDrive and SharePoint sites, so you don't need to assign them.

You can enable multi-factor authorization (MFA) on this account.

Synchronize user permissions with Azure Active Directory

You can manually synchronize your user permissions with Azure Active Directory from within SaaS Backup for Microsoft 365.

Steps

1. Click 

from the left navigation pane.
2. Click the Microsoft 365 link.

3. Click **Rediscover Permissions**.

If permissions for a services are discovered, the service is displayed with the option to active.

Grant permissions to enable shared mailboxes

You can grant permissions to enable shared mailboxes within NetApp SaaS Backup for Microsoft 365.

Steps

1. Click 

from the left navigation pane.
2. Click the Microsoft 365 link.

3. Click **Grant Consent**.

You are redirected to the Azure authorization page for authentication.

4. Select your tenant account.
5. **Accept** the permissions.
Your shared mailboxes will be discovered during the next scheduled **Auto Sync** or you can perform a **Sync Now**. If you **Sync Now**, it will take a few minutes for your shared mailboxes to be discovered.
6. To access shared mailboxes after an **Auto Sync** or a **Sync Now** do the following:
   a. Click 

from the left navigation pane.
   b. Click **Microsoft Exchange Online**.
   c. Click the number of unprotected mailboxes.
   d. Click the **Shared** tab.

Role-based account access

Assign administrative roles to user accounts

You can assign administrative roles to user accounts to grant administrative privileges to selected users for one or more services.

You can assign the following roles to users:

- Global Tenant: Grants administrative privileges to all services, storage target, and license updates (renewal/upgrade).
- Exchange Administrator: Grants administrative privileges to Microsoft Exchange Online only. Other services cannot be viewed or modified.
- OneDrive Administrator: Grants administrative privileges to Microsoft OneDrive for Business only. Other services cannot be viewed or modified.
- SharePoint Administrator: Grants administrative privileges to Microsoft SharePoint Online only. Other services cannot be viewed or modified.

Steps

1. Click the settings icon  next to your user ID in the top left of the screen.
2. Click **ACCOUNT SETTINGS**.
3. Click **ROLE MANAGEMENT**.
4. Click the  icon.
5. Enter the email address for the user you want to add.
6. Click the drop-down menu to select the role.
   You can assign one or more roles to a user.
7. Click **Confirm**.

Update administrative roles assigned to user accounts

If an update is made to a user's administrative roles, the user is automatically logged out of SaaS Backup for Microsoft 365. When the user logs back in, administrative role updates are reflected in the user's account.

Steps

1. Click the settings icon  next to your user ID in the top left of the screen.
2. Click **ACCOUNT SETTINGS**.
3. Click **ROLE MANAGEMENT**.
4. Click **Update User** next to the user name that you want to update.
5. Click the drop-down menu to select the role.
   You can assign one or more roles to a user.
6. Click **Confirm**.

Delete all administrative roles from a user account

If all administrative roles are deleted from a user's account, the user is automatically logged out of SaaS Backup for Microsoft 365.

Steps

1.

Click the settings icon  next to your user ID in the top left of the screen.

2. Click **ACCOUNT SETTINGS**.
3. Click **ROLE MANAGEMENT**.
4. Click **Delete User** next to the user name that you want to remove.
5. Click **Yes**.

Manage users

Licenses

Add a license

If you have just received a license for a paid subscription, please follow workflow for getting started with a paid subscription. You will enter your license key as part of the workflow.

If you are already using SaaS Backup, you can follow these steps to add additional licenses.

Education domains can have a license for faculty and a separate license for students.

Steps

1. Click 

from the left navigation pane.
2. Click  in the right corner.
3. Enter the license information.
4. Click **Validate Subscription**.
5. Click **Next**.
6. Click **Save**.

Update subscription information

After you purchase an add-on license or subscription extension, you can update your subscription details inside of SaaS Backup.

Any regular user mailbox, whether protected or unprotected, consumes a license. Shared mailboxes do not consume a license.

Steps

1. Click **Services** from the left navigation pane.
2. Click  in the right corner.
3. Click **Update** next to Subscription Details.
4. Enter the same username and password you used when you first signed up.
5. Click **Submit**.

Release a user license

Any regular or archive mailbox user, whether protected or unprotected, consumes a license. If a license is no longer needed for a particular user, you can release the license so that it can be reassigned. When a user license is released, the user is moved to the unprotected tier and backups for that user are discontinued.

Shared mailboxes do not consume a license.

Steps

1. Click  next to your SaaS Backup user id in the top left corner.
2. Select **ACCOUNT SETTINGS**.
3. Click **RETAIN AND PURGE**.
4. Under **Release License**, begin typing the account name for the user whose license you want to release.
5. When the account is found, select it from the auto-populated list and click  .
6. Add additional accounts, if needed.
7. Click **Release**.
8. Click **Yes, please release license(s)**.
9. Click **Confirm**.

Rules

Create new rules

Rules allow you to automatically move users to a preselected backup tier based on predefined criteria.

You can create rules for Microsoft Exchange Online, OneDrive for Business, SharePoint Online, and Microsoft Office 365 Groups.

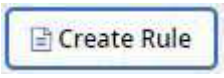
You must apply a user defined filter to your data before you can create a rule. Applied filters are displayed below the **Filter** icon. NetApp SaaS Backup for Microsoft 365 default filters appear in gray. User defined filters appear in light blue.

Create a user defined filter

You can create multiple rules. The rules are applied in the order they appear in the **Manage Rules** list.

Steps

1. From the Dashboard, click the number above **UNPROTECTED** in the box of the service for which you want to create rules.

If no user created filter is applied,  does not appear.

2. Click **Filter**.

3. Click the **Select** dropdown menu and select your filter.
   A search field appears.
4. Enter your search criteria.
5. Click **Apply Filter**.
6. Click **Create Rule**.
7. Enter a name for the rule.
8. For **Destination Group**, select the tier to which you want users who meet the rule's criteria to be moved.
9. Select **Apply to existing items** if you want the rule to be immediately applied to all unprotected items. If not selected, the rule is applied to newly discovered items and any unprotected items the next time new items are discovered.
10. If you have multiple rules, you can click the  to move a rule up or down in the list. The rules are applied in the order they appear in the list.

Apply existing rules

Rules allow you to automatically move users to a preselected backup tier based on predefined criteria.

You can apply existing rules to unprotected items, change the order in which rules are applied, and delete rules.

Steps

1. From the Dashboard, click the number above **UNPROTECTED** in the box of the service for which you want to create rules.

2. Click **Filter**.

3. Click **Rules**.
   The existing rules are displayed.
4. Click **Apply Now** to apply the rule to existing unprotected items.

Delete rules

If you no longer need a existing rule, you can delete it. Also, if you need to delete a security group that is used in a rule, you must delete the rule using the security group

before the security group can be removed.

Steps

1. From the Dashboard, click the number above **UNPROTECTED** in the box of the service for which you want to create rules.

2. Click **Filter**.

3. Click **Rules**.
   The existing rules are displayed.
4. Click  to delete the rule.
   The status of the items to which the rule was previously applies is not changed when the rule is deleted.

Security groups

Add security groups

Security groups can be used as filtering options to view your data and to create rules.

You can add up to 3 security groups. You can then use your security groups as filtering options in SaaS Backup.

New security groups must be discovered through an AutoSync or a manual synchronization before they can be added.
Create, edit, or delete a security group in the Admin Center.

Steps

1. Click **ACCOUNT SETTINGS**.
2. Click **SECURITY GROUPS**.
3. In the search field, enter the name of the security group you want to add.
4. Click **Add**.

Delete security groups

If a security group is being utilized in a user-defined rule, it cannot be deleted. You must remove the user-defined rule, then delete the security group.
Deleting rules

Steps

1. Click **ACCOUNT SETTINGS**.

2. Click **SECURITY GROUPS**.
3. Click the delete icon next to the group you want to remove.

Manage backups

Schedule a backup or changing backup frequency

You can back up your unprotected data by assigning it to a backup policy. When unprotected data is assigned to a backup policy, it moves to a **PENDING** state until the next scheduled backup for the assigned policy occurs, after which it is moved to a **PROTECTED** state.
If you want to change the backup frequency of protected data, you can assign the data to a different backup policy tier.

Steps

1. From the Dashboard, click the number above **PROTECTED** or **UNPROTECTED** in the box of the service you want to change.
   If you want to change the backup frequency of protected data, click **PROTECTED**. If you want to backup newly discovered mailboxes, sites, or MySites, select **UNPROTECTED**.

2. Select your backup options.
   1. For Exchange
      - If you are backing up shared mailboxes (Tier 3 only), click the **SHARED** tab.
      - If you are backing up archive mailboxes (Tier 3 only), click the **ARCHIVE** tab.
      - If you are backing up or changing regular mailboxes, remain on the **USER** tab.
   2. For SharePoint
      - If you are backing up or changing the backup policy for sites, remain on the **SITES** tab.
   3. For OneDrive
      - If you are backing up or changing the backup policy for users, remain on the **USER** tab.
   4. For Microsoft 365 groups
      - If you are backing up groups (Tier 3 only), remain on the **GROUPS** tab.
      - If you are backing up teams (Tier 3 only), click the **TEAMS** tab.
3. Select the items you want to backup.
4. Click the **Groups** menu.

5. Select the new policy tier for the backup.

Microsoft 365 groups and archive mailboxes can only be moved to the tier 3 policy.

6. Click **Apply**.

Perform an immediate backup of a service

As needed, you can perform an immediate backup of any Microsoft 365 service.

Steps

1. From the Dashboard, click the number above **PROTECTED** in the box of the service for which you want to perform an immediate backup.
2. Select your backup option.
    1. For Exchange
        - If you are backing up shared mailboxes, click the **SHARED** tab.
        - If you are backing up archive mailboxes, click the **ARCHIVE** tab.
        - If you are backing up regular mailboxes, remain on the **USER** tab.
    2. For SharePoint
        - If you are backing up sites, remain on the **SITES** tab.
    3. For OneDrive
        - If you are backing up users, remain on the **USER** tab.
    4. For Microsoft 365 groups
        - If you are backing up groups, remain on the **GROUPS** tab.
        - If you are backing up teams, click the **TEAMS** tab.

