IBM Storage Protect for Cloud Microsoft 365

User Guide

Contents

Note:

Before you use this information and the product it supports, read the information in "Notices" on page 294.

Edition Notice (June 2024)

This edition applies to IBM® Storage Protect for Cloud (product number 5900-AP6) all subsequent releases and modifications until otherwise indicated in new editions.

About this publication

This publication provides overview, planning, and user instructions for IBM® Storage Protect for Cloud Microsoft™ 365.

Who should read this publication

This publication is intended for administrators and users who are responsible for implementing a backup and recovery solution with IBM® Storage Protect for Cloud Microsoft™ 365 in one of the supported environments.

System administrators can use this guide to help start the application, manage users, and catalog resource information. Users can find procedures on how to search and browse for objects, generate and interpret reports, schedule jobs, and orchestrate backup and restore jobs.

What's new

Learn about new features and updates in IBM® Storage Protect for Cloud Microsoft™ 365.

Release Date: November 2, 2025

General Updates

You can now prioritize which containers and objects get backed up first. This gives you more control over your backup process, ensuring that your most critical data is always protected without delay.

Power BI restore is now available. You can restore Power BI workspace permissions, reports, and datasets. This feature supports both in-place and out-of-place restoration, with conflict handling and BYOS options.

IBM® Storage Protect for Cloud Microsoft™ 365 now supports custom apps with delegated permissions, including Power Platform and Viva Engage scenarios, across all service types.

SharePoint site, OneDrive, and Group sites can now be restored directly to Microsoft Teams channel sites as destinations, to expand restore flexibility for Teams-centric organizations.

Teams based on the education-specific templates can now be restored with correct metadata and channels, preserving the original structure.

Support for exporting mailbox data from Microsoft Teams is now available. This allows you to export data at the Group mailbox level, as well as from individual mailbox folders and items. Note that exporting Group mailbox data is only available in the Search mode.

About IBM® Storage Protect for Cloud Microsoft™ 365

IBM® Storage Protect for Cloud Microsoft™ 365 is designed to ensure resiliency of service in the event of a disaster and helps to recover lost or corrupted content from your backup. IBM® Storage Protect for Cloud Microsoft™ 365 offers backup capabilities for all Microsoft™ 365 instances, such as **Exchange Online**, **OneDrive**, **SharePoint Online**, Microsoft™ **365 Groups**, **Teams**, **Microsoft Teams Chat**, **Project Online**, **Public Folders**, **Viva Engage**, **Power BI**, **Power Automate**, and **Power apps** to protect your data. These object types are backed up and restored independently of one another.

The date format displayed in the interface and job reports follows the **Culture settings** in IBM® Storage Protect for Cloud.

You can also customize the view of the **Backup** or **Restore** page to hide or show the workspace of each service and change their display order by drag & drop.

In the IBM® Storage Protect for Cloud Microsoft™ 365 interface, the following actions are available on each page:

- The **Notification center** (🔔) displays alerts for subscription expiration, out-of-policy conditions, and changes to BYOS.
- With **Quick check** (⚡), you can review the backup configurations on app profiles, scan profiles and service accounts, and take the necessary actions as soon as possible to ensure your data is properly protected. To refresh the configuration information, click **Refresh**.

The **Help & Resources** section on the left navigation pane contains the user guide and release notes links to help you catch up with what’s new and direct you to the IBM® Storage Protect for Cloud interface to submit feedback.

Single Sign-On

With Single Sign-On (SSO) supported, you can access IBM® Storage Protect for Cloud Microsoft™ 365 interface via direct URL without providing user credentials once it is detected that you have signed into the IBM® Storage Protect for Cloud interface.

Supported Languages

IBM® Storage Protect for Cloud Microsoft™ 365 interface supports being browsed in French or German if the default language or the first preferred language of the browser you are using is French or German.

SharePoint Online, OneDrive, and Project Online:

- The hidden lists in SharePoint sites (including SharePoint Online sites, Teams team sites, Group team sites, Viva Engage community sites, and Project Online sites) are now excluded from the backup scope for better performance. If you want to include the hidden lists in your backup, contact IBM Software Support for assistance. For the hidden lists that you can include in the backup, refer to “Hidden Lists” on page 199.
- You can change the SharePoint domain name for your organization in Microsoft™ 365 as introduced in the Microsoft™ article: Rename your SharePoint domain. This feature affects only the SharePoint and OneDrive URLs. It doesn’t impact email addresses. After the domain name is changed and updated into Auto Discovery, IBM® Storage Protect for Cloud Microsoft™ 365 will run a full backup for SharePoint Online sites and OneDrive objects with new URLs.
- IBM® Storage Protect for Cloud Microsoft™ 365 for OneDrive will protect the **Documents** library and will protect the **Site Assets** library as well if the site feature **Site NoteBook** is activated.
  The service only protects content and permissions for OneDrive since OneDrive is the cloud service used to help securely store, share, and access your files.
- As Microsoft™ API has a 2 GB file size limit of OneNote notebooks saved in One Drive or SharePoint, backup jobs will skip the OneNote files that are larger than 2 GB. In addition, due to API limitations,IBM® Storage Protect for Cloud Microsoft™ 365 cannot protect the history versions of OneNote files.

- If there are security changes but no changes on the content in the sites, the scheduled incremental backup jobs will not back up the securities. Moving forward, the changes on the securities in the sites (including the SharePoint Online sites, OneDrive, and Microsoft™ 365 Groups/Teams team sites) that have not yet been backed up, in this case, will be included in an incremental backup once a week.
  If some items in a site encounter errros in a backup but there are no changes on the content in the site for the next backup, the scheduled incremental backup jobs will not back up these items with errors. Moving forward, they will be included in an incremental backup once a week.

- If you would like to filter the folders to protect a **OneDrive** service or **Exchange Online** service, or filter the folders or lists/libraries within the site collections of **SharePoint Online** service, **Project Online** services, Microsoft™ **365 Groups** services, or **Teams** service, you can contact the IBM Software Support team for assistance. Note that if your subscription to IBM® Storage Protect for Cloud Microsoft™ 365 is based on the protected data size, the total consumed data size in your subscription will not be affected by the filter policy. IBM will not exclude the size of the filtered items from the total consumed data size.

- The files in the SharePoint site and the mailbox items in Exchange Online that are applied with the labels created via **AIP (Azure Information Protection)** can be protected by IBM® Storage Protect for Cloud, as well as the applied Label. The documents applied with the sensitivity labels of DKE (Double Key Encryption) are also supported, but only the user who has permission can access them.

- The files in the SharePoint site and the mailbox items in Exchange Online that are applied with the labels created via **AIP (Azure Information Protection)** can be protected by IBM® Storage Protect for Cloud Microsoft™ 365, as well as the applied Label. The documents applied with the sensitivity labels of DKE (Double Key Encryption) are also supported, but only the user who has permission can access them.

- By default, the **Preservation Hold** library is not protected by IBM® Storage Protect for Cloud Microsoft™ 365. If you want to enable this protection, contact IBM Software Support support for assistance.

- IBM® Storage Protect for Cloud Auto discovery now supports including orphaned OneDrive in scan profiles of OneDrive, but the objects cannot be synchronized to IBM® Storage Protect for Cloud Microsoft™ 365.

- IBM® Storage Protect for Cloud Microsoft™ 365 for SharePoint Online also supports protecting **Communication Sites**. When restoring a deleted Communication Site to its original location, IBM® Storage Protect for Cloud Microsoft™ 365 supports restoring the custom design of the Communication Site in the backup. If the Communication Site is registered through App Profile, the Communication Site can only be restored with the default design. Note that the comments in Communication Sites are not currently supported.

- As the locked site collections are inaccessible, the backup job will check the lock status and skip backing up the locked site collections, which will be recorded in the job report; for read-only site collections, only the full backup job that runs once every year will back them up. Since no changes can be made to read-only site collections, the incremental backup jobs will skip them.

- You can now use an app profile to scan the Project Online site collections. However, Project Online data cannot be protected in the app context (using app profile authentication). A service account with enough permissions is still required for the backup and restore for Project Online. Note the following for the Project Online data types:
  - IBM® Storage Protect for Cloud for Project Online service supports restoring **Project Permission Mode** features.
  - Project Online service cannot protect the **Project for the web** data and cannot fully support the data added through Microsoft 365 subscription Project Online desktop client. For example, custom fields.
  - For additional details on the protected data types, refer to "Project Online Data Types" on page 202.

Exchange Online and Public Folders:

- You can now choose to protect the **Recoverable Items** folder in the user's primary mailbox for the Exchange Online service. If you want to enable this feature, contact IBM Software Support support for assistance. Note that an additional cost is required. Currently, we support the **Deletion**, **Purges**, **Versions** , and **Discovery Holds** subfolders in the **Recoverable Items**. For more information about Recoverable Items, refer to this Microsoft article: Recoverable Items folder in Exchange Online. On the backup data tree, you can find the data in the following directory: `mailbox address/Recoverable Items folder (System)`. This folder cannot be a destination for an out of place restore, and the backup data of this folder being restored to its original mailbox will use the following name: **Recovery Items folder (System) _**

Restored. Note that due to the API limitation, this folder directory will always be displayed in English regardless of the preferred display language of Microsoft 365.

- The hidden folders in the mailboxes (including Exchange Online mailboxes, Group mailboxes, and Teams group mailboxes) will be excluded from the backup for better performance. If you want to include the hidden folders in your backup, contact IBM Software Support for assistance.
- If you would like to filter the folders to protect a **OneDrive** service or **Exchange Online** service, or filter the folders or lists/libraries within the site collections of **SharePoint Online** service, **Project Online** services, Microsoft™ **365 Groups** services, or **Teams** service, you can contact the IBM Software Support team for assistance. Note that if your subscription to IBM® Storage Protect for Cloud Microsoft™ 365 is based on the protected data size, the total consumed data size in your subscription will not be affected by the filter policy. IBM will not exclude the size of the filtered items from the total consumed data size.
- The service for **Public Folders** only supports restoring content and permissions of Public Folders to the original location. IBM® Storage Protect for Cloud Microsoft™ 365 now supports the backup of Public Folder metadata via app profile authentication. To protect Public Folder metadata, ensure your backup for Public Folder metadata is enabled and the Exchange Administrator role is assigned to the app in Microsoft Entra ID. Note that the impersonation accounts that you configured for Public Folders in IBM® Storage Protect for Cloud interface will be synchronized to IBM® Storage Protect for Cloud Microsoft™ 365 after July 2023 release and the IBM® Storage Protect for Cloud in app context only supports using impersonation accounts for the backup and restore of Public Folders. If you are a new customer, you must navigate to the **Settings** > **Backup** page to configure impersonation accounts. For details, refer to "Configure Backup Settings" on page 87 .
- For subscriptions with Multi-Geo enabled, the public folders can only be protected in the Central IBM® Storage Protect for Cloud Location.
- Use Object ID instead of mailbox address as the unique identifier for Exchange Online mailboxes and Public Folders. This change has been made to IBM® Storage Protect for Cloud Microsoft™ 365. Due to this change, the mailboxes that have been re-created with the same address will no longer be regarded as the same one. This might require a broader search to ensure you find all the backup data for restoring, exporting, or deleting; the mailbox being renamed can only be found by the new name with the former backup data associated, and its former name will be displayed in its row.
- The Exchange Online service does not support protecting the **Search Folders**.

Microsoft™ 365 Groups and Teams

- The Teams service is now available for customers using Microsoft 365 operated by 21Vianet in China. Note that hosted content is unsupported and will be skipped in the backup
- To protect Teams mailboxes, at least one owner/member in the team should have the Exchange Online product license.
- The hidden folders in the mailboxes (including Exchange Online mailboxes, Group mailboxes, and Teams group mailboxes) will be excluded from the backup for better performance. If you want to include the hidden folders in your backup, contact IBM Software Support for assistance.
- IBM® Storage Protect for Cloud Microsoft™ 365 can now check the status of groups and teams in Microsoft™ 365 and provides the option to help you restore the soft-deleted groups and teams (within the 30-day retention period) from the Microsoft™ 365 recycle bin.
- If you are using service account authentication for the backup of Teams' shared/private channels, the service account must be the owner of the shared/private channels.

Teams Chat

- The Teams Chat service can protect the 1:1 chats and the group chats in Teams.
- Before you enable the Teams chat backup service, you must register a **custom app profile** for Microsoft 365 for Auto Discovery to scan the **Microsoft 365 users** request access to the default Microsoft Graph API or Microsoft Graph Teams Export API. To request access to Export APIs, read the Prerequisites and complete the request form. For details on the required permissions for custom app, refer to "App Profile Authentication" on page 57.
- Microsoft Teams Chat service in IBM® Storage Protect for Cloud Microsoft™ 365 supports to use the **default Microsoft Graph API** or **Microsoft Graph Teams Export API model B** to retrieve Teams chat messages

from Microsoft Teams Chat for backup. Note that the Export API model B will charge the app creator $ 0.00075 per message and that the cost may be high if there are a large number of chat messages in your tenant. Since the **Teams Export API model B** requires payment for use, you must follow the steps described in Enable metered Microsoft 365 APIs and services to set up an active Azure subscription for your application for billing purposes. You can follow this Microsoft article to estimate the number of Teams chat messages that may be backed up.

> **Note:** The number of messages in the Microsoft 365 Admin Center is just for the specific duration you define when exporting the report, not the full total amount. Additionally, the Microsoft Export API only supports export at a user level, so if there is a group chat with multiple users, the same message will be exported multiple times if all these users are included in the scope, which means the number of messages which will be backed up by IBM® Storage Protect for Cloud Microsoft™ 365 has the potential to be higher than the number of messages in the Microsoft admin center report. For confirmation, you can check the job report after the job has finished for the backup chat messages count to compare with the bill from Microsoft. If necessary, you can also limit the user scope for the export. Here is an example: In the report in the Microsoft 365 admin center shows the last 180 days' number of Teams chat messages are 1000. Then for the whole year, the number of messages will be approximately 2000. Because there is no deduplication logic for the Microsoft 365 export API, the same message will be exported multiple times if all these users are included in the scope. So let's say that all are 1V1 chats, then the message number charge by export API will be doubled to approximately 4000 messages. If most of chats are group chats with multiple users, the cost will be even higher.

- For the **default Microsoft Graph API**, the backup of chats started by external users is not supported, but chats started by internal users that include external users can be protected. For the **Teams Export API model B**, only plain text can be protected.
- The group chat messages cannot be protected if the user has been removed from the group.
- Only the default Microsoft Graph API can be used to protect Teams Chat in GCC environments.

Viva Engage

- To protect Viva Engage data, you must have a Viva Engage app or a custom Azure app with delegated permissions connected to your tenant. The authentication user of this Viva Engage app must have the **Verified Admin** role and the **Yammer administrator** role with the Via Engage product license. For details on configuring a Viva Engage app, refer to App Profile for Yammer. Viva Engage service currently supports in place restore only (restoring to the original location), meaning the Viva Engage community needs to already be there, as well as the ability to export files and conversations.
- If you have Microsoft™ 365 connected Viva Engage communities protected under Microsoft™ 365 Groups service, once the Viva Engage service is enabled, the connected groups will be removed from Microsoft™ 365 Groups service and can only be protected in Viva Engage even if you disable the Viva Engage service again. IBM® Storage Protect for Cloud Microsoft™ 365 job will start a new backup cycle for these Viva Engage communities, but their former backup data as Microsoft™ Groups will not be deleted until the data retention period expires.

Power BI

- Power BI service can only protect the Power BI content in the new workspace experience. (The personal workspace is the classic workspace, which is not supported.)
- To use IBM® Storage Protect for Cloud Microsoft™ 365 to protect the Power BI data, you must configure an app profile for the Microsoft Delegated app with the Power BI option selected or a custom Azure app with delegated permissions. For the list of the required permissions added to the Delegated app for Power BI, refer to "App Profile Authentication" on page 57. If you have been using a scan profile with service account authentication for Power Platform object types, the Auto discovery scan jobs and the IBM® Storage Protect for Cloud jobs can continue using the service account authentication.
- If you use service account authentication or the Delegated app to protect the Power BI data, the service account or the authentication user of the Delegated app must have a **Power BI Pro** license or a **Premium Per User (PPU)** license, and have the **Fabric Administrator** role (the former **Power BI admin** role).

- Before you enable the Power BI service, ensure the Download reports feature in the tenant settings has been enabled. This feature was enabled by default. In addition, IBM® Storage Protect for Cloud Microsoft™ 365 Power BI service now can only protect the .pbix Power BI files that can be downloaded. Note that the backup data can only be exported and downloaded. For the limitations on downloading report from Power BI, refer to Limitations when downloading a report .pbix file. The exported .pbix file includes both the report you're downloading and the dataset (the data on which the report is based), the same as the "A copy of the report and data" download mode in Power BI. If a Power BI report is created using data from Dataverse, neither the report nor the data in Dataverse will be protected.
- If you use the service account authentication to protect Power BI data or use the Delegated app to scan Power BI workspaces in IBM® Storage Protect for Cloud Microsoft™ 365, the Auto Discovery scan job will automatically add the service account or the authentication user of the Delegated app as the workspace admin.
- Due to the API limitation, the backup job of Power BI can back up at most 200 workspaces per hour.
- Power BI service can now protect Power BI reports larger than 1 GB in the small semantic model storage format.

Power Automate

- Power Automate service can only protect the cloud flows.
- To use IBM® Storage Protect for Cloud Microsoft™ 365 to protect the Power Automate flow data, you must configure a Microsoft Delegated app or a custom Azure app with delegated permissions. For the list of the required permissions added to the Delegated app for Power Automate, refer to the Required Permissions of Microsoft Delegated App. If you have been using a scan profile with service account authentication for Power Platform object types, the Auto discovery scan jobs and the IBM® Storage Protect for Cloud jobs can continue using the service account authentication.
- If you use the Delegated app to protect the Power Automate data, the authentication user of the Delegated app must be the **Global Administrator** and the Environment admin or System Administrator. If you use service account authentication to protect the Power Automate data, the service account must be the **Global Administrator**.
- The backup job will automatically add the service account or the authentication user of the Delegated app (the user who consents the app permissions) as the flow owner. Due to the Microsoft native logic, after the authentication user is added as the flow owner, the corresponding flows will be listed under the **My flows** > **Shared with me** tab for the existing flow owners.

Power Apps

- Power Apps service can only protect standard Canvas apps which have been published and the component libraries. Note that the Restore action is unsupported and the backup data can only be exported. For a full support list, refer to Power Apps Data Types.
- To use IBM® Storage Protect for Cloud Microsoft™ 365 to protect the Power Apps data, you must configure an app profile for the Microsoft Delegated app with the Power Apps option selected or a custom Azure app with delegated permissions. For the list of the required permissions added to the Delegated app for Power Apps, refer to the Required Permissions of Microsoft Delegated App. If you have been using a scan profile with service account authentication for Power Platform object types, the Auto discovery scan jobs and the IBM® Storage Protect for Cloud jobs can continue using the service account authentication.
- If you use service account authentication or the Delegated app to protect the Power Apps data, the service account or the authentication user of the Delegated app must be the **Global Administrator** and the **Environment Admin/System Administrator**, and have the **Power Apps for Microsoft 365** license to proceed.
- The backup job will automatically add the service account or the authentication user of the Delegated app as the app's co-owner and flow owner (if the app has an associated flow).

For more information on the supported and unsupported data types of Microsoft 365 Backup, refer to:

- "SharePoint Sites Data Types" on page 181
- "Modern Team Site Data Types" on page 200
- "Project Online Data Types" on page 202

- “Exchange Online Data Types” on page 216
- “Public Folders Data Types” on page 222
- “Microsoft 365 Groups Data Types” on page 225
- “Teams Data Types” on page 229
- “Teams Chat Data Types” on page 242
- “Viva Engage Data Types” on page 244
- “OneDrive Data Types” on page 247
- “Document-Related Data Types” on page 249
- “Power BI Data Types” on page 262
- “Power Automate Data Types” on page 262
- “Power Apps Data Types” on page 263

Backup Schedule

The backup service will perform scheduled backups automatically and compress and encrypt backup data by default. The schedule of an object type starts with the first backup job. Note that the first backup job of the Distribution MSP’s customers will start in 24 hours after the backup wizard is set up.

For new customers, IBM has now adjusted the backup frequency to once a day by default. Your second scheduled backup job on the next day will run ten hours after the start time of the first backup job, to ensure your backups all run at night for the best throughput. The subsequent jobs inherit the schedule automatically. In the meantime, you still have the option to adjust the backup frequency and the start time for the backup jobs.

> **Note:** IBM cannot guarantee the completion of four backups per day, even if the backup frequency is set to four times daily. Various factors, such as data size, can impact job performance and are beyond our control. If a scheduled backup is due to start but the previous one is still in progress, the new backup job will be skipped.

Backup jobs can also be run manually if some items encounter errors during the last backup job. For detailed instructions on manually running backup jobs, refer to “Monitor and Manage Your Backup” on page 67.

Storage Location

You can choose to store the backup data to the default storage location provided by IBM® Storage Protect for Cloud or your custom storage location. If you are currently using the default storage location and you want to use your own storage afterward, you can contact IBM® Software Support to update your subscription and change the default storage to your own storage.
The storage type of the default storage location is Microsoft™ Azure Blob Storage. The custom storage location can be one of the following nine storage types: **Amazon S3**, **Amazon S3-Compatible**, **Dropbox**, **FTP**, Microsoft™ **Azure Blob Storage**, **SFTP**, **IBM® Storage Protect - S3**, **IBM® Cloud Object Storage**, and **Google Cloud Storage**.

If you have purchased a subscription for BYOS (Bring your own storage) but are currently using IBM® Storage Protect for Cloud default storage for your backup data, your backup jobs will fail and we will send you an email notification every 7 days to remind you to update your BYOS storage configuration.

If you are using your own Azure storage (BYOS), note the following:

- Existing BYOS customers applying immutability policies to Azure blob storage, should note the following:
  - **Backup job behavior**: The first backup job executed after applying an immutability policy will fail. However, subsequent backup jobs will process your data within the defined backup scope.
  - **Data deletion restriction**: If immutability polices are active on your Azure blob storage, all data deletion operations, including unprotected data removal, data retention, manual deletion, and Data Subject Access Requests (DSARs) will be blocked. Data governed by these polices will remain immutable and cannot be altered or deleted unless the policies are modified.
- After the January 2024 release, IBM® Storage Protect for Cloud will write your new backup data to the cold tier by default to reduce storage costs. The supported Azure account kinds are **StorageV2** and **BlobStorage**

of **Standard** performance type. For existing customers, your former backup data are still stored in the cool tier. This intelligent tiering also extends to additional BYOS storages appended to the system.

For details about blob access tiers and how to change access tiers, refer to the Microsoft™ article: Azure Blob storage: hot, cool, and archive access tiers.

If you are using your own Microsoft Azure Blob Storage and facing the upper limit on your storage account, you can append a new Microsoft Azure Blob storage account. The maximum storage account capacity for a standard storage account is 5 PiB. You can contact Microsoft Azure support to request an increase. Currently, you can only append one additional storage account, and this is only available for BYOS customers on Azure.

The backup data will be purged from the storage after the data reaches the retention period. If you use the default storage location, you can purchase a subscription with a retention period of multiple years (between 1 and 99) or unlimited years.

You can restore the backup data of these object types to the original location where they are backed up, to another destination, or restore them to a custom storage location. For details, refer to Restore Options for Different Object Types and “Restore and Recover Your Data” on page 110.

Retention

If you use your own storage device or IBM default storage, you can customize the data retention period for each service type. Note that the Teams Chat service does not support the retention policy and all backup data of Teams Chat will be retained until the subscription expires. To enable the day unit retention policy, contact IBM Software Support for assistance.

Before any data deletion, IBM® Storage Protect for Cloud Microsoft™ 365 will send a notification email informing you of the service data which will be deleted. You will still have time to either extend your retention period or export your data (a paid service).

Other than Power Apps and Power Automate, you can choose to customize the retention settings at container level. You can now configure a retention period that is less than 1 year (from 30 days to 365 days) for services and containers.

Report Center

By monitoring the subscription consumptions and jobs operations, your application administrator can have an overall understanding of the resource usage, review and analyze the job progress and details, and predict the service usage trends for the unusual activities.

For details, you can refer to:

- “Monitor Subscription Consumption” on page 156
- “View Storage Consumption Report” on page 148
- “Use the Job Analytics Report” on page 149
- “Use the Unusual Activities Analysis Report” on page 150
- “View the End-User Restore Report” on page 151
- “View the Coverage Report” on page 151

Use Public APIs

You can now use the IBM® Storage Protect for Cloud Microsoft™ 365 Public APIs to get the audit records, subscription consumption, job information, and basic of unusual activities detected by IBM® Storage Protect for Cloud Microsoft™ 365. For details, refer to Use Public APIs.

Multi-Geo Support

IBM® Storage Protect for Cloud Microsoft™ 365 supports protecting your Microsoft™ 365 tenant that has the Multi-Geo capability.

Example

For details on how it should be configured through the IBM® Storage Protect for Cloud platform and how it is protected in the IBM® Storage Protect for Cloud Microsoft™ 365 app, refer to Does IBM Storage Protect for Cloud Support Microsoft 365 Tenants with Multi-Geo Licenses?.

To leverage Multi-Geo capabilities, you must navigate to Manage Data Center Mappings in IBM® Storage Protect for Cloud to map the list of geo locations to the supporting data centers.

Once you turn Multi-Geo on in your tenant, we're going to start routing your data to different regions according to your configurations in Manage Data Center Mappings. To run backup and restore for a specific region, you must have the service administrator role or have access to manage that corresponding region.

Users assigned with multiple regions will be asked to select a region when accessing the IBM® Storage Protect for Cloud Microsoft™ 365 interface. Users with only one region will be automatically redirected to the regional IBM® Storage Protect for Cloud Microsoft™ 365 instance.

Note the following:

- Mailboxes – The first time you start the Multi-Geo service, user mailboxes will be moved to the new region automatically, but the backup data previously generated by IBM® Storage Protect for Cloud Microsoft™ 365 will still be managed in either the central tenant or the region where it was moved from. The mailbox will be registered as new through IBM® Storage Protect for Cloud Auto Discovery and get protected by IBM® Storage Protect for Cloud Microsoft™ 365. This means, in the IBM® Storage Protect for Cloud Microsoft™ 365 instance for the new region, the new backup data is isolated exclusively to this region, and the previous backup data cannot be used for the data recovery in the new region. However, you can still use the previous backup data in the following ways:
    - Run an export job through the Restore wizard
    - Restore to your own storage location (BYOS subscription)
    - Restore to another mailbox in its original region
    - Run an in-place restore to restore backup data to the original region

    > **Note:** To in-place restore the backup data to its original region, ensure there is a service account or app profile configured with proper permissions for the same Microsoft™ 365 tenant as the original data.

- OneDrive/SharePoint sites – If the OneDrive library or SharePoint site existed before your tenant enabled Multi-Geo, the OneDrive library/SharePoint site data will not be automatically moved to the preferred data location. Your SharePoint Administrator or Global Administrator can respond to the move. As stated in the Microsoft™ article: Move a SharePoint site to a different geo location, there is a read-only window during the OneDrive/SharePoint site geo move of approximately 4-6 hours, depending on site contents. During the move, the OneDrive library/SharePoint site will continue being protected in the IBM® Storage Protect for Cloud Microsoft™ 365 instance for the former region. After the move is completed and the site is registered as new through IBM® Storage Protect for Cloud Auto Discovery, the site will be protected in the IBM® Storage Protect for Cloud Microsoft™ 365 instance for the destination region. The previous backup data is not available for the data recovery in the new instance.
- Microsoft™ 365 Groups and Teams – If you are using a multi-geo tenant, ensure the app profile has an Exchange Administrator role. The role is required to restore the region information for Microsoft™ 365 Groups and Teams. Otherwise, your group or team backed up from a specific region will be restored to the default region. For details on how to assign the role to an app, refer to How to Assign the Exchange Administrator Role to an App.
- Power Platform – For subscriptions with Multi-Geo enabled, Power BI data can be protected in multiple geo locations. For Power Automate and Power Apps, flows and apps can only be protected in the IBM Central Location due to API limitations.
- We isolate the backup data sets for each region. Therefore, you cannot restore across different regions. For example, from France to the US.
- If you are using default IBM® Storage Protect for Cloud storage with a Multi-Geo subscription, IBM® Storage Protect for Cloud Microsoft™ 365 allows you to change the storage to your own storage device for specific regions, and the other regions can still use the default IBM® Storage Protect for Cloud storage.

- The subscription consumption report in **Subscriptions** is only available to the IBM® Storage Protect for Cloud administrator.
- The **System Auditor** report and **Job Analytics** report only show the jobs and activities that are operated in the current region.
- The **Remove Unprotected Data** feature is not applicable to subscriptions with the Multi-Geo enabled. Your backup data cannot be automatically detected to determine if it is in or out of the protection scope.
- The retention configuration for multi-geo tenants is the same as the others. If you want to configure custom retention settings, such as setting up different retention years for specific regions, service types, or containers, refer to “Configure Retention Policy” on page 90.

Recovery Portal for End Users

IBM® Storage Protect for Cloud Recovery Portal is a data recovery center designed to connect end users in your organization to their lost OneDrive, SharePoint Online site, Exchange mailbox, or Teams Chat, the files in the Microsoft 365 Groups or the Teams where they are working as owners or members, or Power BI reports in workspaces where they are working as admins, members or contributors. This interface allows users to search the most common fields to find the backup data to recover along with a preview of the email messages which can also help ensure a successful restore with minimal effort.

You can find this app through **IBM® Storage Protect for Cloud › All Apps** view. For end-user access, IBM recommends adding this portal as a custom tile to your organization’s Microsoft 365 app launcher.

Before your end users can use this portal, your service administrator must complete a few necessary configurations. For details, refer to the Recovery Portal User Guide.

Split-Off and Pause Backups

If an incremental backup job for **SharePoint Online**/**OneDrive**/**Project Online**/**Exchange Online**/**Teams**/**Groups** has been running for 47 hours, we will look into it and identify if there is a higher volume of changes or very large sites/mailboxes that are causing the job to run longer. Rather than let these large sites/mailboxes slow down the rest of your backups, we will split off the running sites/mailboxes into their own backup process, which will continue to run in the background. Long-running full backup jobs for will not be automatically split off and the incremental backup jobs will run in parallel. For any content we’ve already finished protecting, we’ll mark this job as “**Partially Finished**” in the backup dashboard to set a valid restore point. Any sites/mailboxes that are still in the queue to be backed up will be skipped and will be automatically included in the next backup, which should be kicking off shortly to maintain the best SLA.

The site collections/mailboxes that are currently being backed up will keep running in the background.

For **Teams/Groups** long-running backups, the split-off will happen when all the following conditions are met.

- The backups for the Teams/Groups metadata, mailboxes, and private sites (for Teams) have been completed.
- The backups for Teams/Groups team sites are still running.
- The incremental backup job has been running for 47 hours (subject to the duration you may have customized).

You can download the job report from Job Monitor to check the backup of the site collections/mailboxes that are currently being protected and the site collections/mailboxes that have been skipped but will be automatically included in the next backup job.

For SharePoint Online sites and Exchange Online mailboxes, you can also navigate to the **Job Analytics** › **Backup Overview** tab to check for the progress of the content being protected. Note that Project Online and Teams service do not support this feature.

If the backup job hasn’t been completed after running for a total 28 days, it will be stopped. The remaining content in the backup will be automatically included in the next backup job. Note that the job pausing does not apply to Exchange Online backups. The Exchange Online backup job will run to the end. You will receive the following email notifications to check the job details:

- IBM® Storage Protect for Cloud Notification: Managing Long-Running Backup Jobs
- Your Long-Running Backup Job Has Completed!

Data Encryption Methods

Data encryption can be divided into two scenarios: data transmission (data in transit) encryption and data storage (data at rest) encryption.

For data transmission encryption, IBM® Storage Protect for Cloud Microsoft™ 365 is deployed on the Microsoft™ Azure framework to make outbound Microsoft™ API calls and internal communications over HTTPS/TLS encrypted channels. Certificate-based authentication is used for internal communications.

For data storage encryption, IBM® Storage Protect for Cloud Microsoft™ 365 encrypts all the Microsoft™ 365 data obtained by calling Microsoft™ APIs with AES 256 using keys unique to each tenant (either default keys or BYOK). The encryption happens before the data is transmitted to storage.

When transmitting the encrypted data to storage, the data transmission encryption differs depending on the target storage's available protocols. For example, Microsoft™ Azure Blob Storage, Amazon S3, and SFTP have their own data transmission encryption algorithm or protocols applied, but for FTP, the data transfer protocol is not encrypted. Although the data being transferred is already encrypted with AES 256, as mentioned above, the preferred method is to use storage types other than FTP that support encrypted protocols.

List of On-Demand Features

IBM® Storage Protect for Cloud Microsoft™ 365 has several features to be delivered or enabled on your demand.

You can contact the IBM Software Support team if you are interested in the following features:

- IBM® Storage Protect for Cloud Microsoft™ 365 new experience removed several backup settings that are not popular in use. For details, refer to "On-Demand Backup Settings" on page 89. If you want to use these settings, contact IBM Software Support.

- To avoid any accidental deletion of your backup data, you can contact IBM Software Support to disable the GDPR-related features (the Data Subject Access Requests function and the Manually Delete Backup Data function) for your tenant.

- By default, successful granular level items will not be included in the job report, except for top-level objects. If you want to view the successful items in the job report, contact IBM Software Support for assistance.

- If you would like to filter the folders to protect the **OneDrive** service or **Exchange Online** service or filter the folders or lists/libraries within the site collections of the **SharePoint Online** service, **Project Online** services, **Microsoft™ 365 Groups** services, or **Teams** service, you can contact the IBM Software Support team for assistance. Note that if your subscription to IBM® Storage Protect for Cloud Microsoft™ 365 is based on the protected data size, the total consumed data size in your subscription will not be affected by the filter policy. IBM will not exclude the size of the filtered items from the total consumed data size.

- If you want to exclude specific file types from backup by filtering file extensions (such as, to exclude the MP4 files from backup), you can contact IBM® Storage Protect for Cloud support for assistance. This feature works for the backup of SharePoint Online sites, OneDrive, Project Online sites, and the sites of Microsoft 365 Groups, Teams, and Viva Engage communities. The files, including the documents in the list attachment with the designated file extension, will be excluded from the backup. Note that this filter is not applicable to system files.

- If you would like to exclude the workflow history list as well as the list items from your backup for better backup job efficiency, contact the IBM Software Support team for assistance.

- For BYOS customers, if you would like to use a separate storage location for each service type, contact the IBM Software Support team for assistance.

- The **Export Encryption Key** feature is by default not available to users who are using default storage hosted by IBM® Storage Protect for Cloud. You can contact the IBM Software Support if needed. For details on exporting encryption keys, refer to "Configure Security Settings" on page 94.

- By default, the HSM restore method using Migration API is enabled to improve the speed of large-scale recoveries. The High-Speed Migration (HSM) restore method supports SharePoint Online, OneDrive, Project Online, Microsoft 365 Groups, Teams, and Viva Engage in both app profile authentication and service account authentication, and HSM restore jobs can support restoring content larger than 15 GB. For details, refer to HSM Restore Method. If you want to disable the HSM restore method, contact IBM Software Support.

- By default, the restore job will restore the Planner task's attachment link to the target. If you want to restore the latest files in the attachment of the Planner tasks, contact the IBM Software Support team for assistance.
- Remove Unprotected Data – If you are a BYOS customer and are looking to save storage space by removing unprotected data, contact the IBM Software Support team to enable this feature for your environment. For additional details, refer to "Remove Unprotected Data" on page 146.
- The Storage Consumption report displays the backup data size in storage, its growth, and trends to help administrators to monitor and manage the storage consumption. By default, this report is not available. If you want to enable this report, contact the IBM Software Support team. For details, refer to "View Storage Consumption Report" on page 148.
- The hidden lists in SharePoint sites (including SharePoint Online sites, Teams team sites, Group team sites, Viva Engage community sites, and Project Online sites) are now excluded from the backup scope for better performance. If you want to include the hidden lists in your backup, contact IBM Software Support for assistance.
- The hidden folders in the mailboxes (including Exchange Online mailboxes, Group mailboxes, and Teams group mailboxes) will be excluded from the backup for better performance. If you want to include the hidden folders in your backup, contact IBM Software Support for assistance.

An additional cost is required to enable the features below:

- For customers using IBM Azure Storage, Locally redundant storage (LRS) is the default option to replicate your data. To use Geo-redundant storage (GRS), contact IBM Software Support. Note that an additional cost is required.
- The Backup Data eDiscovery function allows you to search for emails across all Exchange Online mailboxes backup data, and then download the file list from the search result and perform data recovery, exportation, or deletion on the backup data. To enable this feature to your tenant, contact IBM Software Support. Note that an additional cost is required.
  If you previously enabled metadata-based search and now want to upgrade your e-discovery capabilities to include content-based search, contact IBM Software Support to upgrade your subscription and an additional cost is required.

Microsoft Graph API Beta Version in Use

IBM® Storage Protect for Cloud Microsoft™ 365 leverages Microsoft Graph beta APIs (the APIs in preview) for some operations that are currently unsupported by version v1.0. The features using the following beta APIs may be affected if Microsoft introduces changes to their beta APIs.

Refer to the table below for the beta version API methods of Microsoft Graph that we use in IBM® Storage Protect for Cloud Microsoft™ 365.

Category	API Method	Is it available in the 1.0 version?	Then, why do we use the Beta version?
Group membership	Get all group owners	Yes	This method in the Beta version can be used to detect the Exchange Online license.
	Get all group members	Yes	This method in the Beta version can be used to detect the Exchange Online license.

Category	API Method	Is it available in the 1.0 version?	Then, why do we use the Beta version?
Channel message	Get all channel messages	Yes	These methods in the 1.0 version currently do not support the **Delegated** permission type. If you are not using service account authentication, IBM® Storage Protect for Cloud will use the version 1.0 Graph APIs for channel messages.
	Get a channel message	Yes	
	Get all channel message replies	Yes	
	Get a reply to a channel message	Yes	
	ChatMessages: delta	Yes	

Use Cases

To learn how IBM® Storage Protect for Cloud Microsoft™ 365 can help you restore lost data and complete other operations, review the use cases.

Use Case - Want to Delegate Restore Permissions?

Event:

Your organization has offices in different regions and has different administrators to manage data. You need a solution to delegate the administration of the backup data to different users or teams.

Resolution:

The IBM® Storage Protect for Cloud Microsoft™ 365 User Management feature is a security trimming solution for restore operations. It provides a built-in Administrator group with full control permission to IBM® Storage Protect for Cloud Microsoft™ 365. Administrators can add groups through User Management and grant their Restore permissions to the objects segregated by containers of different service types.

Use Case - Want to Restore Exchange Online Data?

Event:

Tom discovers that he accidentally deleted an important email, and it has already been deleted from his recycle bin. He comes to you, his IT Administrator, for help recovering the email.

Problem:

Native restore functionality in Exchange Online cannot restore an email that was deleted more than 90 days ago. You ask Tom if he remembers when he deleted the email, but he does not recall when he deleted it.

Resolution:

You have an IBM® Storage Protect for Cloud Microsoft™ 365 account and already have the Exchange Online backup service enabled for the backup of the Mailbox container where his mailbox resides. You log into IBM® Storage Protect for Cloud Microsoft™ 365 to recover Tom's deleted email. Tom remembers a keyword that is contained within the subject field of the email, but he cannot remember when he deleted the email. You can use IBM® Storage Protect for Cloud Microsoft™ 365's **Advanced Search** to conduct a keyword-based search to recover the email. If Tom remembers when he deleted the email, you can refine your search to select a date on the backup calendar that is before he remembers deleting the email to recover the backup data and then restore Tom's deleted email.

To get started with IBM® Storage Protect for Cloud services, refer to "Get Started" on page 38. For more information on restoring Exchange Online data, refer to "Restore Exchange Online Data" on page 111.

Use Case - Want to Restore SharePoint Online Data?

Event:

Tom discovers that he accidentally deleted a SharePoint Online folder, and it has already been deleted from his SharePoint Online recycle bin. He comes to you, his IT Administrator, for help recovering the folder.

Problem:

Native restore functionality in Microsoft™ 365 does not enable you to restore a single folder, but rather the entire site would need to be restored, which would interrupt Tom's other business activities. Tom wants his folder back and all the documents contained within it with minimal impact on his day.

Resolution:

You have an IBM® Storage Protect for Cloud Microsoft™ 365 account and have the SharePoint Online backup service enabled for the backup of the SharePoint Online container where this folder resides. You log into IBM® Storage Protect for Cloud Microsoft™ 365 to recover Tom's deleted SharePoint Online folder. Tom remembers the URL of the site collection that his folder was originally stored in, so you enter the URL in the **URL** field and search for the folder. After you find the folder in the search results, you can restore it back to its original location.

To get started with IBM® Storage Protect for Cloud Microsoft™ 365, refer to "Get Started" on page 38. For more information on restoring SharePoint Online data, refer to "Restore SharePoint Online Data" on page 113.

Use Case - Want to Restore OneDrive Data?

Event:

Tom left the company six months ago. Tom stored many business documents in his personal OneDrive site. Bob, Tom's boss, would like access to one of Tom's OneDrive libraries because he knows Tom stored many important business documents there. Bob comes to you, his IT Administrator, and asks you to transfer Tom's OneDrive library to Bob's OneDrive site.

Problem:

When Tom left the company, his OneDrive site was automatically deleted. You know that you cannot restore the deleted site using the OneDrive native restore functionality because the retention period has passed.

Resolution:

You have an IBM® Storage Protect for Cloud Microsoft™ 365 account and have the OneDrive backup service enabled for the backup of this OneDrive site. You log into IBM® Storage Protect for Cloud Microsoft™ 365 to recover Tom's deleted library. You select Tom's username for OneDrive from the drop-down list in the **Name** field, and you search all lists and libraries that are contained in the site. After you find the correct library in the search results, you can restore it to Bob's OneDrive site.

To get started with IBM® Storage Protect for Cloud Microsoft™ 365 services, refer to "Get Started" on page 38. For more information on restoring OneDrive data, refer to "Restore OneDrive Data" on page 118.

Use Case - Want to Restore Microsoft™ 365 Groups Data?

Event:

Tom and three of his colleagues are owners of a Microsoft™ 365 Group. Tom did not think anyone used this Microsoft™ 365 Group anymore, so he deleted it. Tom discovered that his colleagues still used the group, and they want to continue using the group. Tom comes to you, his IT Administrator, for help recovering the deleted Microsoft™ 365 Group.

Problem:

Tom did not remember when he deleted that group, so you need to check if this group still exists in the Microsoft™ 365 recycle bin. The default data retention period in the Microsoft™ 365 recycle bin is 30 days. If the retention period has passed, Tom's deleted Microsoft™ 365 group cannot be restored using Microsoft™ 365 native restore functionality.

Resolution:

You have an IBM® Storage Protect for Cloud Microsoft™ 365 account and already have the Microsoft™ 365 Groups backup service enabled for the backup of the Microsoft™ 365 Group container where this group resides. You log into IBM® Storage Protect for Cloud Microsoft™ 365 to recover Tom's deleted Microsoft™ 365 Group. You select the group name from the drop-down list in the **Name** field and search the backup data of this group. The IBM® Storage Protect for Cloud Microsoft™ 365 Groups service automatically checks group status in Microsoft™ 365. If the group is detected in soft-deleted status, you can choose to either restore the entire group from the Microsoft™ 365 recycle bin to its last known good state, or restore the group or its contents from the backup data to its original location.

To get started with IBM® Storage Protect for Cloud Microsoft™ 365, refer to "Get Started" on page 38. For more information on restoring Microsoft™ 365 Groups data, refer to "Restore Microsoft 365 Groups Data" on page 122.

Use Case - Want to Restore Project Online Data?

Event:

Tom discovers that he accidentally deleted a project, and it has already been deleted from his Project Online recycle bin. He comes to you, his IT Administrator, for help recovering the project.

Problem:

Native restore functionality in Microsoft™ 365 does not enable you to restore a single project, but rather the entire site would need to be restored, which would interrupt Tom's other business activities. Tom just wants his project back and all items contained within it with minimal impact on his workday.

Resolution:

You have an IBM® Storage Protect for Cloud Microsoft™ 365 account and have the Project Online backup service enabled for the backup of the Project Online container where this project resides. You log into IBM® Storage Protect for Cloud Microsoft™ 365 to recover Tom's deleted project. Tom remembers the URL of the site collection that his project was originally stored in, so you enter the URL in the **URL** field and search for the project. After you find the project in the search results, you can restore it back to its original location.

To get started with IBM® Storage Protect for Cloud Microsoft™ 365, refer to "Get Started" on page 38. For more information on restoring Project Online data, refer to "Restore Project Online Data" on page 127.

Use Case - Want to Restore Public Folder Data?

Event:

Tom discovers that he accidentally deleted an important file from a public folder. He comes to you, his IT Administrator, for help recovering the file.

Problem:

Native restore functionality in Exchange Online Public Folder cannot restore a file that has been deleted more than 90 days ago. Tom does not recall when he deleted the file.

Resolution:

You have an IBM® Storage Protect for Cloud Microsoft™ 365 account and already have the Public Folder backup service enabled for the backup of the Public Folder where that file resides. You log into IBM® Storage Protect for Cloud Microsoft™ 365 to recover Tom's deleted file. Tom remembers a keyword that is contained within the file name, but he cannot remember when he deleted the file. You can use IBM® Storage Protect for Cloud Microsoft™ 365's **Advanced Search** using the **Subject Name** field to conduct a keyword-based search to recover the file. If Tom remembers when he deleted the file, you can refine your search to select a date on the backup calendar that is before he remembers deleting the file to recover the backup data and then restore Tom's deleted file.

To get started with IBM® Storage Protect for Cloud Microsoft™ 365, refer to "Get Started" on page 38. For more information on restoring Public Folders data, refer to "Restore Public Folder Data" on page 131.

Use Case - Want to Restore Teams Data?

Event:

Tom is the owner of his department's team in Microsoft™ Teams. Two months ago, he deleted one of his Team's channels; however, today, he realized that the deleted channel contains a file that he now needs access to. Tom comes to you, his IT Administrator, for help recovering the deleted channel.

Problem:

You cannot restore Tom's deleted channel using Microsoft™ 365 native restore functionality because the retention period has already expired.

Resolution:

You have an IBM® Storage Protect for Cloud Microsoft™ 365 account and already have the Teams backup service enabled for the backup of the team where the channel resides. You log into IBM® Storage Protect for Cloud Microsoft™ 365 to recover Tom's deleted channel. You select the team name from the drop-down list in the **Name** field and search the backup data of this team. After you find the correct backup data of the channel in the search results, you can restore it back to its original location. The conversations in this Channel will be restored as HTML files to the Files tab.

To get started with IBM® Storage Protect for Cloud Microsoft™ 365, refer to "Get Started" on page 38. For more information on restoring teams, refer to "Restore Teams Data" on page 132.

Use Case - Want to Restore Teams Chat Messages?

Event:

Some Teams chat messages of Microsoft 365 users were removed after an accidental change was made to the retention policies.

Problem:

You cannot restore the Teams chat data using Microsoft 365 native restore functionality.

Resolution:

You have an IBM® Storage Protect for Cloud Microsoft™ 365 account and have the Microsoft Teams Chat backup service enabled for the backup of the Microsoft 365 users. You can use the Restore wizard to search and select the chat messages to export. The chat messages can be exported to HTML files.

To get started with IBM® Storage Protect for Cloud Microsoft™ 365, refer to "Get Started" on page 38. For more information on restoring teams, refer to "Export Teams Chat Messages" on page 104.

Use Case - Want to Restore Viva Engage Data

Event:

The Human Resources team would like to retrieve messages posted in the All Company Viva Engage community that relate to company events. They contact you, their IT Administrator, for help recovering the deleted Viva Engage posts.

Problem:

The retention period for some of the messages has expired, and they are now permanently deleted.

Resolution:

You have a IBM® Storage Protect for Cloud Microsoft™ 365 account and already have the Viva Engage backup service enabled for the backup of the Viva Engage community. You can use the Viva Engage service to restore or export Viva Engage messages. To locate the Viva Engage messages from the backup, you can browse to the corresponding recovery point and search for the messages with keywords. The messages that contain the searched keywords within the first 100 characters will be displayed in search results.

To get started with IBM® Storage Protect for Cloud Microsoft™ 365, refer to "Get Started" on page 38. For more information on restoring teams, refer to "Restore Viva Engage Data" on page 138.

Use Case – Want the Ability to Detect a Potential Ransomware Attack and Safely Recover Encrypted Files?

Event:

You are the IT Admin at a large organization. Joe, who is a member of the Marketing team, had a file in his OneDrive account that got encrypted in a ransomware attack. A OneDrive sync brought the file into the cloud. Joe is unaware that the attack occurred.

Problem:

Native Microsoft 365 solutions, such as versioning, offer protection against some attacks, but there are also limitations that do not always offer full protection. As the IT Admin at a large organization, you have many responsibilities that can be very time-consuming. However, you want to ensure that employees, such as Joe, are protected from ransomware attacks, 26 and you want to ensure that you can mitigate and/or minimize any potential damage in the event of an attack before it is too late.

Resolution:

To ensure your organization is safe from ransomware attacks, you want to have early detection in place along with options for a safe restore in the event of an attack. You have a IBM® Storage Protect for Cloud Microsoft™ 365 account in place with OneDrive already set up to be protected with regular backups in place. Plus, IBM® Storage Protect for Cloud Microsoft™ 365 provides early detection when any changes occur that may indicate suspicious behavior. You selected the option to send email notifications for jobs that have **Potential Ransomware Detected**, and as the IT admin, you will now receive an email notification alerting you if a potential ransomware attack has been detected. You can then review the details in the **Unusual Activities Analysis Report**, find the date detected to have had a potential ransomware attack, and browse to a safe recovery point to either restore Joe's entire OneDrive or restore the individual encrypted file back to a healthy state.

> **Note:** This report requires Joe's OneDrive to have at least 12 days of successful backups with incremental changes.

For details, refer to "Use the Unusual Activities Analysis Report" on page 150.

Use Case - Want to Obtain a Better Understanding of Your Subscription Consumption?

Event:

Your organization uses IBM® Storage Protect for Cloud Microsoft™ 365 to protect your Microsoft™ 365 tenant. The IT team wants to fully monitor the subscription consumption, from the application level down to an individual object level such as a site collection, mailbox, OneDrive for an object, group, or team, to understand and identify trends in utilization.

Resolution:

The subscription consumption report in **Subscriptions** provides a complete breakdown of subscription utilization and consumption. The report includes the following components: a dashboard which provides full subscription details, the Usage tab that points out trends in utilization including spikes (i.e. migrations), identifies top storage consumers, highlights the growth rates of data in your environment, and displays the consumed subscription of each protected object along with the ranking in its service type in the Utilization tab. The reports are also downloadable in CSV format.

For details, refer to "Monitor Subscription Consumption" on page 156.

Use Case - When Do I Need Container Specific Retention Policies?

Event:

You may have used IBM® Storage Protect for Cloud Auto Discovery and distributed your assets to different containers based on how your organization is defined: member firms, domains, geo-locations, offices, departments, roles, etc. The administration of backup data for different containers can be delegated to different users or groups. At the same time, it may also require the flexibility to pick up specific retention policies for each container.

Resolution:

If you have purchased a BYOS subscription or have been using default IBM® Storage Protect for Cloud storage with an unlimited retention subscription, you can customize the retention policies for each service type and each container. Note that the default retention period applied on your own storage is one year. You need to manually update the retention year on the **Retention Policy** page if you want to retain the data longer.

For details, refer to “Configure Retention Policy” on page 90.

Supported Browsers

The table below outlines the required browser versions to support IBM® Storage Protect for Cloud Microsoft™ 365.

Browser	**Version**
Google Chrome	The latest version
Mozilla Firefox	The latest version
Safari	The latest version
Microsoft™ Edge based on Chromium	The latest version

FAQs

Refer to the frequently asked questions and answers divided into the following categories: license and subscription, security and integrity, and backup and restore.

License and Subscription

If a user's Microsoft™ 365 license expires, will their data become out-of-scope?

Refer to the table below for reaction details for each backup service:

> **Note:** Only when the object being removed from the backup scope still exists in Microsoft 365 will the object be detected by the **Out-of-scope object** report and its backup data marked for deletion. By default, the **Out-of-scope object** feature does not support BYOS customers. The backup data for the objects that have been protected by IBM® Storage Protect for Cloud but removed from your Microsoft 365 tenant is not within this scope. For the **Exchange Online** and **OneDrive**, the corresponding objects will be added to the **Offboarded users** report and you can configure separate retention period for their backup data. For other service types, IBM® Storage Protect for Cloud will keep such backup data according to your global retention policy. For details, refer to "Remove Unprotected Data" on page 146.

Service Type	Reactions
Exchange Online	Service account authentication and app profile cannot detect the users' mailboxes if their mailboxes become inactive or their license has expired, and the backup data of these mailboxes will be detected by the **Offboarded users** report. You can configure retention period for the backup data in **Remove unprotected data** > **Offboarded users**. If the service account or app has not been assigned the Exchange Administrator role in Microsoft Entra ID, the backup data of the users' mailboxes will not be properly deleted. To ensure the integrity of backup data, make sure you have assigned the Exchange Administrator role.
OneDrive	If the user's My Site still exists in Microsoft 365 and is included in the backup scope, the site can still be discoverable to IBM® Storage Protect for Cloud and protected, regardless of the license. If it has been removed from the backup scope, it will be detected by the **Out-of-scope object** report and be deleted. If either the user or the user's My Site no longer exists in Microsoft 365, the user's OneDrive will not be protected, and its backup data will be detected by the **Offboarded users** report.
Project Online	License expiration does not affect the Auto Discovery but will fail the backup.

I am currently using IBM® Storage Protect for Cloud default storage to store backup data. If I end my subscription, would I ever be able to recover the backup data from IBM® Storage Protect for Cloud?

When an Enterprise subscription ends, IBM® Storage Protect for Cloud will retain the backup data in IBM® Storage Protect for Cloud storage for 60 days, subject to the terms of your service agreement. The backup data in IBM® Storage Protect for Cloud storage can be exported to your own storage as a paid service. You must submit an export request if you wish to export your data from IBM® Storage Protect for Cloud storage. The data deletion process in IBM® Storage Protect for Cloud default storage will start 30 days after the expiration date. If you renew the subscription before the deletion completes, you may be able to keep the old backup data and use it for data recovery.

If you have the BYOS (bring your own storage) subscription, the backup data will remain in your own storage until you delete it, and you will not need to pay an export fee.

Note that the backup data is stored in IBM® Storage Protect for Cloud format and not as pure copies of Microsoft™ 365 data. Therefore, before you move away from the product, ensure you have exported the encryption key in case you will not be able to sign in to the IBM® Storage Protect for Cloud Microsoft™ 365 interface once your subscription has ended. For details on exporting encryption keys, refer to “Configure Security Settings” on page 94.

If you would like additional details or assistance with this process, contact IBM Software Support. For more details, refer to “Introduction to Data Export Service” on page 159.

Features unavailable in trial subscription

The following features are unavailable to trial users:

- Change backup scope
- Remove unprotected data
- View storage consumption report

What features are available for different subscription types?

Refer to the list below for the supported/unsupported features in Core and Flex subscriptions:

Note the following:

- An additional cost is required to enable Backup Data eDiscovery. For details, refer to Backup Data eDiscovery.

Features		Standard
Storage	IBM® Storage Protect for Cloud hosted storage	Supported
	Bring your own storage	Supported
Unlimited retention		Supported
Back up Recordings folder		Supported
Manually Delete Backup Data		Supported

If I purchase the Power Platform subscription by capacity, how can I get the number of Power BI workspaces, Power Automate flows, and Power Apps in my environment?

