Managing SaaS Backup

SaaS Backup For Office 365

NetApp
March 22, 2021

Table of Contents

Managing SaaS Backup

Managing backups

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

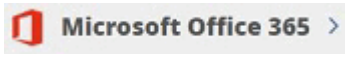
Backup setting	Description	Enabled	Available in…
Include Version History	Enables maintenance of multiple file versions in the backup. This setting only applies to individual files. It does not apply to entire folders, tiers, or services.	By default	• Microsoft SharePoint Online • Microsoft OneDrive for 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

Updating 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**.

Scheduling 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**.

Performing 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

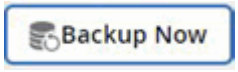
- If you are backing up shared mailboxes, click the **SHARED** tab.
- If you are backing up archive mailboxes, click the **ARCHIVE** tab.
- If you are backing up regular mailboxes, remain on the **USER** tab.

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.

Browsing 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.

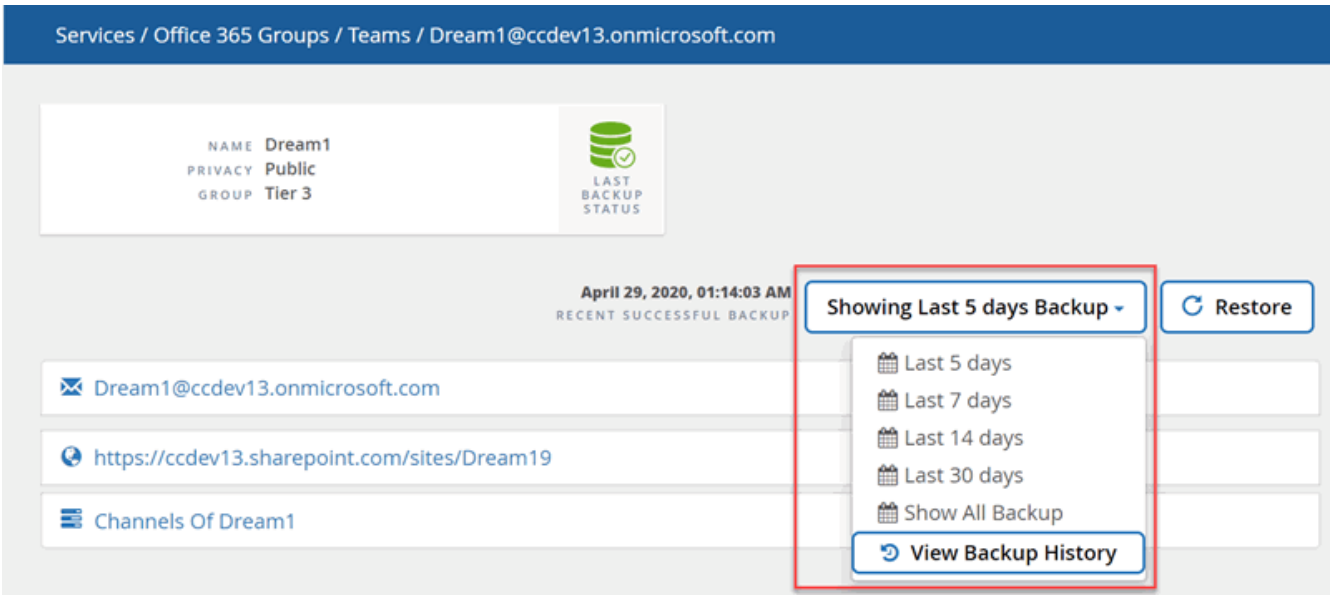
To be sure you find what you are looking for, check the date to the left of the time range dropdown menu.

[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.

Updating 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.

Updating 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**.

Updating 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.

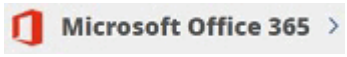
Enabling backups for OneNote

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.

Updating backup settings

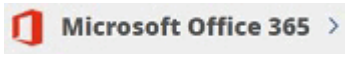
You can update your backup settings to control various backup options. Available backup settings vary based on service.