        TeamsChat messages are only backed up if TeamsChat is enabled under settings. Contact Support to enable this feature.

        Due to API limitations, SaaS backup cannot differentiate between public and private channels.
3. Select the items that you want to back up.
4. Click **Backup Now**.

    A message is displayed indicating that the selected services will be placed in the job queue for backup.
5. Click **Confirm**.
   A message is displayed indicating that the backup job was created.
6. Click **View the job progress** to monitor the progress of the backup.

Browse backups

You can browse protected instances in recent backups or in all of your backups for Microsoft 365 Exchange, SharePoint, OneDrive for Business, and Groups.

The default browse setting is **Showing Last 5 days Backup**. If you select 5 days, only items backed up in the last 5 days appear. You can change the time range as needed.

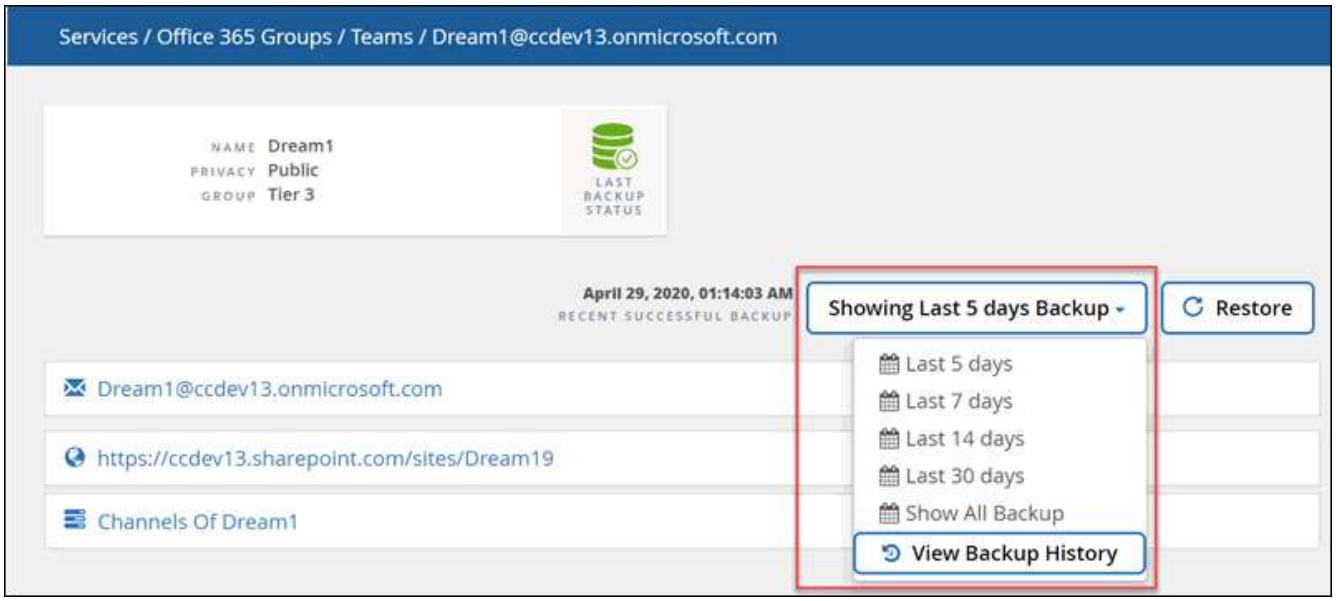
To be sure you find what you are looking for, check the date to the left of the time range dropdown menu.

[image highlights date and count for a browse of a user mailbox]

Steps

1. In the **Dashboard**, select the service you want to browse for backups, and then select protected instances.

2. Select the account you want to browse.
3. Select the time range for the backed up items you wish to browse.



View Backup History shows a calendar view of your backups. If you select **View Backup History**, and you select a date prior to the current day, this changes the time range for the backups you see. For example, if today is 8 October, you select 5 October in the calendar view, then you select to browse the last 5 days starting from 5 October, the items you can browse will be from 1-5 October.

4. Click on the type of items you wish to view: Mail, Calendar, Tasks, Contacts, Files, Contents, or other.
5. Browse the backed up items.

Cancel a job

If you have initiated an immediate backup or an immediate restore, but need to cancel it before it is completed, you can do so.

Steps

1. Click 

from the left navigation pane.
2. Under **Recent Running Jobs**, click the job that you want to cancel.
3. Click **Cancel**.
The progress of the cancelled job is displayed under **Recent Completed Jobs**.

Update the backup retention period

You can update the length of time, in number of years, that data is retained for individual tiers, mailboxes, sites, and MySites to 7 years, 10 years or unlimited. SaaS Backup retains the backup data for the retention period if the subscription is active. If all your backup tiers have the same retention period, you can perform a global update to simultaneously change the retention period for all tenants.

Update the backup retention period for a specific tier

Steps

1. From the **Dashboard**, click any service.
2. Under **Backup Policies**, click the dropdown menu next to **RETENTION PERIOD** for the tier you want to change.
3. Select the desired retention period from the pre-defined list.
4. Click **UPDATE RETENTION PERIOD**.

Update the backup retention period for individual users and tenants

Steps

1. Click the configuration icon  next to your SaaS Backup userid in the top left corner.
2. Click **ACCOUNT SETTINGS**.
3. Click **RETAIN AND PURGE**.
4. To update the data retention policy for a specific user in a specific service, do the following:
   a. Under **Data Retention Policies**, click the dropdown menu next to **TYPE OF PROVIDER** and select the provider.
   b. Click the dropdown menu next to **SERVICE NAME** and select the service.
   c. Click the dropdown menu next to **RETENTION PERIOD** and select the period you want from the list of preset times.
   d. In the search box, begin entering the user, site, or MySite you want to update.
   e. Select the user, site, or MySite you want from the matching results.
   f. Click  .
   g. Continue to search for and add individual mailboxes, sites, or MySites as needed.
   h. Click **Save**.
   The individual mailboxes, sites, or MySites you selected are updated to the selected retention period.

5. To update the data retention policy at the tenant level, do the following:
   a. Under **Tenant Level Data Retention Policies**, click dropdown menu next to **RETENTION PERIOD** and select the period you want from the list of preset times.
   b. Click **Save**.
   All backup policy tiers are updated to the retention period you selected.

Enable backups for OneNote

By default, backups for OneNote notebooks are note enabled. If you want your OneNote notebooks backed up, you must enable the backup in the desired service.

Steps

1. Click **Services** from the left navigation pane.

2. Click Microsoft 365.

3. Under **Manage Services**, click the backup settings icon  next to the service that you need to update.

   A list of your backup settings available for the selected service is displayed.

4. Select **ENABLE ONENOTE BACKUP**.
5. Click **Confirm**.
   Notebooks will be included in the next scheduled backup. If you want them backed up immediately, perform an immediate backup.

Templates and apps supported for backup in Microsoft SharePoint Online

Only certain templates and certain apps are supported for Microsoft SharePoint Online backups.

Supported templates

Only the following templates are supported for Microsoft SharePoint Online backups.

- STS#0 (Team Site)
- BLOG#0 (Blog Site)
- DEV#0 (Developer Site)
- PROJECTSITE#0 (Project Site)
- COMMUNITY#0 (Community Site)
- BDR#0 (Document Center)

- COMMUNITYPORTAL#0 (Community Portal)
- ENTERWIKI#0 (Enterprise WIKI)
- EHS#1 (Root Site)
- EHS#0 (Root Site)
- SITEPAGEPUBLISHING#0 (Communication Site)
- SPSPERS#10 (Personal Sites)
- STS#1 (Blank Site)
- STS#2 (Document Workspace)
- STS#3 (Modern Team Site)
- APP#0 (App Template)
- BLANKINTERNET#0 (Publishing Site)
- TEAMCHANNEL#0
- TEAMCHANNEL#1 (Private Team Channel)

Supported apps

The following apps are supported for Microsoft SharePoint Online backups.

- Custom List
- Badge (Community Site)
- Document Library
- Style Library
- Survey
- Link
- Announcement
- Contact
- Calendar
- Discussion Board
- Photos
- Picture Library
- Content Web Parts
- List Template Gallery
- Master Page Gallery
- Site Pages
- Custom List in Dataset View
- Solution Gallery
- Theme Gallery
- Composed Looks
- Promoted Links

- Tasks
- Posts (Blog Site)
- Comments (Blog Site)
- Community Discussions (Community Site)
- Categories (Blog Site)
- Community Categories (Community Site)
- Report
- Wiki Pages
- Site Collection Images
- Community Members (Community Site)
- Issue Tracking
- Record Library
- Sharing Links

Manage restores

About restores

With SaaS Backup for Microsoft 365, you can perform high-level and granular-level restores for Exchange Online, SharePoint Online, OneDrive for Business, and Microsoft 365 Groups and Teams.

Learn how to perform high-level and granular-level restores:

- Perform a high-level restore
- Perform a granular-level restore for Exchange Online
- Perform a granular-level restore for SharePoint Online
- Perform a granular-level restore for OneDrive for Business
- Perform a granular-level restore for Groups and Teams

The following tables show the high-level restore options that are supported per service and where to find the restored data in SaaS Backup.

When your data is deleted, or deprovisioned, you can restore the data to another location (mailbox, site, Mysite, group, or team) or export the data. You cannot restore to the same location.