To get the number of Power BI workspaces, Power Automate flows, or Power Apps, refer to the following Microsoft articles:

- For Power BI workspaces, see Manage workspaces.
- For Power Automate flows, see View analytics for cloud flows.
- For Power Apps, see Admin Analytics for Power Apps.

You can check their types and filter out the items which can be protected in IBM® Storage Protect for Cloud Microsoft™ 365 according to Power BI Data Types, Power Automate Data Types, and Power Apps Data Types.

When I renew my IBM® Storage Protect for Cloud Microsoft™ 365 subscription, what will happen to my data retention settings?

Upon subscription renewal, your data retention settings will be adjusted based on a comparison between the new and previous retention period:

- **If the new subscription has a shorter retention period:** Your retention periods will be automatically adjusted to match the new subscription limits.
- **If the new subscription has the same or longer retention period:** No changes will be made to your existing retention settings.

To verify your configuration and ensure you are aware of any changes, refer to **Settings** > **Retention**. Additionally, you will receive notification emails 90 days, 60 days, and 30 days before any data deletion. Upon subscription renewal, a notification email will advise you to check and update your retention settings in IBM® Storage Protect for Cloud Microsoft™ 365 as needed.

Security and Integrity

Does IBM® Storage Protect for Cloud Microsoft™ 365 Support Data Deduplication and Compression?

IBM® Storage Protect for Cloud Microsoft™ 365 applies standard .zip compression to data. Although our DAT files can support deduplication algorithms, we currently do not support deduplication on Blob storage as this requires a physical/virtual storage system that is not as cost-effective as Azure Cold storage. Additionally, since our backup data is encrypted and the encryption key is dynamic, the deduplication performance may not be optimal.

My organization plans to use the Customer Key feature in Microsoft™ 365, so we will be in control of our own encryption keys for our data in Microsoft™ 365. Will IBM® Storage Protect for Cloud Microsoft™ 365 back up and restore this data if it is enabled?

The customer key feature in Microsoft™ 365 encrypts the data at rest in Microsoft™ 365, which indicates that Microsoft™ cannot access this encrypted data. However, IBM® Storage Protect for Cloud Microsoft™ 365 uses user credentials or app profiles to access customer data with an API, same as the end user accessing scenario where the data will be decrypted to real content. Therefore, the backup and restore service will not be affected. For additional details, you can refer to Customer Key Overview from the Microsoft™ website.

Is backup data immutable?

Yes, IBM® Storage Protect for Cloud ensures that backup data is immutable, and we employ several measures to protect and control access to always encrypts the backup data:

- Encryption**:** Backup data is encrypted using with unique keys for each tenant. All data in transit is encrypted utilizing TLS 1.2/1.3 and IBM strictly uses officially supported APIs that maintain encrypted connections for backups. Data at rest is secured by default with an IBM-managed key, although customers can choose to use their own keys.

- **Storage Isolation:** IBM provides customers with the option to isolate their data within a single region, supports multi-geo configurations, and offers customer-owned storage. This ensures that data remains physically isolated within the region and is never replicated across data center regions.

- **Logical Isolation:** IBM® Storage Protect for Cloud is segregated separately from your production environment. It includes delegated administration and role-based access controls to prevent unauthorized users from modifying or deleting backups.

- **Immutable Storage:** Backup data copies cannot be directly accessed through the product user interface or API and cannot be compromised by either privileged or non-privileged users of the platform. Data can only be exported, restored to production, or defensibly destroyed when a pre-defined data retention policy is met.
  Under special circumstances, customers may request manual deletion of data through IBM Support, which requires verification. IBM also allows authorized admins to handle the DSAR (Data Subject Access Request) by removing personal information from the systems as requested. The DSAR can also be disabled completely within our platform for an added level of protection.

- **Ransomware Protection:**IBM® Storage Protect for Cloud learns from your backups and alerts you of unusual activities that could indicate a compromise or ransomware attack. Recovery points prior to the incident are clearly identified, and alerts can be configured to reach administrators to minimize the impact of a breach.

How is data handled after running a data deletion process in compliance with GDPR?

The process can be categorized into two scenarios:

- **Deletion of entire object** – This scenario involves the complete removal of an object, such as a mailbox or OneDrive account. The entire object, along with all associated data, is permanently deleted.

- **Deletion of individual items** – This scenario involves the removal of specific items, such as files or documents. The index entries associated with these individual items are permanently deleted, ensuring that the data is destroyed and non-recoverable.

Public APIs

Can I pull the daily job information into my backup reporting software to monitor IBM® Storage Protect for Cloud Microsoft™ 365?

Yes. You can use the public APIs from IBM® Storage Protect for Cloud to get the audit records, subscription consumption, and job information of IBM® Storage Protect for Cloud Microsoft™ 365. However, these public APIs provided by will be retired in the future. We recommend using the IBM Graph API instead. For details, refer to Use Public APIs.

Backup and Restore

Will the backup services survive if my tenant blocks access from the apps that don't use modern authentication?

From the July 2022 release, all IBM® Storage Protect for Cloud Microsoft™ 365 using service accounts support modern authentication. But if the service account has enabled the MFA, the modern authentication will not work, and we will use the classic authentication.

How to remove the admin role from a service account or an authentication user of the delegated app?

To remove the administrator role of the service account from all OneDrive sites, download the script.

To remove the administrator role of the service account from all SharePoint sites, refer to download the script.

To remove the user from all teams and groups, either as owner or member, refer to download the script.

To remove the user from all apps, refer to download the script.

To remove the user from all flows, refer to download the script.

To remove the user from all workspaces, download the script.

What can I do if I cannot find my backup data for channel files through a time-based restore wizard?

If your Team's channel name is not in English, Dutch, Japanese, or German, you may encounter this problem. When you go to use the time-based restore wizard to browse a channel's backup data (select a backup job to drill down to the backup data), you may find that no folders or files are displayed under the channel's Files folder. This is because the index for channel backup data is recorded with channel names, but so far, only the backup data of the channels whose names are in English, Dutch, Japanese, and German can be mapped. You can contact the IBM Software Support team for assistance.

What if my site collection URL has been updated after backup? (applicable for SharePoint Online sites, Microsoft™ 365 Groups team sites, and Teams team sites)

IBM® Storage Protect for Cloud Microsoft™ 365 will start a full backup on this site collection if it is included in the backup scope. Moving forward, to recover the data from previous backups, you must perform an out-of-place restore to restore the backup of the old-URL site collection to the new-URL site collection.

If the site collection, in this case, is a Microsoft™ 365 Groups or Teams team site, IBM® Storage Protect for Cloud Microsoft™ 365 will also perform a full backup on this site, and the previous backup data of the site can only be restored via an out of place restore. For the object-based restore method, you can search for the backup data of the old-URL site via the keywords; for the time-based restore method, you can find the old-URL site from the backup jobs performed before the URL changes.

What if my domain name has been changed after backup?

For **Exchange Online mailboxes**, **Public Folders**, **Power Automate flows**, **Power Apps**, and **Power BI reports**:

The domain name change will not affect the backup and restore process. Backups will continue as incremental backups. Whether a user searches for the old or new domain name in the restore page, the system will recognize both as the same object. All legacy backup data will be retained until it reaches the set retention period.

For **SharePoint sites**, **Team/Group team site**, and **OneDrive**:

If your Auto Discovery scan profile uses a domain name as the scan rule, you will need to update the scan rule for Auto Discovery. After the Auto Discovery scan job is finished, IBM® Storage Protect for Cloud Microsoft™ 365 will run a full backup for the objects with new URLs; If the old URLs can still be accessed, the old URLs will be moved to the unprotected scope, and their backup data will be deleted on time. If the old URLs are no longer accessible, the backup data will only be deleted when it reaches the retention period.

Where is Wiki data stored and how to restore?

The wiki data is stored in a hidden list in the Teams team site named by **ChannelID_wiki**. To get the ID of the channel where the Wiki tab resides, sign into https://teams.microsoft.com, and click the channel where the Wiki tab resides. You can get the channel ID (**threadId=**) from the URL.

Microsoft Teams channel no longer supports Wiki tab. You can download your Wiki SharePoint or use IBM® Storage Protect for Cloud Microsoft™ 365 to export the Wiki backup data.

What if my Project Online site has been moved to the SharePoint Online site after backup? (same as Microsoft™ 365 Group to Team, SharePoint Online site to Group team site)

The objects in your tenant may be moved to another type after being backed up, such as the following cases in the table. The objects in these cases will continue to be protected by the service they are moved to, and IBM® Storage Protect for Cloud Microsoft™ 365 will keep their previous backup data until the backup data reaches the retention date. They will not be regarded as objects moved to the unprotected scope for deletion.

> **Note:** If a SharePoint Online site is connected to a Microsoft™ 365 Group (groupified site), IBM® Storage Protect for Cloud will keep it in both the **SharePoint Sites** container and the **Microsoft™ 365 Groups** container. IBM® Storage Protect for Cloud Microsoft™ 365 will protect this site in the corresponding container separately as you selected. To keep the previous backup data, ensure that the SharePoint site is included in the backup scope. Otherwise, the SharePoint site will be moved to the unprotected scope for backup data deletion.

From	To
Project Online sites	SharePoint Online sites
Microsoft™ 365 Group	Team
SharePoint Online site	Microsoft™ 365 Group team site

Can IBM® Storage Protect for Cloud Microsoft™ 365 protect the mailboxes on Litigation Hold?

IBM® Storage Protect for Cloud Microsoft™ 365 can protect mailboxes that are placed on Litigation Hold but cannot keep the Litigation Hold configuration for the mailboxes since that configuration needs to be configured in Exchange Admin, which is out of reach of Exchange Online backup and restore.

I have a document that was shared with an external user. Does IBM® Storage Protect for Cloud Microsoft™ 365 support restoring the external user and its permissions that were part of that document?

For an external user who has been added to your Microsoft Entra ID, the user’s permissions will be kept when the document that this user is shared with has been restored. Currently, if an external user has accessed the shared item, the restore job will restore this user and the user’s permission to this item and trigger the external sharing email notification. If an external user has not yet accessed the item, the user’s permission will not be restored, and the external user can no longer use the previous sharing link to access the document.

How do I restore term store-only data?

You can choose the following solutions:

- If you want to restore the entire global term store data, perform the restore as follows:
  a. Select any site collection from the backup data and then select a useless or an empty site collection as the destination.

  b. Choose the **Restore terms in both global term store and site term store**option for the restore setting “How do you want to restore the Managed Metadata Service?”

  c. Use **Skip** as the conflict resolutions to perform a restore job.

  d. After the restore completes, you can delete the site collection from the destination.
- Currently there is no a method only to restore the entire site store only. You can use the following method as a workaround, but the objects with no conflicts will be restored to the destination as well. Perform the restore as the following:
  a. Select that site collection to restore.

  b. Choose the **Restore terms in site term store only**option for the restore setting “How do you want to restore the Managed Metadata Service?”

  c. Use **Skip** as the conflict resolutions to perform a restore job.

How does IBM® Storage Protect for Cloud Microsoft™ 365 protect the OneNote notebooks?

As Microsoft has a 2 GB file size limit of OneNote notebooks saved in OneDrive or SharePoint, backup jobs will skip the OneNote files that are larger than 2 GB. In addition, due to API limitations, IBM® Storage Protect for Cloud Microsoft™ 365 cannot protect the history versions of OneNote files.

What will the exported Teams Chat messages be like?

We support exporting Teams Chat messages to an HTML file.

Notification

I purchased the backup service from a service provider. Regarding email notifications sent to the administrator group, which group will receive the notifications: the service provider’s administrator group or my administrator group?

The recipient of the email notification depends on the service provider's access to your IBM® Storage Protect for Cloud environment.

- **If the service provider has access**, the email notifications will be sent to the service provider’s administrator group.
- **If the service provider does not have access**, the email notifications will be sent to your administrator group.

Storage

How backup data can be stored in your Azure blob storage?

If you are using your own **Microsoft Azure Blob Storage** (BYOS subscription), you may be interested in how the backup data is stored in Azure Blob storage.

For BYOS customers using Azure Blob storage, IBM® Storage Protect for Cloud will write your new backup data to the cold tier by default reduce storage costs. The supported Azure storage account types are **StorageV2** and **BlobStorage** of **Standard** performance type. For existing customers, your former backup data are still stored in the cool tier. This intelligent tiering also extends to additional BYOS storages appended to the system. Note that it is not available if your storage region is Qatar Central (Doha) or you are using IBM® Storage Protect for Cloud Microsoft™ 365 in the data center operated by 21Vianet in China.

To use your Azure blob storage in the most cost-effective manner, you can also store the backup data to the archive tier. If you are an existing customer with the archive settings configured before, you will continue with your current setup.

Hot Tier	Cold Tier	Archive Tier

Index database	The backup job stores backup data to the cold tier automatically from the January 2024 release and will always keep at least a full backup cycle in the cold tier.	Older backup data can be moved to the archive tier.

Does IBM® Storage Protect for Cloud Microsoft™ 365 use HTTPS (SSL) for Amazon S3 communication?

Yes. IBM® Storage Protect for Cloud Microsoft™ 365 uses HTTPS (SSL) instead of HTTP to access Amazon S3 by default. For details on Amazon S3 storage configuration, refer to “Storage Information” on page 79.

Will your backup services incur additional costs on BYOS storage during backup and restore?

Yes. For example, for BYOS customers with Microsoft Azure Blob Storage, below are the main factors to consider:

Table 7: BYOS customers with Microsoft Azure Blob Storage

Additional Costs	**Comment**
Data storage	The cost to store backup data. For information on storage tiers for different storage types, refer to Storage Information
Data read & write operations	During a backup job in IBM® Storage Protect for Cloud, data will be written to the customer's BYOS storage. Similarly, during a restore job, data will be read from the storage. Data are stored in blobs which are around 10 to 50 MB in size. Each blob will incur one operation.
Data retrieval	Additional costs apply for data retrieval during restore jobs. These costs vary depending on the storage tier.
Data transfer	The primary cost concern is data transfer out. If your default Azure Blob Storage is the same region as the data center you signed up for in IBM® Storage Protect for Cloud, there will be no transfer costs. Otherwise, additional charges will be incurred.

Best Practices

Backup Scheduling

Microsoft has implemented tighter throttling limits on background apps, including content migration, data loss prevention, and backup solutions for SharePoint Online and OneDrive, during weekday daytime hours, to ensure that SharePoint and OneDrive services remain highly available and reliable for users who depend on the service more than ever in remote work scenarios. For additional details, see this Microsoft article.

You should expect that these background apps will achieve very limited throughput during these times. However, during the evening and weekend hours for the region, the service will be ready to process a significantly higher volume of requests from background apps. We now recommend the following scheduling practices to ensure successful backups:

- Schedule backups outside of business hours.
- You may also consider reducing the frequency of backups down to two or three as necessary during the workweek.

App Profile Authentication in Auto Discovery, Backup, and Restore

To help enhance security for your Microsoft™ 365 tenant and avoid SharePoint Online throttling during your backup jobs, you can create an app profile for Microsoft™ 365 and choose **Use an app profile** as the authentication method when you create an Auto Discovery scan profile.

To protect multiple service types by IBM® Storage Protect for Cloud, we recommend creating multiple IBM® Storage Protect for Cloud Microsoft™ 365 service apps (created through **App management** > **Modern mode**) in IBM® Storage Protect for Cloud.

- IBM® Storage Protect for Cloud Microsoft™ 365 (Exchange permissions) app, recommended for the backup and restore of Exchange Online and Public folders.
- IBM® Storage Protect for Cloud Microsoft™ 365 (SharePoint permissions) app, recommended for the backup and restore of SharePoint Online, OneDrive, and Project Online.
- IBM® Storage Protect for Cloud Microsoft™ 365 (All permissions) app, recommended for the backup and restore of Teams, Microsoft 365 Groups, and Yammer.
- To protect Viva Engage, you need both the Cloud Backup for Microsoft 365 (All permissions) app and the Viva Engage app.
- The IBM® Storage Protect for Cloud Microsoft™ 365 (delegated permissions) app is necessary for protecting Power BI, Power Automate, and Power Apps. Additionally, this app is required if you want to restore Teams channel conversations as posts or restore Planner task comments.

If you use only one IBM® Storage Protect for Cloud Microsoft™ 365 app with all permissions to protect all services, there is an increased potential for throttling issues since every application has its own API call limit in a Microsoft tenant.

Note the following:

- For more information on the app profile, Auto Discovery, and how to set up an Auto Discovery Profile, refer to the IBM Storage Protect for Cloud User Guide.
- For site collections (of SharePoint Online, Microsoft 365 Groups, Teams, or Viva Engage), the hybrid mode is now provided. In the hybrid mode, IBM® Storage Protect for Cloud Microsoft™ 365 jobs will, by default, use an app profile in backup and restore. For the data types that are unsupported in the app context, service account authentication will be used automatically. Note that the use of service accounts is not the recommended method as it attracts an increased potential for throttling issues. To learn more and enable the mode, contact the IBM support team.

EWS Throttling in Exchange

Microsoft™ uses throttling to manage Microsoft™ 365 operations, and throttling limits can affect backup performance. You can contact Microsoft™ support to adjust the following Exchange parameters to significantly reduce throttling in Microsoft™ 365.

- EwsCutoffBalance: Unlimited

- EwsMaxBurst: Unlimited
- EwsRechargeRate: Unlimited
- EWSMaxConcurrency: Highest limit

Get Started

Follow these steps to get started with IBM® Storage Protect for Cloud Microsoft™ 365, you must obtain a full license to IBM® Storage Protect for Cloud Microsoft™ 365 and configure the Auto Discovery profile to scan the objects you want to protect.

1. **Obtain a Subscription**
    - To obtain a free 30 day trial of IBM® Storage Protect for Cloud Microsoft™ 365, visit the IBM Storage Protect for Cloud Microsoft 365.
    - To find out how IBM charges for licenses for IBM® Storage Protect for Cloud Microsoft™ 365, refer to IBM Storage Protect for Cloud Microsoft 365.
2. Access IBM® Storage Protect for Cloud
   Use your web browser to navigate to the IBM® Storage Protect for Cloud portal and enter your login credentials (username and password). For details, refer to the IBM® Storage Protect for Cloud User Guide.
3. **Connect your tenant**
   Your IBM® Storage Protect for Cloud tenant owner or service administrators must first connect your Microsoft 365 tenants to IBM® Storage Protect for Cloud. For details, refer to Connect your Tenants to IBM Storage Protect for Cloud.

   If your Microsoft 365 tenant has Multi-Geo enabled (https://docs.microsoft.com/en-us/office365/enterprise/office-365-multi-geo), you can start by going to the Data Center Mappings in IBM® Storage Protect for Cloud to review and map the list of geo locations from your Microsoft 365 tenant that we've detected and the supporting data centers.

   > **Note:** The mapping for SharePoint Online sites depends on the region of the SharePoint Administrator.

4. **Configure App Profiles**
   Create IBM® Storage Protect for Cloud Microsoft™ 365 app profiles in IBM® Storage Protect for Cloud for the services and objects that you want to enable or protect. For details, refer to Create an App Profile in the IBM® Storage Protect for Cloud User Guide.
    - For the app profile that you must prepare with the least permissions for a specific backup service, refer to Enable the Backup Service. You can also get an overall reference from the Configure Auto Discovery section.
    - For the required permissions for app profile authentication, refer to App Profile Authentication.
5. **Configure Auto Discovery**
   IBM® Storage Protect for Cloud Auto Discovery now uses app profile authentication to scan and register the objects you want to protect in IBM® Storage Protect for Cloud Microsoft™ 365.

   > **Note:** If your tenant is Multi-Geo, ensure that you are using the filters provided in the advanced scan mode to separate the mailboxes, One Drives, sites, and other Microsoft 365 content by their preferred data locations. We'll use these boundaries to help distribute the management for each of these containers globally.

   If your administrator has blocked access from apps that don't use modern authentication, IBM® Storage Protect for Cloud jobs using a service account will now use modern authentication for backup and restore.
6. **Configure Backup Scope and Frequency**
    - When you log into IBM® Storage Protect for Cloud Microsoft™ 365 for the first time, you will be prompted to an onboarding wizard to check your preparations and select the objects you want to back up. For details, refer to Set Up the Backup Wizard.
    - To configure which containers and objects will be backed up first during backup jobs, refer to Configure Backup Prioritization.

- To change the backup scope and frequency, refer to Change the Backup Scope and Change the Backup Frequency.

7. **Monitor and Manage Backups**

    - To configure notifications and user management, refer to Configure Notifications and User Management.
    - To configure other settings for IBM® Storage Protect for Cloud, refer to Configure Settings for IBM Storage Protect for Cloud:
      You can directly enable the following common backup settings in **Settings** > **Backup**. For details, refer to Configure Backup Settings.
        - Back up private/shared channels
        - Back up the Recordings folder
        - Back up Planner data
        - Select an API to protect Teams Chat and customize the backup time range for Teams chat messages
        - Configure impersonation accounts for Public Folders backup
        - Skip specific errors by error codes
    - Regularly monitor the backup status to ensure backups are running as scheduled. For details, refer to Monitor and Manage Your Backup.
    - Monitor Subscription Consumption for IBM® Storage Protect for Cloud:
        - View Storage Consumption Report.
        - Use the Job Analytics Report.
        - Use Unusual Activities Analysis Report.
        - View the End-User Restore Report.
        - View the Coverage Report.

8. **Finalize Setup**
   Verify that all backup configurations are correct and complete. Double-check the settings for each service, notification preferences, backup options, and storage location.

   If you want to perform restore and export, refer to the following:

    - To restore backup data from the IBM® Storage Protect for Cloud Microsoft™ 365 interface, refer to Restore and Recover Your Data.
    - To export and download backup data protected by IBM® Storage Protect for Cloud, refer to Export and Download Your Data.

Set Up the Backup Wizard

When you log into IBM® Storage Protect for Cloud Microsoft™ 365 for the first time, the onboarding wizard will appear and you can now get a thorough check on your preparations before enabling the backup services.

About this task

Note:

- If your organization has a Multi-Geo enabled, the users assigned to multiple regions in IBM® Storage Protect for Cloud will need to select a region. The users with only one region will be automatically redirected to that regional IBM® Storage Protect for Cloud Microsoft™ 365 instance.
- If you signed up to IBM® Storage Protect for Cloud with the data center **Germany West Central (Frankfurt)**, and you have purchased the subscription to use IBM® Storage Protect for Cloud Azure

> storage to store the backup data, IBM® Storage Protect for Cloud Microsoft™ 365 will store your data in the data center you signed up for IBM® Storage Protect for Cloud.

If you have the BYOS subscription, you must configure a custom storage location to store the backup data to your own storage on the **Storage location** page. Note that the storage location information cannot be changed once saved. If you purchased the backup service from a service provider and the service provider has already configured the BYOS storage location, the storage information is read-only on this page.

Procedure

To get started with your backup service, follow the steps below.

1. On the **Backup modules** page, you must select at least one service that you want to enable. By default, no services are selected. You can click **Set up later** to skip the following steps and go to the home page of the IBM® Storage Protect for Cloud Microsoft™ 365 with no services enabled.
2. Click **Next step**, after you select the backup modules that you want to enable.

   > **Note:** If you select the Teams Chat service and click **Next**, a pop-up window will appear, and you must select an API to protect Teams Chat. You can change the API for Teams Chat later in **Settings** > **Backup**.

3. On the **Backup configuration** step, you can check whether you have scan profiles for the selected backup services and whether your apps have enough permissions.
   - Navigate to the **App management** page in the IBM® Storage Protect for Cloud interface to configure the app profiles. For the apps you can use for each backup service, refer to “App Profile Authentication” on page 57.
   - Navigate to **Auto Discovery** in the IBM® Storage Protect for Cloud interface to configure scan profiles for the objects that you want to protect in IBM® Storage Protect for Cloud Microsoft™ 365. For details, refer to Auto Discovery for Microsoft 365.
4. If you want to protect Public Folders, you must also configure impersonation accounts on the **Settings** > **Backup** page since we only support using impersonation accounts to protect Public Folders after the June 2023 release. Note that the Public Folders backup will perform operations by using the permissions that are associated with the impersonation accounts. We recommend a 1:500 ratio for the impersonation accounts and the Public Folders. For more information about impersonation technology, see Impersonation and EWS in Exchange.
   The impersonation accounts configured must meet the following conditions:
   - The impersonation account must have the Exchange Online product license.
   - This user must also have the **Owner** permission to the Public Folders.
5. If you want to protect Teams Chat, you must customize the backup time range for Teams chat messages on the **Backup configurations** page. Note that the backup time range cannot be changed once saved.
6. On the **Backup scope** page, you can select the **All objects in existing and any further containers** option for all selected services, which will automatically include all existing containers and the objects registered later. If you want to customize the backup scope for each service, select **Custom backup scope per service type**. For each service, you can select **All objects in existing and any further containers** option to include all objects in existing and any further containers in the backup scope or select **Custom backup scope** to include the containers that you want to back up.
7. When you finish selecting the objects to back up, you can click **Start backup** to save the configurations and start the backup jobs.
   After you click **Start backup**, the backup job for an object type will not start if the backup service for this object type is disabled.

   > **Note:** After you click **Start backup**, the backup job for an object type will not start if the backup service for this object type is disabled.

Enable the Backup Service

Before you get started with a backup service, ensure your IBM® Storage Protect for Cloud Microsoft™ 365 subscription contains that service.

You can refer to the Subscription and Licensing Information for how IBM® charges for a license.

The sections below will help you get ready to enable the backup services that you want to use:

At first, if your Microsoft 365 tenant has Multi-Geo enabled (Microsoft Windows Multi-Geo), you can contact support to enable the multi-geo capability for your subscription and start by going to the Manage Data Center Mappings in IBM® Storage Protect for Cloud to review and map the list of geo locations from your Microsoft 365 tenant we've detected and the supporting data centers. Note that the mapping for SharePoint Online sites depends on the region of the SharePoint Administrator.

Next, you must consider which authentication method and Auto Discovery scan profile to register your objects to IBM® Storage Protect for Cloud.

supports backup for all Microsoft 365 instances, such as Exchange Online, OneDrive, SharePoint Online, Microsoft 365 Groups, Teams, Microsoft Teams Chat, Project Online, Public Folders, Viva Engage, Power BI, Power Automate, and Power Apps to protect your data.

Once the backup is enabled, IBM® Storage Protect for Cloud will perform a full backup to cover all contents within the backup scope. Subsequent incremental backups will follow the configured frequency to capture changes based on the corresponding timestamps.

> **Note:** IBM cannot guarantee the completion of four backups per day, even if the backup frequency is set to four times daily. Various factors, such as data size, can impact job performance and are beyond our control. If a scheduled backup is due to start but the previous one is still in progress, the new job will be skipped.

For site collections (of SharePoint Online, Microsoft 365 Groups, Teams, or Viva Engage), the hybrid mode is now provided. In the hybrid mode, IBM® Storage Protect for Cloud Microsoft™ 365 jobs will, by default, use an app profile in backup and restore. For the data types that are unsupported in the app context, service account authentication will be used automatically. Note that the use of service accounts is not the recommended method as it attracts an increased potential for throttling issues. To learn more and enable the mode, contact the IBM Software Support team.

For the authentication method and permission requirements for Auto Discovery and Backup & Restore, continue with the following instructions.

Exchange Online

To protect Exchange Online mailboxes with IBM® Storage Protect for Cloud, ensure you have at least one of the following apps configured for your tenant for the Auto discovery and data protection:

- IBM® Storage Protect for Cloud Microsoft™ 365 (Exchange Online) service app.
- Microsoft 365 default app with at least the Exchange Online permissions.
- Custom app profile with the required permissions.
  For details on creating an app profile, refer to . For the app permissions, refer to "Required Permissions of Microsoft 365 App Profile" on page 58.

Note the following for Exchange Online service using IBM® Storage Protect for Cloud:

- You can now choose to protect the **Recoverable Items** folder in the user's primary mailbox for the Exchange Online service. If you want to enable this feature, contact IBM Software Support for assistance. Note that an additional cost is required. Currently, we only support the **Deletions**, **Purges**, **Versions**, and **DiscoveryHolders** subfolder in the **Recoverable Items**. For more information about Recoverable Items, refer to this Microsoft article: Recoverable Items folder in Exchange Online. On the backup data tree, you can find the data in the following directory: `mailbox address/Recoverable Items folder (System)/`. This folder cannot be a destination for an out of place restore, and the backup data of this folder being restored to its original mailbox will use the following name: **Recovery**

Items folder (System) _ Restored. Note that due to the API limitation, this folder directory will always be displayed in English regardless of the preferred display language of Microsoft 365.

- The hidden folders in the mailboxes (including Exchange Online mailboxes, Group mailboxes, and Teams group mailboxes) will be excluded from the backup for better performance. If you want to include the hidden folders in your backup, contact IBM Software Support for assistance.
- By default, the **Deleted Items** folder and the **Junk Emails** folder will be excluded from the backup for better performance. If you want to include the folders in your backup, contact IBM Software Support for assistance
- In Manage Scan Profiles, you can select the option to scan the **In-Place Archived Mailboxes** using the app profile. By default, the **Scan in-place archived mailboxes** option is deselected, as there may be performance issues due to API limitations.
  Even though you use Service Account Authentication to scan and register this type of mailbox, with hybrid approaches applied for the backup and restore of Exchange Online, IBM® Storage Protect for Cloud Microsoft™ 365 can back up and restore this type of mailbox via app profile.
- If you would like to filter the folders to protect for **Exchange Online** or **OneDrive** service, or filter the folders or lists/libraries within the site collections of **SharePoint Online** service, **Project Online** services, **Microsoft 365 Groups** services, or **Teams** service, you can contact the IBM Software Support for assistance. Note that if your subscription to IBM® Storage Protect for Cloud Microsoft™ 365 is based on the protected data size, the total consumed data size in your subscription will not be affected by the filter policy. IBM will not exclude the size of the filtered items from the total consumed data size.
- Use Object ID instead of mailbox address as the unique identifier for Exchange Online mailboxes and Public Folders. This change has been made to the IBM® Storage Protect for Cloud Microsoft™ 365 service. Due to this change, the mailboxes that have been re-created with the same address will no longer be regarded as the same one. This might require a broader search to ensure you find all the backup data for restoring, exporting, or deleting, the mailbox being renamed can only be found by the new name with the former backup data associated, and its former name will be displayed in its row.
- The Exchange Online service does not support protecting the **Search Folders**.

After your app profile is ready, navigate to **Auto Discovery** in the IBM® Storage Protect for Cloud interface to configure a scan profile for the **Exchange Online mailboxes** that you want to protect in IBM® Storage Protect for Cloud Microsoft™ 365. For details, refer to Auto Discovery for Microsoft 365.

Then, you can navigate to the IBM® Storage Protect for Cloud Microsoft™ 365 interface to enable the backup service of Exchange Online after the Auto Discovery scan job completes.

- Refer to “Set Up the Backup Wizard” on page 39 for details, if this is your first time signing into IBM® Storage Protect for Cloud Microsoft™ 365.
- To enable and manage a backup service, refer to the following instructions:
  - “Monitor and Manage Your Backup” on page 67
  - “Change the Backup Scope” on page 70
  - “Change the Backup Frequency” on page 71
  - “Configure Backup Settings” on page 87
  - “Configure Notifications” on page 68
  - “Disable a Backup” on page 72

SharePoint Online

To protect SharePoint Online site collections with IBM® Storage Protect for Cloud, you must have at least one of the following apps configured for your tenant for Auto discovery and data protection:

- IBM® Storage Protect for Cloud Microsoft™ 365 (SharePoint Online) service app
- Microsoft 365 default app with at least the SharePoint Online permissions
- Custom Azure app with the required permissions

For details on creating an app profile, refer to Create an App Profile. For the app permissions, refer to Required Permissions of Microsoft 365 App Profile.

Note the following for the SharePoint Online service:

- The hidden lists in SharePoint sites (including SharePoint Online sites, Teams team sites, Group team sites, Viva Engage community sites, and Project Online sites) are now excluded from the backup scope for better performance. If you want to include the hidden lists in your backup, contact IBM Software Support for assistance. For the hidden lists that you can include in the backup, refer to "Hidden Lists" on page 199.
- If a SharePoint site is connected to a Microsoft 365 Group (a groupified site), IBM® Storage Protect for Cloud will keep it in both the **SharePoint Sites** container and the **Microsoft 365 Groups** container. IBM® Storage Protect for Cloud Microsoft™ 365 will protect this site in the corresponding container separately as you selected.
- It is possible to change the SharePoint domain name for your organization in Microsoft 365 as introduced in the Microsoft article: Rename your SharePoint domain. This change affects only the SharePoint and OneDrive URLs. It doesn't impact email addresses. After the domain name is changed and updated into Auto Discovery, IBM® Storage Protect for Cloud Microsoft™ 365 will run a full backup for SharePoint Online sites and OneDrive objects with new URLs.
- If you would like to filter the folders to protect for **OneDrive** service or **Exchange Online** service, or filter the folders or lists/libraries within the site collections of **SharePoint Online** service, **Project Online** services, **Microsoft 365 Groups** services, or **Teams** service, you can contact the IBM Software Support for assistance. Note that if your subscription to IBM® Storage Protect for Cloud Microsoft™ 365 is based on the protected data size, the total consumed data size in your subscription will not be affected by the filter policy. IBM will not exclude the size of the filtered items from the total consumed data size.
- IBM® Storage Protect for Cloud Microsoft™ 365 for SharePoint Online also supports protecting **Communication Sites**. When restoring a deleted Communication Site to its original location, IBM® Storage Protect for Cloud Microsoft™ 365 supports restoring the custom design of the Communication Site in the backup. If the Communication Site is registered through App Profile, the Communication Site can only be restored with the default design. Note that the comments in Communication Sites are not currently supported.
- As the locked site collections are inaccessible, the backup job will check the lock status and skip backing up the locked site collections, which will be recorded in the job report; For read-only site collections, only the full backup job that runs once every year will back them up. Since no changes can be made to read-only site collections, the incremental backup jobs will skip them.
- The files in the SharePoint site and the mailbox items in Exchange Online that are applied with the labels created via **AIP (Azure Information Protection)** can be protected by IBM® Storage Protect for Cloud Microsoft™ 365, as well as the applied Label. The documents applied with the sensitivity labels of DKE (Double Key Encryption) are also supported, but only the user who has permission can access them.
- By default, the **Preservation Hold** library is not protected by IBM® Storage Protect for Cloud Microsoft™ 365. An additional cost is required to enable the feature. You can contact IBM Software Support to enable the protection for the **Preservation Hold** library.
- As Microsoft API has a 2 GB size limit to download **OneNote notebooks** saved in OneDrive or SharePoint, backup jobs will skip the OneNote files that are larger than 2 GB. In addition, due to API limitations, IBM® Storage Protect for Cloud Microsoft™ 365 cannot protect the history versions of OneNote files.

After your authentication method is ready, navigate to **Auto Discovery** in the IBM® Storage Protect for Cloud interface to configure a scan profile for the **SharePoint Online site collections** that you want to protect in IBM® Storage Protect for Cloud Microsoft™ 365. For details, refer to Auto Discovery for Microsoft 365.

Then, you can navigate to the IBM® Storage Protect for Cloud Microsoft™ 365 interface to enable the backup service after the Auto Discovery scan job completes.

- Refer to "Set Up the Backup Wizard" on page 39 for details, if this is your first time signing into IBM® Storage Protect for Cloud Microsoft™ 365.
- To enable and manage a backup service, refer to the following instructions:
  - "Monitor and Manage Your Backup" on page 67
  - "Change the Backup Scope" on page 70
  - "Change the Backup Frequency" on page 71
  - "Configure Backup Settings" on page 87
  - "Configure Notifications" on page 68

    - “Disable a Backup” on page 72

OneDrive

To protect OneDrive with IBM® Storage Protect for Cloud, you must have at least one of the following apps configured for your tenant for auto discovery and data protection:

- IBM® Storage Protect for Cloud Microsoft™ 365 (SharePoint Online) service app
- Microsoft 365 default app with at least the SharePoint Online permissions
- Custom Azure app with the required permissions
- For details on creating an app profile, refer to App Profile for Microsoft 365 or “Required Permissions of Microsoft 365 App Profile” on page 58.

Note the following for the OneDrive service:

- Backup for OneDrive now uses Microsoft Graph API for improved performance. Graph API has been more focused on protecting OneDrive content, and it has some limitations, such as it cannot protect the file versions. The file version number cannot be kept either after being restored to the destination. The restored file will use version: **1.0**. You can refer to “OneDrive Data Types” on page 247 for additional details. If you require any additional assistance, contact IBM Software Support.
- IBM® Storage Protect for Cloud Microsoft™ 365 for OneDrive will protect the **Documents** library and protect the **Site Assets** library if the site feature **Site NoteBook** is activated. The service only protects content and permissions for OneDrive since OneDrive is the cloud service used to securely store, share, and access your files.
- As Microsoft API has a 2 GB size limit to download OneNote notebooks saved in OneDrive or SharePoint, backup jobs will skip the OneNote files that are larger than 2 GB. In addition, due to API limitations, IBM® Storage Protect for Cloud Microsoft™ 365 cannot protect the history versions of OneNote files.
- If there are security changes but no changes on the content in the sites, the scheduled incremental backup jobs will not back up the securities. Moving forward, the changes on the securities in the sites (including the SharePoint Online sites, OneDrive , and Microsoft 365 Groups/Teams team sites) that have not yet been backed up, in this case, will be included in an incremental backup once a week.
  If some items in a site encounter errors in a backup but there are no changes on the content in the site for the next backup, the scheduled incremental backup jobs will not back up these items with errors. Moving forward, they will be included in an incremental backup once a week.
- If you would like to filter the folders to protect for **OneDrive** service or **Exchange Online** service, or filter the folders or lists/libraries within the site collections of **SharePoint Online** service, **Project Online** services, **Microsoft 365 Groups** services, or **Teams** service, you can contact the IBM Software Support for assistance. Note that if your subscription to IBM® Storage Protect for Cloud Microsoft™ 365 is based on the protected data size, the total consumed data size in your subscription will not be affected by the filter policy. IBM will not exclude the size of the filtered items from the total consumed data size.
- IBM® Storage Protect for Cloud Auto discovery now supports including orphaned OneDrive in scan profiles of OneDrive but the objects cannot be synchronized to IBM® Storage Protect for Cloud Microsoft™ 365.

After your app profile is ready, navigate to the **Auto discovery** in IBM® Storage Protect for Cloud interface to configure a scan profile for the **OneDrive users** that you want to protect in IBM® Storage Protect for Cloud Microsoft™ 365. For details, refer to Auto Discovery for Microsoft 365.

Then, you can navigate to IBM® Storage Protect for Cloud Microsoft™ 365 interface to enable the backup service of OneDrive after the Auto Discovery scan job completes.

- Refer to “Set Up the Backup Wizard” on page 39 for details, if this is your first time signing into IBM® Storage Protect for Cloud Microsoft™ 365.
- To enable and manage a backup service, refer to the following instructions:
    - “Monitor and Manage Your Backup” on page 67
    - “Change the Backup Scope” on page 70
    - “Change the Backup Frequency” on page 71
    - “Configure Backup Settings” on page 87
    - “Configure Notifications” on page 68

    - “Disable a Backup” on page 72

Microsoft 365 Groups

Microsoft 365 Groups service will protect the group team site, group mailbox, and the planner data.

For a detailed list of data types supported and unsupported by IBM® Storage Protect for Cloud Microsoft™ 365, refer to “Microsoft 365 Groups Data Types” on page 225.

For Auto discovery and data protection of Microsoft 365 Groups, you must have at least one of the following apps configured for your tenant:

- IBM® Storage Protect for Cloud Microsoft™ 365 (All permissions) service app
- Microsoft 365 default app with all permissions
- Custom Azure app with the required permissions

For details on creating an app profile, refer to Create an App Profile. For the app permissions, refer to Required Permissions of Microsoft 365 App Profile.

If you are using a **Multi-geo** tenant, ensure the app profile has the Exchange Administrator role. This role is required to restore the region information for Microsoft 365 Groups and Teams. Otherwise, your group or team backed up from a specific region will be restored to the default region. For details on how to assign the role to an app, refer to How to Assign the Exchange Administrator Role to an App.

Before you perform the Auto Discovery scan job for Microsoft 365 Groups, consider the following for your own condition:

- If a SharePoint site is connected to a Microsoft 365 Group (a groupified site), IBM® Storage Protect for Cloud will keep it in both the **SharePoint Sites** container and the **Microsoft 365 Groups** container. IBM® Storage Protect for Cloud Microsoft™ 365 will protect this site in the corresponding container separately, as selected.
- The hidden folders in the mailboxes (including Exchange Online mailboxes, Group mailboxes, and Teams group mailboxes) will be excluded from the backup for better performance. If you want to include the hidden folders in your backup, contact IBM support for assistance.

After your authentication method is ready, navigate to **Auto Discovery** in the IBM® Storage Protect for Cloud interface to configure a scan profile for the **Microsoft 365 Groups** that you want to protect in IBM® Storage Protect for Cloud Microsoft™ 365. For details, refer to .

Then, you can navigate to IBM® Storage Protect for Cloud Microsoft™ 365 interface to enable the backup service after the Auto Discovery scan job completes.

- Refer to “Set Up the Backup Wizard” on page 39 for details, if this is your first time signing into IBM® Storage Protect for Cloud Microsoft™ 365.
- To enable and manage a backup service, refer to the following instructions:
    - “Monitor and Manage Your Backup” on page 67
    - “Change the Backup Scope” on page 70
    - “Change the Backup Frequency” on page 71
    - “Configure Backup Settings” on page 87
    - “Configure Notifications” on page 68
    - “Disable a Backup” on page 72

Teams

Teams service can protect all the Teams channels, Teams settings and permissions, channel conversations and files, primary team site, private or shared channel sites, planner data, etc.

For a full list of the supported data types, refer to “Teams Data Types” on page 229. To protect Teams mailboxes, at least one owner/member in the team should have the Exchange Online product license.

The Teams service is now available for customers using Microsoft 365 operated by 21Vianet in China. Note that hosted content is unsupported and will be skipped in the backup.

For Auto discovery and data protection of Microsoft 365 Teams, you must have at least one of the following apps configured for your tenant:

- IBM® Storage Protect for Cloud Microsoft™ 365 (All permissions) service app
- Microsoft 365 default app with all permissions
- Custom Azure app with the required permissions

For details on creating an app profile, refer to App Profile for Microsoft 365 or .

If you are using a Multi-geo tenant, ensure the app profile has the Exchange Administrator role. This role is required to restore the region information for Microsoft 365 Groups and Teams. Otherwise, your group or team backed up from a specific region will be restored to the default region. For details on how to assign the role to an app, refer to How to Assign the Exchange Administrator Role to an App.

After your authentication method is ready, navigate to the **Auto Discovery** in IBM® Storage Protect for Cloud interface to configure a scan profile for the **Teams** that you want to protect in IBM® Storage Protect for Cloud Microsoft™ 365. For details, refer to Auto Discovery for Microsoft 365.

Then, you can navigate to IBM® Storage Protect for Cloud Microsoft™ 365 interface to enable the backup service after the Auto Discovery scan job completes.

- Refer to "Set Up the Backup Wizard" on page 39 for details, if this is your first time signing into IBM® Storage Protect for Cloud Microsoft™ 365.
- To enable and manage a backup service, refer to the following instructions:
  - "Monitor and Manage Your Backup" on page 67
  - "Change the Backup Scope" on page 70
  - "Change the Backup Frequency" on page 71
  - "Configure Backup Settings" on page 87
  - "Configure Notifications" on page 68
  - "Disable a Backup" on page 72

Teams Chat

The Teams Chat service can protect 1:1 chats and group chats in Teams.

For the **default Microsoft Graph API**, the backup of chats started by external users is not supported, but chats started by internal users and including external users can be protected. For the **Teams Export API model B**, only plain text can be protected.

Follow the steps to enable the Teams Chat backup:

1. Configure a **custom app profile** in the IBM® Storage Protect for Cloud interface and add required permissions to it. Teams Chat service only supports using **Custom app profile** authentication. For details on how to create a custom app, refer to Create a Custom Azure App. For details on the required permissions for a custom app, refer to Required Permissions of Microsoft 365 App Profile Authentication.
2. Navigate to **Auto Discovery** in the IBM® Storage Protect for Cloud interface to configure a scan profile for the **Microsoft 365 Users** that you want to protect in IBM® Storage Protect for Cloud Microsoft™ 365 after your app profile is ready. For details, refer to Auto Discovery for Microsoft 365.
3. Go to the IBM® Storage Protect for Cloud Microsoft™ 365 interface to enable the backup service after the Auto Discovery scan job completes.

Note the following:

- To protect the Teams chats, you must have access to the default Microsoft Graph API or Microsoft Graph Teams Export API. Note that starting May 18, 2023, the online form and the protected API approval process are no longer needed. You can call the protected APIs as long as the requirements for accessing without a user (https://learn.microsoft.com/en-us/graph/auth-v2-service) are met. Since the API requires payment for use, you must follow the steps described in Enable metered Microsoft 365 APIs and servicesto set up an active Azure subscription for your application for billing purposes.
- Microsoft Teams Chat service in IBM® Storage Protect for Cloud Microsoft™ 365 supports using the **default Microsoft Graph API** or **Microsoft GraphTeams Export API model B** to retrieve Teams chat messages from

Microsoft Teams Chat for backup. Note that the Export API model B will charge the app creator $ 0.00075 per message and that it may cost a lot if you have a large scale of chat messages to protect. You can follow this Microsoft article to estimate the number of Teams chat messages that may be backed up.

- The number of messages in the M365 Admin Center is just for the specific duration you define when exporting the report, not the full total amount. Additionally, the Microsoft Export API only supports export at a user level, so if there is a group chat with multiple users, the same message will be exported multiple times if all these users are included in the scope, which means the number of messages which will be backed up by IBM® Storage Protect for Cloud has the potential to be higher than the number of messages in the Microsoft admin center report. For confirmation, you can check the job report after the job has finished for the backup chat messages count to compare with the bill from Microsoft. If necessary, you can also limit the user scope for the export.
- Here is an example: In the report in the Microsoft 365 admin center shows the last 180 days' number of Teams chat messages are 1000. Then for the whole year, the number of messages will be approximately 2000. Because there is no deduplication logic for the Microsoft 365 export API, the same message will be exported multiple times if all these users are included in the scope. So let's say that all are 1V1 chats, then the message number charge by export API will be doubled to approximately 4000 messages. If most of chats are group chats with multiple users, the cost will be even higher.
- Only the default Microsoft Graph API can be used to protect Teams Chat in GCC environments.
- The group chat messages cannot be protected if the user has been removed from the group.
- For additional details on the supported data types, refer to Teams Chat Data Types. Note that it may cost a lot if there are a large number of chat messages in your tenant.
- For details about the format and content of exported Teams Chat messages, refer to the FAQ: What will the exported Teams Chat messages be like

For more information:

- Refer to "Set Up the Backup Wizard" on page 39 for details, if this is your first time signing into IBM® Storage Protect for Cloud Microsoft™ 365.
- To enable and manage a backup service, refer to the following instructions:
  - "Monitor and Manage Your Backup" on page 67
  - "Change the Backup Scope" on page 70
  - "Change the Backup Frequency" on page 71
  - "Configure Backup Settings" on page 87
  - "Configure Notifications" on page 68
  - "Disable a Backup" on page 72

Project Online

Project Online service cannot protect the **Project for the web** data and cannot fully support the data added through Microsoft 365 subscription Project Online desktop client. For example, custom fields.

If you would like to filter the folders within the site collections of **Project Online** services, you can contact IBM Software Support for assistance. Note that if your subscription to IBM® Storage Protect for Cloud Microsoft™ 365 is based on the protected data size, the total consumed data size in your subscription will not be affected by the filter policy. IBM will not exclude the size of the filtered items from the total consumed data size.

You can now use an app profile to scan the Project Online site collections. In this way, the service account does not require the Site Collection Administrator role. However, the Project Online data cannot be protected in the app context (using app profile authentication). Therefore, a service account with enough permissions is still required for the backup and restore for Project Online. For the required permissions of a service account, refer to Service Account Authentication.

Once the app profile and the service account is ready, you can navigate to the **Auto discovery** page to create a scan profile for Project Online site collections. After the Auto discovery scan job is completed, you can go to IBM® Storage Protect for Cloud Microsoft™ 365 interface to enable the backup service.

- Refer to "Set Up the Backup Wizard" on page 39 for details, if this is your first time signing into IBM® Storage Protect for Cloud Microsoft™ 365.

- To enable and manage a backup service, refer to the following instructions:
  - “Monitor and Manage Your Backup” on page 67
  - “Change the Backup Scope” on page 70
  - “Change the Backup Frequency” on page 71
  - “Configure Backup Settings” on page 87
  - “Configure Notifications” on page 68
  - “Disable a Backup” on page 72

Public Folder

The service for Public Folders only supports restoring content and permissions of Public Folder to the original location and you must use impersonation accounts to protect the Public Folder data..

IBM® Storage Protect for Cloud Microsoft™ 365 now supports the backup of Public Folder metadata via the app profile authentication. To protect Public Folder metadata, ensure your backup for Public Folder metadata is enabled and the **Exchange Administrator** role is assigned to the app in Microsoft Entra ID.

The Public Folders backup will perform operations by using the permissions that are associated with the impersonation accounts. To configure impersonation accounts, refer to Configure Backup Settings. We recommend a 1:500 ratio for the impersonation accounts and the Public Folders. For more information about impersonation technology, see Impersonation and EWS in Exchange. The impersonation accounts configured must meet the following conditions:

- The impersonation account must have the Exchange Online product license.
- This user must also have the **Owner** permission to the Public Folders.

If you have configured impersonation accounts for Public Folder in the IBM® Storage Protect for Cloud interface, the impersonation accounts will be synchronized to IBM® Storage Protect for Cloud Microsoft™ 365 after June 2023 release. You can check and configure the impersonation accounts through **Settings** > **Backup** page on the IBM® Storage Protect for Cloud Microsoft™ 365 interface.

For the Auto discovery of Public Folders, ensure you have at least one of the following apps configured for your tenant:

- IBM® Storage Protect for Cloud Microsoft™ 365 (Exchange Online) service app
- Microsoft 365 default app with at least the Exchange Online permissions
- Custom app profile with the required permissions.

For details on creating an app profile, refer to *Create an App Profile* in IBM® Documentation. For the app permissions, refer to“Required Permissions of Microsoft 365 App Profile” on page 58.

For details on creating and managing service account profile, refer to Manage Service Account Profiles.

Note the following for the Public Folder service:

- Use Object ID instead of mailbox address as the unique identifier for Exchange Online mailboxes and Public Folders. This change has been made to the IBM® Storage Protect for Cloud Microsoft™ 365. Due to this change, the mailboxes that have been re-created with the same address will no longer be regarded as the same one. This might require a broader search to ensure you find all the backup data for restoring, exporting, or deleting; the mailbox being renamed can only be found by the new name with the former backup data associated, and its former name will be displayed in its row.
- For subscriptions with Multi-Geo enabled, the public folders can only be protected in the Central Location.

After your app profile is ready, navigate to the **Auto Discovery** in IBM® Storage Protect for Cloud interface to configure a scan profile for the **Public Folders** that you want to protect in IBM® Storage Protect for Cloud Microsoft™ 365. For details, refer to Auto Discovery for Microsoft 365.

Then, you can navigate to IBM® Storage Protect for Cloud Microsoft™ 365 interface to enable the backup service after the Auto Discovery scan job completes.

- Refer to “Set Up the Backup Wizard” on page 39 for details, if this is your first time signing into IBM® Storage Protect for Cloud Microsoft™ 365.
- To enable and manage a backup service, refer to the following instructions:

  - “Monitor and Manage Your Backup” on page 67
  - “Change the Backup Scope” on page 70
  - “Change the Backup Frequency” on page 71
  - “Configure Backup Settings” on page 87
  - “Configure Notifications” on page 68
  - “Disable a Backup” on page 72

Viva Engage

For the Auto discovery of Viva Engage communities, you must have at least one of the following app configurations. For details on creating an app profile, refer to Create an App Profile.

- Microsoft 365 app (All permissions) or IBM® Storage Protect for Cloud Microsoft™ 365 app (All permissions), and the Viva Engage app.
  - For the required permissions for the Microsoft 365 app For the app permissions, refer to Required Permissions of Microsoft 365 App Profile.
  - For the required permissions for the Viva Engage app, refer to Required Permissions of Viva Engage App.
    When consenting to the Viva Engage app profile, the consent user must be a **Microsoft 365 Global Administrator** with the Viva Engage product license. To re-authorize the Viva Engage app, the authentication user of this Viva Engage app must have the **Verified Admin** role and the **Yammer administrator** role with the Viva Engage product license. IBM® Storage Protect for Cloud will use the Viva Engage app for the backup and restore.
- Custom Azure app with delegated permissions.
  For minimum API permissions that you must grant to the app, refer to Required Permissions of Viva Engage App

After your authentication method is ready, navigate to the **Auto Discovery** in IBM® Storage Protect for Cloud interface to configure a scan profile for the **Viva Engage communities** that you want to protect in IBM® Storage Protect for Cloud Microsoft™ 365. For details, refer to .

Note the following for the Viva Engage service:

- If you have Microsoft 365 connected Viva Engage communities protected under Microsoft 365 Groups service, once the Viva Engage service is enabled, the connected groups will be removed from Microsoft 365 Groups service and can only be protected in Viva Engage even if you disable the Viva Engage service again. IBM® Storage Protect for Cloud job will start a new backup cycle for these Viva Engage communities, but their former backup data as Microsoft Groups will not be deleted until the data expires retention period. Then, you can navigate to IBM® Storage Protect for Cloud Microsoft™ 365 interface to enable the backup service after the Auto Discovery scan job completes.
- Refer to “Set Up the Backup Wizard” on page 39 for details, if this is your first time signing into IBM® Storage Protect for Cloud Microsoft™ 365.
- To enable and manage a backup service, refer to the following instructions:
  - “Monitor and Manage Your Backup” on page 67
  - “Change the Backup Scope” on page 70
  - “Change the Backup Frequency” on page 71
  - “Configure Backup Settings” on page 87
  - “Configure Notifications” on page 68
  - “Disable a Backup” on page 72

Power BI

Power BI service can only protect the Power BI content in the new workspace experience. (The personal workspace is the classic workspace, which is not supported.)

To use IBM® Storage Protect for Cloud Microsoft™ 365 to protect the Power BI data, you must configure an app profile for the Microsoft Delegated app or a custom Azure app with delegated permissions.

> **Note:** If you have been using a scan profile with service account authentication for Power Platform object types, the Auto discovery scan jobs and the IBM® Storage Protect for Cloud jobs can continue using the service account authentication.

- For the list of the required permissions added to the Delegated app for Power BI, refer to "App Profile Authentication" on page 57.
- If you use service account authentication or the Delegated app to protect the Power BI data, the service account or the authentication user of the Delegated app must have a **Power BI Pro** license or a **Premium Per User** license and have the **Fabric Administrator** role (the former Power BI admin role).

Before you enable the Power BI service, ensure the Download reports feature in the tenant settings has been enabled. This feature was enabled by default.

Note the following for Power BI service.

- If you use the service account authentication to protect Power BI data or use the Delegated app to scan Power BI workspaces in IBM® Storage Protect for Cloud Microsoft™ 365, the Auto Discovery scan job will automatically add the service account or the authentication user of the Delegated app as the workspace admin.
- Power BI service can now only protect the .pbix Power BI files that can be downloaded. For the limitations on downloading report from Power BI, refer to Limitations when downloading a report .pbix file. The exported .pbix file includes both the report you're downloading and the dataset (the data on which the report is based), the same as the "A copy of the report and data" download mode in Power BI. If a Power BI report is created using data from Dataverse, neither the report nor the data in Dataverse will be protected.
- Due to an API limitation, the backup job of Power BI can back up at most 200 workspaces per hour.
- Power BI service can now protect Power BI reports larger than 1 GB.