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 the desired backup settings.
5. Click **Confirm**.

Teams data locations

Data for Microsoft Teams has different locations in SaaS Backup for Microsoft 365.

The table shows you where to locate Teams data in SaaS Backup.

Teams data	Where is it in SaaS Backup?
Teams email	Microsoft 365 Groups > Teams > SampleTeam > Mailbox
Teams channels	Microsoft 365 Groups > Teams > SampleTeam > Channels
Teams Standard Channel Documents	Microsoft 365 Groups > Teams > SampleTeam > SharePoint Site > Documents > SampleTeam-StdChannel
Teams Standard Channel Chat	• Microsoft 365 Groups > Teams > SampleTeam > Mailbox > Conversations > Team Chat • Microsoft 365 Groups > Teams > SampleTeam > Mailbox > Mail > Conversation History > Team Chat (actual location)

Teams data	Where is it in SaaS Backup?
Teams Private Channel Documents	SharePoint > SampleTeam – SampleTeam-PrivChannel > Documents > SampleTeam-PrivChannel  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.
Teams Private Channel Chat	• Exchange > “User in Private Channel” > Mail > Conversations > Team Chat • Exchange > “User in Private Channel” > Mail > Conversation History > Team Chat (actual location)
Individual User Chat and Group Chats	• Exchange > “User” > Mail > Conversations > Team Chat • Exchange > “User” > Mail > Conversation History > Team Chat (actual location)
Files shared in Individual User Chat and Group Chats	OneDrive > “User” > Files > Microsoft Teams Chat Files

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)
- GROUP#0 (Group Site Collection Prefix)
- STS#1 (Blank Site)
- STS#2 (Document Workspace)

- STS#3 (Modern Team Site)
- APP#0 (App Template)

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

Managing restores

Performing 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. You can update your backup settings to maintain a specified number of backed-up versions of individual files. If you have more versions of a file than you have specified for backup, only the number of versions that you have specified is available for restore.

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:
      - 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.

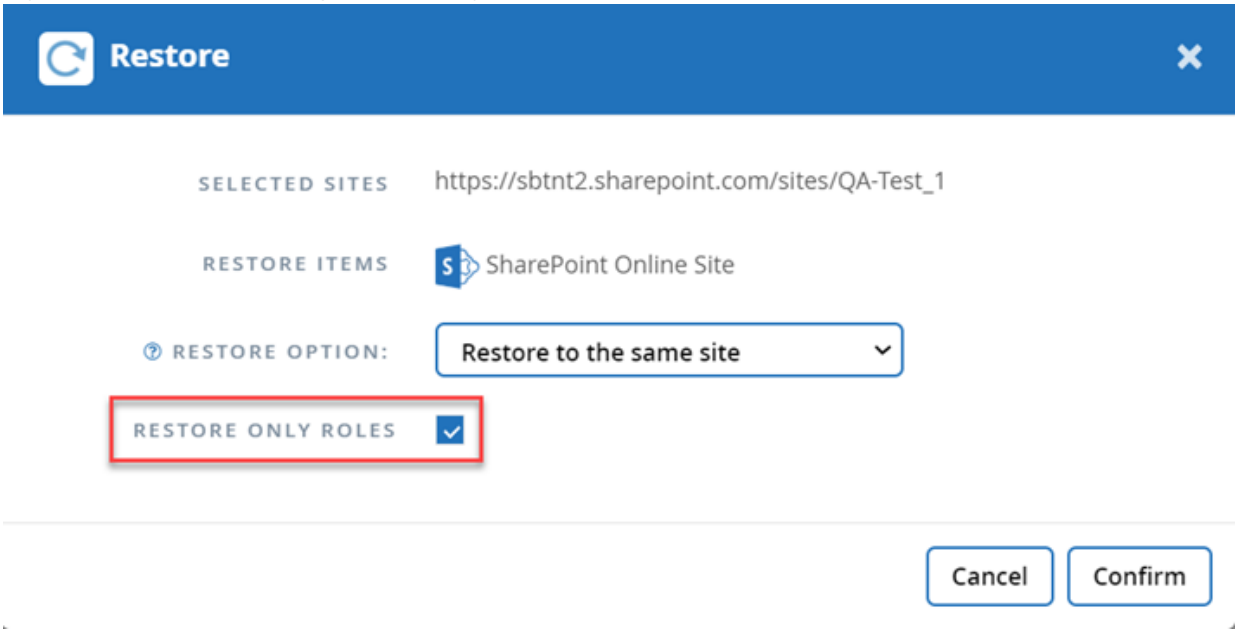
- Export data
  If you export data, you need to download it. Go to Reporting on the left menu. Find your export data job. Click on **Total Folders**. Then click **Export Data Download Link**. A zip file downloads. Open the zip file to extract the data.