Exchange Online

Type of item	Restore to the same mailbox	Restore to another mailbox	Export to PST	Where to find it in SaaS Backup
Single mailbox	Yes	Yes	Yes	Exchange Online > Mailboxes - Users/Shared/Archive
Multiple mailboxes	Yes	Yes	No	Exchange Online > Mailboxes - Users/Shared/Archive
Mailbox content	Yes	Yes	Yes	Exchange Online > Mailboxes - Users/Shared/Archive > <User name>

SharePoint Online

Type of item	Restore to the same site	Restore to another site	Export data	Where to find it in SaaS Backup
Single SharePoint site	Yes	Yes	Yes	SharePoint Online > Sites

Type of item	Restore to the same site	Restore to another site	Export data	Where to find it in SaaS Backup
Multiple SharePoint sites	Yes	Yes	No	SharePoint Online > Sites
SharePoint site content	Yes	Yes	Yes	SharePoint Online > Sites > <Site name>
Single SharePoint site with restore only roles enabled	Yes	No	No	SharePoint Online > Sites
Single subsite	Yes	Yes	Yes	SharePoint Online > Sites > <Site name>
Multiple subsites	Yes	Yes	Yes	SharePoint Online > Sites > <Site name>
SharePoint subsite content	Yes	Yes	Yes	SharePoint Online > Sites > <Site name>
Single/Multiple subsite with restore only roles enabled	Yes	No	No	SharePoint Online > Sites > <Site name>

OneDrive for Business

Type of item	Restore to the same MySite	Restore to another MySite	Export data	Where to find it in SaaS Backup
Single drive	Yes	Yes	Yes	OneDrive for Business > MySites
Multiple drives	No	No	No	OneDrive for Business > MySites
Single drive content	Yes	Yes	Yes	OneDrive for Business > MySites> <OneDrive user>

Groups

Type of item	Restore to the same group	Restore to another group	Export data	Where to find it in SaaS Backup
Single group	Yes	Yes	Yes	Office 365 Groups > Groups

Type of item	Restore to the same group	Restore to another group	Export data	Where to find it in SaaS Backup
Multiple groups	Yes	No	No	Office 365 Groups > Groups
Group content	Yes	Yes	Yes	Office 365 Groups > Groups > <Group Name>
Mailbox content	Yes	No	Yes	Office 365 Groups > Groups > (Group email) > Group Name
SharePoint content	Yes	No	Yes	Office 365 Groups > Groups > <Group name> <Site name>

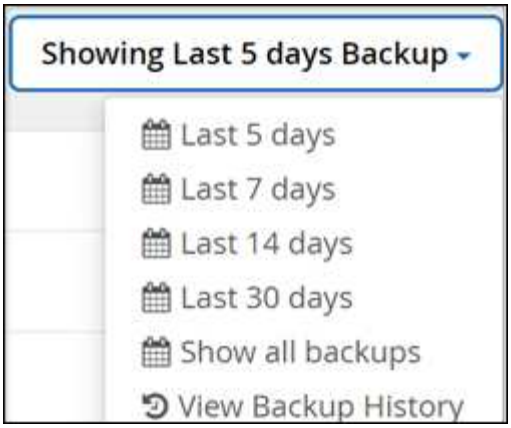
Teams

Type of item	Restore to the same team	Restore to another team	Export data	Where to find it in SaaS Backup
Single team	Yes	Yes	Yes	Office 365 Groups > Teams
Multiple teams	Yes	No	No	Office 365 Groups > Teams
Team content	Yes	Yes	Yes	Office 365 Groups > Teams > <Team name>
Mailbox content	Yes	No	Yes	Office 365 Groups > Teams > (Team email) > Team Name
SharePoint content	Yes	No	Yes	Office 365 Groups > Teams > <Team name> <Site name>
Channels	Yes	No	No	Office 365 Groups > Teams > (Team email)

Perform a high-level service restore

You follow the same procedure to perform high-level restores of mailboxes for Microsoft Exchange Online, MySites for Microsoft OneDrive for Business, sites for Microsoft SharePoint Online, and for Microsoft 365 groups.

By default, only the most recent backup is available for restore. Other available options include:



Steps

1. From the Dashboard, click the number above **PROTECTED** in the box of the service for which you want to perform the restore.
2. Select the name of the mailbox, group, team, Mysite, or site to restore.
3. Select a restore option:

   If you select the export to PST restore option, the provided link is valid for seven days and is pre-authenticated.

   a. If you are restoring mailboxes for **Microsoft Exchange Online** select one of the following options:

      Restoring mailboxes with messages larger than 140 MB may encounter upload failures back to the server. We recommended that you perform a high-level restore using the Export to PST option. For more information, see Microsoft Exchange Online limits: Message limits.

      - Restore to the same mailbox
      - Export to PST
        If you export to PST, you will receive a notification email with the location of the PST file when the export is completed.
      - Restore to another mailbox
        If you restore to another mailbox, you must enter the destination mailbox in the search field. You can type in a portion of the destination email address in the search field to initiate an automatic search for matching destination mailboxes.

   b. If you are restoring groups for **Microsoft Office 365 Groups** select one of the following options:

      - Restore to the same group
      - Restore to another group
      - Export data
        If you export, a PST file is created with your Microsoft Exchange files and a .zip file is created with your Microsoft SharePoint sites. You will receive a notification email containing the location of the PST file and an authenticated URL to the location of the .zip file.

   c. If you are restoring teams under **Microsoft Office 365 Groups** select one of the following options:

      - Restore to the same team
      - Restore to another team

This is ideal for situations where a team is deleted from Microsoft 365. You should create a new team to use this restore option. If you have recently created a new team in MS Teams, discover it by syncing the service. Go to **Services Settings** on the left. Click **Office 365**. Under **Manage Services**, click **Sync Now** for Microsoft 365 Groups.

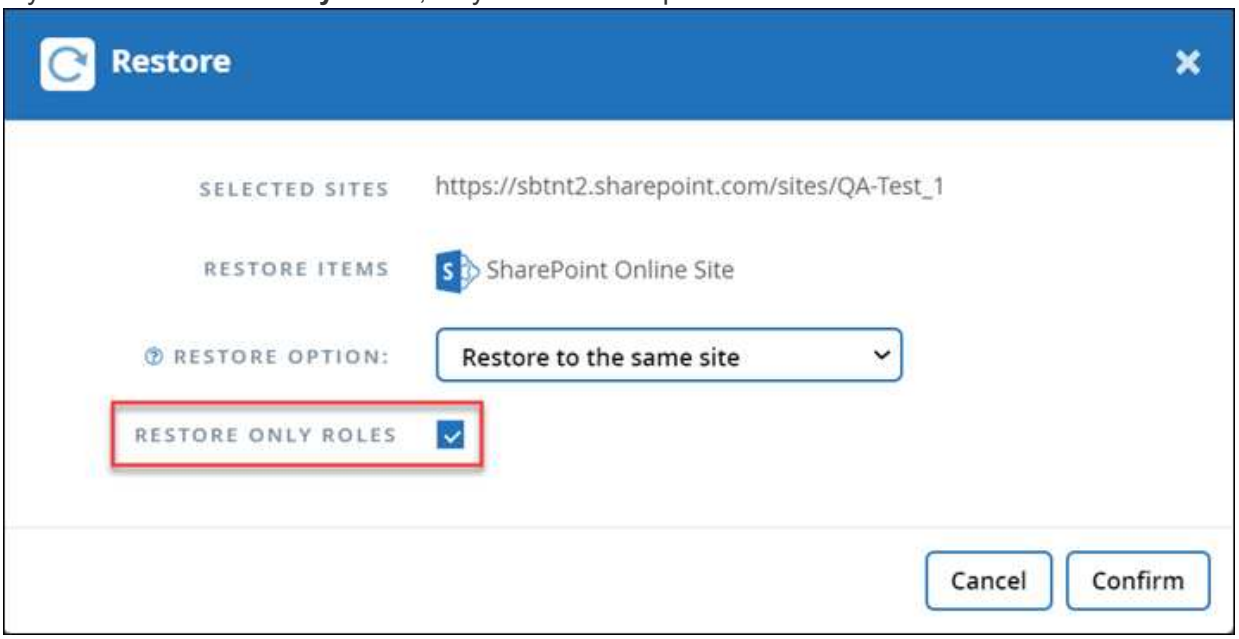
- Export data
  If you export data, you need to download it. Go to Reporting on the left menu. Find your export data job. Click on **Total Folders**. Then click **Export Data Download Link**. A zip file downloads. Open the zip file to extract the data.

d. If you are restoring MySites for **Microsoft OneDrive for Business**, select one of the following options:

- Restore to the same MySite
- Restore to a different MySite
  If you restore to a different MySite, enter the destination MySite in the search field. You can type in a portion of the destination MySite in the search field to initiate an automatic search for matching destination MySites.
- Export data
  If you export, a .zip file is created with your MySites. You will receive a notification email containing an authenticated URL to the location of the .zip file.

e. If you are restoring sites for **Microsoft SharePoint Online**, select one of the following options:

- Restore to the same site
  If you select **Restore Only Roles**, only the roles and permissions restore.



- Restore to another site
  If you restore to another site, enter the destination site in the search field. You can type in a portion of the destination site in the search field to initiate an automatic search for matching destination sites.
- Export data
  If you export, a .zip file is created with your site collection. You will receive a notification email containing an authenticated URL to the location of the .zip file.

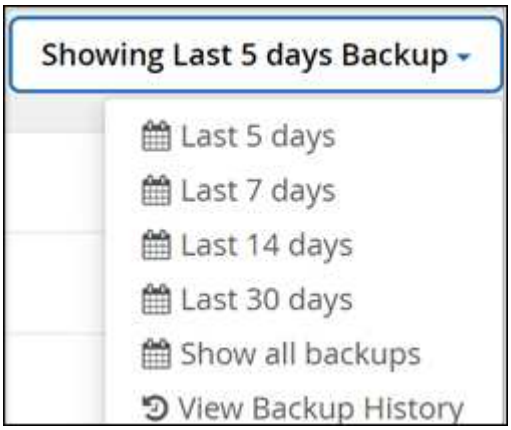
4. Click **Confirm**.
   A message is displayed indicating that the restore job was created.
5. Click **View the job progress** to monitor the progress of the restore.