After your authentication method is ready, navigate to the **Auto Discovery** in IBM® Storage Protect for Cloud interface to configure a scan profile for the **Power BI workspaces** that you want to protect in IBM® Storage Protect for Cloud Microsoft™ 365Cloud Backup for Microsoft 365. For details, refer to Auto Discovery for Microsoft 365.

Then, you can navigate to IBM® Storage Protect for Cloud Microsoft™ 365 interface to enable the backup service after the Auto Discovery scan job completes.

- Refer to "Set Up the Backup Wizard" on page 39 for details, if this is your first time signing into IBM® Storage Protect for Cloud Microsoft™ 365.
- To enable and manage a backup service, refer to the following instructions:
  - "Monitor and Manage Your Backup" on page 67
  - "Change the Backup Scope" on page 70
  - "Change the Backup Frequency" on page 71
  - "Configure Backup Settings" on page 87
  - "Configure Notifications" on page 68
  - "Disable a Backup" on page 72

Power Automate

Power Automate service can only protect the cloud flows.

For subscriptions with Multi-Geo enabled, flows can only be protected in the Central IBM® Storage Protect for Cloud Location due to API limitations.

To use IBM® Storage Protect for Cloud Microsoft™ 365 to protect the Power Automate flow data, you must configure an app profile for the Microsoft Delegated app or a custom Azure app with delegated permissions.

> **Note:** If you have been using a scan profile with service account authentication for Power Platform object types, the Auto discovery scan jobs and the IBM® Storage Protect for Cloud jobs can continue using the service account authentication.

- For the list of the required permissions added to the Delegated app for Power Automate, refer to Required Permissions of Microsoft Delegated App.
- If you use the Delegated app to protect the Power Automate data, the authentication user of the Delegated app must have the **Global Administrator** and the **Environment Admin/System Administrator** role. If you use service account authentication to protect the Power Automate data, the service account must be the **Global Administrator**.

  > **Note:** The backup job will automatically add the service account or the authentication user of the Delegated app (the user who consents the app permissions) as the flow owner. Due to the Microsoft native logic, after the authentication user is added as the flow owner, the corresponding flows will be listed under the **My flows** > **Shared with me** tab for the existing flow owners.

After your authentication method is ready, navigate to the **Auto Discovery** in IBM® Storage Protect for Cloud interface to configure a scan profile for the **Power Automate flows** that you want to protect in IBM® Storage Protect for Cloud Microsoft™ 365. For details, refer to Auto Discovery for Microsoft 365.

Then, you can navigate to IBM® Storage Protect for Cloud Microsoft™ 365 interface to enable the backup service after the Auto Discovery scan job completes.

- Refer to “Set Up the Backup Wizard” on page 39 for details, if this is your first time signing into IBM® Storage Protect for Cloud Microsoft™ 365.
- To enable and manage a backup service, refer to the following instructions:
  - “Monitor and Manage Your Backup” on page 67
  - “Change the Backup Scope” on page 70
  - “Change the Backup Frequency” on page 71
  - “Configure Backup Settings” on page 87
  - “Configure Notifications” on page 68
  - “Disable a Backup” on page 72

Power® Apps

Power Apps service can only standard protect Canvas apps which have been published and component libraries.

For subscriptions with Multi-Geo enabled, flows can only be protected in the Central IBM® Storage Protect for Cloud Location due to API limitations.

To use IBM® Storage Protect for Cloud Microsoft™ 365 to protect the Power Apps data, you must configure an app profile for the Microsoft Delegated app or a custom Azure app with delegated permissions.

> **Note:** If you have been using a scan profile with service account authentication for Power® Platform object types, the Auto discovery scan jobs and the IBM® Storage Protect for Cloud jobs can continue using the service account authentication.
>
> - For the list of the required permissions added to the Delegated app for Power® Apps, refer to the “Required Permissions of Microsoft 365 App Profile” on page 58.
> - If you use service account authentication or the Delegated app to protect the Power Apps data, the service account or the authentication user of the Delegated app must be the **Global Administrator**

> and the **Environment Admin/System Administrator**, and have the **Power Apps for Microsoft 365** license to proceed.
>
> > **Note:** The backup job will automatically add the service account or the authentication user of the Delegated app as the apps' co-owner and flow owner (if the app has an associated flow).

After your authentication method is ready, navigate to **Auto Discovery** in the IBM® Storage Protect for Cloud interface to configure a scan profile for the **standard Canvas apps and component libraries** in **Power Apps** that you want to protect in IBM® Storage Protect for Cloud Microsoft™ 365. For details, refer to .

Then, you can navigate to the IBM® Storage Protect for Cloud Microsoft™ 365 interface to enable the backup service after the Auto Discovery scan job completes.

- Refer to Set Up the Backup Wizard for details, if this is your first time signing into IBM® Storage Protect for Cloud Microsoft™ 365.
- To enable and manage a backup service, refer to the following instructions:
  - "Monitor and Manage Your Backup" on page 67
  - "Change the Backup Scope" on page 70
  - "Change the Backup Frequency" on page 71
  - "Configure Backup Settings" on page 87
  - "Configure Notifications" on page 68
  - "Disable a Backup" on page 72

Configure Auto Discovery

Prior to running backup jobs in IBM® Storage Protect for Cloud Microsoft™ 365, you must register the objects below that you want to protect in the **Auto Discovery** of IBM® Storage Protect for Cloud.

- Exchange Online mailboxes
- OneDrive
- SharePoint Online site collections
- Microsoft™ 365 Groups/Microsoft Teams/Viva Engage Community
- Project Online site collections
- Exchange Online public folders (For subscriptions with Multi-Geo enabled, the public folders can only be protected in the Central IBM® Storage Protect for Cloud Location)
- Microsoft 365 Users
- Power BI workspaces
- Power Automate flows
- Power Apps (standard Canvas apps and component libraries)

To increase security for your Microsoft™ 365 tenant and avoid throttling during your backup jobs, IBM® Storage Protect for Cloud recommends using an app profile for Microsoft™ 365 in Auto Discovery and data protection. For more information on the app profile, Auto Discovery, and how to set up an Auto Discovery Profile, refer to the Auto Discovery for Microsoft 365

The backup services in IBM® Storage Protect for Cloud Microsoft™ 365 support the following app profiles:

> **Note:** If you do not have service apps configured, the Auto Discovery scan jobs and IBM® Storage Protect for Cloud jobs will use the default Microsoft 365 app or the custom Azure app with the required permissions.

Backup Service	Service App (Modern Mode)	Default App (Classic Mode)	Custom App (Custom Mode)
SharePoint Online	IBM® Storage Protect for Cloud Microsoft™ 365 (SharePoint Online) IBM® Storage Protect for Cloud Microsoft™ 365 (All permissions)	Microsoft 365 (All permissions)	Azure App
OneDrive	IBM® Storage Protect for Cloud Microsoft™ 365 (SharePoint Online) IBM® Storage Protect for Cloud Microsoft™ 365 (All permissions)	Microsoft 365 App (All permissions)	Azure App
Project Online	IBM® Storage Protect for Cloud Microsoft™ 365 (SharePoint Online) IBM® Storage Protect for Cloud Microsoft™ 365 (All permissions)	Microsoft 365 App (All permissions)	Azure App

Exchange Online	IBM® Storage Protect for Cloud Microsoft™ 365 (Exchange Online) IBM® Storage Protect for Cloud Microsoft™ 365 (All permissions)	Microsoft 365 App (All permissions)	Azure App
Public Folders	IBM® Storage Protect for Cloud Microsoft™ 365 (Exchange Online) IBM® Storage Protect for Cloud Microsoft™ 365 (All permissions)	Microsoft 365 App (All permissions)	Azure App
Microsoft 365 Groups	IBM® Storage Protect for Cloud Microsoft™ 365 (All permissions)	Microsoft 365 App (All permissions)	Azure App
Teams	IBM® Storage Protect for Cloud Microsoft™ 365 (All permissions)	Microsoft 365 App (All permissions)	Azure App
Teams Chat	×	×	Azure App
Viva Engage	Viva Engage App	Viva Engage App	Via Engage App
Power BI	IBM® Storage Protect for Cloud Microsoft™ 365 delegated app	Delegated App	×
Power Automate	IBM® Storage Protect for Cloud Microsoft™ 365 delegated app	Delegated App	×
Power Apps	IBM® Storage Protect for Cloud Microsoft™ 365 delegated app	Delegated App	×

Authentications in Auto Discovery and Backup

The Auto Discovery in IBM® Storage Protect for Cloud and the backup services will now use the IBM® Storage Protect for Cloud Microsoft™ 365 service apps (created through **App management** > Modern mode) first to scan and protect the objects in your tenants. If you do not have service apps, we will use the default Microsoft 365 apps or custom Azure apps with the required permissions.

Note: If you have auto discovery scan profiles using the service account authentication or using app profile authentication to scan but with a service account as an additional method, the service account can still be used to protect the data that are unsupported in the app context (using app profile authentication). For the required permissions for the service account and account pool user, refer to "Service Account Authentication (Obsolete)" on page 55. However, if you modify these scan profiles after June 2023 release, the service account authentication will be obsolete. Auto discovery scan jobs and the IBM® Storage Protect for Cloud jobs will look for the following apps for the operations:

- IBM® Storage Protect for Cloud Microsoft™ 365 service apps (For permissions authorized by default, refer to App Profile Authentication)
- Default Microsoft 365 app profile. For permissions authorized by default, refer to Microsoft 365 (App Permissions) section in App Profile Authentication.
- Custom app profile (For permissions that you must manually add, refer to the table in App Profile Authentication

Required Permissions

Refer to the sections below for the required permissions of service account, app for Microsoft 365, and the Microsoft Delegated app.

Service Account Authentication (Obsolete)

Service account authentication requires credentials of a Microsoft™ Global Administrator, SharePoint Administrator, or Exchange Administrator account and then use the credentials to scan objects in your tenant. However, SharePoint Online has a built-in throttling feature that prevents one account from processing several requests simultaneously.

After July 2023 release, if your Auto Discovery scan profiles are modified, the service account authentication method and the service account pool users will be obsolete from Auto discovery. For site collections (of SharePoint Online, Microsoft 365 Groups, Teams, or Viva Engage), the hybrid mode is now provided. In the hybrid mode, IBM® Storage Protect for Cloud Microsoft™ 365 will, by default, use an app profile in backup and restore. For the data types that are unsupported in the app context, service account authentication will be used automatically. Note that the use of service accounts is not the recommended method as it attracts an increased potential for throttling issues. To learn more and enable the mode, contact the IBM support team.

Effective March 2025, Microsoft will be retiring Role Based Access Control (RBAC) Impersonation in Exchange Online. Please note that if you are leveraging Service Account (SA) configurations across IBM® Storage Protect for Cloud Microsoft™ 365, successful completion of any scans and/or running jobs for mailbox in Exchange Online, Teams, Microsoft 365 Group, and Public Folders will be impacted.

Service account authentication requires credentials of a Microsoft Global Administrator, SharePoint Administrator, or Exchange Administrator account, and then use the credentials to scan objects in your tenant. However, SharePoint Online has a built-in throttling feature that prevents one account from processing several requests simultaneously.

The service account and configured account pool users used for Auto Discovery and backup and restore must meet the permission requirements for the corresponding service types. For details, refer to “Required Permissions of Service Account” on page 55.

Required Permissions of Service Account

When backing up and restoring the registered objects, make sure the accounts have the corresponding permissions.

Example

The required permissions involve the **SharePoint Administrator** and **Exchange Administrator** roles in Microsoft 365. For details about these roles, refer to the Microsoft article: About Microsoft 365 admin roles.

Object Types	Permissions or Roles	Notes
SharePoint Online, **Project Online**, and **OneDrive**	**SharePoint Administrator** role for object registration, backup and restore. IBM® Storage Protect for Cloud Microsoft™ 365 will automatically add this service account as the **Site Collection Administrator** for backup and restore. **Note:** The account pool users used to protect the Project Online data must have one of the following Project Online licenses: **Essentials**, **Project Plan 1**, **Project Plan 3** (formerly, **Professionals**), or **Project Plan 5** (formerly, **Premium**).	When restoring the data related to terms, the restore job will add the service account as the **Term Store Administrator** automatically, and IBM® Storage Protect for Cloud Microsoft™ 365 will use the service account to back up and restore the Managed Metadata Service.
Exchange Online mailboxes	**Exchange Administrator** role	
Public Folders	The service account must have Exchange Online license and must be the **Owner** of the Public Folder.	Accounts that have the **Publishing Editor** permission can also back up Public Folders successfully, but this permission is not enough to restore them; users with **Publishing Edito**r permission can assign **Reviewer** permission to others but cannot assign **Owner** permission to others.
Microsoft 365 Groups	The service account must have both the **SharePoint Administrator** and **Exchange Administrator** roles for protecting the Microsoft 365 Groups.	The **SharePoint Administrator** role is required for protecting the Microsoft 365 group team site; the **Exchange Administrator** role is required for protecting the Microsoft 365 group mailbox. The Auto Discovery scan job will add the service account as the **Terms Store Administrator** automatically, and IBM® Storage Protect for Cloud Microsoft™ 365 will use the service account to back up and restore the Managed Metadata Service. Other than that, the backup and restore of the Microsoft 365 group team site only requires the **Site Collection Administrator** permission.

Object Types	Permissions or Roles	Notes
Teams	The account that performs backup and restore jobs must have the Microsoft Teams product license and Exchange Online license assigned in Microsoft 365, and must be **SharePoint Online Administrator**, **Exchange Online Administrator**, **Teams admin**, and both the **owner** and **member** of the Teams that you want to protect.	For private Groups and Teams, at least one member or owner must have the Exchange Online license. To protect Teams' **Private Channel**, the service account must also be the **owner** of all the current and future private channels. The Auto Discovery scan job can now automatically add the service account as the private channel owner if the **Automatically add the service account as the owner of private channels in all scanned Teams** option is set to **Yes**. For details, refer to Manage Scan Profiles. **Note:** If you are using the hybrid approach for the backup and restore, the Private Channel's site will be protected in the app context. The **owner** role to the private channels is not required.
Viva Engage	The service account must have both the **SharePoint administrator** and **Exchange administrator** roles for protecting the Viva Engage community.	
Power BI	The service account must be a **Pro account** or a **Premium per user account** and have the Power BI admin role.	If you use service account authentication to protect Power BI data, IBM® Storage Protect for Cloud Microsoft™ 365 will automatically add this service account as the workspace admin.
Power Automate	The service account must be the environment admin/system administrator, and the Power Platform admin.	These roles are required for Auto Discovery scan and for the backup. In addition, the backup job will automatically add the service account as the flow owner.
Power Apps	The service account must be the global admin and the environment admin/system administrator.	The backup job will automatically add this service account as the app's co-owner and flow owner (if the app has an associated flow).

App Profile Authentication

App profile authentication (IBM® Storage Protect for Cloud Microsoft™ 365, default Microsoft 365 apps, or use a custom Azure app) ensures that all Auto Discovery and IBM® Storage Protect for Cloud Microsoft™ 365 jobs are tagged as the activities of that app, and also ensures that we do not need to store any service accounts and passwords, with only the consent being recorded. The consent can be monitored in your Microsoft Entra ID and can be revoked at any time.

You can consent to apps separately for the services you want to protect. If you do not have service apps, IBM® Storage Protect for Cloud will use the default Microsoft 365 app or custom Azure app to scan or protect the data.

- If you want to use IBM® Storage Protect for Cloud for **SharePoint Online**, **OneDrive**, **Exchange Online**, **Public Folders**, **Microsoft 365 Groups**, and **Teams** service in app context, you need a **IBM® Storage Protect for Cloud Microsoft™ 365** app or **Microsoft 365 app** connected to your tenant. If you use the Teams Chat service, you need to configure a custom app for **Teams Chat**.
- If you use the Viva Engage service, you need to configure the Microsoft 365 app (All permissions) or IBM® Storage Protect for Cloud app (All permissions), and the Viva Engage app. Alternatively, you can have a custom Azure app with delegated permissions.
  - For the permissions required by the Microsoft 365 app, refer to Required Permissions of Microsoft 365 App Profile.
  - For the permissions required by the Viva Engage app, as well as the minimum API permissions that you must grant to the custom app, refer to Required Permissions of Viva Engage App.
  - The authentication user for the Viva Engage app must be a **Microsoft 365 Global Administrator** with the Viva Engage product license. To re-authorize the Viva Engage app, the authentication user must have the **Verified Admin** role and the **Yammer administrator** role with the Viva Engage product license.
- If you want to use IBM® Storage Protect for Cloud for Project Online, you can use an app profile to scan the Project Online site collections. In this way, the service account does not require the Site Collection Administrator role. However, the Project Online data cannot be protected in the app context (using app profile authentication). Therefore, a service account with enough permissions is still required for the backup and restore for Project Online. For the required permissions of a service account, refer to Service Account Authentication.
- If you want to use IBM® Storage Protect for Cloud for Power BI, Power Automate, or Power Apps in app context or restore the Teams channel conversations as new posts to the channel, or restore Planner task comments, you must configure an app profile for **Microsoft Delegated** app or a custom Azure app with delegated permissions. If you want to restore the Teams channel conversations as new posts, the authentication user must have the **Teams** license.
  For the permissions required by the Microsoft Delegated app, refer to Required Permissions of Microsoft Delegated App.

> **Note:** If you are using a multi-geo tenant, ensure the app profile has the Exchange Administrator role. This role is required to restore the region information for Microsoft™ 365 Groups and Teams. Otherwise, your group or team backed up from a specific region will be restored to the default region. This known issue also exists in the service account authentication. For details on how to assign the role to an app, refer to How to Assign the Exchange Administrator Role to an App.

For the permission requirements of an app profile for a specific service type, refer to the section below.

Required Permissions of Microsoft™ 365 App Profile

Refer to the table below for the API permission requirement for the Microsoft 365 app. They are the API permissions that are automatically granted to the **IBM® Storage Protect for Cloud Administrator for Microsoft 365** application added to your tenant by default app profile, and also the minimum API permissions that you must grant to the custom app for using IBM® Storage Protect for Cloud Microsoft™ 365 services to protect different data types in your tenant.

If you are using custom app authentication, ensure that your app has access to the protected APIs of Microsoft Teams. Otherwise, the public and private channel's conversations cannot be protected. To request access to the protected APIs, refer to the Microsoft article: Protected APIs in Microsoft Teams.

For a full list of permissions that are automatically granted to the default app, refer to .

Note: If your service contains not only the Microsoft™ **365 Groups** or **Teams**, you will notice that other than **Teams Chat**, the permissions required for Microsoft™ 365 Groups or Teams are sufficient to protect the **SharePoint Online**, **OneDrive**, **Exchange Online**, and **Exchange Public Folder**. Note that the **Project Online** service does not support app profile authentication.

Service Type	App Profile Type	APIs	Permission	Why You Need
SharePoint Online	IBM® Storage Protect for Cloud Microsoft™ 365app (SharePoint Permissions)	SharePoint	Application Permission: **Sites.FullControl.All** (Have full control of all site collections)	Back up and restore site collections.
			Application Permission: **User.ReadWrite.All** (Read and write user profiles)	Back up and restore Microsoft™ 365 user profiles related information in sites
			Application Permission: **TermStore.ReadWrite.All** (Read and write managed metadata)	Back up and restore Managed Metadata Service.
OneDrive	IBM® Storage Protect for Cloud Microsoft™ 365 app (SharePoint Permissions)	Microsoft™ Graph	Application Permission: **Files.ReadWrite.All** (Read files in all site collections)	OneDrive files.
			Application Permission: **Sites.ReadWrite.All** (Read and write items in all site collections)	Back up and restore the OneDrive content.
			Application Permission: **Sites.Manage.All** (Create, edit, and delete items and lists in all site collections)	Back up and restore the lists in OneDrive, and it is required if the SharePoint list has content approval settings enabled.
			Application Permission: **Site.FullControl.All** (Have full control of all site collections)	Back up some files in specific conditions, such as DLP-sensitive files.

Service Type	App Profile Type	APIs	Permission	Why You Need
			Application Permission: **User.Read.All** (Read all users’ full profiles)	Back up and restore Microsoft 365 user profiles related information in sitesOneDrive, Groups, and Teams.
		SharePoint	Application Permission: **Sites.FullControl.All** (Have full control of all site collections)	Back up and restore the OneDrive sites.
Exchange Online/ Public Folder	IBM® Storage Protect for Cloud Microsoft™ 365app (Exchange Permissions)	Exchange	Application Permission: **full_access_as_app** (Use Exchange Web Services with full access to all mailboxes)	Back up and restore mailboxes.
		Microsoft Graph	Application Permission: **User.Read.All** (Read all users' full profiles)	Verify the impersonation accounts for Public Folders.

Service Type	App Profile Type	APIs	Permission	Why You Need
Microsoft™ 365 Groups/Teams/ Viva Engage **Note:** If the Team/ Group/Viva Engage domain is not the default domain, the app must have the **Exchange Administrator role** to update the domain during the restore job. For details, refer to How to Assign the Exchange Administrator Role to an App?	Microsoft 365 app (All permissions)/ IBM® Storage Protect for Cloud Microsoft™ 365 app (All permissions) **Note:** If you user the Viva Engage service, you need to configure the Viva Engage app besides the Microsoft 365 app (All permissions) or IBM® Storage Protect for Cloud Microsoft™ 365 app (All permissions).	SharePoint	Application Permission: **Sites.FullControl.All** (Have full control of all site collections)	Back up and restore site collections.
			Application Permission: **User.ReadWrite.All** (Read and write user profiles)	Back up and restore Microsoft™ 365 user profiles related information in OneDrive, Groups, and Teams.
			Application Permission: **TermStore.ReadWrite.All** (Read and write managed metadata)	Back up and restore Managed Metadata Service.
		Exchange	Application Permission: **full_access_as_app** (Use Exchange Web Services with full access to all mailboxes)	Back up and restore mailboxes.
			Exchange.ManageAsApp (Manage Exchange as Application)	Scan in-place archived mailboxes.
	All Permissions	Microsoft™ Graph	Application Permission: **Directory.Read.All** (Read directory data)	Retrieve information for the members of Groups/ Teams. Retrieve the Groups from recycle bin.
Microsoft™ 365 Groups/Teams/ Viva Engage	All Permissions	Microsoft™ Graph	Application Permission: **Group.ReadWrite.All** (Read and write all groups)	Scan Microsoft™ 365 Groups via Auto Discovery. Back up and restore Microsoft™ Teams and Microsoft™ 365 Groups data.
			Application Permission: **Sites.ReadWrite.All** (Read and write items in all site collections [preview])	Back up and restore Microsoft™ Teams and Microsoft™ 365 Groups team sites data.

Service Type	App Profile Type	APIs	Permission	Why You Need
			Application Permission: **ChannelMember.ReadWrite.All** (Add and remove members from all channels) **ChannelMessage.Read.All** (Read all channel messages)	Back up and restore the members and messages of the Team's private channels.
Microsoft™ 365 Groups/Teams/ Yammer	All Permissions	Microsoft™ Graph	Application Permission: **ChannelSettings.ReadWrite.All** (Read and write the names, descriptions, and settings of all channels)	Required by the restore jobs of Teams service.
			Application Permission: **Reports.Read.All** (Read all usage reports)	Retrieve data size directly to improve the efficiency of subscription consumption report in **Subscriptions**.
			Application Permission: **TeamsTab.ReadWrite.All** (Read and write tabs in Microsoft Teams)	Back up and restore teams’ tabs.
			Application Permission: **TeamSettings.ReadWrite.All** (Read and change all teams’ settings)	Back up and restore teams’ settings.
			Application Permission: **Team.Create** (Create teams)	Restore teams.
			Application Permission: **Files.Read.All** (Read files in all site collections)	Back up teams’ files.

Service Type	App Profile Type	APIs	Permission	Why You Need
			Application Permission: **TeamsAppInstallation.ReadWriteForTeam.All** (Manage Teams apps for all teams)	Back up and restore teams' apps.
Microsoft™ 365 Groups/Teams/ Viva Engage	All Permissions	Microsoft™ Graph	Application Permission: **Channel.Create** (Create channels)	Restore teams' channels.
			Application Permission: **TeamMember.ReadWrite.All** (Add and remove members from all teams)	Back up and restore teams' members.
			Application Permission: **Tasks.ReadWrite.All** (Read and write all users' tasks and tasklists)	Back up and restore Planner data.
Microsoft Teams Chat **Note:** Teams Chat service supports to use the default Microsoft Graph API or Microsoft Graph Teams Export API Export API model B.	Only support custom app	Microsoft Graph	Application Permission **User.Read.All** (Read all users' full profiles)	Retrieve the Microsoft 365 Users' user profiles.
			Application Permission **Chat.Read.All** (Read all chat messages)	Back up the Teams chat messages.

Required Permissions of Microsoft™ Delegated App

If you want to perform the following, you must configure a default Microsoft Delegated app. Note that **the Custom Azure app with delegated permissions** has not yet been supported by IBM® Storage Protect for Cloud Microsoft™ 365.

- Restore Teams Channel conversations as new posts to the channel.

> **Note:** In this case, the authentication user of the delegated app must have the Teams license. The Restore conversations as posts features are not available in the data center that is operated by 21Vianet in China. Only the backup data generated in a new backup cycle that is after June 1, 2021 can be used to restore the conversations as posts.

- Protect Power® BI workspaces.
- Protect Power® Automate cloud flows.
- Protect Power Apps data (standard Canvas apps and component libraries).
- Restore Planner task comments

Consent from a **Microsoft 365 Global Administrator** is required when creating a delegated app profile and must be retained. The consent user of the delegated app for Power Automate must also have the **Environment Admin** /**System Administrator** role. However, the consent can be revoked in the following cases:

- If you only use this delegated app to restore Teams channel conversations as posts or restore Planner task comments, the consent can be revoked and the Global admin role can be removed.
- If you only use this delegated app to protect the Power BI content, the consent can be revoked, but the authentication user must have a **Power BIPro** license or a **Premium Per User (PPU)** license, and have at least the **Fabric Administrator** role (the former **Power BI admin** role) for Auto Discovery scan and the backup.
- If you only use this delegated app to protect Power Automate, the consent can be revoked as well, but the authentication user must have at least the **Environment Admin**/**System Administrator** role and the **Power Platform admin** role for Auto Discovery scan and the backup.
- If you use this delegated app to protect the Power Apps data, the consent can be revoked, but the authentication user must have at least the **Power Platformadmin** role and **Environment Admin/System Administrator**role for Auto Discovery scan and the backup, and the **Power Apps for Microsoft 365** license to proceed.
  Refer to the following table for the permissions that are granted to the Microsoft™ Delegated app:

Table representing permissions granted to the Microsoft™ Delegated app:

API	Permissions	Why do we need it?	Feature Category
	openid (Sign users in)	Allows to authenticate users by retrieving their consent.	All
	profile (View users' basic profile)	Retrieves users' profile information.	All
	offline_access (Maintain access to data you have given it access to)	Maintains access over an extended period without requiring the user to re-authorize frequently	All
Microsoft™ Graph	**ChannelMessage.Send** (Send channel messages)	Sends messages to channels in Microsoft™ Teams.	Restore channel conversations as posts
	TeamMember.ReadWrite.All (Add and remove members from teams)	Adds members to Microsoft™ Teams.	Restore channel conversations as posts
	ChannelMember.ReadWrite.All (Add and remove members from channels)	Adds members to channels in Microsoft™ Teams.	Restore channel conversations as posts

API	Permissions	Why do we need it?	Feature Category
	Directory.Read.All (Read directory data)	Retrieves all user’s full profiles and user domain information.	Power® BI & Power® Automate & Power® Apps
	Group.ReadWrite.All (Read and write all groups)	Retrieves the conversation thread.	Restore Planner task comments
Power® BI Services	**Tenant.ReadWrite.All** (Read and write all content in tenant)	Retrieves the workspaces and backs up, or adds users to the workspace.	Power® BI
	Workspace.ReadWrite.All (Read and write all workspaces)	Gets and restores workspaces.	Power® BI
	Capacity.Read.All (View all capacities)	Retrieves capacities (including multi-geo).	Power® BI
	Report.ReadWrite.All (Read and write all reports)	Performs backup for reports.	Power® BI
	Dataset.ReadWrite.All (Read and write all datasets)	Performs backup and restore for reports.	Power® BI
PowerApps Service	**User** (Access PowerApps Service API)	Retrieves Power® Automate Cloud Flows for Auto Discovery scan and for IBM® Storage Protect for Cloud.	Power® Automate
		Retrieves standard Canvas apps and component libraries in Power Apps for Auto Discovery scan and for IBM® Storage Protect for Cloud.	Power® Apps
Dynamics CRM	**User_impersonation** (Access Common Data Service as organization users)	Retrieves Power® Automate desktop flows and Business process flows for Auto Discovery scan.	Power® Automate
		Retrieves standard Canvas apps and component libraries in Power Apps for Auto Discovery scan.	Power® Apps

Required Permissions of Viva Engage App

If you use the Viva Engage service, you need to have the Microsoft 365 app (All permissions) or IBM® Storage Protect for Cloud Microsoft™ 365 app (All permissions), and the Viva Engage app. Alternatively, you can have a custom Azure app with delegated permissions.

Refer to the following for the permissions required by the Viva Engage app, as well as the minimum API permissions that you must grant to the custom app:

API	Permission	Type	Purpose
Microsoft Graph	User.Read (Sign in and read user profile)	Delegated	Support signing into IBM® Storage Protect for Cloud Microsoft™ 365 with Microsoft 365 accounts.
Yammer	access_as_user (Read and write to the Yammer platform)	Delegated	To access the Viva Engage platform on behalf of the signed-in user.
	user_impersonation (Read and write to the Yammer platform)	Delegated	To access the Viva Engage platform on behalf of the signed-in user.

Monitor and Manage Your Backup

On the **Backup** page of the new interface, you can view all the backup services in your subscription. Each service type has a separate tile displaying the backup service status, the number of objects being protected, the last backup job status, and the next backup job start time.

About this task

You can click a service tile to view the backup details of that service. By default, the **Backup details** page displays the last backup job details, including the number of successful, skipped, and failed objects in this job or the progress of the running backup, the backup status, start time, finish time, data size, duration, and the operator on the main pane.

For services protected by **IBM® Storage Protect for Cloud,** the **Backup details** page displays the last backup job details by default, including the number of successful, skipped, and objects with errors in this job or the progress of the running backup, the backup status, start time, finish time, data size, duration, and the operator on the main pane. For the backup jobs in progress, the successful items and items with errors during the backup are provided in the page.

Procedure

You can generate the job report directly from the **Backup details** page. Follow the steps below:

1. Click the **Generate report** option from the More commands (•••) list button. The Generate report window appears.
2. You can choose to generate a simple or detailed report as needed, and then click **Generate**.
3. After the report is successfully generated, expand the **Job report** list and click the **Download report** option to download the job report to a local location.
   You can also click the **View more in job monitor** link to navigate to the Job monitor page to check the job history or download report. For details, refer to "Job Monitor" on page 153.

In the **Backup history** area, you can click any badge to view the details of a preview backup job from the last 20 backup job records.

Note the following:

- The backup job will not back up the SharePoint sites that have not had any changes made since the last backup. If there are security changes but no changes on the content in the sites, the scheduled incremental backup jobs will not back up the securities too. The changes on the securities in the sites (including the SharePoint Online sites, OneDrive, and Microsoft 365 Groups/Teams team sites) that have not yet been backed up, in this case, will be included in an incremental backup once a week.
  If some items in a site encounter errors in a backup but there are no changes made on the content in the site for the next backup, the scheduled incremental backup jobs will not back up these items with errors. Moving forward, they will be in the Exchange Online backup job report, the number of consecutive failed attempts for the backup will be displayed in the **Failed Attempts** column.
- The objects with errors in the backup job for OneDrive, SharePoint Online, Exchange Online, and Microsoft 365 Groups will be backed up again in the next incremental backup job within the same backup cycle, if these objects have not been modified before the next incremental backup job. The objects with errors in the backup job will always be included in the subsequent backup jobs until they are successfully backed up. In the Exchange Online backup job report, the number of consecutive failed attempts for the backup will be displayed in the **Failed Attempts** column.
  If the objects with errors have been modified before the next incremental backup job, they will not be regarded as the objects with errors and will be included in the next incremental backup job.

Configure Notifications

With IBM® Storage Protect for Cloud Microsoft™ 365, you can define certain statuses of jobs and reports which will trigger alerts, including backup, restore, retention, exportation, and the unusual activities analysis report.

About this task

> **Note:** Your notification settings will be disabled if you are a distributor or partner-managed customer, and your account manager has configured this setting through IBM® Storage Protect for Cloud Partners platform. If you are a service provider, refer to the Manage Job Notification Profiles section in IBM® Storage Protect for Cloud Partners user guide for details.

The **Default service monitoring** profile is built-in to control who will receive the following high-level notification emails:

- Notification for long-running backup split-off
- Notification for legacy backup data reaching retention limit
- Notification for removing unprotected backup data
- Notification for configuring storage settings for BYOS

> **Note:** For new customers, the **Default service monitoring** profile will automatically perform a one-time synchronization with the built-in administrators from **User management** once your account is initialized. For existing customers, a one-time synchronization occurred in January 2025 that synchronized administrators from User management. You can edit this profile by navigating to **Settings** > **Notification**. After the updates, notifications will be sent according to the **Default Service Monitoring** profile, rather than to the built-in administrator group.

Procedure

To create a new notification profile, follow the steps below:

1. In the IBM® Storage Protect for Cloud Microsoft™ 365 interface, navigate to **Notification**.
2. Click the **Create notification profile** button. The **Create a new notification profile** pane appears.
3. Enter the name and description for this notification profile. The description is optional.
4. Configure the following notification settings:
   a. **Send email notifications to the following email addresses** – Enter the email addresses in the text box to configure the recipients for the email notifications. You can enter the email addresses of users or groups. For groups, you must ensure the group you entered can receive emails. Otherwise, the group members will not be notified of the activities in IBM® Storage Protect for Cloud Microsoft™ 365.

   b. **Send the email notifications for the jobs in the following status** – Select the job status for the Backup, Restore, Export, and Retention jobs which will trigger the notification, and select whether they will receive notifications when a potential ransomware attack is detected, or unusual activities are detected.
5. Click **Save** when you finish configuring the profile.

Configure Backup Prioritization

About this task

Backup prioritization allows administrators to specify which containers and objects will be backed up first during backup jobs, ensuring that critical data receives priority protection. This feature is only supported for IBM® Storage Protect for Cloud.

Procedure

To configure backup prioritization, follow the steps below:

1. Navigate to the **Backup** page and click the More commands (⋯) button in the upper-right corner of the service tile.
2. Click **Configure backup** from the drop-down list. If you want to configure backup prioritization for **Exchange Online**, **OneDrive**, **SharePoint Online**, **Teams** or **Groups**, click the **IBM® Storage Protect for Cloud Microsoft™ 365** tile and navigate to the **Backup prioritization** tab.
3. Turn on the**Enable backup prioritization** switch to activate prioritization for the selected service.
4. In the **Priority configuration** tab, all containers and objects included in the backup scope are displayed.

   To assign priority, click the Star (☆) icon next to the desired containers or objects. You can also use the search box to find specific objects by name.

   > **Note:** If you mark both a container and specific objects within it, marking the container includes all remaining unmarked objects in that container.

5. Once you have marked containers and objects for priority, navigate to the **Priority overview** tab. All marked containers and objects are listed separately and sorted based on the time they were marked. Each object displays its associated container name.
   You can do the following:
   - Unmark containers or objects directly from this tab.
   - Drag and drop containers and objects to adjust their priority order. Note that marked objects will always take precedence over containers.
   - Click the Move to top (⤒) icon to elevate an object to the highest priority.

   > **Note:** The system allows simultaneous backups. Therefore, due to their size, lower-priority items may complete before higher-priority ones.

6. Click **Save** to apply backup prioritization settings.

Change the Backup Scope

After you get started, you can make changes to the objects you want to back up. When you select a container to back up, all objects contained within the container will be backed up. After you make the changes to the backup scope, all subsequent backup jobs will back up the data according to the new scope.

Procedure

Complete the following steps to change the backup scope:

1. Navigate to the **Backup** page and click the More commands (⋯) button in the upper-right corner of the service tile.
2. Click **Configure backup** from the drop-down list.
3. With the backup service enabled, select the containers that you want to back up in the **Backup Scope** tab. You can select the **All objects in existing and any further containers** option to select all containers in the backup scope, which will automatically include the objects registered later, or select **Custom backup scope** to include the containers that you want to back up.

   To view objects included in the containers, click the Expand (⌄) button next to the container.

   To search for an object, enter the object name in the search box and click the Search (🔍) button.
4. Click **Save** when finished changing the backup scope. The changes will take effect from the next backup job. You can also click **Cancel** to return to the **Backup** page without saving any changes.
   Note the following for changing the backup scope:

   - If the backup service for an object type is disabled, no backup jobs for this object type will start until you enable the backup service again.
   - If you enable the Teams Chat service using IBM® Storage Protect for Cloud, a pop-up window will appear. If you want to protect the Teams Chat, you must click **Go to Settings > Backup** and navigate to **Settings** > **Backup** to choose an API to protect Teams Chat and customize the backup time range for Teams chat messages. Note that the backup time range cannot be changed once saved.
   - With **IBM® Storage Protect for Cloud**, if you modify your scope by either unchecking a container (such as a set of mailboxes) or turning off the backup for a Microsoft 365 service entirely (such as Microsoft 365 Groups), we assume that you do not need to protect this content any longer and will remove this data after 30 days. This also includes cases where data moves from a protected container to an unprotected container, such as during role-changes for users (one set of mailboxes to another) or when there is a change in classification for Groups and Teams.
   - For example: if you are only protecting SharePoint sites exclusively, you are not protecting Microsoft 365 Groups. If you convert your Site Collection to become a Microsoft 365 Group, this will count as a change in scope. Since Microsoft 365 Groups were not selected to be backed up, the original SharePoint site’s data will be removed in 30 days. You can correct this by re-enabling the new scope.

Change the Backup Frequency

You can change the frequency of backup operations to meet the requirements of your organization.

About this task

Microsoft™ has implemented tighter throttling limits on background apps (migration, DLP, and backup solutions) during weekday daytime hours.

To reduce issues that cause the Microsoft™ error code 429 (Too many requests), IBM® Storage Protect for Cloud Microsoft™ 365 will adjust the default value of the backup frequency from 4 to 1 for new customers. If you have a requirement for 4 backups per day, you can change it accordingly. For existing customers, we will update your backup frequency.

After the backup service has been enabled, you can change the backup frequency. You can customize the backup frequency and schedule each backup service by setting up the backup frequency 1 to 4 times per day and define a start time for the first backup job.

> **Note:** IBM cannot guarantee the completion of four backups per day, even if the backup frequency is set to four times daily. Various factors, such as data size, can impact job performance and are beyond our control. If a scheduled backup is due to start but the previous one is still in progress, the new job will be skipped.

Procedure

To change the backup frequency, follow these steps below:

1. Navigate to the **Backup** page and click the More commands (•••) button in the upper-right corner of the service tile.
2. Click **Configure backup** from the drop-down list.
3. Select a number from the **How many backup jobs would you like to run per day?** list. IBM® Storage Protect for Cloud Microsoft™ 365 will automatically provide the job schedule according to the frequency you selected.
4. You can change the start time for the first backup job. The rest of the schedules will be automatically calculated and displayed.
5. Click **Save** when you finish changing the backup frequency and schedule. The changes will take effect from the next backup job. You can also click **Cancel** to return to the **Backup** page without saving any changes.

Disable a Backup

The backup services can be disabled. If the backup service for an object type is disabled, no backup jobs for this object type will start until you enable the backup service again.

Procedure

To disable a backup service, follow the steps below:

1. Navigate to the **Backup** page and click the More commands (•••) button in the upper-right corner of the service tile.
2. Click **Configure backup** from the drop-down list.
3. Turn off the switch to disable the backup service.
4. Click **Save** and click **OK** to confirm your operation.

Configure Settings for IBM® Storage Protect for Cloud

Refer to the following instructions to configure settings for IBM® Storage Protect for Cloud:

- Account Management
- Manage Your Storage
- Configure Backup Settings
- Configure Retention Policy
- Configure Mapping Settings
- Configure End-User Restore Settings
- Configure Notifications
- Configure Security Settings

Manage Your Storage

In the **Settings** > **Storage** page, the storage location and data retention time will be displayed. For custom storage location, you can configure when the backup data will be purged from the storage after the data expires the retention time. The default retention period for Bring Your Own Storage (BYOS) is 1 year, and you can customize it for specific containers or object types upon your purchased retention in the subscription.

> **Note:** If you purchased a subscription for BYOS (Bring your own storage) but are currently using IBM® Storage Protect for Cloud default storage for your backup data, your backup jobs will fail and we will send you an email notification every 7 days to remind you to update your BYOS storage configuration.

There are two types of storage locations: the default storage location and the custom storage location.

- The default storage location is hosted by IBM® Storage Protect for Cloud is Microsoft Azure Blob Storage and cannot be modified. The storage information on Microsoft Azure storage is displayed on the **Settings** > **Storage** page. If you want to use your own storage, contact IBM to update your subscription. The default storage location resides in the same Data Center that was selected during your registration to IBM® Storage Protect for Cloud. If you choose to use **IBM® Storage Protect for Cloud default storage**, you can choose the storage type of your IBM® Storage Protect for Cloud default storage location from the **Microsoft Azure Blob Storage** type and the **Amazon S3 storage** type.
  For data redundancy, note the following:
  - For **Microsoft Azure Blob Storage**, Locally redundant storage (LRS) is the default option to replicate your data.
  - For **Amazon S3 storage**, objects will be redundantly stored on multiple devices across a minimum of three Availability Zones in an AWS Region.

  > **Note:** For Multi-Geo customers, the default storage locations are distributed according to the data center mappings. If you are using default storage for Multi-Geo, you have a chance to choose to use the default storage or your own storage for each region while configuring data center mappings in the IBM® Storage Protect for Cloud interface. Once the configurations are saved, you can no longer change the storage path.

- If your subscription has BYOS (bring your own storage) enabled, you can configure a custom storage location for all service types or configure separate storage for each service type to store your data, upon your subscription agreement.
  The storage information, apart from its path information, can be modified.

  Currently, you can choose from the following supported storage types for BYOS:
  - Microsoft Azure Blob Storage

- Amazon S3
- Amazon S3-Compatible Storage
- FTP
- SFTP
- Dropbox
- IBM Storage Protect-S3
- IBM Cloud Object Storage
- Google Cloud Storage

If you are using your own Microsoft™ Azure storage account, note the following:

Existing BYOS customers applying immutability policies to Azure blob storage should note the following:

- **Backup job behavior**: The first backup job executed after applying an immutability policy will fail. However, subsequent backup jobs will process your data within the defined backup scope.
- **Data deletion restriction**: If immutability polices are active on your Azure blob storage, all data deletion operations, including unprotected data removal, data retention, manual deletion, and Data Subject Access Requests (DSARs) will be blocked. Data governed by these polices will remain immutable and cannot be altered or deleted unless the policies are modified.
- If you are about to use your own Microsoft™ Azure Blob Storage as the storage location, the preferred method is to use the device in the same Data Center as your IBM® Storage Protect for Cloud Microsoft™ 365 tenant for the best network performance.
- Before you add the Azure storage account to the IBM® Storage Protect for Cloud Microsoft™ 365, you must first add the IBM® Storage Protect for Cloud IP addresses to your Azure storage account firewall and configure the firewall to allow IBM® Storage Protect for Cloud agent servers running on a dedicated ARM Vnet subnet to access your storage location. For details, refer to “Allow IBM Storage Protect for Cloud Agent Servers to Access Your Storage Account” on page 74.
- After the January 2024 release, IBM® Storage Protect for Cloudwill write your new backup data to the cold tier by default to reduce storage costs. The supported Azure account kinds are **StorageV2** and **BlobStorage** of **Standard** performance type. For existing customers, your former backup data is still stored in the cool tier.
- Additionally, you can keep the index database in a cool or hot tier, to ensure restore jobs automatically rehydrate data from the archive storage tier.
  For details about blob access tiers and how to change access tiers, refer to the Microsoft™ article: Azure Blob storage: hot, cool, and archive access tiers.
- If you are using your own Microsoft™ Azure Blob storage and facing the upper limit of your storage account, you can contact Microsoft™ Azure support to request an increase. If you have another Azure storage account, you can also append it through the **Storage Location** tab in IBM® Storage Protect for Cloud Microsoft™ 365. Currently, you can only append one additional storage account, and this is only available for BYOS customers on Azure. Once the new storage location is saved, the new storage will be used to store backup data for the further incremental backup jobs and restore jobs. IBM® Storage Protect for Cloud Microsoft™ 365 services will no longer write to the legacy storage location. However, you must ensure your legacy storage is accessible if the backup job to start later is an incremental backup. Otherwise, the incremental backup will fail. The full backup job to start a new cycle will not been impacted in this case.

Allow IBM® Storage Protect for Cloud Agent Servers to Access Your Storage Account

If you are using or plan to use your own storage device, read the instructions in this section carefully and adjust the settings as needed. Otherwise, you can skip this topic.

When you are using your own storage device, you may have set up the storage firewall to only allow the trusted clients for security concerns. To ensure that IBM® Storage Protect for Cloud Microsoft™ 365 can access your storage, complete the settings as required in the following conditions:

> **Note:** If you are using a trial subscription and the storage account you want to use in the trial has a firewall enabled, read the conditions below and complete the configuration.

For **Microsoft Azure Cloud Platform** data centers:

- If you are using Microsoft™ Azure storage, refer to the following:
  - **If your storage account is in the same data center as the one you use to sign up for IBM® Storage Protect for Cloud or your storage account is in its** paired region, you must add the Azure Resource Manager (ARM) vNet subnets where the IBM® Storage Protect for Cloud servers are running on to your storage networking. You can find additional details in this Microsoft™ article: Grant access from a virtual network, and get the subnet ID of the subnet ID of IBM® Storage Protect for Cloud products for your data center from Download ARM Vnet IDs. For detailed instructions, refer to the **Add ARM Virtual Networks** section below.
  - Other than the condition above, you need to add all the reserved IP addresses to the Azure storage firewall. For details, refer to the **Add Reserved IP Addresses to Azure Storage Firewall** section below.
- If you are using Amazon S3 in Southeast Asia (Singapore) data center, you need to add all the reserved IP addresses and specific VPC ID to the bucket policy. For details, refer to Add reserved IP addresses and VPC ID to Amazon S3 bucket policy.
- If you use a storage type other than Microsoft Azure storage and Amazon S3, you must add reserved IP addresses to your storage firewall. To get the list of the reserved IP addresses, refer to Download a List of Reserved IP Addresses.

For **Google Cloud Platform (GCP)** data centers:

- If you use the Google Cloud Storage in Google Cloud Platform (GCP) data centers, you need toadd specific VPC ID to the bucket policy. For details, refer to the**Update the lP Filter on a Google Cloud Storage Bucket Policy** section below.
- If you use a storage type other than Google Cloud Storage, you must add reserved IP addresses to your storage firewall. To get the list of the reserved IP addresses, refer to Download a List of Reserved IP Addresses

Add Reserved IP Addresses to Azure Storage Firewall

1. Navigate to **IBM® Storage Protect for Cloud** interface **> Administration > Security**.
2. Click **Download** next to the **Reserved IP Addresses** tile to download the list of reserved IP addresses of IBM® Storage Protect for Cloud. For details, refer to .
3. Navigate to the storage account that you want to secure.
4. Select **Networking** on the menu.
5. Check that you've selected to allow access from **Selected networks**.
6. Enter the IP address or address range under **Firewall › Address Range**.
7. Select **Save** to apply your changes.

Add Reserved IP Addresses and VPC ID to Amazon S3 Bucket Policy

To use the Amazon S3 storage in Southeast Asia (Singapore) data center, you must add all the reserved IP addresses and the IBM® Storage Protect for Cloud AWS VPC ID to your bucket policy.

Follow the instructions in the bucket policy template below.

```
{
"Version": "2012-10-17", // Specifies the language syntax rules that are to be used to
process a policy. 2012-10-17 is the latest version.
"Statement": [
{
"Sid": "S3_IPAllow", // An optional identifier used as a description for the policy
statement.
"Effect": "Deny", // You must set the Effect element to Deny here, which indicates that the
access to the resources will be denied if the IP Address is not listed in aws:SourceIP and
the VPC is not listed in aws:SourceVpc.
"Principal": {
"AWS": "*" // Specifies the IAM users who have access to the resources.
},
"Action":[
"s3:GetObject",
"s3:DeleteObject",
"s3:PutObject",
"s3:DeleteObjectVersion",
"s3:ListBucket"
],
"Resource": [
"XXXXXXXXXXXXXXXXX", // Specifies the resources that this S3 bucket policy applies to.
"XXXXXXXXXXXXXXXXX"
],
"Condition": {
"NotIpAddress": {
"aws:SourceIp": [
"XXXXXXXXXXXXXXXXX", // Specifies the IP addresses. Add the IBM reserved IP addresses to
the list. To get a list of IBM reserved IP addresses, refer to Download a List of Reserved
IP Addresses.
"XXXXXXXXXXXXXXXXX" //
]
},
"StringNotEquals": {
"aws:SourceVpc": "vpc-04c390b29bb119f8f" // Example of the AWS VPC ID of Southeast Asia
(Singapore) data center.
}
}
}
]
}
```

Add ARM Virtual Networks

There are two ways to add ARM Virtual Networks:

- Use the Azure CLI tool (https://docs.microsoft.com/en-us/cli/azure/install-azure-cli?view=azure-cli-latest)

```
## Use the Azure CLI tool

# Step 1 (Optional): If you have multiple Azure subscriptions, please switch to the
correct subscription
# This command sets the active subscription to the specified subscription ID.
az account set --subscription xxxxxxxx-xxxx-xxxx-xxxx-yyyyyyyyyyyy

# Step 2 (Optional): Confirm whether the subscription switch is correct
# This command displays the current subscription information in a table format.
az account show --output table

# Step 3: Get the IBM® Storage Protect for Cloud network subnet resource ID
# This variable stores the resource ID of the subnet in the virtual network.
# Replace with the Azure Resource Manager (ARM) VNet ID downloaded from
your IBM® Storage Protect for Cloud tenant.
$SUBNETID="/subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-yyyyyyyyyyyy/resourceGroups/
ResourceGroupName/providers/Microsoft.Network/virtualNetworks/VirtualNetworkName/
subnets/SubnetName"

# Step 4: Set your resource group name
# This variable stores the name of the resource group where your storage account is
located.
$DESTRG="customer_resource_group_name"

# Step 5: Set your storage account name
# This variable stores the name of the storage account to which you want to add the
network rule.
$DESTSTA="customer_storage_account_name"

# Step 6: Add the firewall virtual network rule to grant access to IBM® Storage Protect
for Cloud
# This command adds a network rule to the specified storage account, allowing access
from the specified subnet.
az storage account network-rule add --resource-group $DESTRG --account-name $DESTSTA --
subnet $SUBNETID

# Step 7: List the current network rules for the storage account to verify the addition
# This command lists the virtual network rules for the specified storage account.
az storage account network-rule list --resource-group $DESTRG --account-name $DESTSTA
--query virtualNetworkRules
```

```
# Step 8 (Optional): Disable the public access to storage account
# This command updates the storage account to deny public network access.
az storage account update --resource-group $DESTRG --name $DESTSTA --default-action
Deny

# Step 9 (Optional): Verify that the default action for network rules is set to Deny
# This command shows the network rule set for the specified storage account, including
the default action.
az storage account show --resource-group $DESTRG --name $DESTSTA --query
networkRuleSet.defaultAction
```

- Use the Azure Az PowerShell (https://docs.microsoft.com/en-us/powershell/azure/install-az-ps?view=azps-5.1.0)

```
## Use the Azure Az PowerShell (Az Module)

# Step 1: Sign in to Azure with your Azure Admin account

Connect-AzAccount

# Step 2 (Optional): If you have multiple Azure subscriptions, please switch to the
correct subscription
# This command sets the active subscription to the specified subscription ID.

Set-AzContext -SubscriptionId "xxxxxxxx-xxxx-xxxx-xxxx-yyyyyyyyyyyy"


# Step 3: Get the IBM® Storage Protect for Cloud network subnet resource ID
# This variable stores the resource ID of the subnet in the virtual network.
# Replace with the Azure Resource Manager (ARM) VNet ID downloaded from
your IBM® Storage Protect for Cloud tenant.

$SUBNETID="/subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-yyyyyyyyyyyy/resourceGroups/
ResourceGroupName/providers/Microsoft.Network/virtualNetworks/VirtualNetworkName/
subnets/SubnetName"

# Step 4: Set resource group name
# This variable stores the name of the resource group where your storage account is
located.

$DESTRG="customer_resource_group_name"

# Step 5: Set storage account name
# This variable stores the name of the storage account to which you want to add the
network rule.
$DESTSTA="customer_storage_account_name"

# Step 6: Add the firewall virtual network rule to grant access to IBM® Storage Protect
for Cloud
# This cmdlet adds a network rule to the specified storage account, allowing access
from the specified subnet.

Add-AzStorageAccountNetworkRule -ResourceGroupName $DESTRG -Name $DESTSTA
-VirtualNetworkResourceId $SUBNETID

# Step 7: VerifyList the newly addedcurrent network rulerules for the storage account
to verify the addition
# This cmdlet retrieves the network rule set for the specified storage account.

Get-AzStorageAccountNetworkRuleSet -ResourceGroupName $DESTRG -AccountName $DESTSTA
```

You will see the virtual network rules in Azure Portal, as the screenshot below shows. You may also notice that a warning message “Insufficient Permission...” is displayed. It is because the subnet is not in your subscription. You can ignore it.

Update the lP Filter on a Google Cloud Storage Bucket Policy

To use the Google Cloud Storage in Google Cloud Platform (GCP) data centers, you must add the IBM Google VPC ID to your bucket policy.

Follow the instructions in the bucket policy template below.

```
{
"mode": "Enabled",
"vpcNetworkSources": [
{
"network": "{VPC id}",
"allowedIpCidrRanges": [
"0.0.0.0/0",
"::/0"
]
}
],
"publicNetworkSource": {
"allowedIpCidrRanges": [
"additional white list ip",
"additional white list ip"
]
},
"allowCrossOrgVpcs": true,
"allowAllServiceAgentAccess": false
}
```

Change Storage Location

About this task

If you want to change to use your own storage location, contact the IBM Software Support team to update your subscription and then complete the following steps. Otherwise, IBM® Storage Protect for Cloud Microsoft™ 365 will continue to store data to the IBM® Storage Protect for Cloud-hosted default storage.

Procedure

1. On the **Storage** page, the **Change to my own storage** link is available. Click **Change to my own storage**. A pop-up window appears.
2. In the pop-up window, you must choose how to handle the existing backup data stored in the default storage location.
   - **Retain all backup data currently stored in IBM® Storage Protect for Cloud storage for 90 days** – The backup data in the default storage location will be retained for 90 days after the storage change. You will get an email notification 7 days before the data deletion. For data migration, contact IBM Software Support. The next backup job for each of the enabled backup types will store the backup data to the configured custom storage location.
   - **Remove all backup data from IBM® Storage Protect for Cloud storage** – The backup data will be removed from the default storage location, and you cannot use the previous backup data for restore. After the storage location is changed, the backup jobs for the enabled backup types will start in a few seconds, and the new backup schedule of an object type will start once the corresponding backup job starts. The backup data will be stored in the configured custom storage location.
3. Click **OK** to save the settings and configure the custom storage location.
   Note the following:
   - If you are using your own storage and would like to configure separate storage locations for each service type, contact the IBM Software Support team. The **Storage** page will display the configurations.
   - If you are using the Microsoft Azure Blob storage and facing the upper limit of your storage account, you can append an additional storage account of Microsoft Azure Blob Storage for backup and restore. If you have already appended the storage, you can view the storage information on the **Storage** page.