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.

Performing a granular-level restore

Performing 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. You can update your backup settings to maintain a specified number of backed-up versions of individual files. If you have more versions of a file than you have specified for backup, only the number of versions that you have specified is available for restore.

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 Group 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 and you cannot replace the existing content. 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** (Available for Microsoft Exchange only)

     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. Note: 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** (Available for Microsoft 365 groups only):

  If you export, a PST file is created with your Microsoft Exchange files and a .zip file is created in 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.

  > If you select the export 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.

Performing 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. You can update your backup settings to maintain a specified number of backed-up versions of individual files. If you have more versions of a file than you have specified for backup, only the number of versions that you have specified is available for restore.

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

Type of item	Restore to the same site	Restore to another site	Export data
Single/multiple items	Yes	Yes	No
Single/multiple files	Yes	Yes	No
Single site	Yes	Yes	Yes
Multiple sites	Yes	Yes	No
Communication sites	No	No	No

Type of item	Restore to the same site	Restore to another site	Export data
Single/multiple subsites	Yes	Yes	Yes
Single/multiple folders	Yes	Yes	Yes
Single/multiple lists	Yes	Yes	Yes
Content	Yes	Yes	Yes
OneNote single/multiple notebooks	Yes	Yes	No
OneNote single/multiple section groups	Yes	Yes	No
OneNote single/multiple sections	Yes	Yes	No
OneNote pages NOTE: Pages within a section restore at the section level.	No	No	No

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.

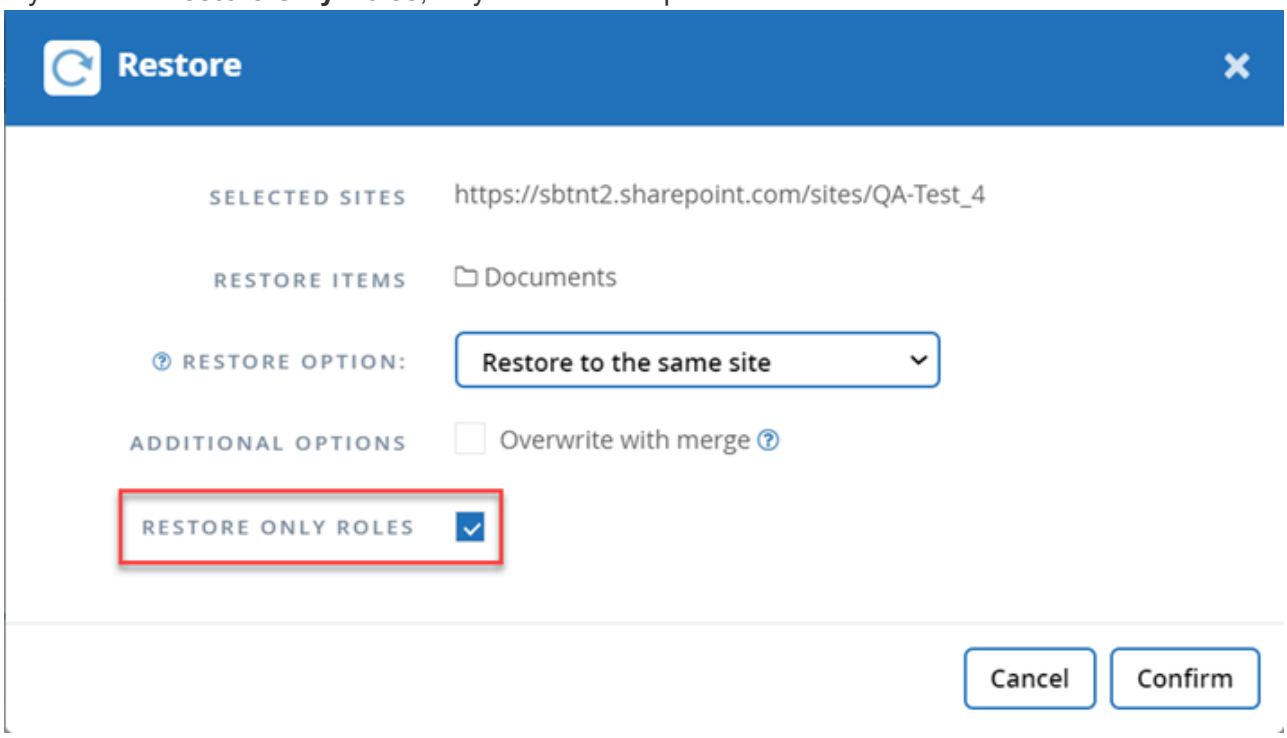
4. To restore from the most recent backup, click **Restore**. To restore a previous version of the item, click **Show versions**, and select the version that you want to restore and then click **Restore**.
5. Select a restore option:

   - **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.

Performing 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. You can update your backup settings to maintain a specified number of backed-up versions of individual files. If you have more versions of a file than you have specified for backup, only the number of versions that you have specified is available for restore.

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
Single drive	Yes	Yes	Yes
Multiple drives	No	No	No
Single/multiple files/items	Yes	Yes	Yes
OneNote single/multiple notebooks	Yes	Yes	No
OneNote single/multiple section groups	Yes	Yes	No
OneNote single/multiple sections	Yes	Yes	No
OneNote pages NOTE: Pages within a section restore at the section level.	No	No	No

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.

Restoring 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.

Locating restored files

When some files or folders are restored, they are contained inside a newly created restore folder. To help you easily identify 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.

Managing permissions

Adding 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.

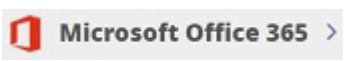
Synchronizing user permissions with Azure Active Directory

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.

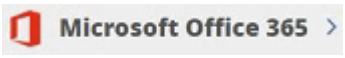
Granting permissions to enable shared mailboxes

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.

Managing licenses

Adding 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  icon in the right corner.
3. Enter the license information.
4. Click **Validate Subscription**.
5. Click **Next**.
6. Click **Save**.

Updating 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  icon 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**.

Releasing 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 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 **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**.

Managing rules

Creating 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.

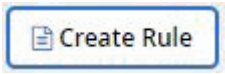
You must apply a user defined filter to your data before you can create a rule. Applied filters are displayed below the **Filter** icon. NetApp SaaS Backup for Microsoft 365 default filters appear in gray. User defined filters appear in light blue.

Creating 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.

Applying 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.

Deleting 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 the trash can  to delete the rule.
   The status of the items to which the rule was previously applies is not changed when the rule is deleted.

Managing services

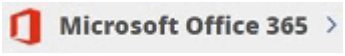
Activating a service

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**.

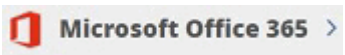
Deactivating a service

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**.

Activating 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**.

Canceling 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**.

Setting 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**.

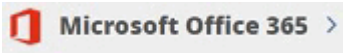
3. Enter the email address of the account you want to receive notifications.
4. Click **Add Notifications**.
   The user is added under the list of accounts for notifications.
5. Select the specific notifications you want the user to receive.
6. Click **Save**.

Discovering 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.

Purging 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.

Managing role-based account access

Assigning 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**.

Updating 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**.

Deleting 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**.

Managing security groups

Adding 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**.

Deleting 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.