Perform a granular-level restore

Perform a granular-level restore for Microsoft Exchange Online

Within Microsoft Exchange Online, you can restore granular-level items for a single user, such as individual emails, tasks, contacts, and calendar events. You can also restore granular-level items for a Microsoft 365 group mailbox.

By default, only the most recent backup is available for restore. Other available options include:



The table indicates the restore options that are supported for granular-level items for Exchange Online.

Type of item	Restore to the same mailbox	Restore to another mailbox	Export to PST/Export to HTML	Where to find it in SaaS Backup
Mail/Task/Contacts/ etc.	Yes	Yes	Yes	Exchange Online > Mailboxes - Users
Single/Multiple mailbox folders (Inbox, Archive, etc.) **Note**: Excludes conversation history.	Yes	Yes	Yes	Exchange Online > Mailboxes - Users > <User Name>
Folder level under Inbox	Yes	Yes	Yes	Exchange Online > Mailboxes - Users > <User Name>
Subfolder level under Inbox	Yes	Yes	Yes	Exchange Online > Mailboxes - Users > <User Name>
Conversation history under Mail folder	No	No	Yes	Exchange Online > Mailboxes - Users > <User Name>

Type of item	Restore to the same mailbox	Restore to another mailbox	Export to PST/Export to HTML	Where to find it in SaaS Backup
Single/Multiple item-level restores	Yes	Yes	No	Exchange Online > Mailboxes - Users > <User Name>
Single/Multiple restore items for "Replace the existing content"	Yes	No	No	Exchange Online > Mailboxes - Users > <User Name>

Steps

1. From the Dashboard, click the number above **PROTECTED** in the Exchange box.

2. Select your restore option.
   a. For shared mailboxes, click the **SHARED** tab.
   b. For archive mailboxes, click the **ARCHIVE** tab.
   c. For regular mailboxes, remain on the **USER** tab.
3. Click the mailbox for which you need to perform the granular-level restore.
4. Restore an entire Microsoft Office Exchange category or restore a specific item within a category. For a Microsoft 365 Groups mailbox, you only have the option to restore from the mail category or the calendar category.
5. Select the category (Mail, Tasks, Contacts, or Other) that you need to restore.

   If you want to restore a single item inside the category, click the category, and then select the items that you want to restore.

6. Click **Restore**.
7. Select a restore option.
   - **Restore to the same mailbox**

     If you restore to the same mailbox, by default, a restore folder with the current date and time stamp is created in the original content location containing the backup copy. If you select **Replace the existing content**, then your current data is completely replaced by the backup.

     For Microsoft 365 Groups, you only have the option to restore to the same mailbox. The existing content is replaced by default. For Microsoft Exchange Online, you can restore to the same mailbox and replace the existing content or you can restore to another mailbox.

   - **Restore to another mailbox**

     If you restore to another mailbox, you must enter the destination mailbox in the search field. You can type in a portion of the destination email address in the search field to initiate an automatic search for

matching destination mailboxes.

- **Export to PST**

  You can select to include all the category subfolders.

  If you export to PST, you will receive a notification email with the location of the PST file when the export is completed.

  > This option is not available for Microsoft 365 Groups.

  > If you select the **Export to PST** restore option, the provided link is valid for seven days and is pre-authenticated.

- **Export to Data** (Available for Microsoft 365 groups only):

  If you export, two zip files are created, one zip file for Microsoft 365 Groups mailbox and another zip file for Microsoft 365 Groups SharePoint sites. You will receive a notification email containing the location of the PST file and an authenticated URL to the location of the .zip file.

  > If you select the **Export to Data** restore option, the provided link is valid for seven days and is pre-authenticated.

8. Click **Confirm**.

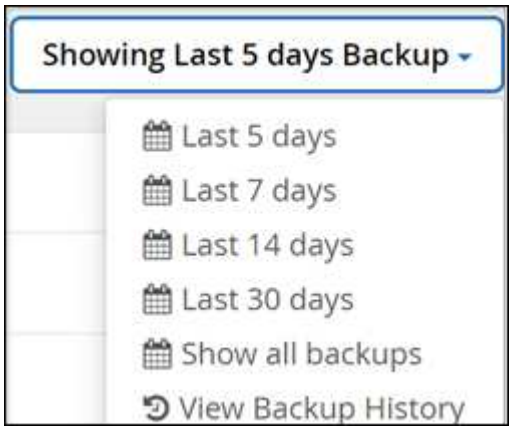
   A message is displayed indicating that the restore job was created.

9. Click **View the job progress** to monitor the progress of the restore.

Perform a granular-level restore for Microsoft SharePoint Online

Within Microsoft SharePoint Online, you can restore granular-level items for a single user, such as individual folders or files. You can also restore granular-level items for a Microsoft 365 group site and OneNote notebooks. Site roles and permissions are protected automatically as part of a restore or backup.

By default, only the most recent backup is available for restore. Other available options include:



The table indicates the restore options that are supported for granular-level items.

For the restore options **Restore to the same site** and **Restore to another site**, the following items restore as subsites under the selected site with the naming convention <sitename_cc_timestamp>: **Single site**, **multiple sites**, and **single/multiple lists** if 3 or more lists are selected.

Type of item	Restore to the same site	Restore to another site	Export data	Where to find it in SaaS Backup
Single/multiple items	Yes	Yes	No	SharePoint Online > Sites > <Site Name> > <List Name>
Single site	Yes	Yes	Yes	SharePoint Online > Sites
Multiple sites	Yes	Yes	No	SharePoint Online > Sites
Communication sites	No	No	No	SharePoint Online > Sites
Single/multiple subsites	Yes	Yes	Yes	SharePoint Online > Sites > <Site name> > Subsites
Single/multiple folders	Yes	Yes	Yes	SharePoint Online > Sites > <Site name> > <List name>
Single/multiple lists	Yes	Yes	Yes	SharePoint Online > Sites > <Site name>
OneNote single/multiple notebooks	Yes	Yes	Yes	SharePoint Online > Sites > <Site name> > <List name>
OneNote single/multiple section groups	Yes	Yes	Yes	SharePoint Online > Sites > <Site name> > <List name> > <Notebook folder>
OneNote single/multiple sections	Yes	Yes	No	SharePoint Online > Sites > <Site name> > <List name> > <Notebook folder>

Steps

1. From the Dashboard, click the number above **PROTECTED** in the SharePoint box.
2. Click the site for which you need to perform the granular-level restore.
3. Select the category that you need to restore.

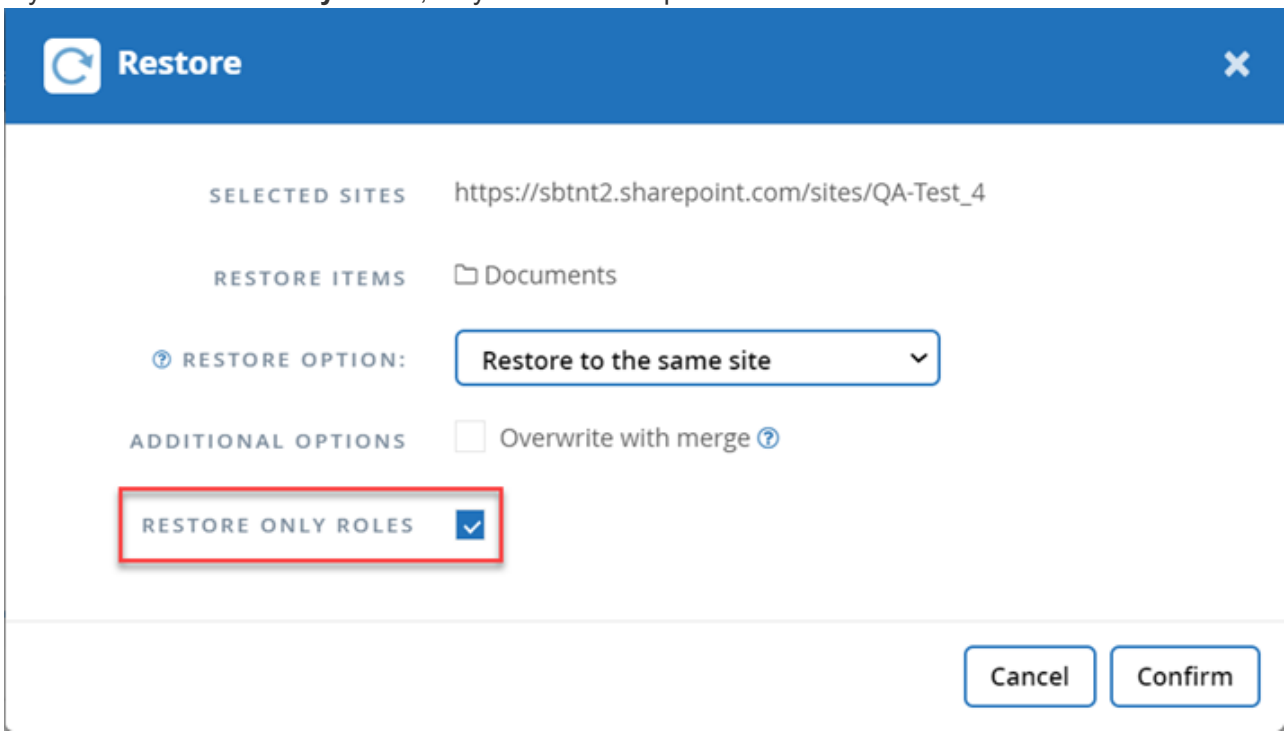
   If you want to restore specific individual items inside a category, click the content category and then select the individual items.

4. To restore from the most recent backup, click **Restore**. To restore a previous version of the item, click **Show versions**, and select the version that you want to restore and then click **Restore**.
5. Select a restore option:
   - **Restore to the same site**
     If you restore to the same site, by default, a restore folder with the current date and time stamp is created in the original file location containing the backup copy.

If you select **Restore only roles**, **Overwrite with merge**, or **Replace the existing content**, the only restore option is **Restore to the same site**.