   > **Note:** We recommend you contacting Microsoft™ Azure support first to request an increase for the maximum capacity of the storage account that you are currently using.
   > To append an additional storage location, you need another Azure storage account. Currently, you can only append one additional storage account, and this is only available for BYOS customers on Azure. Once you save the new storage location, the new storage will be used to store backup data for the further incremental backup jobs and restore jobs. IBM® Storage Protect for Cloud Microsoft™ 365 will no longer write to the legacy storage location. For details on storage configuration, refer to "Microsoft Azure Blob Storage" on page 81.

4. Configure the storage information. For details of configuring storage information, refer to "Storage Information" on page 79. Click **Validation Test** to test whether the entered information is valid. If successful, click **Apply** to save and apply your own storage.

   > **Note:** The changes from the default storage to a custom storage cannot be reverted, and the custom storage cannot be changed to another custom storage once saved.

   Either using the IBM® Storage Protect for Cloud default storage or your own storage, the data retention settings can be applied to your backup data to help save your storage costs. Once there is backup data approaching the retention period, your administrator group will receive the **Data Retention Notification**. Once the next full snapshot of your Microsoft™ 365 scope takes place, we will begin pruning the old backup data that met your retention settings.

   - If you want to keep your data in default storage, you can contact IBM Software Support team to update your subscription and increase your retention settings, but please note that increasing your data retention may increase the price you pay for your backup. If you want to archive the backup data that met the retention settings for potential restore in the future, instead of letting them be deleted from IBM® Storage Protect for Cloud storage, you can submit an export request to export the data from the default storage as a paid service. For details, refer to "Introduction to Data Export Service" on page 159.
   - If your subscription is the BYOS type, you can update your retention settings by navigating to **General Settings › Retention Policy**. Increasing your data retention may increase the price you pay for your backup.

Storage Information

Refer to the sections below for the storage configuration details of the supported storage types.

Amazon S3

IBM® Storage Protect for Cloud will by default use HTTPS (SSL) communication to access your Amazon S3 storage and store your backup data to the S3 Glacier Instant Retrieval automatically. Your existing backup data before the March 2025 release will remain in the S3 Standard storage class. You can move the backup data from S3 Standard/S3 Glacier Instant Retrieval to S3 Standard-IA®, S3 One Zone-IA®, or S3 Intelligent-Tiering, and IBM® Storage Protect for Cloud Microsoft™ 365 can restore the backup data of those storage classes. However, you should carefully consider the consequences before you activate the archive access tier if you are using S3 Intelligent-Tiering. Activating the archive access tier will cause data object files that have not been accessed for 90 days to be archived, and IBM® Storage Protect for Cloud Microsoft™ 365 cannot access the archived data in your Amazon S3 storage.

Procedure

Follow the instructions below:

1. **Storage Type** – Select **Amazon S3** from the drop-down list.
2. **Bucket name** – Enter the bucket name you wish to access.
   Note the following:
   - The entered name must match an existing bucket. If no bucket is available, refer to Creating a bucket to create one.
   - Ensure the bucket policy in Amazon S3 storage applied to your account contains the following required permissions:
     - **Read:** Get Object
     - **List:** ListBucket
     - **Write:** DeleteObject; PutObject; DeleteObjectVersion
3. **Access key ID** – Enter the corresponding access key ID to access the specified bucket. You can view the **Access key ID** from your AWS account.

> **Note:** The AWS account must have the **AmazonS3FullAccess** policy assigned.

4. **Secret access key** – Enter the corresponding secret key ID to access the specified bucket. You can view the **Secret access key** from your AWS account.

5. **Storage region** – Select the **Storage region** of this bucket from the drop-down menu.
   The available regions are:

US East (N. Virginia)	US East (Ohio)	US West (Northern California)
US West (Oregon)	Canada (Central)	EU (Ireland)
EU (Frankfurt)	EU (London)	Asia Pacific (Singapore)
Asia Pacific (Tokyo)	Asia Pacific (Sydney)	Asia Pacific (Seoul)
Asia Pacific (Mumbai)	South America (Sao Paulo)	

6. **Extended Parameters** – Enter the following extended parameters if necessary. If you have multiple parameters to enter, press **Enter** on your keyboard to separate the parameters. Refer to the instructions below to add parameters.

   - **RetryInterval** – Customize the retry interval when the network connection is interrupted. Enter any positive integer between 0 and 2147483646 (the unit is millisecond). For example, RetryInterval=30000 means that it will try to reconnect every 30000 milliseconds.
     If you do not configure this parameter, the value is 30000 milliseconds by default.

   - **RetryCount** – Customize the reconnection times after the network connection is interrupted. Enter any positive integer between 0 and 9. For example, RetryCount=9 represents when the network connection is interrupted, it can reconnect at most 9 times.
     If you do not configure this parameter, the value is 6 by default.

   - **CustomizedMetadata** – Configure if customized metadata or user-added metadata is supported. By default, customized metadata and user-added metadata are all supported.

   - **CustomizedMode=Close** – This physical device will not support customized metadata or user-added metadata.

   - **CustomizedMode=SupportAll** – This physical device will support all customized metadata and user-added metadata.

   - **CustomizedMode=CustomizedOnly** – This physical device will only support user-added metadata.

   - **CustomizedRegion** – Configure the customized region of the physical device. For example, enter **CustomizedRegion=s3-us-gov-west-1.amazonaws.com** to configure the GovCloud account.

Amazon S3-Compatible Storage

You can configure Amazon S3-compatible storage.

Procedure

Follow the instructions below:

1. **Storage Type** – Select Amazon S3-Compatible Storage from the drop-down list.

2. **Bucket name** – Enter the bucket name you wish to access.
   Note the following:

   - The entered name must match an existing bucket. If no bucket is available, refer to Creating a bucket to create one. Note that it's a general guidance, the exact steps may vary depending on the specific product, refer to your specific product documentation for any additional configurations required.

   - Ensure the bucket policy in Amazon S3-compatible storage applied to your account contains the following required permissions:

     - **Read**: Get Object

     - **List**: ListBucket

    - **Write**: DeleteObject; PutObject; DeleteObjectVersion

3. **Access key ID** – Enter the corresponding access key ID to access the specified bucket.
4. **Secret access key** – Enter the corresponding secret key ID to access the specified bucket.
5. **Endpoint** – Enter the URL used to connect to the place where you want to store the data.

    > **Note:** It is recommended that you enter a URL that begins with “https://”.

6. **Extended Parameters** – Enter the following extended parameters if necessary. If you have multiple parameters to enter, press **Enter** on your keyboard to separate the parameters. Refer to the instructions below to add parameters.

    - **Allow_Insecure_SSL** – By default, the storage client expects an SSL certificate issued by a public trusted certificate authority over HTTPS transport to ensure integrity. A self-signed certificate on the storage server side will fail the certificate validation. If you choose to use a self-signed certificate, you can set the **Allow_Insecure_SSL** to **true** in the **Extended parameters** to bypass the certificate validation.
    - **SignatureVersion** – By default, IBM® Storage Protect for Cloud Microsoft™ 365 uses V2 authentication to access your storage. If you want to use V4 authentication, add **SignatureVersion=V4** into the extended parameters.
    - **RetryInterval** – Customize the retry interval when the network connection is interrupted. Enter any positive integer between 0 and 2147483646 (the unit is millisecond). For example, RetryInterval=30000 means that it will try to reconnect every 30000 milliseconds.
      If you do not configure this parameter, the value is 30000 milliseconds by default.
    - **RetryCount** – Customize the reconnection times after the network connection is interrupted. Enter any positive integer between 0 and 9. For example, RetryCount=9 represents when the network connection is interrupted, it can reconnect at most 9 times.
      If you do not configure this parameter, the value is 6 by default.
    - **CustomizedMetadata** – Configure if customized metadata or user-added metadata is supported. By default, customized metadata and user-added metadata are all supported.
    - **CustomizedMode=Close** – This physical device will not support customized metadata or user-added metadata.
    - **CustomizedMode=SupportAll** – This physical device will support all customized metadata and user-added metadata.
    - **CustomizedMode=CustomizedOnly** – This physical device will only support user-added metadata.
    - **Cert_thumbprint** – If you have a self-signed certificate for S3 server and only want to pass the certificate validation with a specific thumbprint, enter your thumbprint as the value of the parameter.
    - **Virtualhosting** – By default, it is set to false. If your bucket does not support using path-style domain names, you need to configure virtualhosting = true to use virtual-hosted-style domain names.

Microsoft™ Azure Blob Storage

Before you begin

If you are using your own **Microsoft Azure Blob Storage** (BYOS subscription) and interested in how the backup data is stored in Azure Blob storage, refer to Storage for details.

Before adding the storage account to the IBM® Storage Protect for Cloud Microsoft™ 365 interface, ensure IBM® Storage Protect for Cloud agents have access to your storage. For details, refer to “Allow IBM Storage Protect for Cloud Agent Servers to Access Your Storage Account” on page 74.

Procedure

Follow the instructions below:

1. **Storage Type** – Select **Microsoft™ Azure Blob Storage** from the drop-down list.
2. **Access point** – Enter the URL for the Blob Storage Service. The default URL is *https://blob.core.windows.net*.
3. **Container name** – Enter the container name you wish to access.
4. **Account name** - Enter the corresponding account name to access the specified container.
5. **Account key** – Enter the corresponding account key to access the specified container.
6. **CDN enabled** – Select this checkbox if the Microsoft™ Azure content delivery network (CDN) is enabled.
7. **Extended Parameters** – Enter the following extended parameters if necessary. If you have multiple parameters to enter, press **Enter** on your keyboard to separate the parameters. Refer to the instructions below to add parameters.
    - **RetryInterval** – Customize the retry interval when the network connection is interrupted. You are allowed to enter any positive integer between 0 and 2147483646 (the unit is millisecond). For example, RetryInterval=30000 means that it will try to reconnect every 30000 milliseconds. If you do not configure this parameter, the value is 30000 milliseconds by default.
    - **RetryCount** – Customize the reconnection times after the network connection is interrupted. You are allowed to enter any positive integer between 0 and 9. For example, RetryCount=9 represents when the network connection is interrupted, it can reconnect at most 9 times. If you do not configure this parameter, the value is 6 by default.
    - **CustomizedMetadata** – Configure if customized metadata or user-added metadata is supported. By default, customized metadata and user-added metadata are all supported.
    - **CustomizedMode=Close** – This physical device will not support customized metadata or user-added metadata.
    - **CustomizedMode=SupportAll** – This physical device will support all customized metadata and user-added metadata.
    - **CustomizedMode=CustomizedOnly** – This physical device will only support user-added metadata.

FTP

You can configure File Transfer Protocol (FTP) storage.

About this task

Note the following guidelines for using FTP storage and then provide the storage information as follows:

- Use a high-performance computer as the FTP server, especially those with fast disk read and write speed.
- Use a high-level port as the port of the FTP server, such as a port after 6000, to prevent other software installed on the FTP server from occupying the same port and affecting the data being uploaded and downloaded.
- Only the passive mode of an FTP device is supported.
- Do not support the FTP device to enable SSL/TLS. If you need high-level data transmission security and encryption, you can use the Secure File Transfer Protocol (SFTP) service instead. IBM® Storage Protect for Cloud Microsoft™ 365 also supports using SFTP devices. You can contact the IBM Software Support team for assistance.
- If the FTP server you want to use is in an internal network environment and there is a firewall between the internal network and external network, ensure all the ports (the connection port and all the ports in the dynamic port range of the FTP server) can pass through the firewall.
- If the FTP server has set access control using IP addresses, you must download the reserved IP addresses from the IBM® Storage Protect for Cloud Microsoft™ 365 interface and add them to the firewall's allow list. For detailed instructions, refer to Download a List of Reserved IP Addresses.

Procedure

Follow the instructions below:

1. **Storage Type** – Select **FTP** from the drop-down list.

2. **Host** – Enter the IP address of the FTP server.
3. **Port** – Enter the port to use to connect to this FTP server. The default port is 21.
4. **Username** – Enter the username to use to connect to this FTP server.
5. **Password** – Enter the password of the specified username.
6. **Extended Parameters** – Enter the following extended parameters if necessary. If you have multiple parameters to enter, press **Enter** on the keyboard to separate the parameters. Refer to the instructions below to add parameters:
    - **IsRetry** – Whether or not to try again when IBM® Storage Protect for Cloud failed to write the data in the physical device.
        - If you enter **IsRetry=true**, it will try again when IBM® Storage Protect for Cloud failed to write the data in the physical device.
        - If you enter **IsRetry=false**, it will not try again when IBM® Storage Protect for Cloud failed to write the data in the physical device.
    - **RetryInterval** – Customize the retry interval when the network connection is interrupted. You are allowed to enter any positive integer between 0 and 2147483646 (the unit is second). For example, RetryInterval=30 means that it will try to reconnect every 30 seconds.
      If you do not configure this parameter, the value is 30 seconds by default.
    - **RetryCount** – Customize the reconnection times after the network connection is interrupted. You are allowed to enter any positive integer between 0 and 9. For example, RetryCount=9 represents when the network connection is interrupted, it can reconnect at most 9 times.
      If you do not configure this parameter, the value is 6 by default.

SFTP

You can configure Secure File Transfer Protocol (SFTP) storage.

Procedure

Follow the instructions below:

1. **Storage Type** – Select **SFTP** from the drop-down list.
2. **Host** – Enter the IP address of the FTP server.
3. **Port** – Enter the port to use to connect to this FTP server. The default port is 21.
4. **Root folder** – Enter the root folder where you wish to access.
5. **Username** – Enter the username used to access the root folder.
6. **Authentication method** – Select the **Password** or **Public key** as the authentication method.
    - **Password** – Enter the corresponding password of the user used to access the root folder.
    - **Public key** – Enter the private key and the corresponding private key password to access the root folder.
7. **Extended Parameters**– Enter the following extended parameters if necessary. If you have multiple parameters to enter, press **Enter** on the keyboard to separate the parameters. Refer to the instructions below to add parameters:
    - **IsRetry** – Whether or not to try again when IBM® Storage Protect for Cloud failed to write the data in the physical device.
        - If you enter **IsRetry=true**, it will try again when IBM® Storage Protect for Cloud failed to write the data in the physical device.
        - If you enter **IsRetry=false**, it will not try again when IBM® Storage Protect for Cloud failed to write the data in the physical device.
    - **RetryInterval**– Customize the retry interval when the network connection is interrupted. You are allowed to enter any positive integer between 0 and 2147483646 (the unit is second). For example, RetryInterval=30 means that it will try to reconnect every 30 seconds.
      If you do not configure this parameter, the value is 30 seconds by default.

- **RetryCount**– Customize the reconnection times after the network connection is interrupted. You are allowed to enter any positive integer between 0 and 9. For example, RetryCount=9 represents when the network connection is interrupted, it can reconnect at most 9 times.

  > **Note:** If you do not configure this parameter, the value is 6 by default.

Dropbox

You can configure storage on the Dropbox file hosting service.

Procedure

Follow the instructions below:

1. **Storage Type** – Select **Dropbox** from the drop-down list.
2. **Root Folder Name** – Enter a name for the root folder, which will be created in Dropbox and used to store the data.
3. **Token secret** – Click **Retrieve Token**. Enter the email address and the password of the Dropbox account in the pop-up window to log into Dropbox, and then the token will appear in this pop-up window. Enter the displayed token in the **Token secret** text box.
4. **Extended Parameters** - Enter the following extended parameters if necessary. If you have multiple parameters to enter, press **Enter** on your keyboard to separate the parameters. Refer to the instructions below to add parameters.
   - **RetryInterval** – Customize the retry interval when the network connection is interrupted. You are allowed to enter any positive integer between 0 and 2147483646 (the unit is millisecond). For example, RetryInterval=30000 means that it will try to reconnect every 30000 milliseconds.
     If you do not configure this parameter, the value is 30000 milliseconds by default.
   - **RetryCount** – Customize the reconnection times after the network connection is interrupted. You are allowed to enter any positive integer between 0 and 9. For example, RetryCount=9 represents when the network connection is interrupted, it can reconnect at most 9 times.
     If you do not configure this parameter, the value is 6 by default.

IBM® Storage Protect - S3

You can configure IBM® Storage Protect - S3 storage.

Before you begin

The IBM Storage Protect Object client (S3) must be installed and configured before setting up IBM® Storage Protect for Cloud. Refer to, Sending data from other object clients to IBM Storage Protect.

Procedure

Follow the instructions below:

1. **Storage Type** – Select IBM® Storage Protect - S3 from the drop-down list.
2. **Bucket name** – Enter the bucket name you wish to access.

   > **Note:** The entered name must match an existing bucket. For details on creating a bucket, see How to create an S3 bucket in IBM Storage Protect.

3. **Access key ID** – Enter the corresponding access key ID to access the specified bucket.
4. **Secret access key** – Enter the corresponding secret key ID to access the specified bucket.
5. **Endpoint** – Enter the URL used to connect to the place where you want to store the data.

> **Note:** The URL must begin with “http://” or “https://”.

6. **Extended parameters** – Enter the following extended parameters if necessary. If you have multiple parameters to enter, press **Enter** on your keyboard to separate the parameters. Refer to the instructions below to add parameters.

   - **Allow_Insecure_SSL**– By default, the storage client expects an SSL certificate issued by a public trusted certificate authority over HTTPS transport to ensure integrity. A self-signed certificate on the storage server side will fail the certificate validation. If you chose to use a self-signed certificate, you can set the **Allow_Insecure_SSL**to **true** in the **Extended parameters** to bypass the certificate validation.
   - **SignatureVersion** – By default, IBM® Storage Protect for Cloud Microsoft™ 365 uses V4 authentication to access your storage. If you want to use V2 authentication, add **SignatureVersion=V2** into the extended parameters.
   - **RetryInterval** – Customize the retry interval when the network connection is interrupted. Enter any positive integer between 0 and 2147483646 (the unit is millisecond). For example, RetryInterval=30000 means that it will try to reconnect every 30000 milliseconds.
     If you do not configure this parameter, the value is 30000 milliseconds by default.
   - **RetryCount** – Customize the reconnection times after the network connection is interrupted. Enter any positive integer between 0 and 9. For example, RetryCount=9 represents when the network connection is interrupted, it can reconnect at most 9 times.
     If you do not configure this parameter, the value is 6 by default.
   - **CustomizedMetadata** – Configure if customized metadata or user-added metadata is supported. By default, customized metadata and user-added metadata are all supported.
   - **CustomizedMode=Close** – This physical device will not support customized metadata or user-added metadata.
   - **CustomizedMode=SupportAll** – This physical device will support all customized metadata and user-added metadata.
   - **CustomizedMode=CustomizedOnly** – This physical device will only support user-added metadata.
   - **Cert_thumbprint** - If you have a self-signed certificate for S3 server and only want to pass the certificate validation with a specific thumbprint, enter your thumbprint as the value of the parameter.
   - **Virtualhosting** – By default, it is set to false. If your bucket does not support using path-style domain names, you need to configure virtualhosting = true to use virtual-hosted-style domain names.

Related information

IBM Storage Protect for Cloud server S3 agent

IBM Cloud® Object Storage

You can configure IBM Cloud® Object Storage.

Before you begin

Ensure that you have HMAC credentials that are created in the IBM Cloud® Object Storage. To create a set of HMAC credentials by using the console mode or CLI mode, follow the instructions in HMAC credentials section of the IBM Cloud® documentation.

> **Tip:** The HMAC credentials can be found in the `cos_hmac_keys` field, which consist of an access key and a secret key paired.

Procedure

Follow the instructions below:

1. **Storage Type** – Select **IBM Cloud Object Storage** from the drop-down list.
2. **Bucket name** – Enter the bucket name that you wish to access.

> **Note:** The entered name must match an existing bucket. If no bucket is available, refer to Creating a bucket to create one.

3. **Access key ID** – Enter the corresponding access key ID to access the specified bucket. You can get the access key ID from your IBM® Cloud Object Storage account.
4. **Secret access key** – Enter the corresponding secret key ID to access the specified bucket. You can get the secret access key from your IBM® Cloud Object Storage account.
5. **Endpoint** – Enter the URL used to connect to the place where you want to store the data. For more details about endpoint, refer to Endpoints and storage locations.

> **Note:** The URL must begin with "http://" or "https://".

6. **Extended parameters** – Enter the following extended parameters in **Extended parameters** settings if necessary. If you have multiple parameters to enter, press **Enter** on your keyboard to separate the parameters. Refer to the instructions below to add parameters.
   - **Allow_Insecure_SSL** – By default, the storage client expects an SSL certificate issued by a public trusted certificate authority over HTTPS transport to ensure integrity. A self-signed certificate on the storage server side will fail the certificate validation. If you choose to use a self-signed certificate, you can set the **Allow_Insecure_SSL** to **true** in the **Extended parameters** to bypass the certificate validation.
   - **SignatureVersion** – By default, IBM® Storage Protect for Cloud Microsoft™ 365 uses V2 authentication to access your storage. If you want to use V4 authentication, add **SignatureVersion=V4** into the extended parameters.

     > **Note:** IBM Cloud Object Storage can be accessed by using both V2 and V4 authentication. For more details, refer to Configure authentication against a system.

   - **RetryInterval** – Customize the retry interval when the network connection is interrupted. Enter any positive integer between 0 and 2147483646 (the unit is millisecond). For example, RetryInterval=30000 means that it will try to reconnect every 30000 milliseconds.
     If you do not configure this parameter, the value is 30000 milliseconds by default.
   - **RetryCount** – Customize the reconnection times after the network connection is interrupted. Enter any positive integer between 0 and 9. For example, RetryCount=9 represents when the network connection is interrupted, it can reconnect at most 9 times.
     If you do not configure this parameter, the value is 6 by default.
   - **CustomizedMetadata** – Configure if customized metadata or user-added metadata is supported. By default, customized metadata and user-added metadata are all supported.
   - **CustomizedMode=Close** – This physical device will not support customized metadata or user-added metadata.
   - **CustomizedMode=SupportAll** – This physical device will support all customized metadata and user-added metadata.
   - **CustomizedMode=CustomizedOnly** – This physical device will only support user-added metadata.
   - **Cert_thumbprint** - If you have a self-signed certificate for S3 server and only want to pass the certificate validation with a specific thumbprint, enter your thumbprint as the value of the parameter.

- **Cert_thumbprint** – If you have a self-signed certificate for S3 server and only want to pass the certificate validation with a specific thumbprint, enter your thumbprint as the value of the parameter.
- **Virtualhosting** – By default, it is set to false. If your bucket does not support using path-style domain names, you need to configure virtualhosting = true to use virtual-hosted-style domain names.

Google Cloud Storage

IBM will, by default, automatically store your backup data in the archive storage class to help reduce storage costs. It is not recommended to enable the AutoClass feature in your storage, as any requests to change the storage class will fail and may result in additional costs.

Note the following:

- The following permissions are required for the Google Cloud Storage. For permission details, refer to IAM permissions for Cloud Storage.
  - storage.buckets.get
  - storage.objects.list
  - storage.objects.create
  - storage.objects.delete
  - storage.objects.get

Follow the instructions below.

1. **Storagetype** – Select **Google Cloud Storage** from the drop-down list.
2. **Bucket name** – Enter the bucket name you wish to access.

   > **Note:** The entered name must match an existing bucket. If no bucket is available, refer to Creating a bucket to create one.

3. **Service account key (.json)** – Click the **Browse** button to select and upload a service account key file in JSON format that has been generated in the Google Cloud Storage platform. To create a service account and a service account key, refer to Create a service account and Create a service account key.

Configure Backup Settings

The **Settings › Backup** page displays the common backup settings that you can directly enable.

You can choose to:

- Back up private/shared channels
- Back up the Recordings folder
- Back up Planner data
- Configure backup for Teams Chat
- Configure impersonation accounts for Public Folders backup
- Skip specific errors by error codes

Other than the settings above, you can also go to the legacy UI for more backup settings or contact the for assistance. For additional backup settings that can be enabled on your demand, refer to “On-Demand Backup Settings” on page 89.

Back up private/shared channels

Select whether to back up private/shared channels in Microsoft Teams. You can configure an app profile to connect your tenant for a successful backup of private/shared channels or you can still use the obsolete service account method. The service account you use must be an **owner** of all current and future private/shared channels. For details refer to Manage Scan Profiles.

Back up Recordings folder

As updated by Microsoft™ for Microsoft™ Teams, all new Teams meeting recordings will be saved to OneDrive and Share Point. (The change from using Microsoft™ Stream to OneDrive for and SharePoint for meeting recordings will be a phased approach. For details, refer to this Microsoft article.

Microsoft™ will create the Recordings folder or use the existing Recordings folder in your OneDrive (user's *OneDrive/Recordings*) or the Recordings folder in the Documents library of the Teams channel (*Teams channel site/Documents/ChannelName/Recordings*) to store the meeting recording files.

You can now use the **Back up Recordings folder** option to control whether to include the **Recordings** folder in the backup. By default, the **Back up Recordings folder** option is deselected.

> **Note:** Once you select this option to back up the **Recordings** folder, the **Recordings** folder will always be included in the subscription consumption, even if you deselect it in the future.

Note the following for excluding the Recordings folder from backup:

- If you are using a custom app to protect OneDrive, to exclude the **Recordings** folder from the OneDrive backup, ensure the Microsoft Graph permission has been updated.
- As there aren't any properties to distinguish the Stream files from the other MP4 files or if the **Recordings** folder was created manually or automatically, the **Recordings** folder found in the specific paths will be excluded, as well as all the content in it. Please do not use this folder to store the other files that you want to protect via IBM® Storage Protect for Cloud Microsoft™ 365.
- If you delete a public channel from Teams, its connected channel folder in the team site (the folder with the channel name under the Documents library) will not be deleted. This folder will no longer be identified as a channel folder, and its **Recordings** folder will no longer be regarded as the folder storing meeting recording files for a channel. If you deselected the **Back up Recordings folder** option at this time, the backup job will still include this Recordings folder as well as its parent folder for the backup of site content.
- (API limitation) In the app context (using app profile authentication or the hybrid mode), the backup service for OneDrive will create the **Recordings** folder automatically if it does not exist.
- If you want to exclude the Recordings folder after this Recordings folder has been protected for a while, you will be notified that deselecting this folder will create a gap in backups for recordings saved between this point in time and whenever you choose to enable this option again. We will not retroactively protect recordings outside this window.

Back up Planner Data

Select whether to protect the Planner data. This option is by default disabled if you are a new customer to IBM® Storage Protect for Cloud Microsoft™ 365 after July 2023 release, or you have been using app profile only for Auto discovery.

If you are an existing customer who has been using service account authentication for auto discovery or using app profile authentication with an additional delegated app to protect Planner data, this option will be enabled in this case, and your Planner data will continuously be protected.

Configure backup for Teams chat

If you enable the Teams Chat service, you can choose whether to use the**default Microsoft Graph API** or**Teams Export API model B** to retrieve Teams chat messages from Microsoft Teams Chat for backup and you must customize the backup start date for Teams chat messages. Note that the backup start date cannot be changed once saved.

Using the free default Microsoft Graph API can potentially result in less optimal performance compared to the Teams Export API model B. The Export API model B will charge the app creator $ 0.00075 per message and that it may cost a lot if you have a large scale of chat messages to protect. You can follow this Microsoft article to look up the number of the Teams chat messages in your tenant and estimate the cost.

Configure impersonation accounts for Public Folders

The impersonation accounts that you configured for Public Folders in IBM® Storage Protect for Cloud interface are synchronized to IBM® Storage Protect for Cloud Microsoft™ 365 after July 2023 release. IBM® Storage Protect for Cloud in app context only will use the impersonation accounts for the backup and restore of Public Folders.

The Public Folders service will perform operations by using the permissions that are associated with the impersonation accounts. We recommend a 1:500 ratio for the impersonation accounts and the Public Folders. For more information about impersonation technology, see Impersonation and EWS in Exchange
The impersonation accounts configured must meet the following conditions:

- The impersonation account must have the Exchange Online product license.
- This user must also have the **Owner** permission to the Public Folders.

Skip specific errors by error codes

For some job errors, IBM® Storage Protect for Cloud Microsoft™ 365 provides error codes, and you can find them in the job report. For more information, refer to the Troubleshooting Guide. If you wish to ignore specific errors and prevent them from affecting the job status, you can skip these errors by error codes.

> **Note:** The configuration will apply to all objects in all service types that encounter the corresponding errors, including newly scanned objects.

On-Demand Backup Settings

We have removed several backup settings that are less common. If you want to enable these settings, you can contact the support team for assistance. For details, refer to the following:

Back up recoverable items and their primary mailboxes

You can choose to protect the **Recoverable Items** folder in the user's primary mailbox for the Exchange Online service. If you want to enable this feature, contact support for assistance. Note that an additional cost is required. Currently, we support the **Deletions**, **Purges**, **Versions**, and **DiscoveryHolders** subfolders in the **Recoverable Items**. For more information about Recoverable Items, refer to this Microsoft article: Recoverable Items folder in Exchange Online. On the backup data tree, you can find the data in the following directory: *mailbox address/Recoverable Items folder (System)*. This folder cannot be a destination for an out of place restore, and the backup data of this folder being restored to its original mailbox will use the following name: **Recovery Items folder (System) _ Restored**. Note that due to the API limitation, this folder directory will always be displayed in English regardless of the preferred display language of Microsoft 365.

Back up the Preservation Hold library

By default, the **Preservation Hold** library is not protected by IBM® Storage Protect for Cloud Microsoft™ 365. If you want to enable this feature, IBM Software Support for assistance. Note that an additional cost is required.

Back up item and file versions

By default, history versions of items and files are not backed up due to the regular recovery points created by backup jobs, as well as Microsoft 365 API overhead and limitations related to versions. Our experience shows that most user and legal requests pertain only to the most recent active version. Additionally, we capture multiple roll-back points during our daily backups to ensure you have a change history for each document outside native versioning.

If you need to back up the versions for some reason and are willing to accept the performance impact, please contact IBM support to have it enabled.

> **Note:** Once the function is enabled, only versions created after this point can be backed up in subsequent jobs. Earlier versions will not be included..
> The backup job will include the most recent 10 versions by default. Due to API limitations, the OneDrive service does not support protecting items and file versions.

Include specific mailbox folders (Deleted Items and Junk Email)

By default, the **Deleted Items** folder and the **Junk Emails** folder will not be protected. Keeping these options unchecked will improve job performance.

Back up Public Folder metadata

By default, Public Folder metadata will not be protected. IBM® Storage Protect for Cloud Microsoft™ 365 now supports the backup of Public Folder metadata via app profile authentication. To protect Public Folder metadata, ensure your backup for Public Folder metadata is enabled and the **Exchange Administrator** role is assigned to the app in Microsoft Entra ID.

Configure Retention Policy

Either using the IBM® Storage Protect for Cloud default storage or your own storage, the data retention settings can be applied to your backup data to help save your storage costs.

About this task

If there is backup data approaching the retention period, your administrator group or partner's administrator group will receive the **Data Retention Notification**. Note that the Teams Chat service does not support the retention policy.

- If you want to keep your data in default storage, you can contact your IBM® Storage Protect for Cloud Account Manager to update your subscription and increase your retention settings, but please note that increasing your data retention may increase the price you pay for your backup. If you want to archive the backup data that met the retention settings for potential restore in the future, instead of letting them be deleted from IBM® Storage Protect for Cloud storage, you can submit an export request to export the data from the default storage as a paid service. For details, refer to "Introduction to Data Export Service" on page 159.

- If your subscription is the BYOS type, you can update your retention settings by navigating to **Settings › Retention Policy › Data retention settings**. Increasing your data retention may increase the price you pay for your backup.

If you changed storage from the default IBM® Storage Protect for Cloud storage to BYOS, or from BYOS to the default storage, your changes on the retention policies would apply to your overall backup data. This means, your legacy backup data in the previous storage will be removed when it reaches the data retention date.

For customers who have purchased a BYOS subscription or subscription using default IBM® Storage Protect for Cloud storage with an unlimited retention subscription, the retention policy supports being configured at container level for each service type. Note that the default retention period for BYOS subscription is one year. Once the next full snapshot of your Microsoft™ 365 scope takes place, we will begin pruning the old backup data that met your retention settings.

Note: We always maintain at least one full backup cycle of your data, so the retained backup data may span a period longer than the configured retention duration.

You can now configure a retention period that is less than one year (from 30 to 365) for services and containers. To enable the day unit retention policy, contact IBM Software Support for assistance.

Note:

- The day unit retention is not applicable to the channel conversations and settings in Teams, and the Viva Engage messages. Note that Power BI, Power Automate, and Power Apps do not support day unit retention.

- The day unit retention job will ensure that any data you deleted from Microsoft 365 only lives for the configured period of time, regardless of your backup cycle. The backup data will be destroyed and unrecoverable. If the data exists in Microsoft 365 but has no recovery points within the retention period, its last recovery point that may have exceeded the retention period will be retained. However, when you search for this content to restore, the recovery point can only be displayed for the start date of the configured retention period.

> **Note:** For BYOS customers, the day unit retention policy is not designed to reduce storage costs. Initially, the backup data will be destroyed and marked for deletion, but it does not immediately reduce the data size in your storage. Additionally, there is an annual task that permanently deletes data deemed unavailable to help manage long-term storage requirements.

- If you contact IBM Software Support to disable the day unit retention policy, your retention policy will be reset according to the retention policy in your subscription. You need to navigate to the IBM® Storage Protect for Cloud Microsoft™ 365 interface to customize your retention policy again.

Procedure

Follow the steps below to update the retention period for a specific service type or configure the container-specific retention policies:

1. Navigate to **Settings › Retention › Data retention settings**.
2. To apply a default retention period for your backup data of all service types, select the **Set a default retention period for all services** option and update the number in the box below. Note that the retention period you can set for the retention policy cannot exceed your purchased retention years. If your subscription contains an unlimited data retention agreement, you can customize the data retention years for each of the services. Before the retention period of your data of a certain service type expires, your tenant owner will receive an email notification.
3. With the **Configure retention policy for each service** option selected, all the enabled service types are displayed. Note that the Teams Chat service does not support the retention policy and all backup data of Teams Chat will be retained until the subscription expires.
4. You can update the number for each service type under the **Retention Period** column to define the default retention period for the specific service type.
5. If you would like to define retention policies for a specific container of that service type, you can turn on the switch under the **Customize Containers** column. The **Customize Container Level Retention Policy** pane will appear. Note that Power Apps and Power Automate do not support container level retention settings.
6. In the **Specialized retention settings** section, you can update the default retention period for newly created containers in the future and for objects that are currently not included in any containers. Then you can update the number under the **Retention Period** column in the table for a specific container. Day unit retention policy is currently supported at the container level.
7. Click **Save** in the **Customize Container Level Retention Policy** pane to save your changes to the retention policy of the corresponding service type, or click **Cancel** to exit.
8. You can repeat the actions from steps 5 to 7 to customize the container level retention policy for the other service types.
9. Click **Apply** at the bottom of the **Date retention settings** page to update the settings.

Configure Mapping Settings

If you want to restore items to another location, you may want to map the source domain or user to the destination to update the permissions and metadata, or map the source language to the target language to display the source content in the target language.

To configure the mapping settings, expand the **Settings** tree on the left pane, and then click **Mapping Settings**. Refer to the section below to configure the "Domain Mapping" on page 93, "Language Mapping" on page 92, and "Language Mapping" on page 92.

> **Note:** Domain mapping only supports Microsoft™ 365 Group Planner data and Project Online data; user mapping does not support mapping Microsoft™ 365 groups.

User Mapping

Procedure

In the **User Mapping** tab, you can perform the following actions:

- Click the **Create a New Profile** button to create a new user mapping profile. For details, refer to "Create a New User Mapping Profile" on page 92.
- Click the mapping profile name to view the details of a user mapping profile. If you want to make changes to this profile, click **Edit**.
- Select the mapping profile and then click the **Edit** button to edit the user mapping profile.
- Select the mapping profile and then click the **Delete** button to delete the user mapping profile.

Create a New User Mapping Profile

Procedure

To create a new user mapping profile, follow the steps below:

> **Note:** User mapping does not support mapping Microsoft™ 365 groups.

1. Click **Create mapping profile**. The **Create a new user mapping** pane appears.
2. Configure the following settings:
   - **Name** – Enter the name of the new user mapping profile.
   - **Description** – Enter an optional description for this user mapping profile for future reference.
   - **Mapping rules** – Configure user mapping rules by clicking **Add**. Enter the **Source username** and **Destination username**. To delete a user mapping rule, click the **Delete** (🗑) button.

     > **Note:** Only one user mapping rule can be configured for a source user.

   - **Customize settings if the user does not exist in destination** – This option is deselected by default. With this option selected, enter the username of the **Target Default User**. Keep this option deselected if you do not want to customize the target default user.
3. Click **Save** to save the configurations for this user mapping profile and return to the **Mapping › User mapping** tab.

Language Mapping

You can configure the language mappings in IBM® Storage Protect for Cloud Microsoft™ 365 for English, German, and French.

Procedure

In the **Language mapping** tab, you can perform the following actions:

- Click the **Create mapping profile** button to create a new language mapping profile. For details, refer to "Create a New User Mapping Profile" on page 92.
- Click the mapping profile name to view the details of a language mapping profile. If you want to make changes to this profile, click **Edit**.
- Select the mapping profile and then click the **Edit** button to edit the language mapping profile.
- Select the mapping profile and then click the **Delete** button to delete the language mapping profile.

Create a New Language Mapping Profile

Procedure

To create a new domain mapping profile, follow the steps below:

1. Click **Create mapping profile**. The **Create a new language mapping** pane appears.
2. Configure the following settings:
   - **Name** – Enter the name of the new language mapping profile.
   - **Description** – Enter an optional description for this language mapping profile for future reference.
   - **Source Language** – Select the language from the drop-down list that the source node is displayed in.
   - **Target Language** – Select the language from the drop-down list that you want to have the destination node display.
   - **Mapping Rules** – Configure language mapping rules by clicking **Add**. Select **List/Library** or **Column** from the **Type** drop-down list. Enter the name of the list/library or column used in the source language. Enter the name of the list/library or column you want the target language to use in the destination node. The source column or list/library name will be replaced by the specified destination column or list name. To delete a language mapping rule, click the Delete (🗑) button.

   > **Note:** The value of the same type in the **Source text** field cannot be the same.

3. Click **Save** to save the configurations for this language mapping profile and return to the **Mappings › Language mapping** page.

Domain Mapping

Procedure

In the **Domain Mapping** tab, you can perform the following actions:

- Click the **Create mapping profile** button to create a new domain mapping profile. For details, refer to "Create a New Domain Mapping Profile" on page 93.
- Click the mapping profile name to view the details of a domain mapping profile. If you want to make changes to this profile, click **Edit**.
- Select the mapping profile and then click the **Edit** button to edit the domain mapping profile.
- Select the mapping profile and then click the **Delete** button to delete the domain mapping profile.

Create a New Domain Mapping Profile

Procedure

To create a new domain mapping profile,s follow the steps below:

1. Click **Create mapping profile**. The **Create a new domain mapping** pane appears.
2. Configure the following settings:
   - **Name** – Enter the name of the new domain mapping profile.
   - **Description** – Enter an optional description for this domain mapping profile for future reference.
   - **Mapping Rules** – Configure domain mapping rules by clicking **Add**. Enter the **Source domain** and **Destination domain** using the format in the example. To delete a domain mapping rule, click the Delete (🗑) button.

> **Note:** Only one domain mapping rule can be configured for each source domain.

3. Click **Save** to save the configurations for this domain mapping profile and return to the **Mappings › Domain Mapping** page.

Configure End-User Restore Settings

Through the **Settings › End-user restore › End-user restore setting for IBM® Storage Protect for Cloud Recovery Portal users page** , you can choose whether to enable the end-user restore functionality for IBM® Storage Protect for Cloud Recovery Portal. This includes allowing users to recover or export, the backup data of the supported services, as well as specifying who has permission to restore or export, the Team/Group/Power BI backup data via IBM® Storage Protect for Cloud Recovery Portal.

You can also choose whether to allow IBM® Storage Protect for Cloud Recovery Portalusers to recover sharing links of the backup data.

The **End-user restore** setting is only available to your application administrators or the service provider.

- If you do not want to allow the end-user restore, you can turn off the **IBM® Storage Protect for Cloud Recovery Portal users to recover backup data** switch. You can also separately disable the end-user restore or export, for the following services: Exchange Online, OneDrive, SharePoint Online, Microsoft 365 Groups, Teams, Teams Chat, Power BI, and Power Automate. Note that Power BI only supports the end-user restore, and Teams Chat and Power Automate only supports the end-user export.
- With the end-user restore enabled, you can select the user roles for who can perform the restore or export, for Teams and Groups, and who can restore Power BI reports from IBM® Storage Protect for Cloud Recovery Portal.

> **Note:** If your subscription was updated to use IBM® Storage Protect for Cloud default storage from using your own storage (BYOS subscription), this page will be unavailable, and your end users cannot restore the backup data stored at the archive tier from your own storage. In this case, you can help them perform the restore from IBM® Storage Protect for Cloud Microsoft™ 365 interface instead.

By default, sharing links for SharePoint Online, OneDrive and Team/Group data won't be restored when end users restore the backup data through IBM® Storage Protect for Cloud Recovery Portal. To enable the restore of sharing links, you can turn on the **Allow IBM® Storage Protect for Cloud Recovery Portal users to recover sharing links** switch.

> **Note:** For OneDrive backup cycles after November 2022, sharing links will always be restored and cannot be controlled by the **Allow IBM® Storage Protect for Cloud Recovery Portal users to recover sharing links** setting.

Configure Security Settings

In **Settings** > **Security**, you can choose to:

- Export Encryption Keys
- Enable the approval process for data deletion
- Enable message search and browsing with the Teams Chat Restore wizard

Export Encryption Keys

This feature is only available for administrators of the IBM® Storage Protect for Cloud tenant. The Support account you invited for troubleshooting will not be able to access the page. To export the encryption key, navigate to **Settings › Security › Encryption keys**.

By default, this page is not available to the users who are using default storage hosted by IBM. You can contact the Support Team to enable this feature if needed.

The backup data generated by IBM® Storage Protect for Cloud is encrypted. If you have chosen our data export service, you will need an encryption key to help you convert the backup data to plain file format. Note that you must export the encryption key before your move away from this product, as you will not be able to sign in to the IBM® Storage Protect for Cloud interface if your subscription has ended.

If you only want to export a small set of backup data to plain file format, use the Export feature we provided in the **Restore** wizard. For details, refer to “Export and Download Your Data” on page 98.

Before generating encryption keys, you should first set a password for encryption keys and click the **Apply** button to apply the password. The password is used to access the encryption keys in the standalone tool. You can also configure whether to allow IBM® Storage Protect for Cloud Microsoft™ 365 to copy the encryption keys to your BYOS storage weekly.

To generate and download the encryption key for the service types for which you have performed a backup, click the **Generate** button to generate the key, and then click **Download** to download the ZIP file and save it to your local computer.

If you have performed backups or updated the password after the last time you generated the key, click **Regenerate** to regenerate the key for the updated backup data and download the file again.

Enable Approval Process for Data Deletion

To avoid accidental data loss, you can set an approval process for the data deletion. With this feature enabled, data deletion requests and email notifications will be sent to the administrators when you delete data in **Manually delete backup data** and **Data subject access requests**.

To enable the approval process for the data deletion, navigate to **Settings** > **Security**, and turn on the **Enable the approval process for data deletion** switch Note that the approval process for data deletion cannot be disabled once it’s enabled due to IBM's security measures.

Then administrators can access the IBM® Storage Protect for Cloud Microsoft™ 365 interface and click **My tasks** (📅) on the upper-right of the interface to view the request details, and then approve or reject your requests.

The deletion jobs will start when the requests are approved. Note that the requests will be automatically invalidated if not approved within 7 days.

Enable Message Search and Browsing with the Teams Chat Restore Wizard

Select whether to allow users to search and browse chat messages in the Teams Chat Restore wizard. Once disabled, in the Teams Chat Restore wizard, users have no permissions to access Chat message search results through the **Search mode**, and cannot browse Teams chat messages through the **Calendar mode**.

User Management

User Management provides centralized management of groups and securities. Administrators can add and manage groups for security control of what users can restore, export and delete, and whether the users can view reports or configure settings in IBM® Storage Protect for Cloud Microsoft™ 365. Security group allows you to organize users in IBM® Storage Protect for Cloud Microsoft™ 365 more efficiently. You can add users to a security group, and then all users in that group will have permission to restore any objects that are contained in the object containers that have been assigned to this group.

Administrators group is the built-in group that has all permissions in IBM® Storage Protect for Cloud Microsoft™ 365. You cannot remove this group or update its permissions. The security groups you created will be listed on the **User Management** page.

> **Note:** The users and groups who have been designated as service administrators of IBM® Storage Protect for Cloud Microsoft™ 365 will be automatically synchronized to the Administrators group. If the user is demoted from the IBM® Storage Protect for Cloud Microsoft™ 365 application administrator to a standard user, IBM® Storage Protect for Cloud Microsoft™ 365 will automatically remove this user from the **Administrators** group as well.

When you add a security group, distribution group, or mail-enabled security group to IBM® Storage Protect for Cloud, the following users cannot sign into IBM® Storage Protect for Cloud Microsoft™ 365:

- The owner of the distribution group or mail-enabled security group.
- If the security group has nested groups and the owner of a nested group is not a member of any other groups that have been added to IBM® Storage Protect for Cloud/IBM® Storage Protect for Cloud Microsoft™ 365, the nested group owner cannot sign into IBM® Storage Protect for Cloud Microsoft™ 365.

Create a Security Group

To manage user permissions more efficiently, you can create a security group for a set of users and configure the group permissions. The users within this group will have the restore permission when the group is granted.

Procedure

1. On the **User Management** page, click **Create Security Group**.
2. In the right pane for creating a new security group, enter the group name and an optional description.
3. Enter the users or groups that you want to add to this group into the **Invite users/groups** box. The users and groups you grant permissions to must exist in your tenant and have license and permissions to access IBM® Storage Protect for Cloud Microsoft™ 365.
4. Then you can **Define services and permission assigned to users**:
   a. **Backup scope -** Turn on the switch. Then choose between **View Only** and **View and Edit** permissions for users and select service types that you want to assign to users.
   Users with the **View and Edit** permission can take the following actions:
      - View the selected services, and configure backup and view backup details for the selected modules in the **Backup** page.
      - View backup jobs for the selected services, and generate and download job report in **Job monitor**.
      - View the **Remove unprotected data** for the selected services.

   Compared to users with the **View and Edit** permission, users with the **View Only** permission cannot configure the backup.

   b. **Data scope**– Turn on the switch and select whether to assign the permission on **Restore**, **Export**, and **Deletion** to users. Then turn on the switch of service types and select containers to define the **Permission scope**for users. To select all containers for this service type, select the **Select all** option in the column header.

The containers you selected will be displayed for the selected service type. The users of this group can run corresponding **Restore**, **Export**, or **Deletion** jobs for the containers in the permission scope of the selected services.

- **Restore**: With the restore permission selected, the **Restore**, **Backup data e-discovery** and the **Mapping** settings will be displayed in the navigation. When selecting some data in **Restore** or **Backup data e-discovery**, the **Restore** button will appear. The user can also view the restore jobs for the selected services, and generate and download job report in **Job monitor.**
  For objects no longer in the backup scope, users with **Restore** permission to the last container where the object existed can now restore its backup data, not just administrators. Note that only objects removed after the November, 2024 release are supported.
- **Export**: With the export permission selected, the **Restore** and **Backup data e-discovery** will be displayed in the navigation. When selecting some data in **Restore** or **Backup data e-discovery**, the **Export** button will appear. The user can also view the export jobs for the selected services, and generate and download job report in **Job monitor.**
- **Deletion**: With the deletion permission selected, the **Data subject access requests**, **Manually delete backup data** and **Backup data e-discovery** will be displayed in the navigation. When selecting some data in **Manually delete backup data** or **Backup data e-discovery**, the **Delete** button will appear. The user can also view the deletion jobs for the selected services, and generate and download job report in **Job monitor.**

c. **Report center -** Turn on the switch so that users can view the reports in **Report center**.
With the permission turned on, the subscription consumption report, in **Subscriptions**, **End-user restore report, Job analytics report**, **System auditor** report, and **Unusual activities analysis** report, **Coverage report** are available to the user.

> **Note:** If some users in a security group have been granted the permission to **Report center** only without the **Restore** or **Export** permission, the Go to Restore page option in the **Microsoft 365 unusual activities analysis** > **View details** page will be hidden.

d. **Settings**– Turn on the switch so that users can view and configure **Settings**.
With the **Settings** permission turned on, the user can configure the **Storage**, **Backup** settings, **Notification**, **Retention** policy (including retention settings for offboarded users, **Mapping** settings, **End-user restore** settings and export **Encryption key**s.

5. Click **Save** to save your configurations; click **Cancel** to exit the creation.

Export and Download Your Data

IBM® Storage Protect for Cloud Microsoft™ 365 helps you export and download your backup data for Exchange Online, SharePoint Online, OneDrive, Microsoft™ 365 Groups, Project Online, Public Folders, Teams, Teams Chat, Yammer, Power BI, Power Automate, or Power Apps.

After you export your data, you can navigate to the **Job Monitor** to download the exported data to a local location. You can stop a running export job as needed.

For customers with more than 100 purchased user seats, you can export up to **500** GB of data per month for all services in total by default. For customers with 100 or less purchased user seats, the monthly limitation is 100 GB. The exported data must be downloaded within seven days; otherwise, the data will be removed. This quota limitation also applies to the BYOS subscription. Contact your IBM sales representative for additional help on quota limitations.

> **Note:** The generic lists will be exported to CSV files with the metadata of their folders and items. The item's attachments will be exported as individual files, and the links will be displayed in the following format: **LinkDisplayName(WebAddress)** in the exported CSV file.

If you cannot extract the exported file with Windows™ built-in "Extract" utility, try with a decompression software, like 7-Zip.

If you are using your own **Azure Blob Storage**, note that the Export job cannot export the backup data from **archive tier**.

A password is used to protect your exported data. After the data has been successfully exported, the account that performs the export job and the email addresses configured for Notification Settings (regardless of job status) will receive an email that notifies them to get the password through Job Monitor for extracting the exported data.

> **Note:** You can configure a set of email notification settings for the restore and export jobs, separate from the backup. For details, refer to "Configure Notifications" on page 68.

For the object levels of each service type that are supported for exporting backup data, refer to the Restore Options for Different Object Types.

Export Exchange Online Data

With IBM® Storage Protect for Cloud Microsoft™ 365, you can export the Exchange Online mailbox, folders, and mailbox items to PST files. The exported PST files can keep the Internet headers property.

About this task

> **Note:** When you select mailboxes to export, you can only select up to 10 mailboxes at once. The data of a mailbox will be exported to one corresponding PST file.

Procedure

Complete the steps below to export Exchange Online backup data:

1. Navigate to the **Restore › IBM® Storage Protect for Cloud Backup**page, and then click the **Exchange Online** tile.
2. Select the items that you want to export. You can choose one of the following methods to find the data to export:
   - **Search mode** - Define a mailbox as the search scope and then use the properties to search for the items within the mailbox. Refer to the steps below:

    a. In the **Name** field, enter or select a mailbox. The default search condition is to search the backup data of that mailbox within the last backup cycle.

    b. In the **Backup Time Range** field, the time range of the last backup cycle is displayed by default. Click the Calendar (📅) button to customize the backup time range. The start date must be earlier than the end date. You can click **Reset** if you want to reset the settings. Click **OK** to save your customization.

    c. Select **Mailbox**, **Folder**, or **Mailbox Item** from the **Level** list for the items you want to search. If you want to search for all folders or mailbox items within the selected mailbox, you can leave the search conditions empty. To search for specific folders, enter the folder name or the keywords in the **Folder Name** field; to search for the **Mailbox Item** level items, you can configure the following search conditions: **Subject**, **Sent From**, **Sent To**, and **Date Sent**.

    d. Click **Search** to search the items according to the conditions you configured. The search conditions and the search results are displayed. The results include all backup items, which meets the search conditions in Exchange Online mailboxes, Group mailboxes and Teams mailboxes. The search results table will display a maximum of 2000 items. You can edit the search conditions and click **Search** to adjust the search results.

    e. Find and select the item you want to export from the search results. In the drop-down list under the **Recovery point** column, select a backup job that backed up this item at the status that you want to export.

- **Calendar mode** - Find a backup job that backed up the items at the time of the status you want to export, and then search and select the items from the backup data of that backup job.

    a. In the calendar, all Exchange Online backup jobs are displayed. You can select whether to display the finished with an exception or failed jobs in the calendar by selecting the **Include jobs with only partial backup data** option. Note that the data of these jobs may be incomplete. Hover over a backup job to show the backup job details.

    b. Select a backup job. All backup data of Exchange Online, up to a maximum of 2000 items, is displayed in the table. To include deleted contents, click the **Show data** field and select **All backup data within the backup cycle**. You can also select the **Backup data only from this recovery point**option to only show the data backed up in the selected backup job.

    c. You can enter keywords to search the items, or you can click the backup data to browse the items you want to export.

3. After you have selected the backup data, click the **Export** button. You can either export all items in the folder/mailbox or export items sent within a specified period by configuring the time range.

Export SharePoint Online Data

With IBM® Storage Protect for Cloud Microsoft™ 365, you can export the backup data for SharePoint Online lists, libraries, folders, documents, and items.

Procedure

Complete the steps below to export Exchange Online backup data:

1. Navigate to the **Restore › IBM® Storage Protect for Cloud Backup**page, and then click the **SharePoint Online** tile.

2. Select the items that you want to export. You can choose one of the following methods to find the data to export:

    - **Search mode** - Define a SharePoint Online site collection as the search scope and then use the properties to search for the items within the scope. Note that this method does not support searching and restoring the list items.

      Refer to the steps below:

        a. In the **URL** field, enter the keywords in the URL or site title to search and select a SharePoint Online site collection. The default search condition is to search the backup data of that site collection within the last backup cycle. In the drop-down list, different types of sites can be distinguished by specific icons.

    b. In the **Backup Time Range** field, the time range of the last backup cycle is displayed by default. Click the Calendar (📅) button to customize the backup time range. The start date must be earlier than the end date. You can click **Reset** if you want to reset the settings. Click **OK** to save your customization.

    c. Select **List/Library**, **Folder**, or **Document** from the **Level** list for the items you want to search. Note that **Site collection**, **Site**, and **App** are not supported for data export. If you want to search for all lists or libraries, folders, or documents in the selected site collection, you can leave the search conditions empty. To search for specific lists/libraries, or folders, enter the title or name or the keywords for search; to search for specific documents, you can configure the following search conditions: **Document Name**, **Created Date**, **Created By**, **Modified By**, or **Document Size**.

    d. Click **Search** to search the items according to the conditions you configured. The search conditions and the search results are displayed. The results include all backup items which meet the search conditions in SharePoint Online sites, Project Online sites, Viva Engage sites, Group sites and Teams sites. The search results table will display a maximum of 2000 items. You can edit the search conditions and click **Search** to adjust the search results.

    e. Find and select the item you want to export from the search results. In the drop-down list under the **Recovery Point** column, select a backup job that backed up this item at the status that you want to export.

- **Calendar mode** – Find a backup job that backed up the items at the time of the status you want to export, and then search and select the items from the backup job data.

    a. In the calendar, all SharePoint Online backup jobs are displayed. You can select whether to display the finished with an exception or failed jobs in the calendar by selecting the **Include jobs with only partial backup data** option. Note that the data of these jobs may be incomplete. Hover over a backup job to show the backup job details.

    b. Select a backup job. All backup data of SharePoint Online, up to a maximum of 2000 items, is displayed in the table. You can select the **Show data from this backup only** option (historical data in this scope from previous backups not included) to only show the data backed up in the selected backup job

    c. You can enter keywords to search the items, or you can click the backup data to browse the items you want to export.

3. After you have selected the backup data, click the **Export** button above the table to export all selected items.

Export OneDrive Data

With IBM® Storage Protect for Cloud Microsoft™ 365, you can export the backup data for the OneDrive libraries, folders, and documents.