If you select	Restore to the same site
Restore only roles	all types of items
Overwrite with merge	all items except site level
Replace with existing content	item level only

If you select **Restore Only Roles**, only the roles and permissions restore.



If you select the **Overwrite with merge** option, no restore folder is created. If the version of the backup file and the current file match, the backup is restored to the original location. Any new content in the destination is ignored and unaffected. For example, if the backup contains File1 version5 and the destination contains File1 version 6, a restore with the **Overwrite with Merge** option selected fails.

If you select the **Replace the existing content** option, the current version of the data is completely replaced with the backup copy.

- **Restore to another site**

  If you restore to another site, you must enter the destination site in the search field. You can type a portion of the site in the search field to initiate an automatic search for matching sites.

- **Export Data**

  If you export data, you need to download it. Go to **Reporting** on the left menu. Find your export data job. Click on **Total Folders**. Then click **Export Data Download Link**. A zip file downloads. Open the zip file to extract the data.

If you select the **Export Data** restore option, the provided link is valid for seven days and is pre-authenticated.

6. Click **Confirm**.

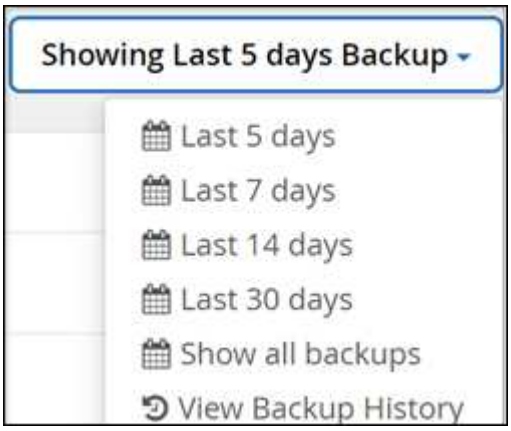
   A message is displayed indicating that the restore job was created.

7. Click **View the job progress** to monitor the progress of the restore.

Perform a granular-level restore for Microsoft OneDrive for Business

Within Microsoft OneDrive for Business, you can restore granular-level items, such as individual folders or files, for a list or library. You can also restore OneNote notebooks or groups.

By default, only the most recent backup is available for restore. Other available options include:



The table indicates the restore options that are supported for granular-level items for OneDrive for Business.

Type of item	Restore to the same MySite	Restore to another MySite	Export data	Where to find it in SaaS Backup
Single drive	Yes	Yes	Yes	OneDrive for Business > MySites
Multiple drives	No	No	No	OneDrive for Business > MySites
Single/multiple folders	Yes	Yes	Yes	OneDrive for Business > MySites > <Drive Name> > Files
Single/multiple items	Yes	Yes	No	OneDrive for Business > MySites > <Drive name> > Files
Notebooks folders	Yes	Yes	No	OneDrive for Business > MySites > <Drive name> > Files
OneNote single/multiple folders	Yes	Yes	No	OneDrive for Business > MySites > <Drive name> > Files > Notebooks

Steps

1. From the Dashboard, click the number above **PROTECTED** in the OneDrive box.
2. Click the MySite for which you need to perform the restore.
3. Select the group of files.

   If you want to restore individual folders or files within a group, click on the group of files. To restore an entire folder, select the folder. To restore individual files within a folder, select the folder containing the files, and then select the individual files.

4. Click **Restore**.
5. Select a restore option:
   - **Restore to the same MySite**

     If you are restoring individual files to the same MySite, by default, a restore folder with the current date and time stamp is created in the original content location containing the backup copy.

     If you select **Replace the existing content**, then your current data is completely replaced by the backup.

   - **Restore to another MySite**

     If you restore to another MySite, you must enter the destination MySite in the search field. You can type in a portion of the destination MySite in the search field to initiate an automatic search for matching destination MySites.

   - **Export Data**

     If you export data, you need to download it. Go to Reporting on the left menu. Find your export data job. Click on **Total Folders**. Then click **Export Data Download Link**. A zip file downloads. Open the zip file to extract the data.

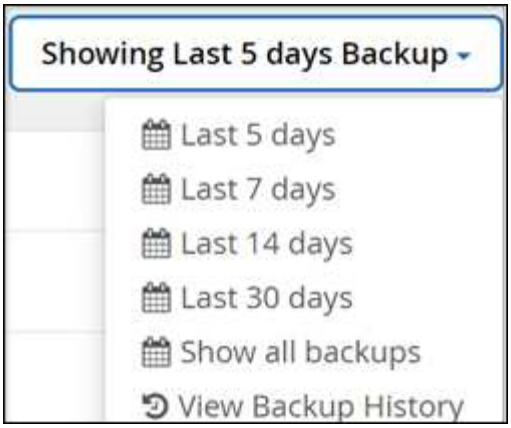
     If you select the **Export Data** restore option, the provided link is valid for seven days and is pre-authenticated.

6. Click **Confirm**.
7. Click **View the job progress** to monitor the progress of the restore.

Perform a granular-level restore for Microsoft 365 Groups and Teams

Within Microsoft 365 Groups and Teams, you can restore granular-level items like mailboxes, SharePoint, conversations, channels, and tabs.

By default, only the most recent backup is available for restore. Other available options include:



The table indicates the restore options that are supported for granular-level items and where to find them in SaaS Backup.

For **Groups**

Type of item	Restore to the same group	Restore to another group	Export data	Where to find it in SaaS Backup
Single/multiple folders	Yes	No	Yes	Office 365 Groups > Groups > (Group Name) > Mailbox
Inbox	Yes	No	Yes	Office 365 Groups > Groups > (Group Name) > Mailbox
Single/multiple items (email or event)	Yes	No	No	Office 365 Groups > Groups > (Group Name) > Mailbox > Mail

For **Teams**

Type of item	Restore to the same team	Restore to another team	Export data	Where to find it in SaaS Backup
Single/Multiple folders	Yes	No	Yes	Office 365 Groups > Teams > (Team Name) > Mailbox
Inbox	Yes	No	Yes	Office 365 Groups > Teams > (Team Name) > Mailbox > Mail
Single/multiple items (email or event)	Yes	No	No	Office 365 Groups > Teams > (Team Name) > Mailbox > Mail

Type of item	Restore to the same team	Restore to another team	Export data	Where to find it in SaaS Backup
Conversations/chat	No	No	Yes (export to HTML only)	• Office 365 Groups > Teams > (Team Name) > Mailbox > Conversations > Team Chat • Office 365 Groups > Teams > (Team Name) > Mailbox > Mail > Conversation History > Team Chat (actual location)
Conversation single/multiple items	No	No	Yes (export to HTML only)	Office 365 Groups > Teams > (Team Name) > Mailbox > Conversation History > Team Chat
Single/multiple channels	Yes	No	No	Office 365 Groups > Teams > (Team Name) > Channels **Note**: Restore includes channel name and tab names only.
Tabs under channels	No	No	No	Office 365 Groups > Teams > (Team Name) > Channels
Channel standard documents	Yes	No	Yes	Office 365 Groups > Teams > (Team Name > SharePoint Site > Documents > (Channel name)
Channel private documents	Yes	No	Yes	SharePoint > (Private channel site name) > Documents > (Private Channel name) **Note**: You will find a separate site collection with name “<Your Team Name – Private Channel Name>”. You can filter for these site collections with Template ID: TEAMCHANNEL#0.
OneNote content	Yes	No	Yes	Office 365 Groups > Teams > (Team Name) > SharePoint Site > Documents > (Channel Name)
Wiki content	Yes	No	Yes	Office 365 Groups > Teams > (Team Name) > SharePoint Site > Teams Wiki Data > (Channel Name)
Files	Yes	No	No	Office 365 Groups > Teams > (Team Name) > SharePoint Site > Documents > (Channel Name)

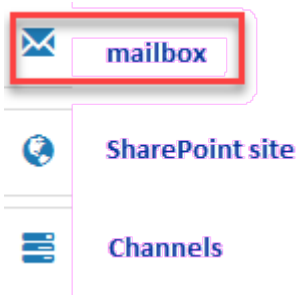
Type of item	Restore to the same team	Restore to another team	Export data	Where to find it in SaaS Backup
Individual user chat and group chats **Note**: Chats included in Exchange Online backups.	No	No	Yes	• Exchange > “User” > Mail > Conversations > Team Chat • Exchange > “User” > Mail > Conversation History > Team Chat
Files in individual user chat and group chats **Note**: Files included in OneDrive for Business backups.	Yes	No	No	OneDrive > “User” > Files > Microsoft Teams Chat Files

Restore mailboxes

Select this granular-level restore to restore inboxes, calendars, and conversation history.

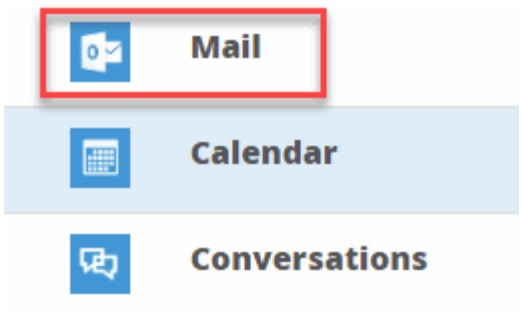
Steps

1. From the Dashboard, click the number above **PROTECTED** in **Microsoft 365 Groups**.
2. Select the **Groups** or **Teams** tab.
3. Click the group or team for which you need to perform the granular-level restore.
4. Select the mailbox category.



For Groups, **Channels** is unavailable.

- Select the **Mail** option to restore inbox or conversation history to the same mailbox or export data.



For Groups, **Conversations** is unavailable.

a. To restore an inbox, select **Inbox** and click **Restore**.

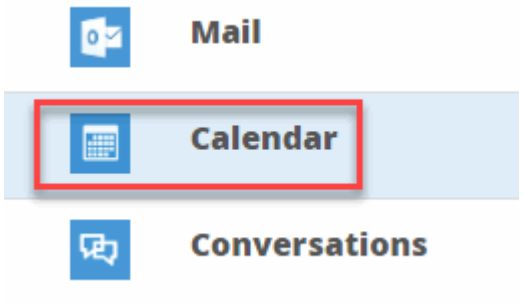
i. Select **Restore to the same mailbox** or **Export Data**.

If you export data, you need to download it. Go to **Reporting** on the left menu. Find your export data job. Click on **Total Folders**. Then click **Export Data Download Link**. A zip file downloads. Open the zip file to extract the data.

If you select the **Export Data** restore option, the provided link is valid for seven days and is pre-authenticated.

ii. Click **Confirm**.

◦ Select the **Calendar** option to restore the calendar to the same mailbox or export data.



a. Select **Calendar** and click **Restore**.

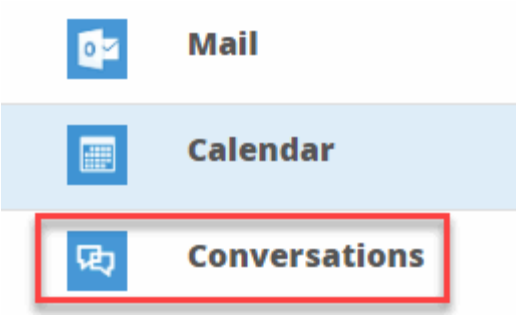
b. Select **Restore to the same mailbox** or **Export Data**.

If you export data, you need to download it. Go to Reporting on the left menu. Find your export data job. Click on **Total Folders**. Then click **Export Data Download Link**. A zip file downloads. Open the zip file to extract the data.

If you select the **Export Data** restore option, the provided link is valid for seven days and is pre-authenticated.

c. Click **Confirm**.

◦ Select the **Conversations** option to restore conversations. The only option for restore is export to HTML.



a. Select the conversations you want to restore and click **Restore**.

> **View Conversations** shows you a list of all conversations from the last "x" days of backups up to the last 30 backups. For example, if you back up seven times in the last five days, then you can only see conversations from the last seven backups.

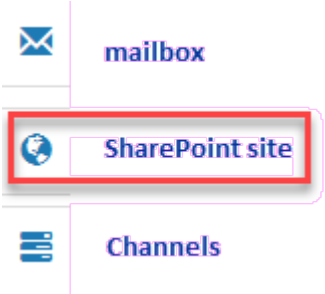
b. Click **Confirm**.

Restore SharePoint sites

Select this granular-level restore to restore tabs and attachments.

Steps

1. From the Dashboard, click the number above **PROTECTED** in **Microsoft 365 Groups**.
2. Select the **Groups** or **Teams** tab.
3. Click the group or team for which you need to perform the granular-level restore.
4. Select SharePoint site option.



5. Click the site for which you need to perform the granular-level restore.
6. Select the category that you need to restore.

> If you want to restore specific individual items inside a category, click the content category and then select the individual items.

7. Click **Restore**.
8. Select a restore option:
   - **Restore to the same site**

     If you restore to the same site, by default, a restore folder with the current date and time stamp is created in the original file location containing the backup copy. If you select the **Overwrite with merge** option, no restore folder is created. If the version of the backup file and the current file match, the backup is restored to the original location. Any new content in the destination is ignored and unaffected. For example, if the backup contains File1 version5 and the destination contains File1

version 6, a restore with the **Overwrite with Merge** option selected fails. If you select the **Replace the existing content** option, the current version of the data is completely replaced with the backup copy.

- **Export Data**

  If you export data, you need to download it. Go to Reporting on the left menu. Find your export data job. Click on **Total Folders**. Then click **Export Data Download Link**. A zip file downloads. Open the zip file to extract the data.

  If you select the **Export Data** restore option, the provided link is valid for seven days and is pre-authenticated.

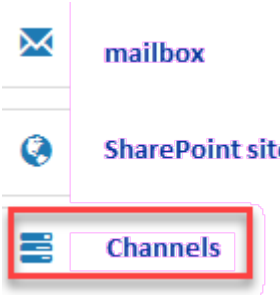
9. Click **Confirm**.

Restore channels

Select this granular-level restore to restore channels.

Steps

1. From the Dashboard, click the number above **PROTECTED** in **Microsoft 365 Groups**.
2. Select the **Teams** tab.
3. Click the team for which you need to perform the granular-level restore.
4. Select **Channels**.



5. Select the channel to restore.
6. Click **Restore**.
7. Select the restore option:
   a. Click **Restore to the same team**.
   b. Click **Restore to another team**.

      To select another team, search for the other team in the search box.

8. Click **Confirm**.

Restore from a previous backup

By default, only your most recent backup is available for restore.

Steps

1. From the Dashboard, click the number above **PROTECTED** in box of the service for which you want to perform the restore.

- For shared mailboxes, click the **SHARED** tab.
- For archive mailboxes, click the **ARCHIVE** tab. Note: Archive mailboxes are restored to the user's regular mailbox.
- For regular mailboxes, remain on the **USER** tab.

2. Click the item that you want to restore.
3. Click **View Backup History**.

   A calendar is displayed. Dates for which backups are available are indicated by a green circle.

4. If you want to display the items backed up over a select number of days, click **Show Selected Backups** and select one of the pre-defined number of days from the drop-down menu.
5. Otherwise, click the date of the backup that you want to restore and then select the specific backup.
6. Select the items that you want to restore.
7. Click 

8. Select a restore option:
   a. If you are restoring mailboxes for **Microsoft Exchange Online** or a mailbox for a Microsoft 365 Group, select one of the following options:
      - **Restore to the same mailbox**

        If you are restoring to the same mailbox, by default, a restore folder with the current date and time stamp is created in the original content location containing the backup copy. If you select **Replace the existing content**, then your current data is completely replaced by the backup.

      - **Restore to another mailbox**

        If you restore to another mailbox, you must enter the destination mailbox in the search field. You can type in a portion of the destination email address in the search field to initiate an automatic search for matching destination mailboxes.

   b. If you are restoring MySites for **Microsoft OneDrive for Business**, select one of the following options:
      - **Restore to the same MySite**

        If you are restoring individual files to the same MySite, by default, a restore folder with the current date and time stamp is created in the original content location containing the backup copy. If you select **Replace the existing content**, then your current data is completely replaced by the backup. If you are restoring an entire folder, the option to **Replace the existing content** is not available.

      - **Restore to a different MySite**

        If you restore to a different MySite, you must enter the destination MySite in the search field. You can type in a portion of the destination MySite in the search field to initiate an automatic search for matching destination MySites.

   c. If you are restoring sites for **Microsoft SharePoint Online**, you can restore to the same site or to a different site. If you are restoring a Microsoft 365 group site, you can only restore to the same site.
      - **Restore to the same site**

        If you restore to the same site, then by default, a restore folder with the current date and time stamp is created in the original file location containing the backup copy. If you select the **Overwrite**

with merge option, no restore folder is created. If the version of the backup file and the current file match, the backup is restored to the original location. Any new content in the destination is ignored and unaffected. For example, if the backup contains File1 version5 and the destination contains File1 version 6, a restore with the **Overwrite with Merge** option selected fails. If you select the **Replace the existing content** option, the current version of the data is completely replaced with the backup copy.

- **Restore to a different site**

  If you restore to a different site, you must enter the destination site into the search field. You can type a portion of the destination site into the search field to initiate an automatic search for matching sites.

9. Click **Confirm**.

   A message is displayed indicating that the restore job is created.

10. Click **View the job progress** to monitor the progress of the restore.

Cancel a job

If you have initiated an immediate backup or an immediate restore, but need to cancel it before it is completed, you can do so.

Steps

1. Click 

from the left navigation pane.
2. Under **Recent Running Jobs**, click the job that you want to cancel.
3. Click **Cancel**.
   The progress of the cancelled job is displayed under **Recent Completed Jobs**.

Find restored files

When some files or folders are restored, they are contained inside a newly created restore folder. To help you easily find your restored items, you can download an Excel file with the names and locations of your restored files and folders.

Steps

1. Click 

on the left navigation pane.
2. Under **Recent Completed Jobs**, click the job for which you want to find restored files.
3. Click **Download** in the upper right.
   An Excel file is downloaded locally containing the names and locations of restored files for the specific job.

View data

Create a user defined filter

You can filter the view of your mailboxes, sites, or MySites to only show results that fit specific criteria. For example, you can set your filters to only see mailboxes in a certain country and a certain department within that country.

Steps

1. From the Dashboard, click the number above **PROTECTED** or **UNPROTECTED** in the box of the service for which you want to create a filter.
   The number above PROTECTED indicates the number of mailboxes, MySites, or groups that are currently protected by a backup policy. The number above UNPROTECTED indicates the number of mailboxes, MySites, or groups that are not protected by a backup policy.

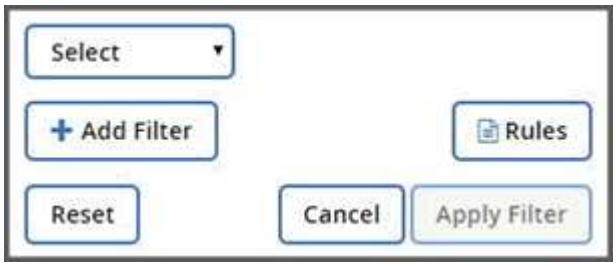
2. Click **Filter**.

3. Click the **Select** drop-down menu, and select the filter of your choice.

   For Microsoft SharePoint Online, you can filter by Template ID. You can enter the Template ID to search for it, or select it from the dropdown menu.

   For all other services, you can filter by group, country, office, department, title, domain or country. If you have security groups, they are also listed as filtering options.

   The second drop-down menu is populated with selections based on the filter you select. For example, if you select Group as your first filter, you can select one of the backup policy group tiers as your secondary filter.



   A search field appears.

4. Enter your search criteria.
5. If you want to add more filters, click **Add Filter** and make your selection.
6. Click **Apply Filter**.

Filter results are displayed.