Before you begin

> **Note:** When you select OneDrive accounts to export, you can only select up to 10 accounts at once.

Procedure

Complete the steps below to export the backup data of OneDrive:

1. Navigate to the **Restore › IBM® Storage Protect for Cloud Backup**page, and then click the **OneDrive** tile.
2. Select the items that you want to export. You can choose one of the following methods to find the data to export:

    - **Search mode** – Define a OneDrive address as the search scope and then use the properties to search for the items within the scope. Note that this method does not support searching and restoring the list items.

      Refer to the steps below:

  a. In the **Name** field, enter or select a OneDrive address or display name to search. The default search condition is to search the backup data for that OneDrive Address within the last backup cycle. The drop-down list will remind you of OneDrive accounts with unusual activities or under ransomware attacks.

  b. In the **Backup Time Range** field, the time range of the last backup cycle is displayed by default. Click the Calendar (📅) button to customize the backup time range. The start date must be earlier than the end date. You can click **Reset** if you want to reset the settings. Click **OK** to save your customization.

  c. Select **OneDrive User**, **Library**, **Folder**, or **Document** from the **Level** list for the items you want to search. If you want to search for all sites, lists or libraries, folders, or the documents of that OneDrive user, you can leave the search conditions empty. To search for specific libraries or folders, enter the title or name or the keywords for search; to search for the specific **Document**-level items, you can choose whether to search for **Suspicious files** under potential ransomware attacks or **File deleted in unusual activities** in **File type** and configure the following search conditions: **Document Name**, **Created Date**, **Created By**, **Modified By**, or **Document Size**.

  d. Click **Search** to search the items according to the conditions you configured. The search conditions and the search results are displayed. The search results table will display a maximum of 2000 items. You can edit the search conditions and click **Search** to adjust the search results.

  e. Find and select the item you want to export from the search results. In the drop-down list under the **Recovery Point** column, select a backup job that backed up this item at the status that you want to export. The recovery points of the objects with unusual activities detected or potential ransomware attack detected will be displayed with 🔔 (**Unusual activities detected**) or 🔔(**Potential ransomware attack detected**).

- **Calendar mode** – Find a backup job that backed up the items at the time of the status you want to export, and then search and select the items from the backup data of that backup job.

  a. In the calendar, all OneDrive backup jobs are displayed. You can select whether to display the failed jobs or jobs that finished with an exception in the calendar by selecting the **Include jobs with only partial backup data** option. Note that the data of these jobs may be incomplete. Hover over a backup job to show the backup job details.

  b. Select a backup job. All backup data for OneDrive, up to a maximum of 2000 items, is displayed in the table. You can select the **Show data from this backup only** option (historical data in this scope from previous backups not included) to only show the data backed up in the selected backup job. Objects with unusual activities detected or potential ransomware attack detected will be displayed with 🔔 (**Unusual activities detected**) or 🔔(**Potential ransomware attack detected**).

  c. You can enter keywords to search the items that you can click the backup data to browse the items you want to export.

3. After you have selected the items that you want to export, click the **Export** button above the table to export all selected items.

Export Microsoft™ 365 Groups Data

With IBM® Storage Protect for Cloud Microsoft™ 365, you can export the backup data for a Microsoft™ 365 group, the lists, libraries, folders, items, and documents in the group team site, and the group mailbox, folders, and mailbox items. The group mailbox, folders, and mailbox items of the Microsoft™ 365 Group will be exported to PST files. The exported PST files can keep the Internet headers property.

Procedure

Complete the steps below to export the backup data of Microsoft™ 365 Groups:

1. Navigate to the **Restore › IBM® Storage Protect for Cloud Backup**page, and then click the **Microsoft 365 Groups** tile.

2. Select the items that you want to export. You can choose one of the following methods to find the data to export:

   - **Search mode** – Define a Microsoft 365 Group as the search scope and then use the properties to search for the items within the scope. Refer to the steps below:

     a. In the **Name** field, enter or select a Microsoft™ 365 Group. The default search condition is to search the backup data for the Microsoft™ 365 Group within the last backup cycle.

     b. To change the search conditions, click **Advanced Search** to expand this field.

     c. In the **Backup Time Range** field, the time range of the last backup cycle is displayed by default. Click the Calendar (📅) button to customize the backup time range. The start date must be earlier than the end date. You can click **Reset** if you want to reset the settings. Click **OK** to save your customization.

     d. Select **Microsoft 365 Group**, **Group Mailbox**, **Folder in Mailbox**, **Mailbox Item**, **Group Team Site**, **Site**, **List/Library**, **App**, **Folder in SharePoint**, **Document**, **Plan**, or **Task** from the **Level** list for the items you want to search. If you want to search for all objects at the level, you select from the selected Microsoft™ 365 Group. You can leave the search conditions empty.

        > **Note:** Group, Group Team Site, Site, App, Plan, and Task do not support data exporting.

     e. Click **Search** to search the items according to the conditions you configured. The search conditions and the search results are displayed. The search results table will display a maximum of 2000 items. You can edit the search conditions and click **Search** to adjust the search results.

     f. Find and select the item you want to export from the search results. In the drop-down list under the **Recovery point** column, select a backup job that backed up this item at the status that you want to export.

   - **Calendar mode** – Find a backup job that backed up the items at the time of the status you want to export, and then search and select the items from the backup data of that backup job.

     a. In the calendar, all Microsoft™ 365 Groups are displayed. You can select whether to display the failed jobs or jobs that finished with an exception in the calendar by selecting the **Include jobs with only partial backup data** option. Note that the data of these jobs may be incomplete. Hover over a backup job to show the backup job details.

     b. Select a backup job. All backup data of Microsoft™ 365 Groups, up to a maximum of 2000 items, is displayed in the table. You can select the **Show data from this backup only** option (historical data in this scope from previous backups not included) option to only show the data backed up in the selected backup job.

     c. You can enter keywords to search the items, or you can click the backup data to browse the items you want to export.

3. After you have selected the backup data, click the Export button.

Export Project Online Data

With IBM® Storage Protect for Cloud Microsoft™ 365, you can export the backup data of projects, libraries, lists, folders, items, and documents in a Project Online site.

Procedure

Complete the steps below to export Project Online backup data:

1. Navigate to the **Restore › IBM® Storage Protect for Cloud Backup**page, and then click the **Project Online** tile.

2. Select the items that you want to export. You can choose one of the following methods to find the data to export:

- **Search mode** – Define a Project Online site collection as the search scope and then use the properties to search for the items within the scope. Note that this method does not support searching and restoring the list items.

  Refer to the steps below:

  a. In the **URL** field, enter or select a Project Online site collection URL. The default search condition is to search the backup data of that site collection within the last backup cycle.

  b. In the **Backup Time Range** field, the time range of the last backup cycle is displayed by default. Click the Calendar (📅) button to customize the backup time range. The start date must be earlier than the end date. You can click **Reset** if you want to reset the settings. Click **OK** to save your customization.

  c. Select **Site Collection**, **Site**, **List/Library**, **Project**, **App**, **Folder**, or **Document** from the **Level** list for the items you want to search. If you want to search for all of the sites, lists or libraries, projects, apps, folders, or documents in the selected site collection, you can leave the search conditions empty. To search for specific sites, lists/libraries, projects, apps, or folders, enter the title or name or the keywords for search; to search for specific documents, you can configure the following search conditions: **Document Name**, **Created Date**, **Created By**, **Modified By**, or **Document Size**.

  d. Click **Search** to search the items according to the conditions you configured. The search conditions and the search results are displayed. The search results table will display a maximum of 2000 items. You can edit the search conditions and click **Search** to adjust the search results.

  e. Find and select the item you want to export from the search results. In the drop-down list under the **Recovery point** column, select a backup job that backed up this item at the status that you want to export.

- **Calendar mode** – Find a backup job that backed up the items at the time of the status you want to export, and then search and select the items from the backup data of that backup job.

  a. In the calendar, all Project Online backup jobs are displayed. You can select whether to display the failed jobs or jobs that finished with an exception in the calendar by selecting the **Include jobs with only partial backup data** option. Note that the data of these jobs may be incomplete. Hover over a backup job to show the backup job details.

  b. Select a backup job. All backup data of Project Online, up to a maximum of 2000 items, is displayed in the table. You can select the **Show data from this backup only** option (historical data in this scope from previous backups not included) to only show the data backed up in the selected backup job.

  c. You can enter keywords to search the items, or you can click the backup data to browse the items you want to export.

3. After you have selected the items, you want to export, click the **Export** button above the table to export all selected items.

Export Teams Data

With IBM® Storage Protect for Cloud Microsoft™ 365, you can export the backup data of Teams files or conversations, as well as Group mailboxes, mailbox folders, and mailbox items. Note that exporting Group mailbox data is only available in the Search mode. For detailed information on supported data types, refer to Restore Options for Different Object Types.

Procedure

Complete the steps below to export Teams backup data:

1. Navigate to the **Restore › IBM® Storage Protect for Cloud Backup**page, and then click the **Teams** tile.
2. 2. Select the items that you want to export. You can choose one of the following methods to find the data to export.
   - **Search mode** – Define a Team as the search scope and then use properties to search for the items within the scope. Refer to the steps below:

a. In the **Name** field, enter or select a Team. The default search condition is to search the backup data within the last backup cycle.

b. In the **Backup time range** field, the time range of the last backup cycle is displayed by default. Click the Calendar (📅)button to customize the backup time range. The start date must be earlier than the end date. You can click **Reset** if you want to reset the settings. Click **OK** to save your customization.

c. Select **Group mailbox**, **Folder in mailbox**, **Mailbox item**, **List/Library**, **Folder in SharePoint**, or **Document**, from the **Level** list for the items you want to search.

d. Click **Search** to search the items according to the conditions you configured. The search conditions and the search results are displayed. The search results table will display a maximum of 2000 items. You can edit the search conditions and click **Search** to adjust the search results.

> **Note: Teams**, **Group Team Site**, **Site**, **App**, **Plan** and **Task** are not supported for data export.

- **Calendar mode** – Find a backup job that backed up the items at the time of the status you want to recover, and then search and select the items from the backup data of that backup job.

a. In the calendar, all backup jobs of Teams are displayed. You can select whether to display the finished with an exception or failed jobs in the calendar by selecting the **Include jobs with only partial backup data** option. Note that the data of these jobs may be incomplete. Hover over a backup job to show the backup job details.

b. Select a backup job. All backup data of Teams, up to a maximum of 2000 items, is displayed in the table. You can select the **Show data from this backup only** option (historical data in this scope from previous backups not included) to only show the data backed up in the selected backup job.

c. You can enter keywords to search the items, or you can click the backup data to browse the items you want to restore.

3. Select a node, and then click **Export**.

4. An export job for Teams will start, and you can navigate to Job Monitor to view the job status and download the exported data.

Export Teams Chat Messages

About this task

You can search and select the users, specific chats, or individual chat messages to export. The chat messages will be exported to an HTML file. For additional details on the supported and unsupported data types of Teams Chat Message, refer to “Teams Chat Data Types” on page 242.
Note the following:

- When you select users to export, you can only select up to 10 users at once.
- When exporting Teams Chat with multiple users whose names contain more than 1000 characters in total, the export ZIP file will be empty.

Procedure

Complete the steps below to export Teams Chat messages:

1. Navigate to the **Restore › IBM® Storage Protect for Cloud Backup**page, and then click the **Teams Chat** tile.
2. Select the items that you want to export. You can choose one of the following methods to find the data to export.

   - **Search mode** – Define the search scope and then use the properties to search for the items within the scope. Refer to the steps below:

a. In the Name field, enter or select the user principal name. The default search condition is to search the backup data within the last backup cycle.

b. In the **Backup Time Range** field, the time range of the last backup cycle is displayed by default. Click the Calendar (📅) button to customize the backup time range. The start date must be earlier than the end date. You can click **Reset** if you want to reset the settings. Click **OK** to save your customization.

c. Select **Users**, **Chats**, or **Chat Messages** from the **Level** list for the items you want to find and enter the keywords in the corresponding property field for search. You can also leave the search conditions empty to search for all the objects of the selected level.

d. Click **Search** to search the items according to the conditions you configured. The search conditions and the search results are displayed. The search results table will display a maximum of 2000 items. You can edit the search conditions and click **Search** to adjust the search results.

- **Calendar mode** – Find a backup job that backed up the items at the time of the status you want to recover, and then search and select the items from the backup data of that backup job.

a. In the calendar, all backup jobs of **Microsoft Teams Chat** are displayed. You can select whether to display the finished with exceptions or failed jobs in the calendar by selecting the **Include jobs with only partial backup data** option. Note that the data of these jobs may be incomplete. Hover over a backup job to show the backup job details.

b. Select a backup job. All backup data, up to a maximum of 2000 items, are displayed in the table. You can select the **Show data from this backup only** option (historical data in this scope from previous backups not included) to only show the data backed up in the selected backup job.

c. You can enter keywords to search the items, or you can click the backup data to browse the items you want to restore.

3. Select a node, and then click **Export**.

4. An export job for Teams will start, and you can navigate to Job Monitor to view the job status and download the exported data.

Export Viva Engage Data

You can export folders and files from the Viva Engage site and export the Viva Engage messages. You can only find the Viva Engage messages through time-based restore wizard (drill down a backup job).

Before you begin

For detailed information on supported data types, refer to Restore Options for Different Object Types.

Procedure

Complete the steps below to export Viva Engage backup data:

1. Navigate to the **Restore › IBM® Storage Protect for Cloud Backup**page, and then click the **Viva Engage** tile.

2. Select the items that you want to export. You can choose one of the following methods to find the data to export.

   - **Search mode** – Define a Viva Engage community as the search scope and then use the properties to search for the items within the scope. Refer to the steps below:

     a. In the **Name field**, enter or select a Viva Engage community. The default search condition is to search the backup data within the last backup cycle.

     b. In the **Backup Time Range** field, the time range of the last backup cycle is displayed by default. Click the Calendar (📅) button to customize the backup time range. The start date must be earlier than the end date. You can click **Reset** if you want to reset the settings. Click **OK** to save your customization.

c. Select **Viva Engage Community, Site Collection, Site, List/Library, App, Folder in SharePoint, Document, Plan**, or **Task** from the **Level** list for the items you want to search. If you want to search for all objects at the level, you select from the selected Viva Engage Community. You can leave the search conditions empty.

d. Click **Search** to search the items according to the conditions you configured. The search conditions and the search results are displayed. The search results table will display a maximum of 2000 items. You can edit the search conditions and click **Search** to adjust the search results.

- **Calendar mode** – Find a backup job that backed up the items at the time of the status you want to recover, and then search and select the items from the backup data of that backup job.

  a. In the calendar, all backup jobs of Viva Engage are displayed. You can select whether to display the finished with an exception or failed jobs in the calendar by selecting the **Include jobs with only partial backup data** option. Note that the data of these jobs may be incomplete. Hover over a backup job to show the backup job details.

  b. Select a backup job. All backup data, up to a maximum of 2000 items, are displayed in the table. You can select the **Show data from this backup only** option (historical data in this scope from previous backups not included) to only show the data backed up in the selected backup job.

  c. You can enter keywords to search the items, or you can click the backup data to browse the items you want to restore.

3. Select a node, and then click **Export**.

4. An export job for Viva Engage will start, and you can navigate to Job Monitor to view the job status and download the exported data.

Export Power BI Data

You can export the backup data of the Power BI reports to a local location.

Procedure

Complete the steps below to export Power BI reports:

1. Go to the **Restore › IBM® Storage Protect for Cloud Backup**page, and then click the **Power BI** tile.

2. Select the items that you want to export. You can choose one of the following methods to find the data to export.

   - **Search mode** – Define a Power BI workspace as the search scope and then use the properties to search for the items within the scope. Refer to the steps below:

     a. In the **Name field**, enter or select a Power BI workspace. The default search condition is to search the backup data within the last backup cycle.

     b. In the **Backup Time Range** field, the time range of the last backup cycle is displayed by default. Click the Calendar (📅) button to customize the backup time range. The start date must be earlier than the end date. You can click **Reset** if you want to reset the settings. Click **OK** to save your customization.

     c. Select **Workspace** or **Report** from the **Leve**l list for the items you want to search.

     d. Click **Search** to search the items according to the conditions you configured. The search conditions and the search results are displayed. The search results table will display a maximum of 2000 items. You can edit the search conditions and click **Search** to adjust the search results.

   - **Calendar mode** – Find a backup job that backed up the items at the time of the status you want to recover, and then search and select the items from the backup data of that backup job.

     a. In the calendar, all backup jobs of Power BI are displayed. You can select whether to display the finished with an exception or failed jobs in the calendar by selecting **the Include jobs with only partial backup data** option. Note that the data of these jobs may be incomplete. Hover over a backup job to show the backup job details.

  b. Select a backup job. All backup data, up to a maximum of 2000 items, are displayed in the table. You can select the **Show data from this backup only** option (historical data in this scope from previous backups not included) to only show the data backed up in the selected backup job.

  c. You can enter keywords to search the items, or you can click the backup data to browse the items you want to restore.

3. Select a node, and then click **Export**.

4. An export job for Power BI will start, and you can go to **Job monitor** to view the job status and download the exported data.

Export Power Automate Data

You can export the backup data of the Power Automate flows. After the export job is completed, you can download the exported data to a local location. The exported data can be used as a template for importing flows to Power Automate.

Procedure

Follow the steps below to export the backup data:

1. Navigate to the **Restore › IBM® Storage Protect for Cloud Backup**page, and then click the **Power Automate** tile.

2. Select the items that you want to export. You can choose one of the following methods to find the data to export.

   - **Search mode** – Search for the Power Automate flows using the **Tenant** filter and the **Backup time range** filter, as well as the keywords in the properties of Flow. Refer to the steps below:

     a. In the **Flow name** field, enter the keyword in the flow name that you want to search for. The default search condition is to search the backup data within the last backup cycle.

     b. In the **Backup time range** field, the time range of the last backup cycle is displayed by default. Click the Calendar (📅) button to customize the backup time range. The start date must be earlier than the end date. You can click **Reset** if you want to reset the settings. Click **OK** to save your customization.

     c. You can also use the **Created date**, **Creator**, **Owner**, **State**, and **Environment** as the search conditions.

     d. Click **Search** to search the flows according to the conditions you configured. The search results table will display a maximum of 2000 items. You can edit the search conditions and click **Search**to adjust the search results.

   - **Calendar mode** – Find a backup job that backed up the items at the time of the status you want to recover, and then search and select the items from the backup data of that backup job.

     a. In the calendar, all backup jobs of Power Automate are displayed. You can select whether to display the finished with an exception or failed jobs in the calendar by selecting the **Include jobs with only partial backup data**option. Note that the data of these jobs may be incomplete. Hover over a backup job to show the backup job details.

     b. Select a backup job. All backup data, up to a maximum of 2000 items, are displayed in the table. You can select the **Show data from this backup only**option (historical data from previous backups will be excluded) to only show the data backed up in the selected backup job.

     c. You can enter keywords to search the items, or you can click the backup data to browse the items you want to export.

3. Select the flows, and then click **Export**.

4. An export job for Power Automate will start, and you can navigate to **Job monitor** to view the job status and download the exported data. You can use the exported files to import the flows back to your Power Platform.

Export Power Apps Data

You can export the backup data of the standard Canvas apps and component libraries to a local location.

Before you begin

The exported component library can be imported to Power Apps via the same entry as Importing a canvas app package. You must publish the imported component library to make it work. The component library will use a new ID after being imported, so the app which is connected with this component library before cannot be reconnected automatically. If you import an app that connects to a component library before, and the component library still exists in Microsoft 365, the app and the component library can be reconnected automatically.

Procedure

1. Navigate to the **Restore › IBM® Storage Protect for Cloud Backup**page, and then click the **Power Apps** tile.
2. Select the items that you want to export. You can choose one of the following methods to find the data to export.
   - **Search mode** – Search for the standard Canvas apps and component libraries using the **Tenant** filter and the **Backup time range** filter, as well as the keywords in the properties of standard Canvas apps and component libraries. Refer to the steps below:
     a. In the **Name** field, enter the keyword in the name of the standard Canvas app or component library that you want to search for. The default search condition is to search the backup data within the last backup cycle.

     b. In the **Backup time range** field, the time range of the last backup cycle is displayed by default. Click the Calendar (📅) button to customize the backup time range. The start date must be earlier than the end date. You can click **Reset** if you want to reset the settings. Click **OK** to save your customization.

     c. Select **All**, **Canvas** or **Component library** from the **Type** List for the items you want to search. The default type is all.

     d. You can also use the **Created date**, **Owner/Co-owner**, **User**, and **Environment** as the search conditions.

     e. Click **Search** to search the standard Canvas apps and component libraries according to the conditions you configured. The search results table will display a maximum of 2000 items. You can edit the search conditions and click **Search**to adjust the search results.
   - **Calendar mode** – Find a backup job that backed up the items at the time of the status you want to recover, and then search and select the items from the backup data of that backup job.
     a. In the calendar, all backup jobs of Power Apps are displayed. You can select whether to display the finished with an exception or failed jobs in the calendar by selecting the **Include jobs with only partial backup data**option. Note that the data of these jobs may be incomplete. Hover over a backup job to show the backup job details.

     b. Select a backup job. All backup data, up to a maximum of 2000 items, are displayed in the table. You can select the **Show data from this backup only**option (historical data from previous backups will be excluded) to only show the data backed up in the selected backup job.

     c. You can enter keywords to search for the standard Canvas apps and component libraries across tenants or in a specific tenant.

     d. You can select **Canvas** or **Component library** from the **Filters** list to only show the type you want. The default type is all.
3. Select the items you want to export, and then click **Export**.
4. An export job for Power Apps will start, and you can navigate to **Job monitor** to view the job status and download the exported data.

Download the Exported Data

In **Job Monitor › IBM® Storage Protect for Cloud Backup**page, find the job record after the job is finished and click the **Download Content** option from the More Commands (•••) list.

In the **Download content** panel, copy the password and click **Download** to save the exported data to your desired location. If a job exported the data of multiple mailboxes/sites, you can download the exported file for each mailbox/site individually.

Note: If the exported data size of any mailbox or site is greater than **20 GB**, or if the data is exported from multiple recovery points through the Search mode, the exported data will also be split for downloading.

Restore and Recover Your Data

IBM® Storage Protect for Cloud Microsoft™ 365 helps you quickly restore and recover your data from Exchange Online, SharePoint Online, OneDrive, Microsoft™ 365 Groups, Teams, Project Online, and Public Folders and Viva Engage. You can restore the backup data to its original location or restore data to a different location. If you have BYOS subscription, you can restore backup data to a custom storage location. After you have started the restore job, you can use Job Monitor to monitor the job progress and download job report. You can also stop a running restore job as needed.

> **Note:** If a top-level object (site collection, mailbox, or group/teams) has been deleted in Microsoft™ 365, you cannot restore the objects within the deleted top-level object individually. Instead, you must first restore their top-level nodes or manually create the top-level node in Microsoft™ 365 before you perform an in-place restore of the lower-level nodes.

If you want to restore items to another location, you may also need to map the domains, users, or languages to update the permissions and metadata in the restore destination. For detailed instructions, refer to “Configure Mapping Settings” on page 91.

You can find the data you want to restore through the **Search mode** or the **Calendar mode**. For the granular restore, the **Search mode** is better. You can also use the **Search mode** if you know the specific properties of the data you are looking for or want to restore deleted objects. To roll back your Microsoft 365 data to a specific snapshot or find the data by browsing the file structure, the **Calendar mode** will be helpful.

The **Search mode** restore wizard for SharePoint Online service allows you to search across all the sites being protected by IBM® Storage Protect for Cloud Microsoft™ 365 and the Exchange Online service **Search mode** restore wizard allows you to search across all the mailboxes being protected by IBM® Storage Protect for Cloud Microsoft™ 365.

When restoring Exchange Online, Sharepoint Online, or OneDrive data in the Calendar mode, you can now select and add items to the **Restore queue**, and then restore them together in a single job.

For detailed instructions on using the Restore wizard in each service, refer to:

- “High Speed Migration (HSM) Restore Method” on page 110
- “Restore Exchange Online Data” on page 111
- “Restore SharePoint Online Data” on page 113
- “Restore OneDrive Data” on page 118
- “Restore Microsoft 365 Groups Data” on page 122
- “Restore Project Online Data” on page 127
- “Restore Public Folder Data” on page 131
- “Restore Teams Data” on page 132
- “Restore Viva Engage Data” on page 138
- Restore Power BI Data

High Speed Migration (HSM) Restore Method

In recent updates, the setting for the IBM® Storage Protect for Cloud Microsoft™ 365 restore job now includes the High-Speed Migration (HSM) restore method and is now enabled by default. This utilizes the Migration API as a new approach to enhance the speed of large-scale recoveries.

The HSM restore supports SharePoint Online, OneDrive, Project Online, Microsoft 365 Groups, Teams, and Viva Engage in both app profile authentication and service account authentication, and HSM restore jobs can support restoring content larger than 15 GB.

However, the Migration API is not available for users of Microsoft 365 operated by 21Vianet in China. It is also not available for users of Microsoft 365 with the German cloud using the data trustee, German Telekom, but it is supported for users in Germany whose data location is not in the German data center.

The data export jobs, the security-only restore, restoring sharing link permissions, and restoring to a storage location will not use the HSM restore method.

Refer to the following for the scenarios of HSM data recoveries:

- Select sites, subsites, document libraries, custom lists, calendar, or folders to restore.

  > **Note:** HSM restore does not support apps either.

- Restore destination must be a container in SharePoint Online site or user's OneDrive.

Note the following known issues:

- If an item with the same row ID exists in the destination's recycle bin, the HSM restore job to restore this item with **Overwrite** content conflict resolution will create this item in the destination with a different row ID.
- If you select multiple folders to restore and there are files using the same name, the HSM restore job to restore those folders with the action of **Merge** may fail because of the conflicts.
- The Device Channels lists are affected by HSM restore jobs. The default channel item cannot be updated.

Restore Exchange Online Data

With IBM® Storage Protect for Cloud Microsoft™ 365, you can restore Exchange Online backup data to its original location in Exchange Online, to another location in Exchange Online, or to a separate, customer-defined storage location. Note that if the user account linked to the mailbox no longer exists in Microsoft 365, the mailbox cannot be restored.

About this task

IBM® Storage Protect for Cloud Microsoft™ 365 can protect mailboxes that are placed on Litigation Hold but cannot keep the Litigation Hold configuration for the mailboxes since that configuration needs to be configured in Exchange Admin, which is out of reach of Exchange Online backup and restore.

> **Note:** If you want to restore the backup data to a storage location, you must have your own storage location configured. The default storage provided by IBM® Storage Protect for Cloud cannot be the destination of the restore.

Procedure

Complete the steps below to restore Exchange Online data:

1. Navigate to the **Restore › IBM® Storage Protect for Cloud Backup** page, and then click the **Exchange Online** tile.
2. Select the items that you want to restore. You can choose one of the following methods to find the data to restore.
   - **Search mode** – Define a mailbox as the search scope and then use the properties to search for the items within the mailbox. Refer to the steps below:
     a. In the **Name** field, enter or select a mailbox. The default search condition is to search the backup data of that mailbox within the last backup cycle.
     b. In the **Backup Time Range** field, the time range of the last backup cycle is displayed by default. Click the Calendar (📅) button to customize the backup time range. The start date must be earlier than the end date. You can click **Reset** if you want to reset the settings. Click **OK** to save your customization.

    c. Select **Mailbox**, **Folder**, or **Mailbox Item** from the **Level** list for the items you want to search. If you want to search for all folders or mailbox items within the selected mailbox, you can leave the search conditions empty. To search for specific folders, enter the folder name or the keywords in the **Folder Name** field; to search for the **Mailbox Item** level items, you can configure the following search conditions: **Subject**, **Sent From**, **Sent To**, and **Date Sent** ,and turn on/off the switch to configure whether to **Search exclusively for mail items that contain attachments**.

    d. Click **Search** to search the items according to the conditions you configured. The search conditions and the search results are displayed. The results include all backup items which meet the search conditions in Exchange Online mailboxes, Group mailboxes and Teams mailboxes. The search results table will display a maximum of 500 items. You can edit the search conditions and click **Search** to adjust the search results.

    e. Find and select the item you want to restore from the search results. In the **Recovery Point** column, click the Calendar (📅) button to select a backup job that backed up this item at the status that you want to restore, and click **Apply**.

    f. Click the **Restore** button above the search result table to restore all selected items.

    g. Proceed to step 3 to continue with the Restore settings.

- **Calendar mode** – Find a backup job that backed up the items at the time of the status you want to recover, and then search and select the items from the backup data of that backup job.

    a. In the calendar, all backup jobs of Exchange Online are displayed. You can select whether to display the finished with an exception or failed jobs in the calendar by selecting the **Include jobs with only partial backup data** option. Note that the data of these jobs may be incomplete. Hover over a backup job to show the backup job details.

    b. Select a backup job. By default, all backup data of Exchange Online within the backup cycle (excluding deleted contents) is displayed in the table. To include deleted contents, click the **Show data** field and select **All backup data within the backup cycle**. You can also select the **Backup data only from this recovery point** option to only show the data backed up in the selected backup job.

    c. You can enter keywords to search the items, or you can click the backup data to browse the items you want to restore. For mailbox items, you can sort the **Name**, **Sent from** and **Sent time** columns it either ascending or descending order.

    d. The following actions are provided for the restore:

        - You can select the items you want to restore, and then click the **Restore** button above the table to restore all selected items directly at the same time. Note that you can only select the items at the same level in this way. Then, proceed to step 3 to continue with the Restore settings.

        - To restore mailboxes, you can select the mailboxes you want to restore, and then click the **Queue for restore** button above the table to add them for batch restore. After adding all desired mailboxes to the queue, click the **Restore queue**( ) icon at the top of the page, and then click the **Restore** button to restore the mailboxes in one restore job.
          In the **Queue for restore** panel, administrators can click **Want to bulk import objects to the queue?** to import multiple mailboxes from CSV files.

          > **Note:** In the restore process, the Exchange Online mailboxes in the **Restore queue** will be restored sequentially from first to last as listed. The objects in the **Restore queue** are ordered by their addition time, from oldest to newest. The batch import maintains the order of objects as specified in the uploaded template.
          > If you leave the recovery point, the restore queue will be cleared.

3. If necessary, you can enter your comments for this restore job in the **Description** text box.

4. Choose where to restore the backup data to.

   - **Restore the data to its original location** – Restore the backup data to where the data are backed up.

   - **Restore the data to another location** – Restore the backup data to another destination. You can enter keywords to search for the restore destination. The items that can be selected as the restore destination are listed under the **Search** box. Select a container as the destination and then select **Attach** or **Merge** as the restore action.

     ◦ **Attach** will restore the backup data as child objects beneath the selected node. For example, if you want to restore a folder to another folder and select **Attach**, the restored folder will become the subfolder of the destination folder.

     ◦ **Merge** will add the contents to the destination node. For example, if you want to restore a folder to another folder and select **Merge**, the subfolders and contents of the restored folder rather than itself will directly become the subfolders and contents of the destination folder.

   - **Restore the data to your storage** – Restore the backup data to your own storage location. This option is not available if you are using the default storage location provided by IBM.

5. Select the items in the folder/mailbox that you want to restore. You can either restore all items in the folder/mailbox or restore items sent within a specified period by configuring the time range.

6. Select how to handle the conflicts in the restore job.

   - Container level conflict resolution – The mailbox and mailbox folders are the container level objects. Select a container level conflict resolution:

     ◦ **Skip** – The destination container settings will remain unchanged.

     ◦ **Merge** – The backup container settings and the content will be merged with the destination container.

   - Content level conflict resolution – The mailbox items are the content level objects. Select a content level conflict resolution:

     ◦ **Append** – All of the mailbox items will be added to the destination container. This option has the best performance but may result in duplicate items if they already exist.

     ◦ **Skip** – The conflicting destination content will be retained in the destination, and the backup data of the conflicting content will not be restored.

     ◦ **Overwrite** – The conflicting destination content will be removed from the destination, and the backup data of the conflicting content will be restored.

7. When restoring mailboxes or folders through the **Search mode**, turn on/off the switch to define whether to **Include the backup data for any previously deleted content in this backup cycle** in the restore scope.

8. The **Advanced settings** is available if you are using BYOS. Click to expand the **Advanced settings** area.

9. Turn on/off the switch to define whether to allow restore jobs to rehydrate the data sets automatically, when the backup data is stored in the Azure archive storage tier. This field is only functional for the BYOS subscription type. For IBM® Storage Protect for Cloud default storage, the restore job will automatically rehydrate data.

   > **Note:** To avoid long response times of the product, do not store the index database to the Azure archive storage tier.

10. Click **Next** to view the restore summary.

11. Click **Restore** to restore the selected items.

Restore SharePoint Online Data

With IBM® Storage Protect for Cloud Microsoft™ 365, you can browse or search for SharePoint Online backup jobs or data to restore items to their original location, to another location, or to a storage location. This module also allows you to search and restore backup data for Project Online sites, Viva Engage sites, Group sites, and Teams sites.

About this task

IBM® Storage Protect for Cloud now supports out-of-place restore operations between SharePoint Online sites, OneDrive, Teams sites, and Group sites. For more information on the supported restore types for SharePoint Online, refer to SharePoint Online Restore Options.

> **Note:** If you want to restore the backup data to a storage location, you must have your own storage location configured. The default storage provided by IBM® Storage Protect for Cloud cannot be the destination of the restore. Additionally, the SharePoint Online site collections, sites, and apps do not support being restored to a custom storage location.

Copilot agent files in SharePoint Online, Microsoft 365 Groups, Teams, and Viva Engage sites can be restored either to their original locations or to other locations. The restoration workflow depends on what you select to restore:

- **Both Copilot agent file and source data:** Restores both the agent file and the source data. At the destination, the restored agent file will remain linked to the corresponding source data.
- **Only Copilot agent file:** Restores the agent file, including its links to the source data, but does not restore the actual source data content itself.
- **Only source data:** Restores only the source data.

Note for URL alignment: For agent files linked to multiple site collections, if a source file is located within the same site collection as the agent file in the backup, its URL link will be adjusted to align with the destination path. If the source file resides in a different site collection, its link will not be updated. In scenarios involving cross-Microsoft 365 tenants, the domain name in all associated URL links will be updated to match the destination tenant.

Procedure

Complete the steps below to restore SharePoint Online data:

1. Navigate to the **Restore › IBM® Storage Protect for Cloud Microsoft™ 365 Backup** page, and then click the **SharePoint Online** tile.
2. Select the items that you want to restore. You can choose one of the following methods to find the data to restore.
   - **Search mode** – Define a SharePoint Online site collection as the search scope and then use the properties to search for the items within the scope. Note that this method does not support searching and restoring the list items.

     Refer to the steps below:

     a. In the **URL** field, enter the keywords in the URL or select a SharePoint Online site collection URL. The default search condition is to search the backup data of that site collection within the last backup cycle. The drop-down list will remind you of SharePoint sites with unusual activities or under potential ransomware attacks.

     b. In the **Backup time range** field, the time range of the last backup cycle is displayed by default. Click the Calendar (📅) button to customize the backup time range. The start date must be earlier than the end date. You can click **Reset** if you want to reset the settings. Click **OK** to save your customization.

     c. Select **Site Collection**, **Site**, **List/Library**, **App**, **Folder**, or **Document** from the **Level** list for the items you want to search. If you want to search for all sites, lists or libraries, apps, folders, or documents in the selected site collection, you can leave the search conditions empty. To search for specific sites, lists/libraries, apps, or folders, enter the title or name or the keywords for search; to search for specific documents, you can configure the following search conditions: **Document Name**, **Created Date**, **Created By**, **Modified By**, or **Document Size**.

     d. Click **Search** to search the items according to the conditions you configured. The search conditions and the search results are displayed. The results include all backup items which meet the search conditions in SharePoint Online sites, Project Online sites, Viva Engage sites, Group sites and Teams sites. The search results table will display a maximum of 500 items. You can edit the search conditions and click **Search** to adjust the search results.

    e. Find and select the item you want to restore from the search results. In the **Recovery Point** column, click the Calendar (📅) button to select a backup job that backed up this item at the status that you want to restore, and click **Apply**. Recovery points with objects with unusual activities detected or potential ransomware attack detected will be displayed with 🔔 (**Unusual activities detected**) or 🔔 (**Potential ransomware attack detected**).

    f. Click the **Restore** button above the search result table to restore all selected items.

    g. Go to step 3 to continue with the Restore settings.

- **Calendar mode** – Find a backup job that backed up the items at the time of the status you want to recover, and then search and select the items from the backup data of that backup job.

    a. In the calendar, all backup jobs of SharePoint Online are displayed. You can select whether to display the jobs that finished with an exception or failed jobs in the calendar by selecting the **Include jobs with only partial backup data** option. Note that the data of these jobs may be incomplete. Hover over a backup job to show the backup job details.

    b. Select a backup job. All backup data of SharePoint Online, up to a maximum of 2000 items, is displayed in the table. You can select the **Show data from this backup only** option (historical data in this scope from previous backups not included) to only show the data backed up in the selected backup job. Recovery points with objects with unusual activities detected or potential ransomware attack detected will be displayed with 🔔 (**Unusual activities detected**) or 🔔 (**Potential ransomware attack detected**).

    c. You can enter keywords to search the items, or you can click the backup data to browse the items you want to restore.

    d. The following actions are provided for the restore:

        ◦ You can select the items you want to restore, and then click the **Restore** button above the table to restore all selected items directly at the same time. Note that you can only select the items at the same level in this way. Then, proceed to step 3 to continue with the Restore settings.

        ◦ To restore site collections, you can select the site collections you want to restore, and then click the **Queue for restore** button above the table to add them for batch restore.

          After adding all desired site collections to the queue, click the **Restore queue** (▦) icon at the top of the page, and then click the **Restore** button to restore the site collections in one restore job.

          > **Note:** In the restore process, the site collections in the **Restore queue** will be restored sequentially from first to last as listed. The objects in the **Restore queue** are ordered by their addition time, from oldest to newest.
          > If you leave the recovery point, the restore queue will be cleared.

3. If necessary, you can enter your comments for this restore job in the **Description** text box. For objects with unusual activities or under ransomware attacks, you can click the **Potential ransomware attack detected** or **Unusual activities detected**in the **Suggested** field below to enter it in the **Description** text box directly.

4. Select what you would like to restore for the selected items. You can choose to restore all of the content and security from the backup, or you can choose to only restore the security or content.

    - The security includes all the user permissions at the selected level and beneath. The restore-security-only restore job cannot add or delete any users in the target site collection.

    - The restore-content-only restore job will skip the conflicting documents/items or restore the documents/items with a suffix “_1” added, depending on which conflict resolution you choose at the content level.

5. Choose where to restore the backup data to. Note that the SharePoint Online site collections, sites, and apps only support being restored to the original location or restored to another location.

    - **Restore the data to its original location** – Restore the backup data to where the data are backed up.

    - **Restore the data to another location** – Restore the backup data to another destination. Configure the following settings:

        - **Select a destination object type** – Select to restore the backup data to SharePoint Online, OneDrive, Microsoft 365 Groups, or Teams. You can enter keywords to search for the restore destination. The items that can be selected as the restore destination are listed under the **Search** box.

            > **Note:** If you choose to restore to OneDrive, only the **Documents** library, **Site Assets** library, and the custom libraries will be displayed in the destination tree. You can click **Show All Libraries** to display all lists and libraries.
            > On the destination tree, click a node to load the nodes under it and click the Previous button to navigate back to the previous node. Select a node where you want to restore the backup data.

        - **Action** – Select how the backup data will be restored to the destination. Select **Attach** to restore the contents as children beneath the selected node, or select **Merge** to add the contents to the destination node. For example, you want to restore a site to another site. If you select **Attach**, the restored site will become the subsite of the destination site; if you select **Merge**, the subsites and contents of the restored site rather than itself will directly become the subsites and contents of the destination site.

    - **Restore the data to your storage** – Restore the backup data to your own storage location configured. This option is not available if the default storage location is used.

        > **Note:** The SharePoint Online site collections, sites, and apps do not support being restored to a custom storage location.

6. Select how to handle the conflicts in the restore job. The conflict occurs if a folder or file in the destination has the same name, or the item in the destination has the same GUID.

    - Container level conflict resolution – Select how to handle the conflicts at the container level.

        - **Skip** – The settings of the conflicting destination container will be retained in the destination.

        - **Merge** – The source container settings and the content will be merged to the conflicting destination container.

        - **Replace** – The settings of the conflicting destination container will be deleted and replaced by the source container settings, as well as the content within the container.

    - Content level conflict resolution – Select how to handle the conflicts at the content level.

        > **Note:** This is not available if **Replace** is selected as the container level conflict resolution. If you select to restore content only, only the **Skip** and the **Append an "_1" to the Item/ Document** are available.

        - **Skip** – The conflicting destination content will be retained in the destination, and the backup data of the conflicting content will not be restored.

        - **Overwrite** – The conflicting destination content will be removed from the destination, and the backup data of the conflicting content will be restored.

        - **Overwrite by Last Modified Time** – If the last modified time of the conflicting destination content is earlier than that of the source content, the conflicting destination content will be removed from the destination, and the backup data of the conflicting content will be restored.

    - **Append an "_1" to the Item/Document** – If the last modified time of the conflicting destination content is the same, the restore will be skipped; if the last modified time is different, the conflicting destination content will be kept, and the backup data of the conflicting content will be added to the destination with a sequential number suffix added to the filename.

      > **Note:** If you want to restore a single file version without affecting other versions, set the content level conflict resolution to **Append an "_1" to the Item/Document**. If the content level conflict resolution is set to **Overwrite**, the restore job will remove all the versions of this file from the destination and keep this file version as the latest and only version of the file.

- Apps conflict resolution – Select how to handle the apps conflict.
    - **Skip** – The conflicting destination app and AppData will be retained in the destination, and the backup data of the conflicting content will not be restored.
    - **Overwrite** – The conflicting destination app and AppData will be removed from the destination, and the backup data of the conflicting content will be restored.

      > **Note:** If you choose to only restore security, you must select how to handle the security conflicts at the container level and content level. **Replace** will overwrite the security in the destination; **Merge** will combine the security in the backup with the security in the destination.

7. Expand the **Advanced settings** area to configure more restore settings. If you choose to restore to another location, the mapping settings will be available to allows you to update the permissions and metadata or language.

8. **User mapping** - Select a user mapping profile from the drop-down list. For more instructions on creating a new user mapping profile, refer to "Configure Mapping Settings" on page 91.

9. **Language mapping** - Select a language mapping profile from the drop-down list. For more instructions on creating a new language mapping profile, refer to "Configure Mapping Settings" on page 91

10. Choose how you would like to restore the version history if file versions are backed up by IBM® Storage Protect for Cloud. You can select **Restore the latest version only**, or you can select the **Restore the current and previous versions** option and enter the maximum number of versions you want to restore in the box. IBM® Storage Protect for Cloud Microsoft™ 365 can restore up to **20** versions for one document. For the best performance and simplest experience, IBM® Storage Protect for Cloud recommends restoring only the latest version.
    Note the following:

    - By default, history versions of items and files are not backed up due to the regular recovery points created by backup jobs, as well as Microsoft 365 API overhead and limitations related to versions. In our experience, most user and legal requests are only for the most recent active version. In addition, we will capture multiple roll-back points during our daily backups to ensure you have a change history for this document outside native versioning. If you need to back up the versions for some reason and are willing to accept the performance impact, please contact IBM support to have it enabled. The backup job will include the most recent 10 versions by default.
    - If you want to restore earlier versions of a document, you can run an export job to export all versions of that document from the backup data.
    - This restore setting is not available when selecting documents or restoring security only.

11. Select how you would like to restore the Managed Metadata Service.

    - If the containers or content you select to restore is under the site collection level, the **Restore terms in site term store only** option and the **Restore terms in both global term store and site term store** option will only restore the terms and their parent terms associated directly with the data from the site store or both. Note that if the data is not restored due to the conflict resolutions you choose, the restored terms cannot be connected to the data either.

- If you select at least the site collection level object to perform the restore, the **Restore terms in site term store only** option will restore all the deleted terms in the site store and the **Restore terms in both global term store and site term store** option will restore all the deleted terms in both the global term store and site term store.
- If you select to **Use existing terms only**, no terms will be restored.
- If you want to perform a term store-only restore, refer to the FAQ: How do I perform term store-only restore?

12. Turn on/off the switch to define whether to restore the sharing link permissions. This feature only works for the sharing of items to specific people inside or outside your organization. For external users, the restore job can only restore the permissions for the users who have accessed the sharing link. After the restore, the sharing links will be changed, and OneDrive users can go to OneDrive > **Shared** library to view the content shared with you and shared by you. The links generated by the **Copy link** function in Microsoft 365 are also regarded as sharing links.

   > **Note:** The Sharing setting is a tenant-level setting, and IBM® Storage Protect for Cloud Microsoft™ 365 does not protect tenant settings. The restore job to restore a deleted site cannot restore the Sharing settings, including the external users and their permissions.

   > **Note:** This restore setting is not available when restoring content only.

13. Turn on/off the switch to define whether to allow restore jobs to rehydrate the data sets automatically, when the backup data is stored in the Azure archive storage tier. This field is only functional for the BYOS subscription type. For IBM® Storage Protect for Cloud default storage, the restore job will automatically rehydrate data.

   > **Note:** IBM® Storage Protect for Cloud recommends not storing the index database to the Azure archive storage tier.

14. Turn on/off the switch to define whether to restore the subsites. This option is only available when you select site collections or sites to restore.
15. Turn on/off the switch to define whether to restore the hub site connection. This option is only available when you select site collection to restore.

   > **Note:** IBM® Storage Protect for Cloud Microsoft™ 365 cannot restore the hub site connection, if it is a cross-tenant restore or the destination hub site requires approval for the associated site to join.

16. Turn on/off the switch to define whether to enable the Custom Scripts setting during the restore. This feature allows you to restore data related to scripts to the destination Microsoft environment.
17. Click **Next** to view the restore summary.
18. Click **Restore** to restore the selected items. After the job has started, you can navigate to the **Job Monitor** to view more job details. For details, refer to "Job Monitor" on page 153.

Restore OneDrive Data

You can browse or search for OneDrive backup jobs or data to its original location in OneDrive, to another location in OneDrive, or to a separate, customer-defined storage location. IBM® Storage Protect for Cloud now supports out-of-place restore operations between SharePoint Online sites, OneDrive, Teams sites, and Group sites.

About this task

> **Note:** If you want to restore the backup data to a storage location, you must have your own storage location configured. The default storage provided by IBM® Storage Protect for Cloud cannot be the destination of the restore. Additionally, the OneDrive site collections and sites do not support being restored to a custom storage location.

For more information on the supported restore types for OneDrive, refer to OneDrive Restore Options. Note that if the associated OneDrive user account no longer exists in Microsoft 365, the OneDrive cannot be restored.

Procedure

Complete the steps below to restore OneDrive data:

1. Navigate to the **Restore › IBM® Storage Protect for Cloud Backup** page, and then click **OneDrive** tile.
2. Select the items that you want to restore. You can choose one of the following methods to find the data to restore.
   - **Search mode** – Define a OneDrive address as the search scope and then use the properties to search for the items within the scope. Note that this method does not support searching and restoring the list items.

     Refer to the steps below:

     a. In the **Name** field, enter or select a OneDrive address. The default search condition is to search the backup data for that OneDrive address within the last backup cycle. The drop-down list will remind you of OneDrive accounts with unusual activities or under potential ransomware attacks.

     b. In the **Backup time range** field, the time range of the last backup cycle is displayed by default. Click the Calendar (📅) button to customize the backup time range. The start date must be earlier than the end date. You can click **Reset** if you want to reset the settings. Click **OK** to save your customization.

     c. Select **OneDrive User**, **Library**, **Folder**, or **Document** from the **Level** list for the items you want to search. If you want to search for all libraries, folders, or the documents of that OneDrive user, you can leave the search conditions empty. To search for specific libraries or folders, enter the title or name or the keywords for search; to search for the specific **Document**-level items, you can can choose whether to search for **Suspicious files** under potential ransomware attacks or **Files deleted in unusual activities** in **File type** and configure the following search conditions: **Document Name**, **Created Date**, **Created By**, **Modified By**, or **Document Size**.

     d. Click **Search** to search the items according to the conditions you configured. The search conditions and the search results are displayed. The search results table will display a maximum of 500 items. You can edit the search conditions and click **Search** to adjust the search results.

     e. Find and select the item you want to restore from the search results. In the **Recovery Point** column, click the Calendar (📅) button to select a backup job that backed up this item at the status that you want to restore and click **Apply**. Recovery points with objects with unusual activities detected or potential ransomware attack detected will be displayed with 🔔 (**Unusual activities detected**) or 🔔 (**Potential ransomware attack detected**).

     f. Click the **Restore** button above the search result table to restore all selected items.

     g. Proceed to step 3 to continue with the Restore settings.
   - **Calendar mode** – Find a backup job that backed up the items at the time of the status you want to recover, and then search and select the items from the backup data of that backup job.

     a. In the calendar, all backup jobs of OneDrive are displayed. You can select whether to display the finished with an exception or failed jobs in the calendar by selecting the **Include jobs**

with only partial backup data option. Note that the data of these jobs may be incomplete. Hover over a backup job to show the backup job details.

b. Select a backup job. All backup data for OneDrive is displayed in the table. You can select the **Show data from this backup only** option (historical data in this scope from previous backups not included) to only show the data backed up in the selected backup job. Recovery points with objects with unusual activities detected or potential ransomware attack detected will be displayed with 🔔 (**Unusual activities detected**) or 🔔(**Potential ransomware attack detected**).

c. You can enter keywords to search the items, or you can click the backup data to browse the items you want to restore.

d. The following actions are provided for the restore:

   - You can select the items you want to restore, and then click the **Restore** button above the table to restore all selected items at the same time. Note that you can only select the items at the same level in this way. Then proceed to step 3 to continue with the Restore settings.

   - To restore OneDrive, you can select the OneDrive you want to restore, and then click the **Queue for restore** button above the table to add them for batch restore. After adding all desired OneDrive to the queue, click the **Restore queue** ( ) icon at the top of the page, and then click the **Restore** button to restore the OneDrive in one restore job.

     > **Note:** In the restore process, the OneDrive in the **Restore queue** will be restored sequentially from first to last as listed. The objects in the **Restore queue** are ordered by their addition time, from oldest to newest.
     > If you leave the recovery point, the restore queue will be cleared.

3. If necessary, you can enter your comments for this restore job in the **Description** text box. For objects with unusual activities or under ransomware attacks, you can click the **Potential ransomware attack detected** or **Unusual activities detected**in the **Suggested** field below to enter it in the **Description** text box directly.

4. Select what you would like to restore for the selected items. You can choose to restore all of the content and security from the backup, or you can choose to only restore the security or content.

   - The security includes all the user permissions at the selected level and beneath. The restore-security-only restore job cannot add or delete any users in the target site collection.

   - The restore-content-only restore job will skip the conflicting documents/items or restoring the documents/items with a suffix "_1" added, depending on which conflict resolution you choose at the content level.

5. Choose where to restore the backup data to. Note that the OneDrive site collections and sites can be restored only to the original OneDrive location or another location in OneDrive.

   - **Restore the data to its original location** – Restore the backup data to where the data are backed up.

   - **Restore the data to another location** – Restore the backup data to another destination. Configure the following settings:

     - **Select a destination object type** – Select to restore the backup data to SharePoint Online, OneDrive, Microsoft 365 Groups, or Teams. You can enter keywords to search for the restore destination. The items that can be selected as the restore destination are listed under the **Search** box.

       > **Note:** If you choose to restore to OneDrive, only the **Documents** library, **Site Assets** library, and the custom libraries will be displayed in the destination tree. You can click **Show All Libraries** to display all lists and libraries.

    On the destination tree, click a node to load the nodes under it and click the Previous button to navigate back to the previous node. Select a node where you want to restore the backup data.

    - **Action** – Select how the backup data will be restored to the destination. Select **Attach** to restore the contents as children beneath the selected node, or select **Merge** to add the contents to the destination node. For example, you want to restore a folder to another folder. If you select **Attach**, the restored folder will become the subfolder of the destination folder; if you select **Merge**, the subfolders and contents of the restored folder rather than itself will directly become the subfolders and contents of the destination folder.

      > **Note:** When restoring a OneDrive library to another library, you can now select the **Attach** action to create a new folder named after the source username in the destination library.

  - **Restore the data to your storage** – Restore the backup data to your own storage location configured. This option is not available if the default storage location is used.

    > **Note:** The OneDrive site collections and sites do not support being restored to custom storage.

6. Select how to handle the conflicts in the restore job. The conflict occurs if a folder or file in the destination has the same name, or the item in the destination has the same GUID.

   - Container level conflict resolution – Select how to handle the conflicts at the container level.

     - **Skip** – The settings of the conflicting destination container will be retained in the destination.

     - **Merge** – The source container settings and the content will be merged to the conflicting destination container.

     - **Replace** – The settings of the conflicting destination container will be deleted and replaced by the source container settings, as well as the content within the container.

   - Content level conflict resolution – Select how to handle the conflicts at the content level.

     > **Note:** This is not available if **Replace** is selected as the container level conflict resolution. If you select to restore content only, only the **Skip** and the **Append an "_1" to the Item/ Document** are available.

     - **Skip** – The conflicting destination content will be retained in the destination, and the backup data of the conflicting content will not be restored.

     - **Overwrite** – The conflicting destination content will be removed from the destination, and the backup data of the conflicting content will be restored.

     - **Overwrite by Last Modified Time** – If the last modified time of the conflicting destination content is earlier than that of the source content, the conflicting destination content will be removed from the destination, and the backup data of the conflicting content will be restored.

     - **Append an "_1" to the Item/Document** – If the last modified time of the conflicting destination content is the same, the restore will be skipped; if the last modified time is different, the conflicting destination content will be kept, and the backup data of the conflicting content will be added to the destination with a sequential number suffix added to the filename.

   - Apps conflict resolution – Select how to handle the app's conflict.

   - - **Skip** – The conflicting destination app and AppData will be retained in the destination, and the backup data of the conflicting content will not be restored.

    - **Overwrite** – The conflicting destination app and AppData will be removed from the destination, and the backup data of the conflicting content will be restored.

    Note the following:

    - If you choose to only restore security, you must select how to handle the security conflicts at the container level and content level. **Replace** will overwrite the security in the destination; **Merge** will combine the security in the backup with the security in the destination.

    - If the source has inherited permissions but the destination has unique permissions, it is not supported by the Graph API to perform a security-only restore to reset the destination to inherited status.

7. Expand the **Advanced settings** area to configure more restore settings. If you choose to restore to another location, the mapping settings will be available to allows you to update the permissions and metadata or language.

8. **User mapping** - Select a user mapping profile from the drop-down list. For more instructions on creating a new user mapping profile, refer to “Configure Mapping Settings” on page 91.

9. **Language mapping** - Select a language mapping profile from the drop-down list. For more instructions on creating a new language mapping profile, refer to “Configure Mapping Settings” on page 91

10. Turn on/off the switch to define whether to **restore the sharing permissions**. The **Restore the sharing link permissions** field will be unavailable if the OneDrive backup cycle of the selected recovery point was started after the November 2022 release. In this case, the restore job will restore the sharing permissions by default and the restore will not trigger the email alert. Note that if you do not want to restore the sharing permissions, you can choose to restore content only.
    Note the following:

    - This feature only works for the sharing of items with specific people inside or outside your organization. For external users, the restore job can only restore the permissions for the users who have accessed the sharing link. After the restore, the sharing links will be changed, and OneDrive users can proceed to OneDrive > **Shared** library to view the content shared with you and shared by you. The links generated by the **Copy link** function in Microsoft 365 are also regarded as sharing links.

    - The Sharing setting is a tenant-level setting, and the IBM® Storage Protect for Cloud service does not protect tenant settings. The restore job to restore a deleted site cannot restore the Sharing settings, including the external users and their permissions.