Perform a search

In SaaS Backup for Microsoft 365, you can search your protected data in all services - Exchange Online, SharePoint Online, OneDrive for Business, and Groups and Teams.

You can search unprotected instances, but it will yield search results only if previous backups have been taken.

To improve your search results, use the following criteria:

- Three character minimum

> If you enter more than 3 characters, previous search results for 3 characters may remain in your search results.

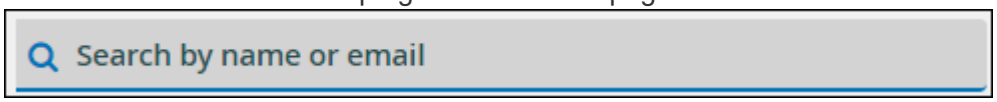
- Alphanumeric input
- Single quotes for an exact match of a word, string of words, or number. Ex: “2014 Budget”.

Follow the steps below to search your protected instances.

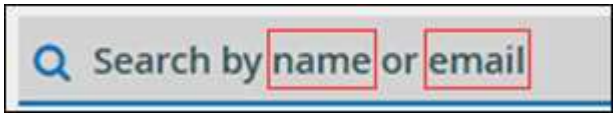
Steps

1. From the Dashboard, click the number above **Protected** in any service in which you want to search.

2. Find the search box at the top right corner of the page.



   Then enter the prompted information you see in the search box, such as “name” or “email" in the search box.



   a. Search by name or email address for Microsoft Exchange Online.
   b. Search by name, email, or MySite for Microsoft OneDrive for Business.
   c. Search by site name or url for Microsoft SharePoint Online.
   d. Search by group name or team name for Microsoft 365 Groups and Teams.

3. Any results that fit or match the search criteria will appear.

You can also perform a search at more granular levels within each service. If you see a dropdown menu to the right of the search box, select **File** or **Folder** from the dropdown menu to narrow your search results.

[search box with file/folder dropdown menu]

Use Advanced Search for Microsoft Exchange Online

You can use **Advanced Search** for Microsoft Exchange Online to search for individual or shared mailbox items and restore these items to their original mailbox.

Administrators can enable **Advanced Search** by going to Support and submitting a request. You can also email the SaaS Backup support team at saasbackupsupport@netapp.com.

After you enable **Advanced Search**, you can turn on Self Service Portal (SSP) for individual tenants. If you do not enable **Advanced Search** before your first backup, no search results appear.

- Enable Advanced Search
- Perform a search
- Find previous search jobs

Enable Advanced Search

You can enable the **Advanced Search** feature in Advanced Search Settings.

Licensed and unlicensed users can use the advanced search feature if enabled.

Steps

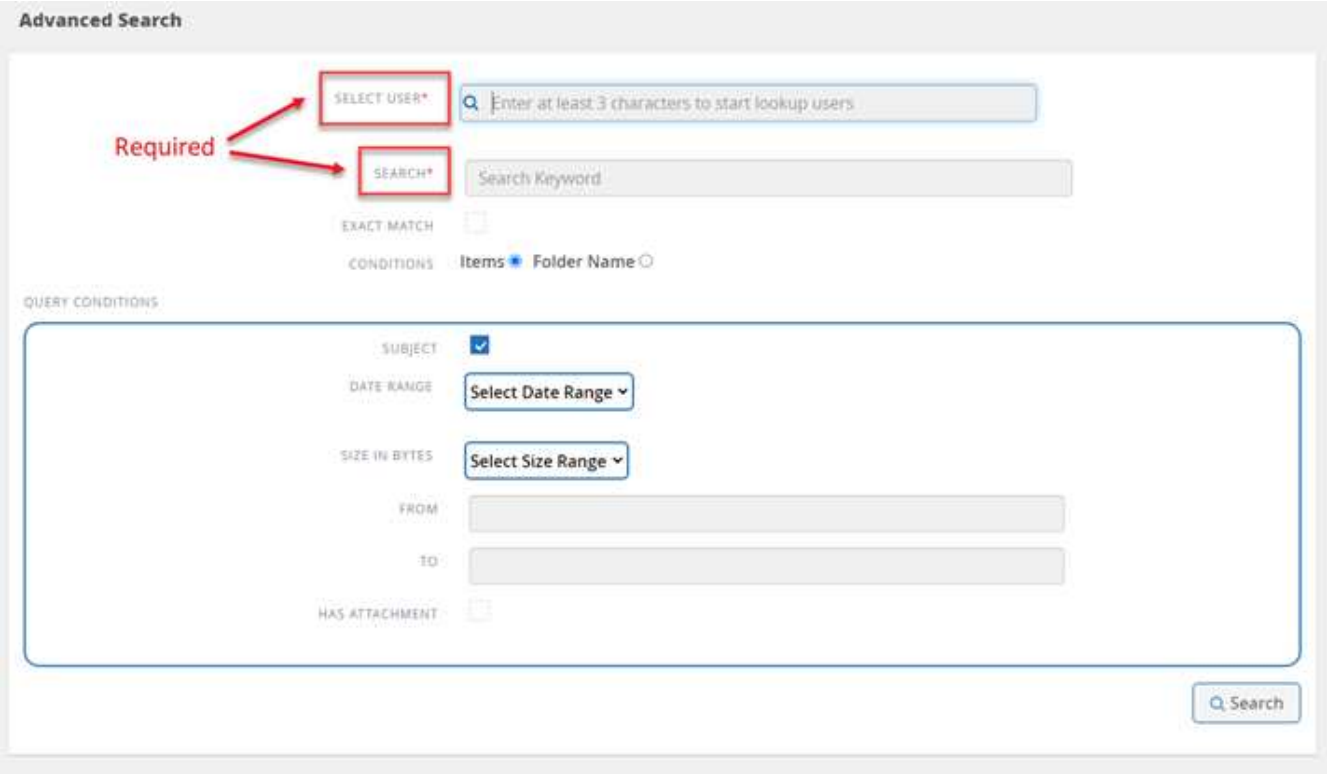
1. From the dashboard, click **Advanced Search** in the left menu.
2. Click **Advanced Search Settings**.
   - By default, the list displays all licensed users. Toggle between **Show All Users** and **Show Only Licensed Users** to filter the user type in the list.
   - Use the Search tool and type at least three characters to find a unique user.
3. To enable a user, under the **Advanced Search** column, select **On**.
   The next time you protect that enabled user in a full or incremental backup, you can perform a search of any new email items.
4. Click **Save Settings**.
5. To backup the enabled users, go to Scheduling a backup or changing backup frequency and remain on the **User** tab to select the users for backup.

Perform a search

You can perform a search for individual or shared mailbox items and restore these items to their original mailbox under **Perform Search**.

Steps

1. From the dashboard, click **Advanced Search** in the left menu.
2. Click **Perform Search**.
3. Enter information into the required fields with an asterisk (*).
   Optional fields: Conditions and Query Conditions.



- **Select User**: Type at least three letters in the user's name to find the user you want to select.
- **Search**: Type at least three characters in a keyword. If you want to search a phrase, place the words in the phrase inside quotations (example: "Hello world"). If the words can be searched separately, quotes are not needed.
- **Exact match**: Select if you want to search only for the exact keywords.
- **Conditions**:
  - **Items**: Select items to search for all items in the mailbox.
  - **Folder Name**: Select folder name to search for items in a specific folder in the mailbox. Type the folder name in the text box provided.
- **Date range**: From the date range drop down menu, select either **Last 7 Days** or **Custom Range** to input start and end date for the search.
- **Size in bytes**: From the size in bytes drop down menu, select either **Greater Than (>)** or **Lesser Than (<)**. Then enter the size in bytes.
- **From**: Enter the email address for the sender.
- **To**: Enter the email address for the receiver.

- **Subject**: Select to search only by subject.
- **Has attachment**: Select if the email item or items have attachments.

4. Click **Search**.
5. To find your search job, go to Finding Previous Search Jobs below.

Find previous search jobs

You can find previous search jobs under **Previous Search Jobs**.

Steps

1. From the dashboard, click **Advanced Search** in the left menu.
2. Click **Previous Search Jobs**.
3. Find the search job you performed previously.
   If zero search results appear, that means no items met the conditions you entered for your search.
4. Click on the number of total search results to display them.
5. From the results display view, you can restore items, select how many entries show using the drop-down menu **Show # entries**, or search to narrow the results further.

> Restored items go back to the original mailbox with the naming convention CC_search_MM.DD_time. To find the restore job, go to **Jobs** in the left menu.

6. To exit the results display for your search, click on **Back To Search Jobs**.

View job history and activity log

SaaS Backup for Microsoft 365 stores a log of your job history and a log of all activities performed inside SaaS Backup.

View job history

You can view or download reports of all your job history in NetApp SaaS Backup for Office 365. You can filter your search by job type, service, start time, end time, and completion status.

Steps

1. Click **Reporting** on the left navigation pane.
   A list of all SaaS Backup jobs is displayed under the **Job History** tab.
2. To filter the results, click **Filter**.
3. Click the **Select** drop-down menu, and select a filter.
   You can filter by policy, service, type, or status. After you select a filter, a search field appears.
4. Enter your search criteria.
5. If you want to add more filters, click **Add Filter**.
6. Click **Apply Filter**.
   Filter results are displayed.

7. Click any job to expand the view for additional job details.

View the activity log

A log is stored of all activity that occurs inside SaaS Backup for Microsoft 365. The log contains the date of each action performed along with the name of the user who performed the action. You can filter the activity log by service and event. For example, if you need to see all of the restore operations that have occurred for Microsoft Exchange Online, you can filter the activity log to view those specific results.

Steps

1. Click **Reporting** on the left navigation pane.
2. Click the **Activity Log** tab.
   A list of all SaaS Backup for Microsoft 365 activity is displayed.
3. To filter the results, click **Filter**.
4. Click the **Select** drop-down menu, and select a filter.
   You can filter by service or event. After you select a filter, a search field appears.
5. Enter your search criteria.
6. If you want to add more filters, click **Add Filter**.
7. Click **Apply Filter**.