    - When restoring the files to another destination, the restored permissions and sharing links will be changed if the user in the original location is not included in the sharing scope in the destination.

11. Turn on/off the switch to define whether to allow restore jobs to rehydrate the data sets automatically, when the backup data is stored in the Azure archive storage tier. This field is only functional for the BYOS subscription type. For IBM® Storage Protect for Cloud default storage, the restore job will automatically rehydrate data.

    > **Note:** IBM® Storage Protect for Cloud recommends not storing the index database to the Azure archive storage tier.

12. Click **Next** to view the restore summary.

13. Click **Restore** to restore the selected items. After the job has started, you can navigate to the **Job Monitor** to view additional job details. For details, refer to “Job Monitor” on page 153.

Restore Microsoft™ 365 Groups Data

IBM® Storage Protect for Cloud Microsoft™ 365 Groups now provides a new option allowing to restore a soft delete Microsoft 365 group from the Microsoft 365 recycle bin to its last known good state.IBM® Storage Protect for Cloud will perform a check for the group status in Microsoft 365 to ensure Microsoft has this data and clearly present the options for you to decide the best way to recover data: using Microsoft native restore function within that 30-day retention period or using IBM® Storage Protect for Cloud backup data to roll back the entire group or granular contents.

About this task

> **Note:** The check will only happen when you select the group as both the restore scope and the search level.

IBM® Storage Protect for Cloud Microsoft™ 365 Groups service now provides a new option allowing to restore a soft-deleted Microsoft 365 group from the Microsoft 365 recycle bin to its last known good state.

The IBM® Storage Protect for Cloud Microsoft™ 365 Groups service supports restoring the group, group team site, group mailbox, and planner data to another location. You can also restore the files in a Group site to another Group site. Additionally, IBM® Storage Protect for Cloud now supports out-of-place restore operations between SharePoint Online sites, OneDrive, Teams sites, and Group sites. For more information on the supported restore types for Microsoft™ 365 Groups objects, refer to Restore Options for Different Object Types. For the supported data types of Microsoft™ 365 Groups, refer to "Microsoft 365 Groups Data Types" on page 225. If you want to restore the backup data to a storage location, you must have your own storage location configured. The default storage provided by IBM® Storage Protect for Cloud cannot be the destination of the restore. Additionally, only the Microsoft™ 365 Group lists or libraries, folders, items, or documents support being restored to a storage location.

Procedure

Complete the steps below to restore the Microsoft™ 365 Groups data:

1. Navigate to the **Restore › IBM® Storage Protect for Cloud Backup** page, and then click the **Microsoft 365 Groups** tile.
2. Select the items that you want to restore. You can choose one of the following methods to find the data to restore.
   - **Search mode** – Select a restore object scope and search for the data to restore. Follow steps 3 to 4.
   - **Calendar mode** – Select a recovery point (backup job) and select data from that backup to restore. Proceed to step 5.
3. Define a Microsoft™ 365 Group as the search scope. You can enter the Group's name or email address to search, and then select the Microsoft™ 365 Group from the **Name** list. The default search condition is to search the backup data for the Microsoft™ 365 Group within the last backup cycle. The drop-down list will remind you of groups with unusual activities or under potential ransomware attacks.
4. You can choose to use the properties on the same page to search for the contents within this group for granular data roll-back, or you can directly proceed to the next step to search and select the data to restore.

   > **Note:** If the group you want to restore has been deleted from Microsoft™ 365, you can let IBM® Storage Protect for Cloud Microsoft™ 365 check if the group is still in soft-deleted status in the Microsoft™ 365 recycle bin to help you decide the best way to restore. In this case, select that group and directly click **Search**.
   > If the group is still in the soft-deleted status in Microsoft™ 365, you can choose the following methods.

   - If you choose to restore the entire scope from Microsoft™ 365, click **Next** and then select a recovery point. Click **OK** to start the restore job. You can navigate to the Microsoft™ 365 environment to monitor and verify the progress.

     > **Note:** If you only want to restore the scope from the recycle bin for the last known status, select this option to help enhance job performance and data integrity.

   - If you choose to restore the selected scope or just content within this scope from backup data, click **Next**, and you can configure search settings to search for the granular contents.

For the details of using the properties on the first page or the **Search** feature on the **Select and restore the data** step, refer to the following:

a. In the **Name** field, you can enter or select another Microsoft™ 365 Group to change the search scope.

b. In the **Backup time range** field, the time range of the last backup cycle is displayed by default.

   Click the Calendar (📅) button to customize the backup time range. The start date must be earlier than the end date. You can click **Reset** if you want to reset the settings. Click **OK** to save your customization.

c. Select Microsoft™ 365 Group, Group Mailbox, Folder in Mailbox, Mailbox Item, Group Team Site, Site, List/Library, App, Folder in SharePoint, Document, Plan, or Task from the Level list for the items you want to search. If you want to search for all objects at the level you select from the selected Microsoft™ 365 Group, you can leave the search conditions empty.

d. Click **Search** to search the items according to the conditions you configured. The search conditions and the search results are displayed. The search results table will display a maximum of 500 items. You can edit the search conditions and click **Search** to adjust the search results.

e. Find and select the item you want to restore from the search results. In the **Recovery point** column, click the Calendar (📅) button to select a backup job that backed up this item at the status that you want to restore, and click **Apply**. Recovery points with objects with unusual activities detected or potential ransomware attack detected will be displayed with 🔔 (**Unusual activities detected**) or 🔔 (**Potential ransomware attack detected**).

f. Click the **Restore** button above the search result table to restore all selected items.

g. Proceed to step 6 to continue with the Restore settings.

5. Find a backup job that backed up the items at the time of the status you want to recover, and then search and select the items from the backup data of that backup job.

   a. In the calendar, all backup jobs of Microsoft™ 365 Groups are displayed. You can select whether to display the finished with an exception or failed jobs in the calendar by selecting the **Include jobs with only partial backup data** option. Note that the data of these jobs may be incomplete. Hover over a backup job to show the backup job details.

   b. Select a backup job. All backup data of Microsoft™ 365 Groups is displayed in the table. You can select the **Show data from this backup only** option (historical data in this scope from previous backups not included) to only show the data backed up in the selected backup job. Recovery points with objects with unusual activities detected or potential ransomware attack detected will be displayed with 🔔 (**Unusual activities detected**) or 🔔 (**Potential ransomware attack detected**).

   c. You can enter keywords to search the items, or you can click the backup data to browse the items you want to restore.

   d. Select the items you want to restore, and then click the **Restore** button above the table to restore all of the selected items.

   > **Note:** If you want to select multiple items to restore at the same time, you can only select the items at the same level.

   e. Continue to step 6 to configure the Restore settings.

6. If necessary, you can enter a description for this restore job in the **Description** text box. For objects with unusual activities or under ransomware attacks, you can click the **Potential ransomware attack detected** or **Unusual activities detected**in the **Suggested** field below to enter it in the **Description** text box directly.

7. If you have selected items from a Microsoft™ 365 team site to restore, you can select what you would like to restore for the selected items. You can choose to restore all content and security from the backup, or you can choose to only restore the security. The security includes all the user permissions at the selected level and beneath. The restore-security-only restore job cannot add or delete any users in the target site collection.

8. Choose where to restore the backup data.

- **Restore the data to its original location** – Restore the backup data to where the data is backed up.
- **Restore the data to another location** – Restore the backup data to another destination. Configure the following settings:
  - **Select a restore destination** – If you select a Group site or site item, you can select to restore the backup data to SharePoint Online, OneDrive, Microsoft 365 Groups, or Teams. For others, select a container as the restore destination. You can enter keywords to search for the restore destination. The items that can be selected as the restore destination are listed under the **Search**box.
  - **Action** – Select how the backup data will be restored to the destination. Select **Attach** to restore the contents as children beneath the selected node, or select **Merge** to add the contents to the destination node. For example, you want to restore a site to another site. If you select **Attach**, the restored site will become the subsite of the destination site; if you select **Merge**, the subsites and contents of the restored site rather than itself will directly become the subsites and contents of the destination site.
- **Restore the data to your storage** – Restore the backup data to your own storage location. This option is not available if the default storage location is used.

  > **Note:** Only the Microsoft 365 Group lists or libraries, folders in SharePoint, items, or documents support being restored to a storage location.

9. Select how to handle the conflicts in the restore job. The available options of conflict resolution will vary for the items you select to restore.
   - Container level conflict resolution – Select how to handle the conflicts at the container level.
     - **Skip** – The settings of the conflicting destination container will be retained in the destination.
     - **Merge** – The source container settings and the content will be merged to the conflicting destination container.
     - **Replace** – The settings of the conflicting destination container will be deleted and replaced by the source container settings, as well as the content within the container.
   - Content level conflict resolution – Select how to handle the conflicts at the content level.

     > **Note:** This is not available if **Replace** is selected as the container level conflict resolution.

     - **Skip** – The conflicting destination content will be retained in the destination, and the backup data of the conflicting content will not be restored.
     - **Overwrite** – The conflicting destination content will be removed from the destination, and the backup data of the conflicting content will be restored.
     - **Overwrite by Last Modified Time** – If the last modified time of the conflicting destination content is earlier than that of the source content, the conflicting destination content will be removed from the destination, and the backup data of the conflicting content will be restored.
     - **Append an "_1" to the Item/Document** – If the last modified time of the conflicting destination content is the same, the restore will be skipped; if the last modified time is different, the conflicting destination content will be kept, and the backup data of the conflicting content will be added to the destination with a sequential number suffix added to the filename.

     > **Note:** If you want to restore a single file version without affecting other versions, set the content level conflict resolution to **Append an "_1" to the Item/Document**. If the content level conflict resolution is set to **Overwrite**, the restore job will remove all the versions of

> this file from the destination and keep this file version as the latest and only version of the file.

10. Expand the **Advanced settings** area to configure more restore settings. If you choose to restore to another location, the mapping settings will be available to allows you to update the permissions and metadata or language.
11. **User mapping** - Select a user mapping profile from the drop-down list. For more instructions on creating a new user mapping profile, refer to "Configure Mapping Settings" on page 91.
12. **Language mapping** - Select a language mapping profile from the drop-down list. For more instructions on creating a new language mapping profile, refer to "Configure Mapping Settings" on page 91
13. Choose how you would like to restore the version history if file versions are backed up by IBM® Storage Protect for Cloud. You can select **Restore the latest version only**, or you can select the **Restore the current and previous versions** option and enter the maximum number of versions you want to restore in the box. IBM® Storage Protect for Cloud can restore up to **20** versions of one document. For the best performance and simplest experience, IBM recommends restoring only the latest version
    Note the following:
    - By default, history versions of items and files are not backed up due to the regular recovery points created by backup jobs, as well as Microsoft 365 API overhead and limitations related to versions. In our experience, most user and legal requests are only for the most recent active version. In addition, we will capture multiple roll-back points during our daily backups to ensure you have a change history for this document outside native versioning. If you need to back up the versions for some reason and are willing to accept the performance impact, please contact IBM support to have it enabled. The backup job will include the most recent 10 versions by default.
    - If you want to restore earlier versions of a document, you can run an export job to export all versions of that document from the backup data.
14. Select how you would like to restore the Managed Metadata Service.
    - If the containers or content you select to restore is under the site collection level, the **Restore terms in site store only** option and the **Restore terms in both global term store and site term store** option will only restore the terms and their parent terms associated directly with the data from the site store or both. Note that if the data is not restored due to the conflict resolutions you choose, the restored terms cannot be connected to the data either.
    - If you select at least the site collection level object to perform the restore, the **Restore terms in site store only** option will restore all the deleted terms in the site store and the **Restore terms in both global term store and site term store** option will restore all the deleted terms in both the global term store and site term store.
    - If you select to **Use existing terms only**, no terms will be restored.
    - If you want to perform a term store-only restore, refer to the FAQ:"How do I restore term store-only data?" on page 33 .

    Note that if you perform the restore from the Legacy UI, all the terms in the global term store and the site term store are restored by default.
15. Turn on/off the switch to define whether to restore the sharing permissions. This feature only works for the sharing of items with specific people inside or outside your organization. For external users, the restore job can only restore the permissions for the users who have accessed the sharing link. After the restore, the sharing links will be changed, and OneDrive users can navigate to OneDrive > **Shared** library to view the content shared with you and shared by you. The links generated by the **Copy link** function in Microsoft 365 are also regarded as sharing links.

    > **Note:** The Sharing setting is a tenant-level setting, and IBM® Storage Protect for Cloud Microsoft™ 365 does not protect tenant settings. The restore job to restore a deleted site cannot restore the Sharing settings, including the external users and their permissions.
16. Turn on/off the switch to define whether to restore the hub site connection. This option is only available when you select the Group or Group team site to restore.

> **Note:** IBM® Storage Protect for Cloud cannot restore the hub site connection for the selected site, if it is a cross-tenant restore or the destination hub site requires approval for the associated sites to join.

17. Select **Yes** or **No** for whether to restore the hub site connection. This option is only available when you select the Group or Group team site to restore.

> **Note:** IBM® Storage Protect for Cloud Microsoft™ 365 cannot restore the hub site connection for the selected site, if it is a cross-tenant restore or the destination hub site requires approval for the associated sites to join.

18. Turn on/off the switch to define whether to enable the Custom Scripts setting during the restore. This feature allows you to restore data related to scripts to the destination Microsoft environment.
19. Click **Next** to view the restore summary.
20. Click **Restore** to restore the selected items. After the job has started, you can navigate to the **Job Monitor** to view more job details. For details, refer to "Job Monitor" on page 153.

Restore Project Online Data

With IBM® Storage Protect for Cloud Microsoft™ 365, you can browse or search for Project Online backup jobs or data to restore items to their original location in Project Online, to a new location in Project Online, or to a separate, customer-defined storage location. Currently, you can only select the Project Online containers as the destination to restore the Project Online backup data.

About this task

For details on the supported restore options of Project Online, refer to Restore Options for Different Object Types and "Project Online Data Types" on page 202.

> **Note:** If you want to restore the backup data to a storage location, you must have your own storage location configured. The default storage provided by IBM® Storage Protect for Cloud cannot be the destination of the restore.

Procedure

Complete the steps below to restore Project Online data:

1. Navigate to the **Restore › IBM® Storage Protect for Cloud Backup** page, and then click the **Project Online** tile.
2. Select the items that you want to restore. You can choose one of the following methods to find the data to restore.

   - **Search mode** – Define a Project Online site collection as the search scope and then use the properties to search for the items within the scope. Note that this method does not support searching and restoring the list items.

   Refer to the steps below:

   a. In the **URL** field, enter or select a Project Online site collection URL. The default search condition is to search the backup data of that site collection within the last backup cycle.

   b. In the **Backup Time Range** field, the time range of the last backup cycle is displayed by default.

      Click the Calendar (📅) button to customize the backup time range. The start date must be earlier than the end date. You can click **Reset** if you want to reset the settings. Click **OK** to save your customization.

   c. Select **Site Collection**, **Site**, **List/Library**, **Project**, **App**, **Folder**, or **Document** from the **Level** list for the items you want to search. If you want to search for all sites, lists or libraries, projects, folders, or documents in the selected site collection, you can leave the search conditions empty. To search for specific sites, lists/libraries, projects, or folders, enter the title or name or the keywords for search; to search for specific documents, you can configure the following search conditions: **Document Name**, **Created Date**, **Created By**, **Modified By**, or **Document Size**.

   d. Click **Search** to search the items according to the conditions you configured. The search conditions and the search results are displayed. The search results table will display a maximum of 500 items. You can edit the search conditions and click **Search** to adjust the search results.

   e. Find and select the item you want to restore from the search results. In the **Recovery Point** column, click the Calendar (📅) button to select a backup job that backed up this item at the status that you want to restore, and click **Apply**. You can click **Restore** next to an item to restore that specific item, or you can click the Restore button above the search result table to restore all selected items.

   f. Continue to step 3 to configure the Restore settings.

- **Calendar mode** – Find a backup job that backed up the items at the time of the status you want to recover, and then search and select the items from the backup data of that backup job.

   a. In the calendar, all Project Online backup jobs are displayed. You can select whether to display the jobs that finished with an exception or failed jobs in the calendar by selecting the **Include jobs with only partial backup data** option. Note that the data of these jobs may be incomplete. Hover over a backup job to show the backup job details.

   b. Select a backup job. All backup data of Project Online is displayed in the table. You can select the **Show data from this backup only** option (historical data in this scope from previous backups not included) to only show the data backed up in the selected backup job.

   c. You can enter keywords to search the items, or you can click the backup data to browse the items you want to restore.

   d. Click the **Restore** button above the table to restore all selected items.

   > **Note:** If you want to select multiple items to restore at the same time, you can only select the items at the same level.

   e. Continue to step 3 to configure the Restore settings.

3. If necessary, you can enter a description for this restore job in the **Description** text box.

4. Select what you would like to restore for the selected items. You can choose to restore all of the content and security from the backup, or you can choose to only restore the security. The security includes all the user permissions at the selected level and beneath. The restore-security-only restore job cannot add or delete any users in the target site collection.

5. Choose where to restore the backup data. Note that the Project Online site collections, sites, projects, and apps only support being restored to the original location in Project Online or another location in Project Online.

   - **Restore the data to its original location** – Restore the backup data to where the data are backed up.

   - **Restore the data to another location** – Restore the backup data to another destination. Configure the following settings:

      - **Select a destination object type** – Select a container as the restore destination. You can enter keywords to search for the restore destination. The items that can be selected as the restore destination are listed under the **Search** box.
        If you select sites, lists, libraries, projects, folders, documents, or apps to restore, you can click a node on the destination tree to load the nodes under it and click the Previous button to navigate back to the previous node. Select a node where you want to restore the backup data.

    - **Action** – Select how the backup data will be restored to the destination. Select **Attach** to restore the contents as children beneath the selected node, or select **Merge** to add the contents to the destination node. . For example, you want to restore a site to another site. If you select **Attach**, the restored site will become the subsite of the destination site; if you select **Merge**, the subsites and contents of the restored site rather than itself will directly become the subsites and contents of the destination site.

  - **Restore the data to your storage** – Restore the backup data to your own storage location configured. This option is not available if the default storage location is used.

    > **Note:** The Project Online site collections, sites, projects, and apps do not support being restored to a custom storage location.

6. Select how to handle the conflicts in the restore job.
   - Container level conflict resolution – Select how to handle the conflicts at the container level.
     - **Skip** – The settings of the conflicting destination container will be retained in the destination.
     - **Merge** – The source container settings and the content will be merged to the conflicting destination container.
     - **Replace** – The settings of the conflicting destination container will be deleted and replaced by the source container settings, as well as, the content within the container.
   - Content level conflict resolution – Select how to handle the conflicts at the content level.

     > **Note:** This is not available if **Replace** is selected as the container level conflict resolution.

     - **Skip** – The conflicting destination content will be retained in the destination, and the backup data of the conflicting content will not be restored.
     - **Overwrite** – The conflicting destination content will be removed from the destination, and the backup data of the conflicting content will be restored.
   - Apps conflict resolution – Select how to handle the apps conflict.
     - **Skip** – The conflicting destination app and AppData will be retained in the destination, and the backup data of the conflicting content will not be restored.
     - **Overwrite** – The conflicting destination app and AppData will be removed from the destination, and the backup data of the conflicting content will be restored.

   > **Note:** If you choose to only restore security, you must select how to handle the security conflicts at the container level and content level. **Replace** will overwrite the security in the destination; **Merge** will combine the security in the backup with the security in the destination.

7. Expand the **Advanced settings** area to configure more restore settings. If you choose to restore to another location, the mapping settings will be available to allow you to update the permissions and metadata or language.
8. **User mapping** - Select a user mapping profile from the drop-down list. For more instructions on creating a new user mapping profile, refer to “Configure Mapping Settings” on page 91.
9. **Language mapping** - Select a language mapping profile from the drop-down list. For more instructions on creating a new language mapping profile, refer to “Configure Mapping Settings” on page 91
10. **Domain mapping** – Select a domain mapping profile from the drop-down list. For additional details on creating a new domain mapping profile, refer to “Configure Mapping Settings” on page 91.
11. In the **Would you like to restore PWA settings** field, select **Yes** or **No** to decide whether to restore the PWA settings.

- **Yes** – With this option selected, all supported PWA settings will be restored. For example, the views and permissions. The restore may interrupt all existing projects in the destination site collection.
- **No** – With this option selected, the restore job will only restore the resources and the Enterprise Project Type associated with the projects and all the Enterprise Custom Fields and Lookup Tables under the PWA.

If you select a Project Online site collection to restore, the recommended option "**Yes**" is by default selected. If you do not want to restore all PWA settings, you can also change the setting to No.

12. Choose how you would like to restore the version history if file versions are backed up by IBM® Storage Protect for Cloud. You can select **Restore the latest version only**, or you can select The **Restore the current and previous versions** option and enter the maximum number of versions you want to restore in the box. IBM® Storage Protect for Cloud can restore up to **20** versions of one document. For the best performance and simplest experience, IBM recommends restoring only the latest version.
    Note the following:
    - By default, history versions of items and files are not backed up due to the regular recovery points created by backup jobs, as well as Microsoft 365 API overhead and limitations related to versions. In our experience, most user and legal requests are only for the most recent active version. In addition, we will capture multiple roll-back points during our daily backups to ensure you have a change history for this document outside native versioning. If you need to back up the versions for some reason and are willing to accept the performance impact, please contact IBM support to have it enabled. The backup job will include the most recent 10 versions by default.
    - If you want to restore earlier versions of a document, you can run an export job to export all versions of that document from the backup data.
13. Select how you would like to restore the Managed Metadata Service.
    - If the containers or content you select to restore is under the site collection level, the **Restore terms in site store only** option and the **Restore terms in both global term store and site term store** option will only restore the terms and their parent terms associated directly with the data from the site store or both. Note that if the data is not restored due to the conflict resolutions you choose, the restored terms cannot be connected to the data either.
    - If you select at least the site collection level object to perform the restore, the **Restore terms in site store only** option will restore all the deleted terms in the site store and the **Restore terms in both global term store and site term store** option will restore all the deleted terms in both the global term store and site term store.
    - If you select to **Use existing terms only**, no terms will be restored.
    - If you want to perform a term store-only restore, refer to the FAQ: How do I perform term store-only restore?
14. Turn on/off the switch to define whether to restore the sharing permissions. This feature only works for the sharing of items to specific people inside or outside your organization. For external users, the restore job can only restore the permissions for the users who have accessed the sharing link. After the restore, the sharing links will be changed, and OneDrive users can navigate to OneDrive > **Shared** library to view the content shared with you and shared by you. The links generated by the **Copy link** function in Microsoft 365 are also regarded as sharing links.

    > **Note:** The Sharing setting is a tenant-level setting, and the IBM® Storage Protect for Cloud Microsoft™ 365 does not protect tenant settings. The restore job to restore a deleted site cannot restore the Sharing settings, including the external users and their permissions.

15. Turn on/off the switch to define whether to enable the Custom Scripts setting during the restore. This feature allows you to restore data related to scripts to the destination Microsoft environment.
16. Click **Next** to view the restore summary.
17. Click **Restore** to restore the selected items. After the job has started, you can navigate to the **Job Monitor** to view more job details. For details, refer to "Job Monitor" on page 153.

Restore Public Folder Data

With IBM® Storage Protect for Cloud Microsoft™ 365, you can restore Public Folder backup data to its original location.

Procedure

Complete the steps below to restore Public Folder data:

1. Navigate to the **Restore › IBM® Storage Protect for Cloud Backup** page, and then click the **Public Folder** tile

2. Select the items that you want to restore. You can choose one of the following methods to find the data to restore.

   - **Search mode** – Define a Project Online site collection as the search scope and then use the properties to search for the items within the scope. Note that this method does not support searching and restoring the list items.

   a. In the **Name** field, enter or select a public folder. The default search condition is to search the backup data of that public folder within the last backup cycle.

   b. In the **Backup time range** field, the time range of the last backup cycle is displayed by default.

   Click the Calendar (📅) button to customize the backup time range. The start date must be earlier than the end date. You can click **Reset** if you want to reset the settings. Click **OK** to save your customization.

   c. Select **Folder** or **Mailbox Item** from the **Level** list for the items you want to search. If you want to search for items within the selected public folder, select the **Mailbox Item** option from the **Level** list, and you can configure the following search conditions: **Subject**, **Sent From**, **Sent To**, and **Date Sent**.

   d. Click **Search** to search the items according to the conditions you configured. The search conditions and the search results are displayed. The search results table will display a maximum of 500 items. You can edit the search conditions and click **Search** to adjust the search results.

   e. Find and select the item you want to restore from the search results. In the **Recovery Point** column, click the Calendar (📅) button to select a backup job that backed up this item at the status that you want to restore, and click **Apply**. In the **Metadata Recovery Point** drop-down list, you can select a backup time that backs up the metadata to overwrite the current metadata with the backup data or select **None** to not overwrite the current metadata. You can click **Restore** next to an item to restore that specific item, or you can click the **Restore** button above the search result table to restore all selected items.

   f. Proceed to step 3 to continue with the Restore settings.

   - **Calendar mode** – Find a backup job that backed up the items at the time of the status you want to recover, and then search and select the items from the backup data of that backup job.

     a. Click the **Find the items in a specific backup job** link or the Next button.

     b. In the calendar, all backup jobs of Public Folder are displayed. You can select whether to display the finished with an exception or failed jobs in the calendar by selecting the **Include jobs with only partial backup data** option. Note that the data of these jobs may be incomplete. Hover over a backup job to show the backup job details.

     c. Select a backup job. All backup data of Public Folder is displayed in the table. You can select the **Show data from this backup only** option (historical data in this scope from previous backups not included) to only show the data backed up in the selected backup job.

     d. You can enter keywords to search the items, or you can click the backup data to browse the items you want to restore.

     e. Select the items you want to restore and then click the **Restore** button above the table to restore all selected items.

> **Note:** If you want to select multiple items to restore at the same time, you can only select the items at the same level.

f. Proceed to step 3 to continue with the Restore settings.

3. If necessary, you can enter a description for this restore job in the **Description** text box.
4. Choose where to restore the backup data to. Public Folder data only can be restored to its original location. Select **Restore the data to its original location** option to restore the selected data to the original location.
5. Select how to handle the conflicts in the restore job.

> **Note:** If there are container conflicts in the Public Folder restore, the backup content in the source container will be merged to the destination conflicting container.

- Select how to handle the content level conflicts:

  Skip

  The destination conflicting content will be retained in the destination, and the backup data of the conflicting content will not be restored.

  Overwrite

  The destination conflicting content will be removed from the destination, and the backup data of the conflicting content will be restored.

- Select how to handle the permission conflicts:

  Skip

  The destination conflicting permission will remain unchanged.

  Overwrite

  The destination conflicting permission will be replaced by the permission in the backup.

6. Turn on/off the switch to define whether to allow restore jobs to rehydrate the data sets automatically when the backup data is stored in the Azure archive storage tier. This field is only functional for the BYOS subscription type. For IBM® Storage Protect for Cloud default storage, the restore job will automatically rehydrate data.

> **Note:** IBM® Storage Protect for Cloud recommends not storing the index database to the Azure archive storage tier.

7. Click **Next** to view the restore summary.
8. Click **Restore** to restore the selected items.

Restore Teams Data

Before you begin

If a team has been deleted from the original location, the restore job can recover that team and the permissions of the owner and members to its original location. To view the supported and unsupported data types of Teams, refer to“Teams Data Types” on page 229 .

You can also choose to restore partial Teams data to another location. IBM® Storage Protect for Cloud Microsoft™ 365 now supports restoring the files in a standard channel or a Team site to another channel site or Team site. Additionally, IBM® Storage Protect for Cloud now supports out-of-place restore operations between SharePoint Online sites, OneDrive, Teams sites, and Group sites. For details on which data types are supported for being restored to another location, refer to Teams Data Supported for Out-of-Place Restore.

You can now select to restore the Channel’s conversations and files to your storage if you have a BYOS subscription.

IBM® Storage Protect for Cloud service for Teams also provides the option allowing you to restore a soft-deleted team from the Microsoft 365 recycle bin to its last known good state. IBM® Storage Protect for Cloud will perform a check for the team status in Microsoft 365 to ensure Microsoft has this data and present the options for you to decide the best way to recover data: using Microsoft native restore function within that 30-day retention period or using IBM® Storage Protect for Cloud backup data to roll back the entire team or granular contents.

> **Note:** The check will only happen when you select the team as both the restore scope and the search level.

Before you restore Teams data, note the following:

- To restore the Private/Shared Channel data, you can only use the **Calendar mode** restore wizard to restore the data to its original location. Private Channels have a lock icon displayed next to their name.
- To restore settings in Teams, the Microsoft™ 365 service account used to perform the restore must be the owner of the team that you want to restore.
- If you want to restore documents or security to another Team and the related users in the backup do not exist in the destination team, the permission of these users will not be kept. They will not have access to the restored documents in the destination Team.
- The accounts’ profile photos in Teams cannot be restored.
- For Channel restoration, only existing channels can be restored. You cannot re-create a channel that was created and then deleted. For the soft-deleted channels that are stored in the Recycle bin of the team site, you can manually restore them from your Microsoft™ 365 tenant. Once a channel name has been created, even if it is deleted, it cannot be recreated either through the API or Teams interface. The system maintains this data for information protection scenarios.
- To restore comments added to Planner tasks, you must configure an app profile for the Microsoft Delegated app in IBM® Storage Protect for Cloud and select the **Restore Planner task comments** function when consenting to the app profile.
- The past conversations can be recovered as read-only HTML files or as new posts to the channel.
  - If you restore the conversations to HTML files, the conversations that are created within the same month will be restored to the same HTML file named in the following format: **ChannelName_March 2022**. Each HTML file will store up to 10,000 records. If the number of records exceeds 10,000, the HTML files will be created with a postfix attached in the file name. For example, **ChannelName_March 2022_1**.
  - If you restore the conversations as new posts, the product will post a new message to the channel's **Posts** with the original message's sender information and sent date in the message body. The new message is posted in the name of the service account or the Delegated app authentication user, depending on the authentication method you choose to scan Teams. To use this feature, you can either use service account authentication or app profile authentication to scan Teams, but you must have a Microsoft Delegated app connected to your tenant. For details on creating an app profile for Microsoft Delegated, refer to Create an App Profile. Note that the authentication user of the delegated app must have a Teams license and an Exchange Online license.

    > **Note:** A restore job to restore conversations as posts via the delegated app will add the authentication user to Teams members or private channel members and then automatically remove them after the restore job completes.
- If there are conversations that have not been backed up before the channel was renamed, these conversations posted before the renaming will be restored to a new folder named by the previous channel name under the **General** channel.
- Does not support backing up and restoring folders added through the **Add cloud storage** method under the **Files** tab in channels.

About this task

If a team has been deleted from the original location, the restore job can recover that team and the permissions of the owner and members to its original location. To view the supported and unsupported data types of Teams, refer to “Teams Data Types” on page 229.

You can also choose to restore partial Teams data to another location. For details on which data types are supported for being restored to another location, refer to Teams Data Supported for Out-of-Place Restore.

You can select to restore the Channel’s conversations and files to your storage if you have a BYOS subscription.

IBM® Storage Protect for Cloud Microsoft™ 365 for Teams also provides the option allowing you to restore a soft-deleted team from the Microsoft™ 365 recycle bin to its last known good state. IBM® Storage Protect for Cloud will perform a check for the team status in Microsoft™ 365 to ensure Microsoft™ has this data and clearly present the options for you to decide the best way to recover data: using Microsoft™ native restore function within that 30-day retention period or using IBM® Storage Protect for Cloud backup data to roll back the entire team or granular contents.

> **Note:** The check will only happen when you select the team as both the restore scope and the search level.

Procedure

Complete the steps below to restore Teams data:

1. Navigate to the **Restore › IBM® Storage Protect for Cloud Backup** page, and then click the **Teams** tile.
2. Select the data that you want to restore. You can choose one of the following methods to find the data to restore.
   - **Search mode** – Select a restore object scope and search for the data to restore. Follow steps 3 to 4.
   - **Calendar mode** – Select a recovery point (backup job) and select data from that backup to restore. Proceed to step 5.
3. Define a Team as the search scope. You can enter the Team’s name or email address to search, and then select the Team from the **Name** list. The default search condition is to search the backup data for the Team within the last backup cycle. The drop-down list will remind you of teams with unusual activities or under potential ransomware attacks.
4. You can choose to use the properties on the same page to search for the contents within this team for granular data roll-back, or you can directly proceed to the next step to search and select the data to restore.

   > **Note:** If the team you want to restore has been deleted from Microsoft™ 365, you can let IBM® Storage Protect for Cloud Microsoft™ 365 check if the team is still in soft-deleted status and exists in the Microsoft™ 365 recycle bin to help you decide the best way to restore. In this case, select that team and directly click **Search**.

   If the team is still in soft-deleted status in Microsoft™ 365, you can choose the following methods:

   - If you choose to restore the entire scope from Microsoft™ 365, click **Next** and then select a recovery point. Click **OK** to start the restore job. You can navigate to the Microsoft™ 365 environment to monitor and verify the progress.

     > **Note:** If you only want to restore the scope from the recycle bin for its last known status, we strongly recommend selecting this option for faster job performance and better data integrity.

   - If you choose to restore the selected scope or just content within this scope from backup data, click **Next**, and you can configure search settings to search for the granular contents.

For the details of using the properties on the first page or the **Search** feature on the **Select and restore the data** step, refer to the steps below:

a. In the **Name** field, you can enter or select another team to change the search scope.

b. In the **Backup Time Range** field, the time range of the last backup cycle is displayed by default.

Click the Calendar (📅) button to customize the backup time range. The start date must be earlier than the end date. You can click **Reset** if you want to reset the settings. Click **OK** to save your customization.

c. Select **Teams**, **Folder in Mailbox**, **Mailbox Item**, **Group Team Site**, **Site**, **List/Library**, **App**, **Folder in SharePoint**, **Document**, **Plan**, or **Task** from the **Level** list for the items you want to search. To search for all objects at the level, leave the search conditions empty.

d. Click **Search** to search the items according to the conditions you configured. The search conditions and the search results are displayed. The search results table will display a maximum of 500 items. You can edit the search conditions and click **Search** to adjust the search results.

e. Find and select the item you want to restore from the search results. In the **Recovery point** column, click the Calendar (📅) button to select a backup job that backed up this item at the status that you want to restore, and click **Apply**. Recovery points with objects with unusual activities detected or potential ransomware attack detected will be displayed with 🔔 (**Unusual activities detected**) or 🔔 (**Potential ransomware attack detected**).

f. Click the **Restore** button above the search result table to restore all selected items.

g. Proceed to step "6" on page 135 to continue with the Restore settings.

5. Find a backup job that backed up the items at the time of the status you want to recover, and then search and select the items from the backup data of that backup job.

   a. In the calendar, all backup jobs of Teams are displayed. You can select whether to display the finished with an exception or failed jobs in the calendar by selecting the **Include jobs with only partial backup data** option. Note that the data of these jobs may be incomplete. Hover over a backup job to show the backup job details.

   b. Select a backup job. All backup data of Teams are displayed in the table. You can select the **Show data from this backup only** option (historical data in this scope from previous backups not included) to only show the data backed up in the selected backup job. Recovery points with objects with unusual activities detected or potential ransomware attack detected will be displayed with 🔔 (**Unusual activities detected**) or 🔔 (**Potential ransomware attack detected**).

   c. You can enter keywords to search the items, or you can click the backup data to browse the items you want to restore. After expanding a Team node, you can select the **Show Team Site** checkbox under the table to show the Team site node.
   When you browse down to a private channel, you can select the **Show the private channel site** option to also display the site of this private channel on the data tree. You can select the site to restore or browse down to find the content that you want to restore.

   Click **Restore** next to an item to restore the specific item or select the items you want to restore and then click the **Restore** button above the table to restore all of the selected items.

   Note that the restore settings will only show the options that support all the selected objects. For example, if you select Team site, Meetings, and Group Conversations at the same time, the restore settings will not display the **Restore security only** option, and the **Would you like to restore the permissions of external users** settings.

   d. Continue to step 6 to configure the Restore settings.

6. If necessary, you can enter a description for this restore job in the **Description** text box. For objects with unusual activities or under ransomware attacks, you can click the **Potential ransomware attack detected** or **Unusual activities detected**in the **Suggested** field below to enter it in the **Description** text box directly.

7. Choose where to restore the backup data to.

   - **Restore the data to its original location** – Restore the backup data to where the data is backed up.

   - **Restore the data to another location** – Restore the backup data to another destination. Configure the following settings:

        - **Select a restore destination** – If you select a Teams site or site item, you can select to restore the backup data to SharePoint Online, OneDrive, Microsoft 365 Groups, or Teams. For others, select a container as the restore destination. You can enter keywords to search for the restore destination. The items that can be selected as the restore destination are listed under the **Search** box.
        - **Action** – Select how the backup data will be restored to the destination. Select **Attach** to restore the contents as children beneath the selected node, or select **Merge** to add the contents to the destination node. For example, you want to restore a folder to another folder. If you select **Attach**, the restored folder will become the subfolder of the destination folder; if you select **Merge**, the subfolders and contents of the restored folder rather than itself will directly become the subfolders and contents of the destination folder.
    - **Restore the data to your storage** – If you have selected the Channels, Conversations, or Files, and you have the BYOS subscription, this option is available. You can restore the Channel's conversations and files to your storage.

8. Select how to handle conflicts in the restore job. The available conflict resolution options will vary for the items you select to restore. Select how to handle the conflicts in the restore job.
    - **Container level conflict resolution** – Select how to handle the conflicts at the container level.
        - **Skip** – The settings of the conflicting destination container will be retained in the destination.
        - **Merge** – The source container settings and the content will be merged to the conflicting destination container. With **Merge** as the container level conflict resolution, the **Privacy**, **Name**, and **Description** will be updated to the destination team, and the team owner and members of the source team will be added to the destination.
        - **Replace** – The settings of the conflicting destination container will be deleted and replaced by the source container settings, as well as the content within the container.

          > **Note:** The **Replace** option is unavailable when you select the whole Team to restore.

    - Content level conflict resolution – Select how to handle conflicts at the content level.
        - **Skip** – The conflicting destination content will be retained in the destination, and the backup data of the conflicting content will not be restored.
        - **Overwrite** – The conflicting destination content will be removed from the destination, and the backup data of the conflicting content will be restored.
        - **Overwrite by Last Modified Time** – If the last modified time of the conflicting destination content is earlier than that of the source content, the conflicting destination content will be removed from the destination, and the backup data of the conflicting content will be restored.
        - **Append an "_1" to the Item/Document** – If the last modified time of the conflicting destination content is the same, the restore will be skipped; if the last modified time is different, the conflicting destination content will be kept, and the backup data of the conflicting content will be added to the destination with a sequential number suffix added to the filename.

          > **Note:** : If you want to restore a single file version without affecting other versions, set the content level conflict resolution to **Append an "_1" to the Item/Document**. If the content level conflict resolution is set to **Overwrite**, the restore job will remove all the versions of this file from the destination and keep this file version as the latest and only version of the file.

    - Apps conflict resolution – Select how to handle the apps conflict.
        - **Skip** – The conflicting destination app and AppData will be retained in the destination, and the backup data of the conflicting content will not be restored.
        - **Overwrite** – The conflicting destination app and AppData will be removed from the destination, and the backup data of the conflicting content will be restored.

9. Expand the **Advanced settings** area to configure more restore settings. If you choose to restore to another location, the mapping settings will be available to allows you to update the permissions and metadata or language.

10. **User mapping** - Select a user mapping profile from the drop-down list. For more instructions on creating a new user mapping profile, refer to "Configure Mapping Settings" on page 91.

11. **Language mapping** - Select a language mapping profile from the drop-down list. For more instructions on creating a new language mapping profile, refer to "Configure Mapping Settings" on page 91

12. Select how you would like to restore the channel conversations. You can choose to restore the channel conversations to the read-only HTML files (stored in **Files**) or restore them as the new posts in the channel. If you want to restore the channel conversations as posts, you must have a Microsoft Delegated app registered in your tenant. For details on configuring the app, refer to Create an App Profile.

    > **Note:** If your Teams are scanned using app profile authentication, a restore job to restore conversations as posts will add the authentication user to Teams members or private channel members and then automatically remove them after the restore job completes.

13. Choose how you would like to restore the version history if file versions are backed up by IBM® Storage Protect for Cloud. You can select **Restore the latest version only**, or you can select the **Restore the current and previous versions** option and enter the maximum number of versions you want to restore in the box. IBM® Storage Protect for Cloud Microsoft™ 365 can restore up to **20** versions for one document. For the best performance and simplest experience, restore only the latest version.
    Note the following:

    - capture multiple roll-back points during our daily backups to ensure you have a change history for this document outside native versioning. If you need to back up the versions for some reason and are willing to accept the performance impact, please contact IBM support to have it enabled. The backup job will include the most recent 10 versions by default.
    - If you want to restore earlier versions of a document, you can run an export job to export all versions of that document from the backup data.
    - This restore setting is not available when selecting documents.

14. Select how you would like to restore the Managed Metadata Service.

    - If the containers or content you select to restore is under the site collection level, the **Restore terms in site store only** option and the **Restore terms in both global term store and site term store** option will only restore the terms and their parent terms associated directly with the data from the site store or both. Note that if the data is not restored due to the conflict resolutions you choose, the restored terms cannot be connected to the data either.
    - If you select at least the site collection level object to perform the restore, the **Restore terms in site store only** option will restore all the deleted terms in the site store and the **Restore terms in both global term store and site term store** option will restore all the deleted terms in both the global term store and site term store.
    - If you select to **Use existing terms only**, no terms will be restored.
    - If you want to perform a term store-only restore, refer to the FAQ: "How do I restore term store-only data?" on page 33

15. Turn on/off the switch to define whether to restore the sharing permissions. This feature only works for the sharing of items with specific people inside or outside your organization. For external users, the restore job can only restore the permissions for the users who have accessed the sharing link. After the restore, the sharing links will be changed, and OneDrive users can navigate to OneDrive > **Shared** library to view the content shared with you and shared by you. The links generated by the **Copy link** function in Microsoft 365 are also regarded as sharing links.

    > **Note:** The Sharing setting is a tenant-level setting, and the IBM® Storage Protect for Cloud Microsoft™ 365 does not protect tenant settings. The restore job to restore a deleted site cannot restore the Sharing settings, including the external users and their permissions.

16. Turn on/off the switch to define whether to restore the hub site connection. This option is only available when you select a Team or a Team site to restore.

> **Note:** IBM® Storage Protect for Cloud cannot restore the hub site connection for the selected site, if it is a cross-tenant restore or the destination hub site requires approval for the associated sites to join.

17. Turn on/off the switch to define whether to allow restore jobs to rehydrate the data sets automatically when the backup data is stored in the Azure archive storage tier. This field is only functional for the BYOS subscription type. For IBM® Storage Protect for Cloud default storage, the restore job will automatically rehydrate data.
18. Turn on/off the switch to define whether to enable the Custom Scripts setting during the restore. This feature allows you to restore data related to scripts to the destination Microsoft environment.
19. Click **Next** to view the restore summary.
20. Click **Restore** to restore the selected items. After the job has started, you can navigate to the **Job Monitor** to view more job details. For details, refer to "Job Monitor" on page 153.

Restore Viva Engage Data

Procedure

With IBM® Storage Protect for Cloud, you can restore Viva Engage backup data to its original location, and restore Viva Engage communities and site collections to another location.

Complete the steps below to restore Viva Engage data:

1. Navigate to the **Restore › IBM® Storage Protect for Cloud Backup** page, and then click the **Viva Engage** tile.
2. Select the data that you want to restore. You can choose one of the following methods to find the data to restore.
   - **Search mode** – Select a restore object scope and search for the data to restore. Follow steps 4 to 5..
   - **Calendar mode** – Select a recovery point (backup job) and select data from that backup to restore. Proceed to step 5.
3. Define a Viva Engage community as the search scope. You can enter the Viva Engage community address or display name to search, and then select the Viva Engage community from the **Name** list. The default search condition is to search the backup data for the selected community within the last backup cycle.
4. You can choose to use the properties on the same page to search for the contents within this community for granular data roll-back, or you can directly proceed to the next step to search and select the data to restore.
   For the details of using the properties on the first page or the **Search** feature on the **Select and restore the data** step, refer to the steps below:
   a. In the **Name** field, you can enter or select another team to change the search scope.
   b. In the **Backup Time Range** field, the time range of the last backup cycle is displayed by default.

      Click the Calendar (📅) button to customize the backup time range. The start date must be earlier than the end date. You can click **Reset** if you want to reset the settings. Click **OK** to save your customization.
   c. Select **Viva Engage community**, **Site collection**, **Site**, **List/Library**, **App**, **Folder in SharePoint**, **Document**, **Plan**, or **Task** from the **Level** list for the items you want to search. If you want to search for all objects at the level, you select from the selected Viva Engage community. You can leave the search conditions empty.
   d. Click **Search** to search the items according to the conditions you configured. The search conditions and the search results are displayed. The search results table will display a maximum of 500 items. You can edit the search conditions and click **Search** to adjust the search results.

e. Find and select the item you want to restore from the search results. In the **Recovery point** column, click the Calendar (📅) button to select a backup job that backed up this item at the status that you want to restore, and click **Apply**. Click the **Restore** button above the search result table to restore all selected items.

f. Proceed to step "6" on page 139 to continue with the Restore settings.

5. Find a backup job that backed up the items at the time of the status you want to recover, and then search and select the items from the backup data of that backup job.

   a. In the calendar, all backup jobs of Viva Engage are displayed. You can select whether to display the finished with an exception or failed jobs in the calendar by selecting the **Include jobs with only partial backup data** option. Note that the data of these jobs may be incomplete. Hover over a backup job to show the backup job details.

   b. Select a backup job. All backup data are displayed in the table. You can select the **Show data from this backup only (historical data in this scope from previous backups not included)** option to only show the data backed up in the selected backup job.

   c. d. You can enter keywords to search the items, or you can click the backup data to browse the items you want to restore.
   Click **Restore** next to an item to restore the specific item or select the items you want to restore and then click the Restore button above the table to restore all of the selected items.

   Note that the restore settings will only show the options that support all the selected objects.

   d. Continue to step "6" on page 139 to configure the Restore settings.

6. If necessary, you can enter a description for this restore job in the **Description** text box.

7. Choose where to restore the backup data to.

   - **Restore the data to its original location** – Restore the backup data to where the data is backed up.
   - **Restore the data to another location** – Restore the backup data to another destination. If you select a Viva Engage community or site collection, this option is available. Configure the following settings:
     - **Select a restore destination** – Select a container as the restore destination. You can enter keywords to search for the restore destination. The items that can be selected as the restore destination are listed under the **Search** box.
     - **Action** – Select how the backup data will be restored to the destination. Select **Attach** to restore the contents as children beneath the selected node, or select **Merge** to add the contents to the destination node. For example, you want to restore a folder to another folder. If you select **Attach**, the restored folder will become the subfolder of the destination folder; if you select **Merge**, the subfolders and contents of the restored folder rather than itself will directly become the subfolders and contents of the destination folder.
   - **Restore the data to your storage** – If you have selected the Viva Engage conversations or files, and you have the BYOS subscription, this option is available. You can restore the Viva Engage conversations and files to your storage.

8. Select how to handle conflicts in the restore job. The available conflict resolution options will vary for the items you select to restore.

   - Container level conflict resolution – Select how to handle conflicts at the container level.
     - **Skip** – The settings of the conflicting destination container will be retained in the destination.
     - **Merge** – The source container settings and the content will be merged to the conflicting destination container. With **Merge** as the container level conflict resolution, the **Privacy**, **Name**, and **Description** will be updated to the destination Viva Engage community, and the owner and members of the source Viva Engage community will be added to the destination.
     - **Replace** – The settings of the conflicting destination container will be deleted and replaced by the source container settings, as well as the content within the container.

     > **Note:** The Replace option is unavailable when you select the whole Team to restore.

- Content level conflict resolution – Select how to handle conflicts at the content level.
  - **Skip** – The conflicting destination content will be retained in the destination, and the backup data of the conflicting content will not be restored.
  - **Overwrite** – The conflicting destination content will be removed from the destination, and the backup data of the conflicting content will be restored.
  - **Overwrite by Last Modified Time** – If the last modified time of the conflicting destination content is earlier than that of the source content, the conflicting destination content will be removed from the destination, and the backup data of the conflicting content will be restored.
  - **Append an "_1" to the Item/Document** – If the last modified time of the conflicting destination content is the same, the restore will be skipped; if the last modified time is different, the conflicting destination content will be kept, and the backup data of the conflicting content will be added to the destination with a sequential number suffix added to the filename.

> **Note:** If you want to restore a single file version without affecting other versions, set the content level conflict resolution to **Append an "_1" to the Item/Document**. If the content level conflict resolution is set to **Overwrite**, the restore job will remove all the versions of this file from the destination and keep this file version as the latest and only version of the file.

- Apps conflict resolution – Select how to handle the apps conflict.
  - **Skip** – The conflicting destination app and AppData will be retained in the destination, and the backup data of the conflicting content will not be restored.
  - **Overwrite** – The conflicting destination app and AppData will be removed from the destination, and the backup data of the conflicting content will be restored.

9. Select how you would like to restore the version history if file versions are backed up by IBM® Storage Protect for Cloud. You can select to only restore the latest version, or you can select The **Restore the current and previous versions** option and enter the maximum number of versions you want to restore in the box. IBM® Storage Protect for Cloud Microsoft™ 365 can restore up to **20** versions for one document. For the best performance and simplest experience, IBM® Storage Protect for Cloud recommends restoring only the latest version.
   Note the following:
   - By default, history versions of items and files are not backed up due to the regular recovery points created by backup jobs, as well as Microsoft 365 API overhead and limitations related to versions. In our experience, most user and legal requests are only for the most recent active version. In addition, we will capture multiple roll-back points during our daily backups to ensure you have a change history for this document outside native versioning. If you need to back up the versions for some reason and are willing to accept the performance impact, please contact IBM support to have it enabled. The backup job will include the most recent 10 versions by default.
   - If you want to restore earlier versions of a document, you can run an export job to export all versions of that document from the backup data.
   - This restore setting is not available when selecting documents.

10. Select how you would like to restore the Managed Metadata Service.
    - If the containers or content you select to restore is under the site collection level, the **Restore terms in site store only**option and the **Restore terms in both global term store and site term store**option will only restore the terms and their parent terms associated directly with the data from the site store or both. Note that if the data is not restored due to the conflict resolutions you choose, the restored terms cannot be connected to the data either.
    - If you select at least the site collection level object to perform the restore, the **Restore terms in site store only**option will restore all the deleted terms in the site store and the **Restore terms in both global term store and site term store**option will restore all the deleted terms in both the global term store and site term store.
    - If you select to **Use existing terms only**, no terms will be restored.

- If you want to perform a term store-only restore, refer to the FAQ: “How do I restore term store-only data?” on page 33.

11. Turn on/off the switch to define whether to restore the hub site connection. This option is only available when you select the Viva Engage community or community site to restore.

    > **Note:** IBM® Storage Protect for Cloud cannot restore the hub site connection for the selected site, if it is a cross-tenant restore or the destination hub site requires approval for the associated sites to join.

12. Turn on/off the switch to define whether to allow restore jobs to rehydrate the data sets automatically when the backup data is stored in the Azure archive storage tier. This field is only functional for the BYOS subscription type. For IBM® Storage Protect for Cloud default storage, the restore job will automatically rehydrate data.
13. Click **Next** to view the restore summary.
14. Click **Restore** to restore the selected items. After the job has started, you can navigate to the **Job Monitor** to view more job details. For details, refer to “Job Monitor” on page 153.

Restore Power BI Data

About this task

With IBM® Storage Protect for Cloud, you can restore Power BI workspace permissions, reports, and datasets to their original location, to another location, or to a storage location. Note that when restoring to another location, reports and datasets can only be restored to another workspace.

Additionally, only workspace-level permissions can be restored. Report-level permissions are not supported.

> **Note:** : If you want to restore the backup data to a storage location, you must have your own storage location configured. The default storage provided by IBM cannot be the destination of the restore.

Procedure

Complete the steps below to restore Power BI data:

1. Navigate to the **Restore** > **IBM® Storage Protect for Cloud Microsoft™ 365** page, and then click the **Power BI** tile.
2. Select the items that you want to restore. You can choose one of the following methods to find the data to restore.
   - **Search mode** – Define a Power BI workspace as the search scope and then use the properties to search for the items within the scope. Refer to the steps below:
     a. In the **Name** field, enter or select a Power BI workspace. The default search condition is to search the backup data within the last backup cycle.

     b. In the **Backup time range** field, the time range of the last backup cycle is displayed by default. Click the Calendar (📅) button to customize the backup time range. The start date must be earlier than the end date. You can click **Reset** if you want to reset the settings. Click **OK** to save your customization.

     c. Select **Workspace** or **Report** from the **Level** list for the items you want to search.

     d. Click **Search** to search the items according to the conditions you configured. The search conditions and the search results are displayed. The search results table will display a maximum of 2000 items. You can edit the search conditions and click **Search** to adjust the search results.

    e. Find and select the item you want to restore from the search results. In the **Recovery point** column, click the Calendar (📅) button to select a backup job that backed up this item at the status that you want to restore, and click **Apply**. Click the **Restore** button above the search result table to restore all selected items.

    f. Continue to step 3 to configure the Restore settings.

- **Calendar mode** – Find a backup job that backed up the items at the time of the status you want to recover, and then search and select the items from the backup data of that backup job.

    a. In the calendar, all backup jobs of Power BI are displayed. You can select whether to display the finished with an exception or failed jobs in the calendar by selecting the **Include jobs with only partial backup data** option. Note that the data of these jobs may be incomplete. Hover over a backup job to show the backup job details.

    b. Select a backup job. All backup data, up to a maximum of 2000 items, are displayed in the table. You can select the **Show data from this backup only** option (historical data in this scope from previous backups not included) to only show the data backed up in the selected backup job.

    c. You can enter keywords to search the items, or you can click the backup data to browse the items you want to restore. Select the items you want to restore and then click the **Restore** button above the table to restore selected items.

    d. Continue to step 3 to configure the Restore settings.

3. If necessary, you can enter a description for this restore job in the **Description** text box.

4. Choose where to restore the backup data to.

    - **Restore the data to its original location** – Restore the backup data to where the data is backed up.

    - **Restore the data to another location** – Restore the backup data to another destination. Reports and datasets can only be restored to another workspace. Configure the following settings:

        ◦ **Select a restore destination** – Select a container as the restore destination. You can enter keywords to search for the restore destination. The items that can be selected as the restore destination are listed under the **Search** box.

        ◦ **Action** – Select how the backup data will be restored to the destination. Select **Attach** to restore the contents as children beneath the selected node, or select **Merge** to add the contents to the destination node. For example, you want to restore a folder to another folder. If you select **Attach**, the restored folder will become the subfolder of the destination folder; if you select **Merge**, the subfolders and contents of the restored folder rather than itself will directly become the subfolders and contents of the destination folder.

    - **Restore the data to your storage** – If you have selected the Viva Engage conversations or files, and you have the BYOS subscription, this option is available. You can restore the selected data to your storage.

5. Select how to handle conflicts at the content level in the restore job.

    - **Skip** – The conflicting destination content will be retained in the destination, and the backup data of the conflicting content will not be restored.

    - **Append the creation date to the report name** – The conflicting destination content will be kept, and the backup data of the conflicting content will be added to the destination with a creation date suffix added to the report name.

6. Turn on/off the switch to define whether to restore permissions. Only workspace-level permissions can be restored. Report-level permissions are not supported.

7. Click **Next** to view the restore summary.

8. Click **Restore** to restore the selected items.

Data Management

Through Data Management, you can work with

- The **Backup Data eDiscovery** wizard allows you to search across all your Exchange Online mailboxes backup data for the emails with specific properties and then you can perform restore, export, or deletion of the selected recovery points. If you want to enable this feature, contact IBM Software Support for assistance.
- The **Data Subject Access Requests** wizard to discover the backup data of a given data subject and delete the backups.
- he **Remove unprotected data** report to check for the out-of-scope objects and offboarded users, and the expiration date for their backup data to be deleted.
- **Manually Delete Backup Data** wizard to discover and remove the backup data of individual files, emails, or other documents to prevent any future restores.

Backup Data eDiscovery

In the **Backup Data eDiscovery** page, you can perform **metadata-based searches for Exchange Online** and **both metadata-based and content-based searches for OneDrive**. After you have found the backup data you want, you can perform a data recovery, exportation, or deletion job directly from search result page. To enable this feature, contact your IBM sales representative or business partner to purchase this feature at an additional cost.

About this task

If you previously enabled metadata-based search for and now want to upgrade your e-discovery capabilities to include content-based search, contact your IBM sales representative to upgrade your subscription at an additional cost.

It may take extra time to update the index for the backup. Therefore, the search that was performed right after the backup job may not be accurate. In addition, if you have ever changed the storage, the eDiscovery can only search from your backups in the current storage.

Procedure

Follow the steps below to search for the emails and perform the operation you need:

1. To enable this feature for the first time, click the **Activate services** button to enable it.
2. Select either Exchange Online or OneDrive service to search for your backup data.
3. Configure search conditions based on your selected service:
   - For **Exchange Online**, configure the search conditions for **Subject**, **Sent from**, **Sent to**, and **Date sent**.
   - You can enter multiple keywords in the **Subject** box and separate them with a semicolon (;).
   - The **Sent From** box and the **Sent To** box also support entering multiple users. Ensure you use semicolon (;) to separate them.
   - The time range you configured for **Date Sent** cannot exceed one year. The search will find the emails that were sent or received within that time range.
4. You can also use the **Advanced search** to narrow down results by filtering the container, mailbox address, folder name, or whether the email has attachments.
   - For OneDrive, configure the search conditions for **Document name**, **Content**, **Created by**, and **Modified date range**.
     - Support document types include .txt, .pdf, .docx, .doc, .xlsx, .xls, .pptx, .ppt, with a file size limit of less than 50 MB.
     - The following characters are not supported for search: +, -, &, ||, !, ( ), { }, [ ], ^, ", :, \, /.
     - The search primarily supports English queries and has limitations for other languages.

        - Documents with sensitive labels are not supported and cannot be found by **Content** search.

    You can also use the **Advanced search** to narrow down results by filtering container, user, folder name, data size or document modifier.

5. Click **Search**.
6. In the search result page, the search results in the latest backup cycle are displayed. You can click the link above the table to check the search result in another backup cycle. In addition, you can update the search conditions to adjust your search results.
7. You can perform the following operations on the emails in the search result:
    - **Download File List** – Download the search results to an XLSX file to your local computer. Extract the ZIP file and open the XLSX file in Excel to view all the records in the search results, including the email subject, recovery point, sent from, and sent to.
    - **Restore** – Restore the email to its original location. For details, refer to "Restore Exchange Online Data" on page 111.
    - **Export** – Export the selected backup data. An export job will start. You can navigate to Job Monitor to check for the job progress and download the exported content. For details, refer to "Download the Exported Data" on page 109.
    - **Delete** – Delete the selected backup data. In the confirmation window, you need select the **I understand that the selected backup data will be permanently deleted** option and click **Yes** to confirm your deletion.

Data Subject Access Requests

To help your organization comply with the General Data Protection Regulation (GDPR), IBM® Storage Protect for Cloud Microsoft™ 365 provides a tool that discovers all copies of the Exchange Online Mailbox, SharePoint Online Site Collections and OneDrive backups of a given data subject that are stored by IBM® Storage Protect for Cloud Microsoft™ 365 solution and deletes the user-generated backups of Mailbox, SharePoint Online Site Collections, and OneDrive. After the deletion, the entire object, along with all associated data, is permanently deleted.

About this task

The IBM® Storage Protect for Cloud Microsoft™ 365 data stored on the backend is immutable to users. Administrators can enable data availability for data subject access requests in accordance with their organization's GDPR policy.

Note the following:

- If you currently have no GDPR requests and want to avoid any accidental deletion of backup data, you can contact IBM Software Support to disable this feature. Note that the **Data Subject Access Requests** feature and the **Manually Delete Backup Data** feature will both be disabled.
- You can enable the approval process for data deletion in **Settings** > **Security** to avoid accidental data loss. With this feature enabled, data deletion requests and email notifications will be sent to the administrators when you delete data in **Manually delete backup data** and **Data subject access requests**. Then administrators can access the IBM® Storage Protect for Cloud Microsoft™ 365 interface and click **My Tasks** (📅) on the upper-right of the interface to approve or reject your requests. The deletion jobs will start when the requests are approved. Note that the requests will be automatically invalidated if not approved within 7 days. Complete the steps below:

Procedure

1. Click **Data Management › Data Subject Access Requests** on the left page.
2. Click **Discover & Delete** to enter the **What type of content are you looking to identify?** page.
3. Select the content type that you are looking for. If you want to delete the mailbox backup of the data subject, select **Exchange Online**; to delete the backup of the data subject's libraries, select **OneDrive**; to delete the backup of the site collection backup of the data subject, select **SharePoint Online**.
4. Enter the keyword to search for the data subject you are looking for. Select the data subject from the list and then click **Apply**. You can select multiple items in the search result.

5. You can export a list of recovery points to view the object backup history. Select the objects and click **Export recovery point**. A ZIP file will be automatically saved to the download location of your browser in the local computer.

6. Click **Delete** to delete all backup data for the selected objects from IBM® Storage Protect for Cloud Microsoft™ 365.
   You can continue to discover and delete data, or click the **View all the right to be forgotten requests** to navigate to the `Job Monitor` page to view deletion jobs in response to right to be forgotten requests.

Manually Delete Backup Data

IT administrators may need to remove the backup data of individual files, emails, or other documents or items to prevent any future restores.

About this task

In IBM® Storage Protect for Cloud Microsoft™ 365, you can navigate to **Data Management › Manually Delete Backup Data** to select and search for the content that you want to delete backup data for. After the removal, the index entries associated with these individual items are permanently deleted, ensuring that the data is destroyed and non-recoverable.

Note that the SharePoint Online search results will include all backup items matching your search conditions across SharePoint Online sites, Group sites, and Teams sites (including private/shared channel sites). Additionally, you can now delete content at both the folder and document level for Exchange Online, OneDrive, and SharePoint Online.

Note the following:

- If you want to avoid any accidental deletion of backup data, you can contact IBM Software Support to disable this feature. Note that the **Data Subject Access Requests** feature and the **Manually Delete Backup Data** feature will both be disabled.
- You can enable the approval process for data deletion in **Settings** > **Security** to avoid accidental data loss. With this feature enabled, data deletion requests and email notifications will be sent to the administrators when you delete data in **Manually delete backup data** and **Data subject access requests**. Then administrators can access the IBM® Storage Protect for Cloud Microsoft™ 365 interface and click **My Tasks** (✓) on the upper-right of the interface to approve your requests. The deletion jobs will start when the requests are approved. Note that the requests will be automatically invalidated if not approved within 7 days.

Procedure

Follow the steps below:

1. In the **Manually Delete Backup Data** page, click the **Exchange Online** tab, **SharePoint Online** tab, **Microsoft 365 Groups** tab, **OneDrive** tab, or the **Teams** tab for the backup data that you are looking for.

2. Enter and select the mailbox, site collection, group, or team where the object that you are looking for belongs or the document in the **Name** or **URL** field, and then configure other conditions.

   > **Note:** For Exchange Online, OneDrive, and SharePoint Online backup data, you can now delete content at both the folder-level and the document-level.

3. Click **Search**. The items that meet the search conditions and have backups are displayed in the table. The search results will display a maximum of 2000 items. You can click **Download list** above the table to download a list of items in the tables.

   > **Note:** For SharePoint Online backup data, the search results will include all backup items which meet the search conditions in SharePoint Online sites, Group sites and Teams sites.

4. You can configure the search conditions to narrow down the search results or search in the other objects of this type or for the items of the other levels.

5. To delete a file, item, or email, you can select the checkbox ahead of it and click the Delete button above the table, or you can directly click the **Delete** button on the right of the row. To delete multiple files, items, or emails, select the checkbox ahead of each of them and then click the Delete button above the table.

6. The **Delete Data** window appears asking for confirmation. Select the **I understand that the selected backup data will be permanently deleted.** option and then click **Delete**. A notification message will appear on the upper-right of the interface to show if the job has successfully started.

Remove Unprotected Data

IBM® Storage Protect for Cloud provides the feature to manage and remove backup data for objects that are no longer protected. This includes **Out-of-scope objects** and **Offboarded users**.

IBM® Storage Protect for Cloud will check unprotected objects once a week and update the reports. You can check for the **Last updated time** in the upper-right corner of this page. Your administrator group or the service provider's administrator group will receive the email notification ”**Legacy IBM® Storage Protect for Cloud Microsoft™ 365 identified and scheduled for removal**”, including to be deleted in seven days and new content added to the list of unprotected data. If some of your content marked for deletion has been moved back before being deleted, you will receive the email notification “**Data protection scope updated -content no longer marked for deletion**” as an update.

The **Deletions history** tab displays the deletion records of **Out-of-scope objects** and **Offboarded users** whose backup data has been removed including their **Unprotected date**, **Deletion date**, unprotected **Reason**, and the Deletion **Job ID**.

On each tab, you can also perform the following:

- Click the **Filters** button, and then select one service type from the drop-down list to filter the objects on the corresponding service type.

- Click **Download** (⤓) button to export all the data on this tab to your computer, or use the **Filters** first and click the **Download** (⤓) button to export the data of that object type.

Out-of-scope Users

If you have moved objects from a protected selection to an unprotected scope (this also means if content dynamically changes to an unprotected container), which indicates that you do not want this data protected, for the sake of your privacy, IBM® Storage Protect for Cloud will delete the corresponding backup data on the **Expiration date**. You can view the reasons for unprotected status in the **Reasons** column. To prevent certain backup data from deletion, you can update the backup scope on the home screen to include the out-of-scope objects.

Note the following:

- This feature does not apply to the BYOS subscription, Trial subscription, or the subscriptions with multi-Geo enabled, which indicates, your backup data already taken will not be deleted, and you can use the backup data of your currently unprotected objects for data recovery.
  If you are a BYOS customer and are looking to save storage space by removing unprotected data, contact the IBM Software Support to enable this feature for your environment.

- The backup data for the objects that have been protected by IBM® Storage Protect for Cloud but removed from your Microsoft 365 tenant is not within this scope. For the **Exchange Online** and **OneDrive**, the corresponding objects will be added to the **Offboarded users** tab. For details, refer to Offboarded Users. For other service types, IBM® Storage Protect for Cloud will keep such backup data according to your retention policy.
  If you have deleted an object from your Microsoft 365 tenant and removed this object or the service type from the backup scope, but you did not perform an Auto Discovery scan job to update the object registration, IBM® Storage Protect for Cloud may include the backup data of this object to the **Out-of-scope objects** tab. Your backup data will not be deleted since the IBM® Storage Protect for Cloud deletion job will check whether the object exists in your Microsoft 365 tenant before deleting the backups. You will receive email notifications of the result.

Offboarded Users

Offboarded users refers to users who have departed the organization, and their corresponding objects no longer exist in Microsoft 365.

With the **Settings** permission, you can click **Configure retention settings** on the tab to specify how long to keep the existing Exchange Online and OneDrive backup data from the date the user was marked as offboarded. IBM® Storage Protect for Cloud will delete the corresponding backup data on the **Expiration date**. Note that the configured retention period here will apply to all users within the specified scope. To edit retention period for a certain object, hover over an object and click the Edit (✎) icon.

To prevent certain backup data from deletion, you can adjust the retention period or disable the deletion function for offboarded users. If the retention settings for offboarded users is not enabled, the data will be deleted according to the global retention settings configured on the **Settings** > **Retention** page. Also, if a shorter retention period is configured in the global retention settings (**Settings** > **Retention**), that will take precedence.

Note that the feature does not apply to the Trial subscription or the subscriptions with multi-Geo enabled, which indicates, your backup data for offboarded users already taken will be deleted according to the global retention settings.

Example

IBM® Storage Protect for Cloud Microsoft™ 365 provides the following reports for IBM® Storage Protect for Cloud:

- The **Storage consumption report** displays the backup data size in storage, its growth, and trends to help administrators to monitor and manage the storage consumption. For details, refer to View Storage Consumption Report.
- The **Job analytics** report displays overview charts for all backup and restore jobs, and job progress details for long-running SharePoint Online and Exchange Online backup jobs. For details, refer to Use the Job Analytics Report.
- The **Unusual activities analysis report** warns you of the OneDrive accounts, SharePoint Online sites, Teams primary site, or the Microsoft 365 Groups team sites with unusual activities or that are under a potential ransomware attack. For details, refer to Use Microsoft 365 Unusual Activities Analysis Report.
- The **End-user restore report** shows the restore requests and details from IBM® Storage Protect for Cloud Recovery Portal. For details, refer to View the End-User Restore Report.
- The **Coverage report** displays what has been protected in IBM® Storage Protect for Cloud Microsoft™ 365 and the protected object details. For details, refer to View the Coverage Report.

IBM® Storage Protect for Cloud now integrates with IBM® Storage Protect for Cloud Microsoft™ 365 to provide reports in **Command centers**.

- The **Data Resiliency** command center provides reports on purchased workspaces, consumed storage capacity, and storage usage history.
- In the **Optimization & ROI** command center, the top dashboard provides the module protected percentage, the total data size protected and restored by IBM® Storage Protect for Cloud Microsoft™ 365, and the corresponding growth rate over the past 30 days.
- In the **Risk Posture** command center, the **Backup scope** dashboard displays the number of objects within the backup scope compared to the total objects detected over the past 12 months. The **Unusual activities analysis (ransomware events)** dashboard shows the number of objects under potential ransomware attacks and those with unusual activities in Microsoft 365 in the past 7 days.

View Storage Consumption Report

The **Storage consumption** report displays the backup data size in storage, its growth, and trends to help administrators to monitor and manage the storage consumption. This report is not available to default storage customers. If you are a BYOS storage customer and want to enable this report, contact the IBM Software Support.

The report is updated once a week and only available to the IBM® Storage Protect for Cloud Administrator and the Application Administrators of IBM® Storage Protect for Cloud Microsoft™ 365. For the Multi-Geo subscription, only the IBM® Storage Protect for Cloud Administrators can view this report.

> **Note:** This report does not support the trial subscription using BYOS, and the report does not include the index file size, which takes about 1% to 1.5% of your total data size.

You can choose whether to display the report with the retention data included by turning on or off the **Include Retention Data** option. If you deselect the **Include Retention Data** option, the report will not include the backup data size that has been deleted by retention jobs. However, the data deleted by other deletion jobs, such as deletion jobs for the Data Subject Access Requests feature and the Manually Delete Backup Data feature, will still be included.

> **Note:** If you have configured a retention period that is less than 1 year, the data deleted by the day unit retention jobs will always be included in the Storage Consumption Report.

In the **Dashboard › Storage Overview** section, you can view and download the storage consumption information of each service type in all your storages or only the legacy or current storage. Click **Download Report** on the upper-right corner of this section to download and save the storage overview data in the XLSX file.

The **Usage History** section at the bottom of this page displays the storage growth history in the line chart for the last 6 months. You can click the arrow (→) button to go to the **Usage** tab for more details.

Usage Tab

The **Usage** tab can show the storage growth history and trends for all object types or a specific object type, the average growth rate in the past 12 months, and the largest spike. You can also choose to display the usage report for all storages, or only the legacy or current storage, as well as whether to include retention data.

You can also click **Download Report** to download the report to your computer to drill down in Excel or other data analysis tools.

Use the Job Analytics Report

The Job analytics report contains three tabs: **Backup analytics**, **Extended backup overview**, and **Restore analytics**. The **Backup analytics** tab provides ovrview charts for all backup jobs performed in **Last 7 Days** or **Last 30 days**. The **Backup overview** tab can help you understand the job progress details of the SharePoint Online backups that are currently running slowly. The **Restore analytics**tab provides overview charts for all restore jobs performed in the last 7, 30, 90 or 180days.

> **Note:**
> Note that the **Job analytics › Backup overview** report now only supports SharePoint Online and Exchange Online backups.

View the Charts for Backup Jobs

The **Backup Alalytics** tab in the Job analytics report displays all backup jobs performed over the last 7 days or 30 days in the following charts: **Status count** chart and the **Object count** chart.

You can click the **Time filter** to switch the report data for the **Last 7 Days** or **Last 30 days** and use the **Object type** filter and **Status type** filter to display the jobs that you want to show in the chart.

Overview for Long-Running SharePoint Online/Exchange Online Backups

The **Backup Overview** tab in the Job Analytics report is provided to help you be aware of the backup progress for long-running SharePoint Online and Exchange Online backup jobs. The Backup Overview feature currently does not support viewing details for the long-running jobs of other backup services, although the Project Online service has applied the Split-Off and Pause feature for the long-running backups.

The long-running backup jobs of **SharePoint Online** and **Exchange Online** that have run for at least 24 hours will be displayed in the Job Analytics Report with the job progress details, such as the progress bar, sub-processes, the start time for backing up main content (such as, the site collections, lists and libraries, mailboxes, and folders), and the in-progress items.

The incremental backups running for 47 hours will be split off.

- Objects that are waiting to be backed up will be skipped and included in the next backup that starts as scheduled from the last good point to ensure a complete initial sync, as well as refresh the backup scope for objects that can potentially be updated.

- Running sites or mails can still run in the background. The backup jobs for sites in the background will be automatically stopped if the jobs have been running for more than 28 days. You can check the job report through Job Monitor, and the remaining content will be included in the next backup automatically as well.

View the Charts for Restore Jobs

The **Restore analytics** tab in the **Job analytics** report displays all restore jobs performed over the last 7, 30, 90 or 180 days in the following charts: **Restore count** chart and the **Restore trends** chart.

You can use the **Time filter** to view the number of restore jobs of each enabled service type for the **Last 7 Days**, **Last 30 Days**, **Last 90 Days** or **Last 180 days** and view the restore trend of each service by month.

Use the Unusual Activities Analysis Report

IBM® Storage Protect for Cloud Microsoft™ 365 will learn from your backup statistics and warn you for the **OneDrive accounts**,**SharePoint Online sites**, **Teams primary site**, or the **Microsoft 365 Groups team sites** with unusual activities or under a potential ransomware attack.

Unusual activities are designed to provide visibility into those patterns within your environment, distinct from regular usage patterns. The unusual activities could be related to malware that is related to ransomware or non-ransomware. But in most cases they be legitimate operations, for example, some users might kick of migration jobs , or run through a clean-up of their OneDrive on their work anniversary. It might be normal for a user to make changes that do not match their day-to-day patterns. While you should be aware that these changes are happening, you likely do not have to respond to every unusual activity report.

However, a Potential Ransomware Attack is much more serious and requires your immediate attention. It refers to the real suspicious files that were detected in a user's OneDrive or a SharePoint Online site that requires investigation.

To learn how you use your environment and build the pattern, the Unusual Activities Analysis Report needs OneDrive accounts to have at least 12 days of successful backups with incremental changes. Once any unusual activities or potential ransomware attack has been detected, your administrators will receive email notifications. To enable alerts for unusual activities and potential ransomware attacks, refer to "Configure Notifications" on page 68.

View the Report

You can navigate to the corresponding page to view the report for OneDrive, SharePoint Online, Teams, or Microsoft 365 Groups. To download a detailed list of files under potential ransomware attack or with unusual activity files, navigate to the **Details** tab of the service, select a OneDrive account/site, click a point in the chart, and then Download list in the **More comments** (••• ▾) list.

On each page, the **Dashboard** tab displays the number of OneDrive accounts or team sites protected by IBM® Storage Protect for Cloud Microsoft™ 365 and the number of suspicious OneDrive accounts/team sites. The main chart in the **Dashboard** tab shows the data tracked over the last 30 days for unusual activities and potential ransomware attacks.

You can click the number to view all the accounts/sites with suspicious activities or click the point on the chart to view the details of that specific date. The **Details** tab will show more information on the unusual activities and suspicious files for the reported accounts/sites. You can download the report in an Excel file.

You can also navigate to **Details** page directly to view the data in a table. You can adjust the time range to change the data scope or click a OneDrive account/site to view the report with its own details.

When you view the details of a specific OneDrive account/SharePoint Online site, you can also adjust the time range to change the data scope and click a point in the chart to view the details of that date. The details are displayed below the chart. You can generate and download a list of the files for record or for further investigation.

Recover OneDrive to a Healthy State

Procedure

To recover OneDrive or site to a safe state, you can choose the following ways:

- In the **Details** tab, select the OneDrive or site, and click **Restore** on the **Restore** pane, find a safe date and select the proper recovery point to restore.
  The **Recovery Point** calendar will display a yellow dot under the date where its recovery points are detected with unusual activities. For details on the common restore settings, refer to "Restore and Recover Your Data" on page 110.
- On the details pane of a OneDrive account or site, click a safe date and click the **Go to Restore Page** button. For details on the common restore settings, refer to "Restore and Recover Your Data" on page 110.

View the End-User Restore Report

The **End-user restore** report shows the restore requests and details from IBM® Storage Protect for Cloud Recovery Portal.

IBM® Storage Protect for Cloud Recovery Portal is designed to connect end users in your organization to their lost OneDrive, SharePoint Online site, and Exchange mailbox, Groups, Teams data, Team Chat, Power BI reports, or Power Automate flows. This interface allows users to search the most common fields to find the backup data to recover along with a preview of the email messages which can also help ensure a successful restore with minimal effort. For details, refer to IBM Storage Protect for Cloud Recovery Portal.

IBM® Storage Protect for Cloud Microsoft™ 365 provides this report as an admin portal for monitoring IBM® Storage Protect for Cloud Recovery Portal's activities throughout your tenant, including reports for:

- How many users have put requests in for lost content
- How many recovery requests have IBM® Storage Protect for Cloud Recovery Portal received or successfully processed
- How many users have authorized IBM® Storage Protect for Cloud Recovery Portalto work in their context

You can perform the following in the report:

- Use the time range filter to view the report of **Last 7 days** or **Last 30 days**.
- Use the **Object type** filter to view separate reports for **ShaePoint Online**, **OneDrive**, **Exchange Online**, **Microsoft 365 Groups**,**Teams**, **Teams Chat**, **Power Automate**, and **Power BI**, including the number of total requests and the number of the restore jobs of the corresponding status.
- To view details for all the restore requests, you can click the **Download report** button on the pane to download the report data to your computer.
- View the trends for authorized users in the current month in the **Authorized User Trends** section.

View the Coverage Report

The **Coverage report** provides a **Dashboard** to show what has been protected in IBM® Storage Protect for Cloud Microsoft™ 365 according to service types, the protected data size of each service, and backup trends. The **Dashboard** consists of four charts: **Backup coverage**, **Protected objects**, **Protected data size**, and **Protected data size trend**. You can click the **Download PDF report** button to download the **Coverage report** as a single PDF.

The **Backup coverage** chart displays how many days each service has been protected for and how many recovery points each service has according to service types in **Last 7 days** or **Last 30 days**. The chart is updated once the backup job is completed. You can click the number of protected days and recovery points to view backup jobs in **Job monitor**. You can also use the **Download report** option to download a report for the backup jobs in the last 30 days.

The **Protected objects** chart has two parts. The display on the left shows the ratio of objects currently backed up, to the total objects detected in your tenant. The right part shows two trends in the past 12 months: the number of objects in backup scope and the number of objects in your tenant. Note that this chart is updated daily.

The **Protected data size** chart displays the total protected data size, the protected data size of each service and its ratio to the total protected data size, and objects with their container and protected data size. The objects are ranked according to their protected data size and only the top 100 objects can be displayed here. The chart is updated once a week and you can click **Download report** to download a report for all protected objects in your tenant.

In the **Protected data size trend** chart, you can click the **Object type** to show the overall protected data size trend or the trend of objects protected by each service. The chart is updated once a week and you can also click **Download report** to download a report for all services.

Details

The **Details** page displays the **Last backup status**, **Last backup time** , and **First backup time** of each object protected by IBM® Storage Protect for Cloud Microsoft™ 365 according to the **Object type**. You can click **Generate report** to generate a **Simple report** or **Detailed report** for protected object details of the object types you selected. A **Simple report** only includes details of top-level objects and a **Detailed report** includes details of top-level objects and the items with errors or skipped items.

For detailed information about specific objects in the last backup job, click the object name under the **Object** column. The **Object details in the last backup job** page displays. In the **Overview** tab, the **General information** section shows last backup job information, including the backup time, job ID, job status, data size/number per hour, backup data size, and the overall backup status and number of items protected under the top-level object in the last backup job. The **Item number analytics** section help you get into details on the backup status and number of items of each level protected in the last backup job.

In the **Error details** tab, you can filter the items with errors and skipped items and get more details. You can also click **Download report** to download a report for details of all items with errors or skipped items under the top-level object in the last backup job.

Job Monitor

The **Job monitor** page displays the essential information of jobs in IBM® Storage Protect for Cloud Microsoft™ 365. For IBM® Storage Protect for Cloud, you can click the **Filters** button to filter jobs by **Object type**, **Job type**, **Status**, and **Data range**, or click the **Column** button to choose which columns can be displayed in the table. You can also use the **Search** box to search for the backup, restore, and export jobs.

About this task

To export job records, click the **Export** button and select the time range for the records you would like to export. The maximum limit of the time range is 1 year.

To view the summary information of a job, click the job ID. The **Job details** page displays the job information of the selected job, including the Job ID, job status, service type, job run by, start time, etc. The **Object details** table on this page provides the source and destination information of each object, as well as their status in the job. For the restore jobs in progress, the **Job details** page displays the successful objects, objects with errors, and remaining objects during the restore.

You can use the **Generate report** option on the **Job details** page to generate and download reports, or you can use the **Generate report** option in the More commands (•••) list for each completed backup, restore, or export job to view the job summary, and the object details in the job.

Procedure

To generate and download a job report, follow the steps below:

1. On the **Job monitor** page, you can click the **Filters** button to filter the user activities.

   - In the **Object type** filter, select **All**, **Exchange Online**, **OneDrive**, **SharePoint Online**, **Microsoft 365 Groups**, **Teams**, **Teams Chat**, **Project Online**, **Public Folders**, **Viva Engage**, **Power BI**, **Power Automate,** or **Power Apps** to search the jobs performed on the corresponding object type.
   - In the **Job type** filter, select **All**, **Backup**, **Restore**, **Export**, **Delete**, or **Retention** to filter the corresponding jobs.
   - In the **Status** filter, select **In progress**, **Finished**, **Finished with exception**, **Failed**, **Stopped**, or **Partially finished** to search the jobs of specified status.
   - In the **Data range** filter, and then select **All**, **Today**, **Last 7 days**, **Last 30 days, Last 90 days** or **Last 180 days**, or configure a custom date range to filter the activities whose start time matches the filter;

   Additionally, you can use the **Search** box to search the activities by username, Job ID, or description (for restore jobs).

2. Click the **Generate report** option from the More commands list.
3. After the report is generated, the **Download report** option will appear. Click the **Download report** link to download the report. If the option does not show up, you can click the **Refresh** (↻) button next to the search box to refresh the data in the Job monitor.
   Two reports are provided in the downloaded zip file: An Excel including the summary of the job, and a CSV file including the **Successful** top-level objects (Exchange Online mailbox, OneDrive, SharePoint Online site collection, Microsoft 365 Group mailbox, and team site, Teams group mailbox and group team site, Project Online site collection, and Exchange Online public folder), items with **Errors** or **Skipped** items.

View Subscription Notifications

You can view notifications of your licenses in the **Notifications** menu by clicking the bell (🔔) button.

About this task

IBM® Storage Protect for Cloud Microsoft™ 365 provides the following Enterprise subscription models:

- **Unlimited Users** – This subscription model requires a license that covers all protected Microsoft 365 capacities. The number of **Purchased** and **Protected** capacities will be displayed on the **Notifications** pane. If the number of the **Protected** capacity is greater than the number of the **Purchased** capacity, your backup service is out of policy.
- **Unlimited Organizations** – This subscription model requires user seats for all assigned Microsoft 365 licenses. The number of **Purchased** and **Assigned** user seats will be displayed on the **Notifications** pane. If the number of **Assigned** user seats is greater than the number of **Purchased** user seats, your backup service is out of policy.

If your backup service is out of policy for 30 days, the **Notifications** pane will appear to inform you. You can click **Dismiss** on the upper-right corner of the **Notifications** pane to close the pane.

Audit User Activities in System Auditor

Navigate to **System Auditor** page to view the user activities in IBM® Storage Protect for Cloud Microsoft™ 365, divided into the following categories: **Time**, **User**, **IP address**, **Operation component**, and **Event**. You can click the time of some user activities to view change details.

Procedure

You can perform the following actions on the records of user activities:

- Use the **Data range**, **Operation Component** filter, and **Object Type** filter to filter the records.
- Use the **Search** box to search for the activities by username.

> **Note:** Searching only supports entering the full username.

- Export the System auditor records. Follow the steps below:
  a. Click the **Export** button. The **Export audit report** window appears.
  b. You can select the time range for the records you would like to export. The maximum limit of the range is 1 year.
  c. Click **Export**. The audit report will be exported to your browser’s download location. Click **Cancel** to cancel the export.

Monitor Subscription Consumption

The subscription consumption report contains two tabs: **Microsoft 365 services** and **Power Platform**. It displays your subscription details and consumption of Microsoft 365 services and Power Platform.

Microsoft 365 Services

The **Microsoft 365 services** tab provides a dashboard that displays your subscription details, usage growth rate, trends, and utilizations. This helps you monitor how your Microsoft 365 subscription is being consumed and anticipate when it may reach its quota.

> **Note:** The subscription consumption report in **Subscriptions** is updated once a week and is only available to the IBM® Storage Protect for Cloud Administrator and the Application Administrators of IBM® Storage Protect for Cloud Microsoft™ 365. For subscriptions with multi-Geo enabled, only IBM® Storage Protect for Cloud Administrators can view this report.

IBM® Storage Protect for Cloud provides one subscription model for Microsoft 365 services:

Per-User Subscription

In the **Subscription utilization** section, you can view a snapshot of the number of consumed seats versus the total purchased seats, and the number of seats currently available or exceeded. You can also view the major consumers by Microsoft 365 subscription type, the largest consumer on your subscription, and the usage history respectively in **Top subscription consumers** section, **Largest consumer** section, and **Usage history** section.

- To view additional usage statistics, such as usage history and trends, average growth rate, and spike, click on the upper right corner of the **Usage history** pane or click the **Usage** tab.
- To view the overall subscription utilization of each subscription type, click button on the upper-right corner of the **Largest consumer** pane or click the **Utilization** tab.

Usage Tab

The **Usage** tab shows the average growth rate in the past 12 months and the largest spike. Also, a usage projection will be displayed in **Usage history and trends** for when your subscription capacity will be reached.

You can click **Download report** to download the usage statistics to your computer and view the size of the protected data on a corresponding date or the number of the assigned user seats for each service type.

Utilization Tab

To view the detailed subscription consumption, click the **Utilization** tab. The subscription consumption of each object type will be listed in descending order.

You can click **Download report** to download the subscription utilization data, including the overall subscription utilization information.

Power Platform

The **Power Platform** tab provides your subscription details and utilization, helping you understand how your subscription to Power Platform is consumed.

IBM® Storage Protect for Cloud Microsoft™ 365 provides two primary choices for the subscription to Power Platform:

- Protection for unlimited users for a set per-object subscription (count the Power Platform object number in the backup scope)

- Protection for an unlimited amount of content in an organization for a set per-user subscription (count the Microsoft 365 assigned user seats. For details, refer to Subscription and Licensing Information.

You can get a glance at the subscription type, the capacity of your purchased subscription, and the number or percentage of the consumed subscription in the **Subscription utilization** section, and view the major consumers on your subscription by Microsoft 365 subscription type.

If you want to increase your subscription capacity, you can reach out to your IBM sales representative.

Submit Feedback

IBM® provides a platform to collect feedback where you can provide suggestions for product features from your IBM® Storage Protect for Cloud Microsoft™ 365 experience.

Procedure

Refer to the instructions below to submit your feedback:

1. Click the Submit Feedback button on the top bar. The **Submit Feedback** pane appears.
2. Configure the following settings:

   Rate your experience

   Click the stars to evaluate your IBM® Storage Protect for Cloud Microsoft™ 365 experience.

   Module Name

   Select IBM® Storage Protect for Cloud Microsoft™ 365 from the **Module Name** drop-down list.

   Feedback Type

   Select **Bug Report**, **Interface Improvement**, **Feature Suggestion**, or **Subscription Cancellation** from the list.

   Your suggestion

   Enter your suggestions about IBM® Storage Protect for Cloud Microsoft™ 365 features.
3. Click **Submit** to submit your feedback to IBM® , or click **Cancel** to leave this pane without submitting feedback.

Introduction to Data Export Service

The Data Export Service is provided to IBM® Storage Protect for Cloud Microsoft™ 365 customers in the following instances:

- Customers who want to archive their legacy backup data as the data comes to the end of the retention period.
- Customers who plan to end their subscription of IBM® Storage Protect for Cloud Microsoft™ 365 and remove their backup data.

Note that if you only want to export a smaller sample set of data to plain file format, use the **Export** button in the restore wizard. For details, refer to "Export and Download Your Data" on page 98.

- For customers using IBM® Storage Protect for Cloud-provided default storage
  IBM® will retain the backup data in IBM® Storage Protect for Cloud storage for 60 days, subject to the terms of your service agreement, if the subscription to IBM® Storage Protect for Cloud Microsoft™ 365 ends. The backup data in IBM® Storage Protect for Cloud storage can be exported to your own storage as a paid service. You must submit an export request if you wish to export data from IBM® Storage Protect for Cloud storage.
- For BYOS customers
  If your license is the BYOS type, ending the subscription will not delete the backup data stored in your own storage. You do not need to pay an export fee.

Additionally, you must export the encryption key before your move away from this product, as you will need the encryption key to convert the encrypted backup data to readable content, and you will not be able to sign in to the IBM® Storage Protect for Cloud Microsoft™ 365 interface once your subscription has ended. For details on exporting encryption keys, refer to "Configure Security Settings" on page 94.

After the backup data is ready in your own device, contact IBM Software Support for additional details on how to convert this data to a readable format.

Job Report Troubleshooting

The following tables provide some key job report comments and their causes and solutions to help you troubleshoot certain issues you may encounter during backup and restore jobs. Error codes are included in job reports to help you troubleshoot issues. Clicking the error code link in the downloaded job report will open the "Troubleshooting" on page 172 guide.

Errors that occur in an IBM® Storage Protect for Cloud Microsoft™ 365 job may cause some items to fail and not be backed up. According to the job report details listed below, some of the items with errors will be marked with a **Warning** status.

The **Warning** backup status will not affect the backup job status, which means you may find backup jobs whose status is **Completed** but contain items with a **Warning** status. The next backup job will automatically include these items, but if the backup for these items continues to encounter errors during the next three backup jobs, the backup status for these items will be marked as **Error**, which may result in the backup job status being changed to **Completed with Exceptions** or **Failed**.

The warning backup status definition is automatically enabled for all customers. If you want to disable this feature to display the following **Warning** items with the **Error** status, contact IBM Software Support for help.

SharePoint Online and Microsoft 365 Group Team Site

Job Report Comment	Status	Causes and Solutions
The remote server returned an error: (403) Forbidden	Warning	Connection authentication is failed. Check the authentication settings and test if it works in a public network environment.
The remote server returned an error: (401) Unauthorized	Warning	
There was no endpoint listening at http://usr17050-420:32843/7b1863ba5d594c95bfc16928967478d3/MetadataWebService.svc that could accept the message. This is often caused by an incorrect address or SOAP action.	Warning	The connection with SharePoint Online Server is unstable. The objects with errors will be automatically included in the next backup job. If this error persists, contact IBM Software Support for help.
The request channel timed out while waiting for a reply after 00:00:30. Increase the timeout value passed to the call to Request or increase the SendTimeout value on the Binding. The time allotted to this operation may have been a portion of a longer timeout.	Warning	The connection with SharePoint Online Server is unstable. For backup, the objects with errors will be automatically included in the next backup job. If this error persists, contact IBM Software Supportfor help.
An existing connection was forcibly closed by the remote host.	Warning	The connection with SharePoint Online Server is unstable. The objects with errors will be automatically included in the next backup job. If this error persists, contact IBM Software Support for help.

Job Report Comment	Status	Causes and Solutions
The underlying connection was closed: The connection was closed unexpectedly.	Warning	The connection with SharePoint Online Server is unstable. The objects with errors will be automatically included in the next backup job. If this error persists, contact IBM Software Support for help.
The HTTP service located at http://usr19962-543:32843/c7d0fe6dfad1485a857d02abf4155815/MetadataWebService.svc is unavailable. This could be because the service is too busy or because no endpoint was found listening at the specified address. Please ensure that the address is correct and try accessing the service again later.	Warning	The connection with SharePoint Online Server is unstable. The objects with errors will be automatically included in the next backup job. If this error persists, contact IBM Software Support for help..
The operation has timed out.	Warning	The connection with SharePoint Online Server is unstable. The objects with errors will be automatically included in the next backup job. If this error persists, contact IBM Software Support for help.
Exception from HRESULT: 0x8107054A	Warning	Throttling issue: Too many requests. To avoid the throttling issue, you can use the account pool to distribute the requests
Exception from HRESULT: 0x80131904	Warning	Throttling issue: Too many requests. To avoid the throttling issue, you can use the account pool to distribute the requests.
The remote server returned an error: (429)	Warning	Throttling issue: Too many requests. To avoid the throttling issue, you can use the account pool to distribute the requests.
The site collection [SiteURL] is not available.	Skipped	Check if the object exists in Microsoft 365. If it exists, contact IBM Software Support for help.
Cannot get object metadata. It may have been deleted.	Skipped	Check if the object exists in Microsoft 365. If it exists, contact IBM Software Support for help.
File not found.	Skipped	Check if the object exists in Microsoft 365. If it exists, contact IBM Software Support for help.
Item does not exist. It may have been deleted by another user.	Skipped	Check if the object exists in Microsoft 365. If it exists, contact IBM Software Support for help.
File does not exist.	Skipped	Check if the object exists in Microsoft 365. If it exists, contact IBM Software Support for help.
The changeToken refers to a time before the start of the current change log.	N/A	The changeToken of an incremental backup has expired. The backup job will perform a full backup for this object automatically.

Job Report Comment	Status	Causes and Solutions
An error occurred while performing the backup. Error: Failed to access the destination site collection. The username or password is incorrect. Site Collection URL: {0}.	Error	{0} displays the URL of the site collection. You must update the service account credentials in IBM® Storage Protect for Cloud and rerun the Auto Discovery scan job.
Access denied. You do not have permission to perform this action or access this resource.	Error	Add the service account you configured or the group used in the account pool to the Site Administrators group.
An error occurred while performing the backup. Error: The request was aborted. Cannot create SSL/TLS secure channel.	Error	Custom ADFS Authentication failed. Check the ADFS authentication settings and test if it works in a public network environment.
List does not exist. The page you selected contains a list that does not exist. It may have been deleted by another user.	Error	Check if the object exists in Microsoft 365. If it exists, contact IBM Software Support for help.
The specified program requires a newer version of Windows. (Exception from HRESULT: 0x8007047E)	Error	The connection with SharePoint Online Server is unstable. If this error persists, contact IBM Software Support for help.
Cannot contact web site '[SiteUrl]' or the web site does not support SharePoint Online credentials.	Error	This error occurs if you have disabled the ability for non-modern (legacy) authentication protocols within your SharePoint Online tenant.
Cannot contact site at the specified URL [SiteURL]. Access to this Web site has been blocked.	Error	The site collection has been blocked. Contact your SharePoint administrator for help.
The remote server returned an error: (400) Bad Request.	Error	Invalid request. Contact IBM Software Support for help.
The attempted operation is prohibited because it exceeds the list view threshold enforced by the administrator.	Error	The number of requests has exceeded the list view threshold limit. Contact IBM Software Support for help.
Cannot complete this action. Please try again.	Error	Invalid SharePoint Online data may exist in your environment. Contact IBM Software Support for help.
Invalid file name.	Error	Invalid SharePoint Online data may exist in your environment. Contact IBM Software Support for help.
Stream was not readable.	Error	An unknown error occurred. Contact IBM Software Support for help.
Microsoft.SharePoint.Client.ServerException: Exception of type ‘System.ArgumentException’ was thrown. Parameter name: value.	Error	Unexpected exception of the Client API. Contact IBM Software Support for help.

Job Report Comment	Status	Causes and Solutions
Microsoft.SharePoint.Client.Server ObjectNullReferenceException: Object reference not set to an instance of an object on server. The object is associated with property CurrentUser.	Error	Unexpected exception of the Client API. Contact IBM Software Support for help.
The request uses too many resources.	Error	Resource limitation of client API. Contact IBM Software Support for help.
Save conflict.	Error	Contact IBM Software Support team to ask about using a single thread to restore.
An error occurred while restoring the item. Item Name: {0}. Error: An error occurred when restoring the document, load file failed: The file "{1}" is pulled for editing by {2}.	Error	Contact IBM Software Support team to ask about using a single thread to restore.

Exchange Online, Teams, and Microsoft™ 365 Group Mailbox

Job Report Comment	Status	Causes and Solutions
This group may have been removed.	Skipped	Check if this group has been removed from Microsoft™ 365. If so, you can rerun the scan job so that this group will be removed from the container. You may also contact IBM Software Support for help.
Cannot find the mailbox for this email address. The mailbox may have been deleted, or this account may not have a mailbox associated. Please check if the Auto Discovery profile has been enabled to remove the objects that were deleted in Microsoft™ 365.	Skipped	Check if this mailbox has been deleted from Microsoft™ 365. If so, you can rerun the scan job so that this mailbox will be removed from the container. You may also contact IBM Software Support for help.
No changes have been detected since the last backup.	Skipped	The backup job is skipped since no emails were sent or received since the last backup.
Microsoft™ Graph API leveraged by our product only allows a Group/Team to have up to 200 plans. Therefore, the new plans cannot be created during the restore if the number of plans in the destination Group/Team has reached 200.	Error	In a Microsoft™ 365 Group or Team, you can have a maximum of 200 plans.

Job Report Comment	Status	Causes and Solutions
This Group ID does not exist in your Microsoft™ 365 tenant. This Group may have been deleted from Microsoft™ 365 and restored from backup data. Since a new Group is created during the restore, the Group ID has changed and needs to be re-scanned by IBM® Storage Protect for Cloud to update the registration information.	Error	If you restored this group after it has been deleted from Microsoft™ 365, this restore job would create a new Group. The Group ID is different. You must rescan the objects in IBM® Storage Protect for Cloud to update the group ID in its registration information.
The account used to scan and register this Microsoft™ 365 Group must have an Exchange Online product license assigned.	Error	Microsoft™ API requires an Exchange Online license in Microsoft™ 365. Assign an Exchange Online license to the Microsoft™ 365 account that has been used for Auto Discovery.
{0} does not have any owners or members. IBM® Storage Protect for Cloud does not protect the groups or teams with no owners or members. Add a user to this group/team if you want to protect it.	Error	{0} displays the name of the private group or team. IBM® Storage Protect for Cloud Microsoft™ 365 must use an existing user to access the private group or team. Therefore, to protect this group or team, add an owner or member into this private group or team.
This Microsoft™ 365 Group has been deleted from Microsoft™ 365. You can either select the entire group to run the restore, or manually create the group in Microsoft™ 365 and then run the restore again to restore the selected content.	Error	This job report comment will appear if the Microsoft™ 365 Group has been deleted and you selected the objects within this Microsoft™ 365 Group rather than the group itself to restore.
A mailbox using the same name as the group "{0}" already exists in the destination.	Error	The email address of this Microsoft™ 365 Group has been used by another user, security group, or distribution list. You can create a new Microsoft™ 365 Group with a different name as the destination of an out-of-place restore, or you can select another Microsoft™ 365 Group as the destination.
Not all items in this folder are backed up successfully. Error: {0}	Error	Failed to synchronize all items in this folder. This may be due to an unstable network or busy Exchange Server.
You have exceeded the available concurrent connections for your account. Try again once your other requests have completed.	Error	Exchange Online Server is busy, or the network is unstable. The next backup job will automatically include objects with errors. If these objects still fail to be backed up, contact IBM Software Support.
The server cannot service this request right now. Try again later.	Error	

Job Report Comment	Status	Causes and Solutions
Too many concurrent connections opened. Cannot open mailbox.	Error	

Common

Job Report Comment	Status	Causes and Solutions
Cannot find the service account "{0}" in IBM® Storage Protect for Cloud. To synchronize new service accounts, either run a one-time scan job in Auto Discovery or wait a scheduled scan job to complete.	Error	You may get this message when a synchronization issue occurred. Run the scan job in Auto Discovery to fix the synchronization issue and then run the backup job again.
The service account "{0}" or account pool user used for running job does not have Project Online license in Microsoft™ 365.	Error	Assign the Project Online license to the user who is used to back up the Project Online site collections in Microsoft™ 365.
The specified mailbox may be expired.	Error	Check if the specific mailbox has a license.
Cannot find the mailbox for this email address. The mailbox may have been deleted, or this account may not have a mailbox associated. Please check if the Auto Discovery profile has been enabled to remove the objects that were deleted in Microsoft™ 365.	Error	Check if the specific mailbox still exists in Microsoft™ 365 or if the user has a mailbox associated.
The mailbox is temporarily unavailable. The mailbox database may be offline, corrupt, shutting down, or exhibiting other conditions.	Error	You can try to access the mailbox first. If the mailbox cannot be accessed, contact Microsoft™ Support; if the mailbox can be accessed, wait for the next backup job to automatically include this mailbox for backup.
Cannot back up the specified data from Exchange Online server. The server is busy now.	Error	This may be due to a throttling issue. You can wait for the next backup job to back up this mailbox.
Cannot connect to the Exchange Online server. The network connection is not stable, or the credentials used to scan the mailboxes are incorrect.	Error	Check the network connection and the credentials of the user who is used to scan the mailbox.
The Microsoft™ 365 user credentials specified for scanning mailboxes cannot be used to connect the Exchange Online server. The user may not have a mailbox.	Error	Check if the user who is used to scan the mailboxes has a mailbox associated.
Cannot connect to the mailbox. The Microsoft™ 365 account does not have permission to access the mailbox.	Error	Check if the user who is used to scan the mailbox has permission or not.
Cannot connect to the device due to network issues.	Error	Check your device and the storage configurations, especially when your device is FTP/SFTP

Job Report Comment	Status	Causes and Solutions
There is no data in the backup scope to protect. You can go to the Auto Discovery interface in the IBM® Storage Protect for Cloud portal to review your rules and include additional objects.	Error	
Cannot find the service account for the destination node. Please configure a service account in IBM® Storage Protect for Cloud and then try again.	Error	The service account may have been deleted from IBM® Storage Protect for Cloud. Go to the IBM® Storage Protect for Cloud interface to configure the service account and run the Auto Discovery job to scan the object into the system.
Cannot find the service account for the source node. Please configure a service account in IBM® Storage Protect for Cloud, and then try again.	Error	The service account may have been deleted from IBM® Storage Protect for Cloud. Navigate to the IBM® Storage Protect for Cloud interface to configure the service account and run the Auto Discovery job to scan the object into the system.
Cannot find a service account or an app profile for this mailbox. Please go to IBM® Storage Protect for Cloud to configure an account or profile with access to this mailbox.	Error	Navigate to the IBM® Storage Protect for Cloud interface to configure a service account or an app profile with the account that has access to the mailbox.
There is no available service account, app profile, or account pool for this Microsoft™ 365 tenant in IBM® Storage Protect for Cloud. Please configure a service account or an app profile with required permissions in IBM® Storage Protect for Cloud, and then try again.	Error	Navigate to the IBM® Storage Protect for Cloud interface to configure a service account or an app profile with required permissions to this tenant, and then retry the backup.
The device currently being used has no free space.	Error	You can expand your device storage space or adjust the retention time for the data in your storage.
The custom storage location is not available. Check your storage configurations and status.	Error	The custom device's credentials may be incorrect, or you changed the device location.

Use Public APIs

> **Note:** We are upgrading to a new API for better user experience, stability, and easier integration. Visit our documentation page for more details.

IBM® Storage Protect for Cloud Microsoft™ 365 provides the `/cloudbackup/jobs` and `/cloudbackup/licenseconsumption` API endpoints. These interfaces empower users to seamlessly retrieve job-related information and monitor subscription consumption through standardized HTTP GET requests. By leveraging these APIs, users gain comprehensive insights and granular access to job reports and subscription consumption metrics, thereby enhancing the ability to manage, analyze, and optimize backup operations with precision and efficiency.

> **Note:** We are upgrading to a new API for better user experience, stability, and easier integration. Visit our documentation page for more details.

Permission

Example

> **Note:** We are upgrading to a new API for better user experience, stability, and easier integration. Visit our documentation page for more details.

Example

The following permissions are required to call this API.

> **Note:** You must register an app through IBM® Storage Protect for Cloud > App registration to authenticate and authorize your access to IBM Graph API. For details, refer to Configure App Registrations.

API Method

> **Note:** We are upgrading to a new API for better user experience, stability, and easier integration. Visit our documentation page for more details.

Method	Path	Description
GET	/cloudbackup/jobs	Gets the job information of IBM® Storage Protect for Cloud Microsoft™ 365.
GET	/cloudbackup/licenseconsumption	Gets the subscription consumption information of IBM® Storage Protect for Cloud Microsoft™ 365.

Path Details

We are upgrading to a new API for better user experience, stability, and easier integration. Visit our documentation page for more details.

[GET]/cloudbackup/jobs

Gets the job information of IBM® Storage Protect for Cloud Microsoft™ 365.

Query Parameters

Parameter	Description	Type
StartTime	Sets a start time (UTC time) for the time range.	long
FinishTime	Sets an end time (UTC time) for the time range.	long
JobType	Sets the job types that you want to get. Defined by #/components/schemas/BackupJobType.	Enum **Valid values:** 0 (for All) 1 (for Backup) 2 (for Restore) 3 (for Export) 4 (for Delete) 5 (for Retention)
ObjectType	Sets the service type of the jobs to get. Defined by #/components/schemas/CloudBackupJobObjectType.	Enum **Valid values:** 0 (for All) 1 (for Exchange Online) 2 (for SharePoint Online) 3 (for OneDrive) 4 (for Microsoft 365 Groups) 5 (for Project Online) 6 (for Public Folder) 7 (Teams) 8 (Viva Engage) 9 (Teams Chat) 10 (Power BI) 11 (Power Automate) 12 (Power Apps)

Parameter	Description	Type
JobState	Sets the job status. Defined by #/components/ schemas/CloudBackupJobState	Enum **Valid values:** 0 (for All) 1 (for In Progress) 2 (for Finished) 3 (for Failed) 4 (for Finished with Exception) 5 (for Partially Finished)
PageIndex	Sets the starting number of the page to get the jobs. The default value is 0.	
PageSize	Sets the number of jobs to display on one page. The default value is 10.	

Responses

If the request has been successfully processed, a 200 OK response will be returned, along with the requested information displayed in the response body.

Retrieved result:

Response	Description	Type
TotalCount	The total count of the retrieved jobs	int
Jobs	A list of jobs	list
NextLink	Reference to the next page of results	string

Job summary:

Response	Description	Type
Id	Job ID	string
State	Job status	string
StartTime	Job started time	long
FinishTime	Job finished time	long
Duration	Duration	long
BackupDetails	Job details	int

Backup details:

Response	Description	Type
TotalCount	Total count	long
FailedCount	Number of failed objects	long
SuccessfulCount	Number of successful objects	long
SkippedCount	Number of skipped objects	long

Job errors:

IsErrorCode	Whether this error has an error code associated	boolean
Value	Error message	string
Url	Error code URL	string

Number	Occurrences of the error in this job	long

Example (application/json):

```
Request
{
StartTime?: long
FinishTime?: long.
JobType?: #/components/schemas/BackupJobType
ObjectType?: #/components/schemas/CloudBackupJobObjectType
JobState?: #/components/schemas/CloudBackupJobState
PageIndex?: int
PageSize?: int
}
Response
{
TotalCount?: int
Jobs:[
{
Id?: string
State?: string
StartTime?: long
FinishTime?: long
Duration?: long
BackupDetails?:
{
TotalCount?: long
FailedCount?: long
SuccessfulCount?: long
SkippedCount?: long
}

JobErrors: [
{
IsErrorCode: boolean,
Value: string
Url: string
Number: long
}
]
}
]
}
```

[GET]/cloudbackup/licenseconsumption

Gets the subscription consumption information of IBM® Storage Protect for Cloud Microsoft™ 365.

Responses

If the request has been successfully processed, a 200 OK response will be returned along with the requested information displayed in the response body.

Response	Description	Type
OutOfPolicyTime	The UTC that the license got out of policy.	long
PurchasedUserSeats	Purchased user seats	int
AssignedUserSeats	Assigned user seats	int
PurchasedStorageSize	Purchased storage size	int
ProtectedSize	Protected size	int

Example (application/json)

```
Response
{
OutOfPolicyTime?: long
PurchasedUserSeats?: int
AssignedUserSeats?: int
PurchasedStorageSize?: int
ProtectedSize?: int
}
```

Troubleshooting

This troubleshooting guide is designed to help you address unexpected issues and errors that you may encounter when usingIBM® Storage Protect for Cloud Microsoft™ 365. If you wish to ignore certain errors and prevent them from affecting the job status, go to the IBM® Storage Protect for Cloud Microsoft™ 365 interface and navigate to **Settings** > **Backup**support to skip specific errors by error codes.

CO-MailboxFolderDeadLoop

Issue:

Some mailbox folders encountered errors during backup with the following error code:

- **CO-MailboxFolderDeadLoop**

Details:

The mailbox folders encountered Microsoft Dead Loop issues in the backup. This is a known issue of Microsoft and we will follow up on it for resolution.

Solution:

Generally, the mailbox folders have been backed up successfully. You can check the backup data in the IBM® Storage Protect for Cloud Microsoft™ 365 interface.

If you want to ignore the exception and avoid the impact on the job status, you can contact IBM support to skip the error.

CO-NotFound

Issue:

The object encountered an error during backup with the following error code:

- **CO-NotFound**

Details:

The object to back up may have been deleted. Deleted or corrupted objects cannot be retrieved.

Solution:

Please check if the object exists, and whether it can be displayed or used properly. Then, you can wait for the subsequent backup job and monitor the status. If the error persists, contact IBM Software Support.

CO-SourceDataDamage

Issue:

An item encountered an error during backup with the following error code:

- **CO-SourceDataDamage**

Details:

The source item may be damaged.

Solution:

Please try to download the item directly using your web browser. If successful, wait for the subsequent backup jobs to handle it. If not, reach out to the Microsoft Support team for help.

If you want to ignore the exception and avoid the impact on the job status, go to the IBM® Storage Protect for Cloud Microsoft™ 365 interface and navigate to **Settings** > **Backup** to skip the error by error code.

CO-Throttling

Issue:

Some items encountered an error during backup with the following error code:

- **CO-Throttling**

Details:

This is the error code for 429 throttling issues.

Solution:

Due to the throttling control by Microsoft during weekday daytime hours, we recommend that you schedule backups outside business hours and consider reducing the frequency of backups as necessary during the workweek.

We also recommend you configure an app profile for your tenant when you are using the service account authentication for Auto Discovery. Therefore, IBM® Storage Protect for Cloud Microsoft™ 365 backup services will switch to the Hybrid Approach for data protection. If you are OK with the data support status in app context (See the Default/Custom App Profile column for the support status of each service type), we strongly recommend that you use app profile authentication for both Auto Discovery and data protection.