   Filter results are displayed.

View a list of deprovisioned items

You can view a list of mailboxes or user accounts that have been deprovisioned.

Steps

1. Click **SERVICES** on the left navigation pane.
2. In the desired service, click the number of unprotected items.
3. Click the **DEPROVISIONED** tab.

View a list of purged data

You can view a list of mailboxes or user accounts that have been purged.

Steps

1. Click  next to your SaaS Backup user id in the top left corner.
2. Select **ACCOUNT SETTINGS**.
3. Click **RETAIN AND PURGE**.
4. Under **Purge Data**, click **Show Purged List**.

   You can view a list of items scheduled to be purged and a list of items that have already been purged.

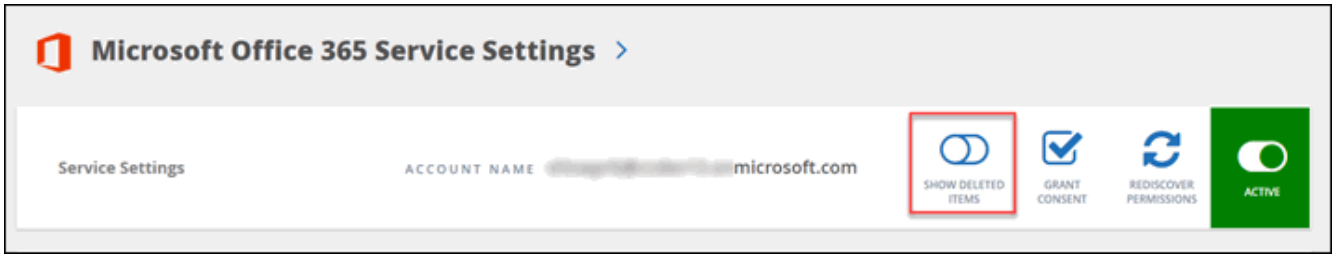
View deleted items

You can view deleted items in all services at any time by switching on **Show deleted items** in Service Settings. This helps you save time; instead of browsing through different backups for deleted items, turn on the switch to find the deleted items immediately.

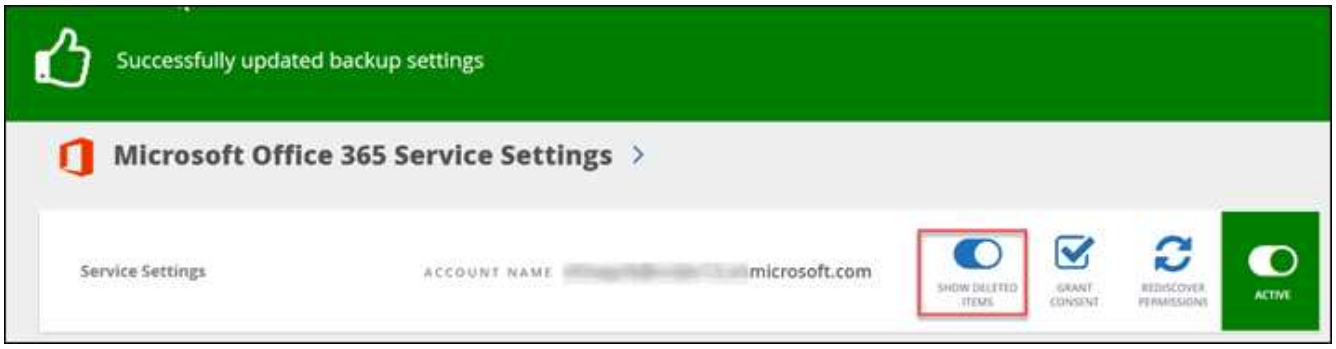
By default, the switch is turned off.

Steps

1. Click **SERVICES** on the left navigation pane.
2. Click the Settings icon .



3. Turn on the **Show Deleted Items** switch.



4. Click **Jobs** on the left navigation pane.
5. Open the most recent backup to see the deleted items.

Download logs

SaaS Backup for Microsoft 365 stores a log of your job history inside SaaS Backup. You can download the job history and a list of completed jobs.

Download the activity log

A log is stored of all activity that occurs inside SaaS Backup for Microsoft 365. The log contains the date of each action performed along with the name of the user who performed the action. You can download the activity log to a .csv file.

Steps

1. Click 

on the left navigation pane.
2. Click the **Activity Log** tab.
A list of all SaaS Backup for Microsoft 365 activity is displayed.
3. Click 

.
The activity log is downloaded as a .csv file.

Download a log of completed jobs

You can download an Excel spreadsheet of successfully completed jobs.

Steps

1. Click **Jobs** from the left navigation pane.
2. Click the recently completed job that you want to download.
3. Click **Successful** under the number of successfully completed jobs.

4. Click **Download** in the top right.
The log is downloaded.

Monitor user data

In SaaS Backup for Microsoft Office 365, you can monitor user data for all services like email or url addresses, mailbox types, license use, discovery state, last discovery, backup status, backup tier, and more.

Steps

1. Click **Services**.
2. Click the service for which you want to export user data.
   a. For Microsoft Exchange Online, click on the number of protected, pending, or unprotected mailboxes.
   b. For Microsoft SharePoint Online, click on the number of protected, pending, or unprotected sites.
   c. For Microsoft OneDrive for Business, click on the number of protected, pending, or unprotected MySites.
   d. For Microsoft Office 365 Groups, click on the number of protected, pending, or unprotected groups.
3. Click **Download** to export an Excel file of user data for the respective service.

Migrate data

To prepare for the end of your license with SaaS Backup for Microsoft 365, you can request data migration from Amazon S3 to tenant-owned Amazon S3 storage or from Microsoft Azure Blob to tenant-owned Microsoft Azure Blob Storage.

Cross migration from Amazon S3 to Microsoft Azure Blob storage or from Microsoft Azure Blob to Amazon S3 storage is not supported.

After data migration completes, you can export your data using the NetApp SaaS Backup Bulk Export Tool. Sign in to the NetApp Support Tools page and search for the NetApp SaaS Backup Bulk Export Tool.

Data migration is an end-of-license activity. All tenants should avoid any form of activity on their SaaS Backup accounts to avoid data and metadata discrepancy during data migration. After data migration completes, all scheduled backups for the tenant will be disabled.

Requirement: To request data migration, log in with tenant account credentials with Global Administrator permissions. Other user roles will not be able to access the Data Migration tab in the user interface.

Recommendation: You should provision the destination storage with sufficient capacity to store all customer data and add 10% more capacity as a buffer for metadata storage.

Steps

1. Go to **Account Settings**  .
2. Select the **Data Migration** tab.
3. In **Storage Details**, enter information into the fields:

Amazon S3	Microsoft Azure
Bucket name	Account name
Region	Container name
Access key	Access point
Secret key	Access key
	Region

Microsoft Azure users must set Public access level to "Blob" for the container provided in Storage Details.

4. Select **Test Connection**.

   A green checkmark indicates the connection is healthy.

5. In **Consent**, select the box to agree to the terms and conditions of data migration, and select **Submit**.

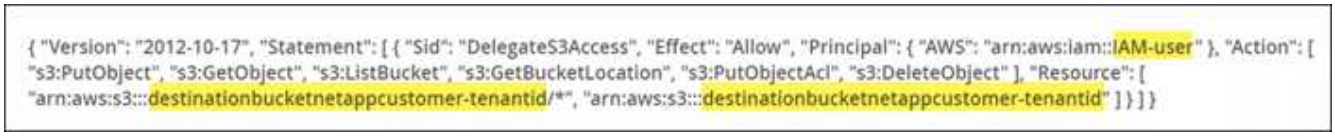
   You have successfully saved the details.
   The tenant ID is now visible in **Migration Status**.

You will need the tenant ID when you export your data using the NetApp SaaS Backup Bulk Export Tool.

Additional steps for SaaS Backup provided Amazon S3 buckets

After you provide consent, Policy and Policy Note now appear below Consent. Follow the next steps to finalize your data migration request.

1. Verify and copy the policy.



2. Go to your Amazon S3 account.
3. Attach the policy provided in **Storage Details** to the Amazon S3 destination bucket.
4. Return to the **Data Migration** tab in **Account Settings** in SaaS Backup for Microsoft 365.
5. In **Policy Confirmation**, select the box to confirm that you have uploaded the policy to the destination bucket, and select **Submit**.
   A green checkmark indicates the data migration request is complete and the data migration is now queued.

Refer to **Migration Status** to monitor the progress of your migration. Migration duration depends on several factors like the amount of data and number of licenses you have.

Provide feedback

Your feedback about the NetApp SaaS Backup for Microsoft 365 product helps us serve you better. You can provide feedback from inside SaaS Backup for Microsoft 365.

Steps

1. Click 

on the left pane navigation.
2. Select **Feedback**.
3. Complete the short feedback survey.
4. Click **Submit**.

If you want to be notified automatically when production-level documentation is released or important changes are made to existing production-level documents, follow Twitter account @NetAppDoc.

Where to get help and find more information

You can get help and find more information in the NetApp SaaS Backup for Microsoft 365 community forum and knowledge base articles.

These resources can be accessed inside SaaS Backup through the **Support** link on the navigation menu.

You can also email the SaaS Backup support team at saasbackupsupport@netapp.com.

Legal notices

Legal notices provide access to copyright statements, trademarks, patents, and more.

Copyright

http://www.netapp.com/us/legal/copyright.aspx

Trademarks

NETAPP, the NETAPP logo, and the marks listed on the NetApp Trademarks page are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.

http://www.netapp.com/us/legal/netapptmlist.aspx

Patents

A current list of NetApp owned patents can be found at:

https://www.netapp.com/us/media/patents-page.pdf

Privacy policy

https://www.netapp.com/us/legal/privacypolicy/index.aspx

Open source

Notice files provide information about third-party copyright and licenses used in NetApp software.

Notice for SaaS Backup

Copyright information

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at http://www.netapp.com/TM are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.