If you need additional assistance, contact IBM Software Support.

EXO-ErrorMailboxConfiguration

Issue:

A mailbox encountered an error during backup with the following error code:

- **EXO-ErrorMailboxConfiguration**

Details:

The mailbox information within Microsoft Entra Domain Services has been improperly configured.

Solution:

Check for whether the user exists, and review and correct the mailbox settings.

For more details on the error code **ErrorMailboxConfiguration** in Microsoft, refer to the link.

Group-AccessDenied

Issue:

A group encountered an error during backup with the following error code:

- **Group-AccessDenied**

Details:

The group owner/member which IBM® Storage Protect for Cloud Microsoft™ 365 used to access the group through impersonation cannot access the group.

Solution:

Verify whether the user is still available. If this error persists, remove the user from the group and add them back to resolve the problem.

Refer to the link to add or remove group members.

Teams-NoAvailableOwnerOrMember

Issue:

A file encountered an error during backup with the following error code:

- **Teams-NoAvailableOwnerOrMember**

Details:

The team does not have any owners or members, or no owners or members in the team have the Exchange Online license.

Solution:

If you want to protect the team, add a user to the team, and ensure at least one owner or member has been assigned an Exchange Online license.

PBI-ExportData_DisabledByTenant

Issue:

A Power BI report encountered an error during backup with the following error code:

- **PBI-ExportData_DisabledByTenant**

Details:

Your organization does not allow the download of reports.

Solution:

Refer to the link to enable the function to download report.

PBI-ExportData_DisabledForModelModifiedByXmlaEndpoint

Issue:

A Power BI report was skipped from backup with the following error code:

- **PBI-ExportData_DisabledForModelModifiedByXmlaEndpoint**

Details:

The reports modified by the XMLA endpoint are not supported for backup. Refer to the link for more details on the data-set connectivity with the XMLA endpoint.

PBI-ModelWithIncrementalRefreshIsNotDownloadable

Issue:

A Power BI report was skipped from backup with the following error code:

- **PBI-ModelWithIncrementalRefreshIsNotDownloadable**

Details:

The reports based on a single dataset with incremental refresh are not supported for backup.

Solution:

Refer to the link to disable the incremental refresh.

PBI-PowerBINotAuthorizedException

Issue:

A Power BI report encountered an error during backup with the following error code:

- **PBI-PowerBINotAuthorizedException**

Details:

The report does not have valid datasets.

Solution:

You can check whether the report can be manually downloaded from Microsoft Power BI. Typically, this report cannot be downloaded in Microsoft either. Please configure a valid dataset for the Power BI report.

If you want to ignore the error and avoid the impact on the job status, go to the IBM® Storage Protect for Cloud Microsoft™ 365 interface and navigate to **Settings** > **Backup** to skip the error by error code.

PBI-PremiumFilesErrors

Issue:

A Power BI report was skipped from backup with the following error code:

- **PBI-PremiumFilesErrors**

Details:

The reports based on a single dataset in large dataset storage format are not supported. Refer to the link for more details on large datasets in Power BI Premium.

PF-AccessDenied

Issue:

A public folder encountered an error during backup with the following error code:

- **PF-AccessDenied**

Details:

The impersonation account whichIBM® Storage Protect for Cloud Microsoft™ 3655 used to access the public folder does not have the permission to access the public folder.

Solution:

Verify the permission of the impersonation account. Refer to the link to assign permissions to the public folder.

PP-ExportPackageException

Issue:

A canvas app encountered an error during backup with the following error code:

- **PP-ExportPackageException**

Details:

An unexpected error occurred when exporting the app from Power Apps.

Solution:

Try exporting the app from Power Apps to see if it functions correctly. If you encounter issues and are unable to export the app, check the corresponding error message for troubleshooting. However, if the app is successfully exported, contact IBM support for further assistance.

If you want to dismiss this error, you can remove this object from the container through the IBM® Storage Protect for Cloud > **Auto discovery** > **Containers** page.

SP-AppSiteUnavailable

Issue:

An app site encountered an error during backup with the following error code:

- **SP-AppSiteUnavailable**

Details:

The app is not working, and the app site is unavailable.

Solution:

Check the app status in Microsoft 365. If you want to ignore the exception and avoid the impact on the job status, go to the IBM® Storage Protect for Cloud Microsoft™ 365 interface and navigate to **Settings** > **Backup**support to skip the error by error code.

SP-CannotCreateSubsite

Issue:

A file encountered an error during backup with the following error code:

- **SP-CannotCreateSubsite**

Details:

Your tenant setting does not allow the creation of subsites, so the subsite cannot be restored.

Solution:

You must update the tenant settings to enable the creation of subsites and try to restore them again.

Follow the steps below to enable the creation of subsites at the tenant level:

1. Sign in to the SharePoint admin center with a Microsoft 365 SharePoint administrator role.
2. Click **Settings** on the left panel.
3. In the **Settings** page, scroll down to the bottom and click **classic settings page**.
4. In the classic **Settings** page, find the **Subsite Creation** field and select the **Enable subsite creation for all sites** option.
5. Click **OK** to save your changes.

SP-DiscoverFailed

Issue:

A list encountered an error during backup with the following error code:

- **SP-DiscoverFailed**

Details:

An error occurred while discovering the data during backup process.

Solution:

Verify whether the affected list is a hidden list that has been migrated from SharePoint server (on-premises). If the list is no longer needed, consider deleting it to prevent future backup errors.

SP-FileBackupFailedDueToVirusScanner

Issue:

A file encountered an error during backup with the following error code:

- **SP-FileBackupFailedDueToVirusScanner**

Details:

SharePoint virus scanner detected invalid information or sensitive code in the file and prevented it from being downloaded.

Solution:

For the file with error, the site URL where the file resides is provided in the job report comment. You can navigate to the site to check whether the file can be manually downloaded from the website. Typically, this file cannot be downloaded in SharePoint either. You can check the file status in SharePoint.

To dismiss this error code, you can delete the file from SharePoint, or go to the IBM® Storage Protect for Cloud Microsoft™ 365 interface and navigate to **Settings** > **Backup**to configure a filter to skip the error by error code.

For more information on the error, refer to the Microsoft article: Built-in virus protection in SharePoint Online, OneDrive, and Microsoft Teams

SP-LargeFileIssue

Issue:

A file encountered an error during backup with the following error code:

- **SP-LargeFileIssue**

Details:

The backup for this object failed due to a job process timeout. It will be automatically included in the next backup. If this error persists, contact support team for assistance.

If you want to ignore the exception and avoid the impact on the job status, go to the IBM® Storage Protect for Cloud Microsoft™ 365 interface and navigate to **Settings** > **Backup**support to skip the error by error code.

SP-OneNoteBackupFailed

Microsoft has updated its API, allowing OneNote section files to be protected. If you previously contacted IBM support to set the status of these OneNote files with errors to Skipped, you can now reach out to IBM support to enable their protection.

Issue:

A OneNote section file encountered an error during backup with the following error code:

- **SP-OneNoteBackupFailed**

Details:

The OneNote section file cannot be downloaded by the Microsoft API.

Solution:

You may find the OneNote section files that failed during backup can still be accessed and viewed through the OneNote client application or OneNote Online because the OneNote client application or the OneNote Online simply loads the page for you. However, IBM® Storage Protect for Cloud needs to download the entire section for backup.

For the failed section file, the site URL where the failed file resides is provided in the report comment. You can navigate to the site to check whether the file can be manually downloaded from the website. If you can’t download it either, try the following resolutions:

- If you still want to back up this file, you can create a new section in your OneNote notebook, copy the pages from the corresponding section with exceptions to the new one, and then delete the original one to avoid exceptions. Then, try again in the next backup job.
- Contact Microsoft support to check it out and share Microsoft’s feedback with us.

If you want to ignore the exception and avoid the impact on the job status, you can contact IBM Software Support to set the status of these failed OneNote files to Skipped.

SP-PDFBackupFailedDueToIRM

Issue:

A PDF file encountered an error during the backup with the following error code:

- **SP-PDFBackupFailedDueToIRM**

Details:

The PDF file is encrypted with non-SharePoint encryption, and the library it resides in has enabled IRM settings. Therefore, this PDF cannot be downloaded and backed up.

Solution:

You can remove the IRM settings of this library or move this file to a library without IRM settings enabled. After that, you can monitor the subsequent backup jobs for the backup status of this file.

SP-SiteLocked

Issue:

A site is skipped from the backup with the following error code:

- **SP-SiteLocked**

Details:

This site is locked or archived, inaccessible, and cannot be backed up.

Solution:

Please check the status of your site. If you want to back up this site, you must unlock or unarchive it first. It will be automatically included in the subsequent backup job. If you want to dismiss this error, you can remove this object from the container through the **IBM® Storage Protect for Cloud › Microsoft & Salesforce › Auto Discovery › Containers** page.

SP-SiteNotExist

Issue:

The site was skipped from the backup with the following error code:

- **SP-SiteNotExist**

Details:

The site may have been removed from your Microsoft™ 365 environment.

Solution:

You can go to Auto Discovery in the IBM® Storage Protect for Cloud interface to rescan and update the site status. For detailed instructions, refer to Manage Scan Profiles.

SP-SiteReadOnly

Issue:

A site is skipped from the backup with the following error code:

- **SP-SiteReadOnly**

Details:

This site is read-only and cannot be backed up.

Solution:

Please check the status of your site. If you want to back up this site, you must unlock it and turn off **Read-only** first. It will be automatically included in the subsequent backup job. If you want to dismiss this error, you can remove this object from the container through the IBM® Storage Protect for Cloud > **Auto discovery** > **Containers** page.

SP-SkipBackupRecordingsFolder

Issue:

The Recordings folder that stores Teams meeting recordings was skipped from backup:

- **SP-SkipBackupRecordingsFolder**

Details:

The **Back up Recordings folder** option in the **Backup Settings** is deselected. Therefore, the Recordings folder that stores the Teams meeting recordings has been excluded from backup. For details on the Recordings folder in OneDrive or SharePoint site, refer to the Microsoft article: Teams meeting recording and transcript storage and permissions in OneDrive and SharePoint..

If you want to back up the Recordings folder, go to **Settings › Backup Settings** to select the **Back up Recordings folder** option.

SP-WebPartNotExist

Issue:

An item encountered an error during the backup with the following error code:

- **SP-WebPartNotExist**

Details:

While backing up the item, the Web parts on the corresponding page may have errors.

Solution:

Check all Web parts on this page to see if they are working properly and try to fix them. Then, you can wait for the subsequent backup job and monitor the status.

If you need additional assistance, contact IBM Software Support.

Teams-AccessDenied

Issue:

A file encountered an error during backup with the following error code:

- **Teams-AccessDenied**

Details:

The team owner/member which IBM® Storage Protect for Cloud Microsoft™ 365 used to access the team through impersonation cannot access the team.

Solution:

Verify whether the user is still available. If this error persists, remove the user from the team and add them back to resolve the problem.

Refer to the link to add team members and the link to remove team members.

Teams-NoAvailableOwnerOrMember

Issue:

A file encountered an error during backup with the following error code:

- **Teams-NoAvailableOwnerOrMember**

Details:

The team does not have any owners or members, or no owners or members in the team have the Exchange Online license.

Solution:

If you want to protect the team, add a user to the team, and ensure at least one owner or member has been assigned an Exchange Online license.

Appendices: Supported and Unsupported Data Types

The following table details the appendices included in this document:

Example

> **Note:** We list all the data types that have been covered in our test for each service. If you do not find the data type that you are interested in, you can consult our consult the IBM® Storage Protect for Cloud Team at the following website: www.ibm.com/support support team.

> **Note:** IBM® Storage Protect for Cloud Auto discovery scan profiles created after July 2023 release will only use app profile authentication. The IBM® Storage Protect for Cloud jobs for protecting objects scanned in app context (app profile authentication) will use app profile authentication only, except for Project Online. For the supported or unsupported data types, refer to the **Default/Custom App Profile** column in the tables below. For the support list of Project Online, refer to “Project Online Data Types” on page 202.

Appendix	Description
“SharePoint Sites Data Types” on page 181	Lists the supported and unsupported data types of SharePoint Online sites in IBM® Storage Protect for Cloud Microsoft™ 365. The support information also applies to the Project Online sites and the team sites of Microsoft™ 365 Groups and Teams.
Modern Team Site Data Types	Lists the supported and unsupported data types of Modern Team Site.
Project Online Data Types	Lists the supported and unsupported data types of Project Online.
Exchange Online Data Types	Lists the supported and unsupported data types of Exchange Online.
Public Folders Data Types	Lists the supported and unsupported data types of Public Folders.
Microsoft™ 365 Groups Data Types	Lists the supported and unsupported data types of Microsoft™ 365 Groups.
Teams Data Types	Lists the supported and unsupported data types of Teams.
“Viva Engage Data Types” on page 244	Lists the supported and unsupported data types of Viva Engage.
“OneDrive Data Types” on page 247	Lists the supported and unsupported data types of OneDrive.
Document-Related Data Types	Lists the supported and unsupported document-related data types.
“Power BI Data Types” on page 262	Lists the data types and limitations of Power BI backup service.
“Power Automate Data Types” on page 262	Lists the supported and unsupported attributes of Power Automate flows.
Power Apps Data Types	Lists the data types and limitations of Power Apps backup service.

Appendix	Description
Restore Options for Different Object Types	Lists the supported and unsupported restore options upon different object types.
"Restore Conflict Resolutions" on page 285	Lists the available container level conflict resolutions, content level conflict resolution, and app conflict resolutions for each object type.

SharePoint Sites Data Types

The table below lists the supported and unsupported SharePoint Sites data types in IBM® Storage Protect for Cloud Microsoft™ 365.

For the document-related data, refer to "Document-Related Data Types" on page 249.

Site Collection Settings

Data Type		Default/Custom App Profile	Service Account (Obsolete)
Recycle bin		Unsupported	Unsupported
Search Result Sources		Unsupported	Unsupported
Search Result Types		Unsupported	Unsupported
Search Query Rules		Unsupported	Unsupported
Search Schema		Unsupported	Unsupported
Search Settings	Enter a Search Center URL	Supported	Supported
	Which search results page should query be sent to?	Supported	Supported
Search Configuration Import		Supported	Supported
Search Configuration Export		Unsupported	Unsupported
Site collection features		Supported	Supported
Site hierarchy		Unsupported	Unsupported
Search Engine Sitemap Settings		Supported	Supported
Search engine optimization settings	Verify ownership of this site with search engines	Supported	Supported
	Consolidate link popularity with canonical URLs	Supported	Supported
Site collection navigation	Navigation Enabled	Supported	Supported
	Security Trimming	Supported	Supported
	Audience Targeting	Supported	Supported
Site collection audit settings	Audit Log Trimming	Supported	Supported
	Documents and Items	Supported	Supported
	Lists, Libraries, and Sites	Supported	Supported
Audit log reports		Supported	Supported
Portal site connection		Unsupported	Supported
Content Type Policy Templates		Supported	Supported
Storage Metrics		Unsupported	Unsupported
Site collection app permissions		Supported	Supported

Data Type		Default/Custom App Profile	Service Account (Obsolete)
Record declaration settings (With in place record management feature activated)	Record Restrictions	Supported	Supported
	Record Declaration Availability	Supported	Supported
	Declaration Roles	Supported	Supported
Site Policies		Unsupported	Supported
Content type service application error log		Supported	Supported
Site collection output cache	Output Cache	Supported	Supported
	Default Page Output Cache Profile	Supported	Supported
	Page Output Cache Policy	Supported	Supported
	Debug Cache Information	Supported	Supported
Popularity and Search Reports		Unsupported	Unsupported
Content type publishing	Refresh All Published Content Types	Supported	Supported
	Content type publishing error log	Unsupported	Unsupported
	Hubs	Supported	Supported
Variations Settings	Site, List, and Page Creation Behavior	Supported	Supported
	Recreate Deleted Target Page	Supported	Supported
	Update Target Page Web Parts	Supported	Supported
	Notification	Supported	Supported
Variation labels		Supported	Supported
Variation logs **Note:** The Row ID of the items cannot be kept. Therefore, the ranking in the restore destination may be different.		Supported	Supported
Translatable columns		Supported	Supported
Suggested Content Browser Locations		Supported	Supported
Document ID Settings	Assign Document IDs	Supported	Supported
	Document ID Lookup Search Scope	Supported	Supported
HTML Field Security	Allow external iframes	Unsupported	Unsupported
SharePoint Designer Settings	Allow Site Owners and Designers to use SharePoint Designer in this Site Collection	Supported	Supported
	Allow Site Owners and Designers to Detach Pages from the Site Definition	Supported	Supported
	Allow Site Owners and Designers to Customize Master Pages and Page Layouts	Supported	Supported
	Allow Site Owners and Designers to See the Hidden URL structure of their Web Site	Supported	Supported
Site collection health checks		Partially Supported	Partially Supported

Data Type	Default/Custom App Profile	Service Account (Obsolete)
Site collection upgrade	Unsupported	Unsupported

Site Settings

Data Types				Default/ Custom App Profile	Service Account (Obsolete)	Comment
Users and Permissions	People and groups			Supported	Supported	
	Site permissions			Supported	Supported	
	Site collection administrators (Top-level site)			Supported	Supported	
	Site app permissions			Supported	Supported	
Web Designer Galleries	Site columns			Supported	Supported	
	Site content types			Supported	Supported	
	Web parts (Top-level site)			Supported	Supported	
	List templates (Top-level site)			Supported	Supported	
	Master pages and page layouts			Partially Supported	Partially Supported	The **Modified by** column value becomes **SharePoint App** after being restored.
	Theme (Top-level site)			Supported	Supported	
	Solutions (Top-level site)			Supported	Supported	
	Composed looks			Supported	Supported	
Site Administration	Regional settings	Time Zone		Supported	Supported	
		Region	Locale	Supported	Supported	The existing Locale setting in the destination will not be updated.
			Sort Order	Supported	Supported	
			Set Your Calendar	Supported	Supported	
			Enable an Alternate Calendar	Supported	Supported	
			Define Your Work Week	Supported	Supported	
			Time Format	Supported	Supported	
			Subsite Settings	Supported	Supported	
Site Administration	Language Settings	Default Language		Supported	Supported	
		Alternate language(s)		Supported	Supported	

Data Types			**Default/ Custom App Profile**	**Service Account (Obsolete)**	**Comment**
		Overwrite Translations	Unsupported	Supported	
	Site libraries and lists		Supported	Supported	
	User alerts		Unsupported	Unsupported	
	RSS	Site Collection RSS	Unsupported	Supported	
		Enable RSS	Supported	Supported	
		Advanced Settings	Supported	Supported	
	Sites and workspaces		Unsupported	Unsupported	
	Workflow settings		Unsupported	Supported	
	Site Closure and Deletion	Site Closure	Supported	Supported	
		Site Deletion	Supported	Supported	
		Site Policy	Unsupported	Supported	
	Site output cache	Page Output Cache Profile	Supported	Supported	
	Term store management		Supported	Supported	
	Popularity Trends		Unsupported	Unsupported	
	Content and structure		Supported	Supported	
	Manage catalog connections		Supported	Supported	
	Content and structure logs		Supported	Supported	
	Site variation settings		Supported	Supported	
	Translation Status		Supported	Supported	
	Content Organizer Settings	Redirect Users to the Drop Off Library	Supported	Supported	
		Sending to Another Site	Supported	Supported	
		Folder Partitioning	Supported	Supported	
		Duplicate Submissions	Supported	Supported	
		Preserving Context	Supported	Supported	
		Rule Managers	Supported	Supported	
		Submission Points	Supported	Supported	
	Content Organizer Rules		Supported	Supported	
Search	Result Sources		Unsupported	Unsupported	
	Result Types		Unsupported	Unsupported	
	Query Rules		Unsupported	Unsupported	
	Schema		Unsupported	Unsupported	
	Search Settings	Enter a Search Center URL	Supported	Supported	
		Which search results page should query be sent to?	Supported	Supported	
		Configure Search Navigation	Supported	Supported	

Data Types			Default/ Custom App Profile	Service Account (Obsolete)	Comment
	Searchable columns		Partially Supported	Partially Supported	The SharePoint Server Publishing Infrastructure site collection feature must be activated.
	Search and offline availability	Indexing Site Content	Supported	Supported	
		Indexing ASPX Page Content	Unsupported	Supported	
		Offline Client Availability	Supported	Supported	
		Reindex site	Supported	Supported	
	Configuration Import		Supported	Supported	
	Configuration Export		Unsupported	Unsupported	
Community Administration (root site)	Manage Discussions		Supported	Supported	
	Manage Categories **Note:** The Categories list will have duplicate items.		Supported	Supported	
	Manage Members		Partially Supported	Partially Supported	The community members of the Discussion List will not be restored to another tenant.
	Community Settings	Established Date	Supported	Supported	
		Auto-approval for permission requests	Supported	Supported	
		Reporting of offensive content	Supported	Supported	
	Reputation Settings	Rating settings	Unsupported	Unsupported	
		Member achievements point system	Unsupported	Unsupported	
		Achievement level points	Unsupported	Unsupported	
		Achievement level representation	Unsupported	Unsupported	
	Manage Reported Posts **Note:** You can navigate to **Community settings** and select the **Enable reporting of offensive content** option to enable this feature.		Unsupported	Unsupported	

Data Types				Default/ Custom App Profile	Service Account (Obsolete)	Comment
Look and Feel	Design Manager	Welcome		Supported	Supported	
		Manage Device Channels	Supported	Supported		
		Upload Design Files	Supported	Supported		
		Edit Master Pages	Supported	Supported		
		Edit Display Templates	Supported	Supported		
		Edit Page Layouts	Supported	Supported		
		Publish and Apply Design	Supported	Supported		
	Master page	Site Master Page		Supported	Supported	
		System Master Page		Supported	Supported	
		Theme		Supported	Supported	
		Alternate CSS URL		Supported	Supported	
	Title, description, and logo	Title and Description		Supported	Supported	
		Logo and Description		Supported	Supported	
	Page layouts and site templates	Subsite Templates		Supported	Supported	
		Page Layouts		Supported	Supported	
		New Page Default Settings		Supported	Supported	
	Welcome Page			Supported	Supported	
	Device Channels			Supported	Supported	
Look and Feel	Tree view	Enable Quick Launch		Supported	Supported	
		Enable Tree View		Supported	Supported	
	Change the look			Supported	Supported	
	Import Design Package			Supported	Supported	
	Navigation	Global Navigation		Supported	Supported	
		Current Navigation		Supported	Supported	
		Structural Navigation: Sorting		Supported	Supported	
		Structural Navigation: Editing and Sorting		Supported	Supported	The Recent navigation will be updated according to the order of objects being restored.
		Show and Hide Ribbon		Supported	Supported	
	Image Renditions			Supported	Supported	
Site Actions	Manage site features			Supported	Supported	
	Reset to site definition			Supported	Supported	
	Delete this site			Supported	Supported	
Hold	Hold Reports			Supported	Supported	
	Holds			Supported	Supported	

Data Types			Default/ Custom App Profile	Service Account (Obsolete)	Comment
	Discover and hold content	Search Criteria	Supported	Supported	
		Local Hold or Export	Supported	Supported	
		Relevant Hold	Supported	Supported	

List/Library Settings

Data Types			Default/ Custom App Profile	Service Account (Obsolete)	Comment
Title, description, and navigation	Name		Partially Supported	Partially Supported	The name will not be updated if a list/library with the same URL exists in the destination.
	Description		Supported	Supported	
	Navigation		Supported	Supported	
	Survey Options	Show user names in survey results?	Supported	Supported	
		Allow multiple responses?	Unsupported	Supported	
	Group Calendar Options	Use this calendar to share member's schedule?	Unsupported	Supported	
Versioning settings	Content Approval		Supported	Supported	Note that the **Approval Status** column values cannot be restored.
	Version History Limits(Admin)	Automatically	Unsupported	Unsupported	
		Manually	Unsupported	Unsupported	
	Version Time Limit(Site)	No time limit	Unsupported	Unsupported	
		Automatic	Unsupported	Unsupported	
		Manual	Unsupported	Unsupported	
	Version Time Limit(Library)	No time limit	Supported	Supported	
		Automatic	Supported	Supported	
		Manual	Supported	Supported	
	Document Version History	No versioning	Supported	Supported	
		Create major versions	Supported	Supported	
		Create major and minor (draft) versions	Supported	Supported	

Data Types			Default/ Custom App Profile	Service Account (Obsolete)	Comment
		Keep the following number of major versions	Supported	Supported	
		Keep drafts for the following number of major versions	Supported	Supported	
	Draft Item Security		Supported	Supported	
	Require Check Out		Supported	Supported	
Advanced settings	Content Types		Supported	Supported	
	Document Template		Supported	Supported	
	Opening Documents in the Browser		Unsupported	Supported	
	Custom Send To Destination	Destination name	Unsupported	Supported	
		URL	Unsupported	Supported	
	Folders		Supported	Supported	
	Item-level Permissions	Read all items	Supported	Supported	
		Read items that were created by the user	Supported	Supported	
		Create and edit all items	Supported	Supported	
		Create items and edit items that were created by the user	Supported	Supported	
		None	Supported	Supported	
	Search		Supported	Supported	
	Index Non-Default Views		Supported	Supported	
	Reindex Document Library		Supported	Supported	
	Offline Client Availability		Unsupported	Supported	
	Site Assets Library		Supported	Supported	
	Quick Edit		Unsupported	Supported	
	Dialogs		Unsupported	Supported	
	Automatic Index Management		Unsupported	Supported	
Validation settings	Formula		Supported	Supported	
	User Message		Supported	Supported	
Column default value settings			Supported	Supported	
Manage item scheduling			Supported	Supported	
Rating settings			Supported	Supported	
Audience targeting settings	Enable Audience Targeting		Supported	Supported	
	Enable Classic Audience Targeting		Supported	Supported	

Data Types		Default/ Custom App Profile	Service Account (Obsolete)	Comment
Metadata navigation settings	Configure Navigation Hierarchies	Supported	Supported	
	Configure Key Filters	Supported	Supported	
	Configure automatic column indexing for this list	Supported	Supported	
Catalog Settings		Partially Supported	Supported	
Save document library as template		Supported	Supported	
Manage files which have no checked-in version		Unsupported	Supported	
Workflow Settings (see workflow for additional details)		Unsupported	Supported	
Generate file plan report		Supported	Supported	
Enterprise Metadata and Keywords Settings		Supported	Supported	
Information management policy settings		Unsupported	Supported	
Permissions for this document library	Group	Supported	Supported	
	User	Supported	Supported	
	Role Assignments	Supported	Supported	
RSS Setting		Unsupported	Unsupported	
Calendar View		Supported	Supported	Mobile list simple view is unsupported
Custom View in SharePoint Designer		Supported	Supported	
Datasheet View		Supported	Supported	
Gantt View		Supported	Supported	
Standard View		Supported	Supported	Mobile list simple view is unsupported
Public View		Supported	Supported	
Personal View		Unsupported	Unsupported	

Admin Center

Data Types				Default/ Custom App Profile	Service Account (Obsolete)
Apps	App Catalog Site Collection			Supported	Supported
BCS				Unsupported	Unsupported
Info path				Unsupported	Unsupported
Records management				Unsupported	Unsupported
Search				Unsupported	Unsupported
Secure Store				Unsupported	Unsupported
Site Collection				Supported	Supported
Term Store	Term Group	General	Group Name	Supported	Supported
			Description	Supported	Supported

Data Types				Default/ Custom App Profile	Service Account (Obsolete)
			Group Managers	Unsupported	Unsupported
			Distributors	Unsupported	Unsupported
	Term Set	General	Term Set Name	Supported	Supported
			Description	Supported	Supported
			Owner	Supported	Supported
			Contact	Supported	Supported
			Stakeholders	Unsupported	Supported
			Submission Policy	Supported	Supported
		Intended Use	Available for Tagging	Supported	Supported
			Use this Term Set for Site Navigation	Supported	Supported
			Use this Term Set for Faceted Navigation	Supported	Supported
		Custom Sort	Custom Sort Order	Supported	Supported
		Term-Driven Pages	Target Page Settings	Supported	Supported
			Catalog Item Page Settings	Supported	Supported
		Custom Properties	Properties	Supported	Supported
Term Store	Term	General	Available for Tagging	Supported	Supported
			Language	Supported	Supported
			Description	Supported	Supported
			Default Label	Supported	Supported
			Other Labels	Supported	Supported
		Navigation	Navigation Node Title	Supported	Supported
			Navigation Hover Text	Supported	Supported
			Visibility in Menus	Supported	Supported
			Simple Link or Header	Supported	Supported
			Term-Driven Page with Friendly URL	Supported	Supported
			Associated Folder	Supported	Supported
		Term-Driven Pages	Target Page Settings	Supported	Supported

Data Types				Default/ Custom App Profile	Service Account (Obsolete)
			Category Image	Supported	Supported
			Catalog Item Page Settings	Supported	Supported
		Faceted Navigation	Refiner	Unsupported	Unsupported
		Custom Properties	Shared Properties	Supported	Supported
			Local Properties	Supported	Supported
User profiles				Unsupported	Unsupported

Features

Example

Note that the features cannot be kept the same as the backup data if its restore destination is a site with a different template.

Data Types		Default/Custom App Profile	Service Account (Obsolete)
Site Collection Features	Aggregated Business Calendar	Supported	Supported
	Content Type Syndication Hub	Supported	Supported
	Cross-Site Collection Publishing	Supported	Supported
	Custom Site Collection Help	Supported	Supported
	Disposition Approval Workflow	Supported	Supported
	Document ID Service	Supported	Supported
	Document Sets	Supported	Supported
	Duet End User Help Collection	Supported	Supported
	Duet Enterprise Reports Content Types	Supported	Supported
	In Place Records Management	Supported	Supported
	Library and Folder Based Retention	Supported	Supported
	Limited-access user permission lockdown mode	Supported	Supported
	Open Documents in Client Applications by Default	Supported	Supported
	Project Server Approval Content Type	Supported	Supported

Data Types		Default/Custom App Profile	Service Account (Obsolete)
	Project Web App Permission for Excel Web App Refresh	Supported	Supported
	Project Web App Ribbon	Supported	Supported
	Project Web App Settings	Supported	Supported
	Publishing Approval Workflow	Supported	Supported
	Reporting	Supported	Supported
	Reports and Data Search Support	Supported	Supported
Site Collection Features	Sample Proposal	Supported	Supported
	Search Engine Sitemap	Supported	Supported
	Search Server Web Parts and Templates	Supported	Supported
	SharePoint 2007 Workflows	Supported	Supported
	SharePoint Server Enterprise Site Collection features	Supported	Supported
	SharePoint Server Publishing Infrastructure	Supported	Supported
	SharePoint Server Standard Site Collection features	Supported	Supported
	Site Policy	Supported	Supported
	Three-state workflow	Supported	Supported
	Video and Rich Media	Supported	Supported
	Workflows	Supported	Supported
Site Features	Access App	Supported	Supported
	Announcement Tiles	Supported	Supported
	Community Site Feature	Supported	Supported
	Content Organizer	Supported	Supported
	Duet Enterprise - SAP Workflow	Supported	Supported
	Duet Enterprise Reporting	Supported	Supported
	Duet Enterprise Site Branding	Supported	Supported
	External System Events	Supported	Supported
	Following Content	Supported	Supported
	Getting Started	Supported	Supported
	Getting Started with Project Web App	Supported	Supported
Site Features	Hold	Supported	Supported
	Metadata Navigation and Filtering	Supported	Supported

Data Types		Default/Custom App Profile	Service Account (Obsolete)
	Minimal Download Strategy	Supported	Supported
	Mobile Browser View	Supported	Supported
	Offline Synchronization for External Lists	Supported	Supported
	Project Functionality	Supported	Supported
	Project Proposal Workflow	Supported	Supported
	Project Web App Connectivity	Supported	Supported
	SAP Workflow Web Parts	Supported	Supported
	Search Config Data Content Types	Supported	Supported
	Search Config Data Site Columns	Supported	Supported
	Search Config List Instance Feature	Supported	Supported
	Search Config Template Feature	Supported	Supported
	SharePoint Server Enterprise Site features	Supported	Supported
	SharePoint Server Publishing	Supported	Supported
	SharePoint Server Standard Site features	Supported	Supported
	Site Feed	Supported	Supported
	Site Mailbox	Supported	Supported
	Site Notebook	Supported	Supported
	Team Collaboration Lists	Supported	Supported
	Wiki Page Home Page	Supported	Supported
	Workflow Task Content Type	Supported	Supported

Templates

Example

Note: Due to Microsoft’s deprecation of classic publishing sites in SharePoint Online, Cloud Backup will now restore classic publishing sites as communication sites.

Data Types			Default/Custom App Profile	Service Account (Obsolete)
Site Collection Templates	Collaboration	Team Site	Supported	Supported
		Blog	Supported	Supported
		Developer Site	Supported	Supported

Data Types			Default/Custom App Profile	Service Account (Obsolete)
		Project Site	Supported	Supported
		Community Site	Supported	Supported
	Enterprise	Document Center	Supported	Supported
		eDiscovery Center	Supported	Supported
		Records Center	Supported	Supported
		Team Site-SharePoint Online Configuration	Supported	Supported
		Business Intelligence Center	Unsupported	Supported
		Compliance Policy Center	Supported	Supported
		Enterprise Search Center	Partially Supported	Partially Supported
		Enterprise Wiki	Supported	Supported
		My Site Host	Supported	Supported
		Community Portal	Supported	Supported
		Basic Search Center	Supported	Supported
		Visio Process Repository	Supported	Supported
	Publishing	Publishing Portal	Partially Supported	Partially Supported
		Publishing Site Blank	Partially Supported	Partially Supported
		Site Directory	Partially Supported	Partially Supported
		News Home Site	Partially Supported	Partially Supported
		Product Catalog	Partially Supported	Partially Supported
		Report Center	Partially Supported	Partially Supported
		Topic Area Template	Partially Supported	Partially Supported
	Communication Site		Supported	Supported
Sub-Site Templates	Collaboration	Team Site	Supported	Supported
		Blog	Partially Supported	Partially Supported
		Project Site	Supported	Supported
		Community Site	Supported	Supported
	Enterprise	Document Center	Supported	Supported
		Records Center	Supported	Supported
		Business Intelligence Center	Supported	Supported
		Enterprise Search Center	Partially Supported	Partially Supported
		Basic Search Center	Supported	Supported

Data Types			Default/Custom App Profile	Service Account (Obsolete)
		Visio Process Repository	Supported	Supported
	Publishing	Publishing Site	Partially Supported	Partially Supported
		Publishing Site with Workflow	Unsupported	Supported
		Enterprise Wiki	Partially Supported	Partially Supported
	Duet Enterprise	SAP Workflow Site	Unsupported	Supported
Normal List Templates	Announcements		Supported	Supported
	Asset Library		Supported	Supported
	Calendar		Supported	Supported
	Contacts		Supported	Supported
	Custom List		Supported	Supported
	Custom List in Datasheet View		Supported	Supported
	Customized Template		Supported	Supported
	Data Connection Library		Supported	Supported
	Discussion Board		Supported	Supported
	Document Library		Supported	Supported
	External List		Unsupported	Unsupported
	Form Library		Supported	Supported
	Import Spreadsheet		Supported	Supported
	Issue Tracking		Supported	Supported
	Links		Supported	Supported
	Picture Library		Supported	Supported
	Promoted Links		Supported	Supported
	Record Library		Supported	Supported
	Related Actions List		Supported	Supported
	Report Library		Supported	Supported
	Survey		Supported	Supported
	Tasks		Supported	Supported
	Wikipage Library		Supported	Supported
Design List Templates	AppData		Supported	Supported
	Badges		Supported	Supported
	Cache Profiles		Supported	Supported
	Composed looks		Supported	Supported
	Content type publishing error log		Supported	Supported
	Converted Forms		Supported	Supported
	Device Channels		Supported	Supported
	Form Templates		Supported	Supported
	FrontPage Data Sources		Supported	Supported
	Images		Supported	Supported

Data Types		Default/Custom App Profile	Service Account (Obsolete)
	List Template Gallery	Supported	Supported
	Long-Running Operation Status	Unsupported	Unsupported
	Maintenance Log Library	Supported	Supported
	Master Page Gallery	Supported	Supported
	Notification List	Supported	Supported
	Hold Reports	Supported	Supported
	Hold	Supported	Supported
	Pages	Supported	Supported
	Project Policy Item List	Supported	Supported
	Quick Deploy Items	Supported	Supported
	Relationships List	Supported	Supported
	Reports List	Supported	Supported
	Search Config List	Supported	Supported
	Site Assets	Supported	Supported
	Site Pages	Supported	Supported
	Solution Gallery	Supported	Supported
	Style Library	Supported	Supported
	Suggested Content Browser Locations	Supported	Supported
	Taxonomy Hidden List	Unsupported	Unsupported
	Theme Gallery	Supported	Supported
	Translation Package	Supported	Supported
Design List Templates	Translation Status	Supported	Supported
	User Information List	Unsupported	Unsupported
	Variation Labels	Supported	Supported
	Variation logs	Supported	Supported
	Web Part Gallery	Supported	Supported
	Workflow Tasks	Supported	Supported
	No Code Public Workflows	Unsupported	Unsupported
	No Code Workflows	Unsupported	Unsupported
	Workflow History	Unsupported	Unsupported
	Nintex Workflow	Unsupported	Unsupported
	MFSVC	Unsupported	Unsupported
	MicroFeed	Unsupported	Unsupported
	AppData Catalog	Unsupported	Unsupported
	SharingLinks	Unsupported	Unsupported
	TaxonomyHiddenList	Unsupported	Unsupported

Web Parts

Note that the table below is only applicable to built-in web parts of Microsoft 365, and the third-party web parts are not supported.

Data Types		Default/Custom App Profile	Service Account (Obsolete)
Blog	Blog Archives	Supported	Supported
	Blog Notifications	Supported	Supported
	Blog Tools	Supported	Supported
Business Data	Business Data Actions	Supported	Supported
	Business Data Connectivity Filter	Supported	Supported
	Business Data Item	Supported	Supported
	Business Data Item Builder	Supported	Supported
	Business Data List	Supported	Supported
	Business Data Related List	Supported	Supported
	Excel Web Access	Supported	Supported
	Indicator Details	Supported	Supported
	Status List	Supported	Supported
	Visio Web Access	Supported	Supported
Community	About this community	Supported	Supported
	Join	Supported	Supported
	My membership	Supported	Supported
	Tools	Supported	Supported
	What's happening	Supported	Supported
Content Rollup	Categories	Supported	Supported
	Content Query	Supported	Supported
	Content Search	Unsupported	Unsupported
	Project Summary	Supported	Supported
	Relevant Documents	Supported	Supported
	RSS Viewer	Supported	Supported
	Site Aggregator	Supported	Supported
	Sites in Category	Supported	Supported
	Summary Links	Supported	Supported
	Table Of Contents	Partially Supported	Partially Supported
	Term Property	Supported	Supported
	Timeline	Supported	Supported
	WSRP Viewer	Supported	Supported
	XML Viewer	Supported	Supported
Document Sets	Document Set Contents	Supported	Supported
	Document Set Properties	Supported	Supported
Duet Enterprise	Aggregated Business Calendar	Supported	Supported
	Documents	Supported	Supported
	Link Viewer	Supported	Unsupported
	My SAP Workflow Tasks	Supported	Supported

Data Types		Default/Custom App Profile	Service Account (Obsolete)
	Task Decision Makers	Supported	Supported
	Task Details	Supported	Supported
Filters	Apply Filters Button	Supported	Supported
	Choice Filter	Supported	Supported
	Current User Filter	Supported	Supported
	Date Filter	Supported	Supported
	Page Field Filter	Supported	Supported
	Query String (URL) Filter	Supported	Supported
	SharePoint List Filter	Supported	Supported
	SQL Server Analysis Services Filter	Supported	Supported
	Text Filter	Supported	Supported
Forms	HTML Form Web Part	Supported	Supported
	InfoPath Form Web Part	Supported	Supported
Media and Content	Content Editor	Supported	Supported
	Get started with your site	Supported	Supported
	Image Viewer	Supported	Supported
	Media Web Part	Supported	Supported
	Page Viewer	Supported	Supported
	Picture Library Slideshow Web Part	Supported	Supported
	Script Editor	Supported	Supported
	Silverlight Web Part	Supported	Supported
Search	Find by Document ID	Supported	Supported
	Refinement	Supported	Supported
	Search Box	Supported	Supported
	Search Navigation	Supported	Supported
	Search Results	Supported	Supported
	Taxonomy Refinement Panel	Supported	Supported
Search-Driven Content **Note:** The **Recently Changed Items** and **Wiki Pages** both display real-time content and cannot keep data in the backup.	Catalog-Item Reuse	Supported	Supported
	Items Matching a Tag	Unsupported	Unsupported
	Pages	Supported	Supported
	Pictures	Supported	Supported
	Popular Items	Supported	Supported
	Recently Changed Items	Supported	Supported
	Recommended Items	Supported	Supported
	Videos	Supported	Supported
	Web Pages	Supported	Supported
	Wiki Pages	Supported	Supported
Social Collaboration	Announcement Tiles	Supported	Supported
	Contact Details	Supported	Supported

Data Types		Default/Custom App Profile	Service Account (Obsolete)
	Note Board	Supported	Supported
	Organization Browser	Supported	Supported
	Site Feed	Unsupported	Unsupported
	Site Users	Supported	Supported
	Tag Cloud	Supported	Supported
	User Tasks	Supported	Supported

Others

Data Types			Default/Custom App Profile	Service Account (Obsolete)
Alert	Alert Configuration	Alert Title	Unsupported	Unsupported
		Change Type	Unsupported	Unsupported
		Delivery Method	Unsupported	Unsupported
		Send Alerts for These Changes	Unsupported	Unsupported
		Send Alerts To	Unsupported	Unsupported
		When to Send Alerts	Unsupported	Unsupported
	Alert Level	Alert on Document/ Item	Unsupported	Unsupported
		Alert on Folder	Unsupported	Unsupported
		Alert on List/Library	Unsupported	Unsupported
App	Provider Host App		Unsupported	Unsupported
	SharePoint Host App		Supported	Supported
Solution	User Solution		Supported	Supported
Discussion Board	Folder version		Unsupported	Unsupported

Hidden Lists

The following lists will not be included for backup by default. If you want to include the hidden lists, you can contact the IBM Software Support team for assistance.

- If a list or library is set to Hidden and the list or library is empty, the backup job will not include such hidden lists or libraries by default.
- Special lists, such as,
  - User Information
  - Workflow
  - wfpub
  - appdata
  - Workflow History
  - MicroFeed
  - SharingLinks
  - WebTemplateExtensionsList

    - Nintex Workflow
- The SYSTEM lists whose URL end with:

Relative URL	Title
/Lists/TaxonomyHiddenList	TaxonomyHiddenList
/Lists/ContentTypeSyncLog	Content type publishing error log
/Long Running Operation Status	Long Running Operation Status

The ghost files in the CATALOG lists whose URLs end with:

Relative URL	Title
/Style Library	Style Library
/_catalogs/masterpage	Master Page Gallery
/_catalogs/theme	Theme Gallery
/_catalogs/wp	Web Part Gallery

Modern Team Site Data Types

The table below shows the specific data types of Modern Team Site that are supported or unsupported in IBM® Storage Protect for Cloud Microsoft™ 365.

Data types table

Data Type			Default/Custom App Profile	Service Account (Obsolete)
Home page	Page Details	Thumbnail	Supported	Supported
	Page Layout	Layout Options	Supported	Supported
		Section background	Supported	Supported
Web part	Text		Supported	Supported
	Image		Supported	Supported
	File viewer		Supported	Supported
	Link		Supported	Supported
	Embed		Supported	Supported
	Highlighted content		Supported	Supported
	Bing Maps		Supported	Supported
	Code Snippet		Supported	Supported
	Countdown Timer		Supported	Supported
	Divider		Supported	Supported
	Document Library		Supported	Supported
	Events		Supported	Supported
	Group Calendar		Supported	Supported
	Hero		Supported	Supported
	Image Gallery		Supported	Supported
	Kindle Instant Preview		Supported	Supported
	List		Supported	Supported
	Markdown		Supported	Supported

Data Type		Default/Custom App Profile	Service Account (Obsolete)
	Microsoft™ Forms **Note:** The restore of this Web part cannot restore the connected forms.	Supported	Supported
	Microsoft™ PowerApps	Supported	Supported
	News	Supported	Supported
	Page properties	Supported	Supported
	People	Supported	Supported
	Power® BI	Supported	Supported
	Quick chart	Supported	Supported
	Quick links	Supported	Supported
	Recent documents	Supported	Supported
	Site activity	Supported	Supported
	Sites	Supported	Supported
	Spacer	Supported	Supported
Web part	Stream (preview)	Supported	Supported
	Twitter (preview)	Supported	Supported
	Weather	Supported	Supported
	Viva Engage	Supported	Supported
	YouTube	Supported	Supported
	Asana	Supported	Supported
	Bitbucket	Supported	Supported
	Bitbucket Server	Supported	Supported
	Button	Supported	Supported
	Call to action	Supported	Supported
	Conversation	Supported	Supported
	Github	Supported	Supported
	Github Enterprise	Supported	Supported
	Google Analytics	Supported	Supported
	Jira	Supported	Supported
	Microsoft™ 365 Connections	Supported	Supported
	Planner	Unsupported	Supported
	RSS	Supported	Supported
	Stack Overflow	Supported	Supported
	Trello	Supported	Supported
	UserVoice	Supported	Supported
	World clock	Supported	Supported
	Wunderlist	Supported	Supported
Site designs	Design	Supported	Supported

Data Type			Default/Custom App Profile	Service Account (Obsolete)
	Script		Supported	Supported
Navigation	Site navigation visibility	On	Supported	Supported
		Off	Supported	Supported
	Orientation	Horizontal	Supported	Supported
		Vertical	Supported	Supported
		Horizontal > Menu style > Mega menu	Supported	Supported
		Horizontal > Menu style > Cascading	Supported	Supported
Header	Layout	Minimal	Supported	Supported
		Compact	Supported	Supported
		Standard	Supported	Supported
		Extended	Supported	Supported
	Background	Theme	Supported	Supported
		Image (Optional)	Unsupported	Unsupported
	Display	Site title visibility	Supported	Supported
		Site logo thumbnail	Supported	Supported
		Site logo	Supported	Supported
		Logo alignment > Left	Supported	Supported
		Logo alignment > Center	Supported	Supported
		Logo alignment > Right	Supported	Supported
Theme	Font		Unsupported	Unsupported
	Background image		Unsupported	Unsupported
	Color		Supported	Supported
Footer (Only communication sites and content center site templates have this property.)	Enable > On/Off		Supported	Supported
	Layout	Simple	Supported	Supported
		Extended	Supported	Supported
	Logo		Unsupported	Unsupported
	Display name		Unsupported	Unsupported
	Background		Supported	Supported
	Link label		Unsupported	Unsupported
	Enable site navigation audience targeting > On/Off		Unsupported	Unsupported

Project Online Data Types

The table below shows the Project Online data types that are supported or unsupported in IBM® Storage Protect for Cloud Microsoft™ 365.

Note: Apart from the data types detailed below, the data types listed as unsupported in “SharePoint Sites Data Types” on page 181 are also unsupported in Project Online site collections.

Additional notes:

- Project Online data is not supported in app context (using app profile authentication).
- Project Online service provided by IBM® Storage Protect for Cloud Microsoft™ 365 cannot protect the **Project for the web** data. It can be protected by IBM® Storage Protect for Cloud Dynamics 365
- Project Online service cannot fully support the data added through Project Online desktop client, for example, custom fields.
- Project Online service cannot protect the data types that can be created through Project Professionals but cannot be created through the Web interface, such as Global template, sub project, etc.

The following table is provided for service account authentication.

Table for service account authentication.

Top Level	Second Level	Third Level		Support Status
Strategy	Driver Library	Name and Description		Supported
		Departments	Supported	
		Status	Supported	
		Project Impact Statements	Supported	
	Driver Prioritization	Define properties	Name and Description	Supported
			Department	Supported
			Prioritization Type	Supported
			Prioritize the following drivers	Supported
		Prioritize Drivers		Supported
		Review Priorities		Supported
	Portfolio Analyses	Define properties	Name and Description	Supported
			Department	Supported
			Prioritization Type	Supported
			Prioritize these projects	Supported
			Analysis Primary Cost Constraint	Supported
			Resource Planning	Supported
			Planning Horizon and Granularity	Supported
			Resource role custom field	Supported
			Resource filtering	Supported
			Resource capacity impact for a project outside the analysis	Supported
			Project start and finish dates	Supported

Top Level	Second Level	Third Level		Support Status
			Alias project Force-in and Force-out options	Supported
		Prioritize Projects		Supported
		Review Priorities		Supported
		Analyze Cost		Supported
		Analyze Resources		Supported
		Project Dependencies		Supported
Project	Project		Project ID	Supported
			Project Name	Supported
			Start Time	Supported
			Finish Time	Supported
			%Complete	Supported
			Work	Supported
			Duration	Supported
			Owner	Supported
			Last Published	Unsupported
			Description	Supported
			Custom Fields	Supported
			Strategic Impact	Unsupported
			Timeline	Supported
			Workflow Instance	Unsupported
			Baseline	Unsupported
			Project Permissions	Supported
	Project Tasks		Mode	Supported
			Task Name	Supported
			Unique ID	Unsupported
			Subtask	Supported
			Duration	Supported
			Start Time	Supported
			Finish Time	Supported
			%Complete	Supported
			Actual Work	Supported
			Work	Supported
			Resource Names	Supported
			Timeline	Supported
			Custom Fields	Unsupported
	Project Site		PWA Settings	Supported
			Custom SharePoint Site Content	Supported
Approvals				Supported

Project Professional

The table below lists the supported and unsupported data types of Project Professional.

The table below lists the supported and unsupported data types of Project Professional.

Top Level	Second Level	Third Level		Support Status
Project Information	Start date			Supported
	Finish date			Unsupported
	Current® date			Supported
	Status date			Supported
	Schedule from			Unsupported
	Calendar			Unsupported
	Priority			Unsupported
	Calculate Resource Utilization from			Unsupported
	Department			Unsupported
	Custom Field Name			Supported
	Value			Partially supported
Project – Custom Fields	Cost	Name		Supported
		Custom attributes	Supported	
		Calculation for task and group summary rows	Supported	
		Calculation for assignment rows	Supported	
		Values to display	Supported	
	Date	Name		Supported
		Custom attributes		Supported
		Calculation for task and group summary rows		Supported
		Calculation for assignment rows		Supported
		Values to display		Supported
	Duration	Name		Supported
		Custom attributes		Supported
		Calculation for task and group summary rows		Supported
		Calculation for assignment rows		Supported
		Values to display		Supported
	Flag	Name		Supported
		Custom attributes		Supported
		Calculation for task and group summary rows		Supported
		Calculation for assignment rows		Supported
		Values to display		Supported
	Number	Name		Supported
		Custom attributes		Supported
		Calculation for task and group summary rows		Supported

Top Level	Second Level	Third Level	Support Status
		Calculation for assignment rows	Supported
		Values to display	Supported
	Text	Name	Supported
		Custom attributes	Supported
		Calculation for task and group summary rows	Supported
		Calculation for assignment rows	Supported
		Values to display	Supported
Resource Information	Name		Supported
	Initials		Supported
	Max units		Unsupported
	Base cal		Supported
	Group		Supported
	Code		Supported
	Costs	Std rate	Unsupported
		Ovt rate	Unsupported
		Per use	Unsupported
		Accrue at	Supported
Resource – Custom Fields	Cost	Name	Unsupported
		Custom attributes	Unsupported
		Calculation for task and group summary rows	Unsupported
		Calculation for assignment rows	Unsupported
		Values to display	Unsupported
	Date	Name	Unsupported
		Custom attributes	Unsupported
		Calculation for task and group summary rows	Unsupported
		Calculation for assignment rows	Unsupported
		Values to display	Unsupported
	Duration	Name	Unsupported
		Custom attributes	Unsupported
		Calculation for task and group summary rows	Unsupported
		Calculation for assignment rows	Unsupported
		Values to display	Unsupported
	Finish	Name	Unsupported
		Custom attributes	Unsupported
		Calculation for task and group summary rows	Unsupported
		Calculation for assignment rows	Unsupported
		Values to display	Unsupported

Top Level	Second Level	Third Level		Support Status
	Flag	Name		Unsupported
		Custom attributes		Unsupported
		Calculation for task and group summary rows		Unsupported
		Calculation for assignment rows		Unsupported
		Values to display		Unsupported
	Number	Name		Unsupported
		Custom attributes		Unsupported
		Calculation for task and group summary rows		Unsupported
		Calculation for assignment rows		Unsupported
		Values to display		Unsupported
	Start	Name		Unsupported
		Custom attributes		Unsupported
		Calculation for task and group summary rows		Unsupported
		Calculation for assignment rows		Unsupported
		Values to display		Unsupported
	Text	Name		Unsupported
		Custom attributes		Unsupported
		Calculation for task and group summary rows		Unsupported
		Calculation for assignment rows		Unsupported
		Values to display		Unsupported
	Outline code	Name		Unsupported
		Custom attributes		Unsupported
		Calculation for task and group summary rows		Unsupported
		Calculation for assignment rows		Unsupported
		Values to display		Unsupported
Task Information	General	Name		Supported
		Duration	Unsupported	
		Estimated	Unsupported	
		Percent complete	Supported	
		Priority	Supported	
		Schedule Mode	Supported	
		Inactive	Supported	
		Dates Start	Supported	
		Dates Finish	Supported	
		Display on Timeline	Supported	
		Hide Bar	Unsupported	
		Rollup	Unsupported	
	Predecessors	Name		Supported
		Duration		Unsupported

Top Level	Second Level	Third Level		Support Status
		Estimated		Unsupported
		ID		Unsupported
		Task name		Unsupported
		Type		Unsupported
		Lag		Unsupported
	Resources	Name		Supported
		Duration		Unsupported
		Estimated		Unsupported
		Resource name		Supported
		Assignment owner		Unsupported
		Request/demand		Unsupported
		Units		Unsupported
		Cost		Unsupported
	Advanced	Name		Supported
		Duration		Unsupported
		Estimated		Unsupported
		Deadline		Supported
		Constraint type		Unsupported
Task Information	Advanced	Constraint date		Unsupported
		Task type		Supported
		Effort driven		Unsupported
		Calendar		Unsupported
		Scheduling ignores resource calendars		Unsupported
		WBS code		Unsupported
		Earned value method		Supported
		Mark task as milestone		Unsupported
	Notes®	Name		Supported
		Duration		Unsupported
		Estimated		Unsupported
		Format and font	Font	Unsupported
			Font style	Unsupported
			Size	Unsupported
			Underline	Unsupported
			Strikethrough	Unsupported
			Color	Unsupported
		Align left		Unsupported
		Center		Unsupported
		Align right		Unsupported
		Bulleted list		Unsupported
		Insert object	Create new	Unsupported
			Create from file	Unsupported
			Link	Unsupported

Top Level	Second Level	Third Level		Support Status
			Display as icon	Unsupported
		Text	Special characters	Unsupported
			Chinese	Unsupported
	Custom fields	Name		Supported
		Duration		Unsupported
		Estimated		Unsupported
		Custom Field Name		Supported
		Value		Partially supported
Task – Custom Fields	Cost	Name		Unsupported
		Custom attributes	Unsupported	
		Calculation for task and group summary rows	Unsupported	
		Calculation for assignment rows	Unsupported	
		Values to display	Unsupported	
	Date	Name		Unsupported
		Custom attributes		Unsupported
		Calculation for task and group summary rows		Unsupported
		Calculation for assignment rows		Unsupported
		Values to display		Unsupported
	Duration	Name		Unsupported
		Custom attributes		Unsupported
		Calculation for task and group summary rows		Unsupported
		Calculation for assignment rows		Unsupported
		Values to display		Unsupported
	Finish	Name		Unsupported
		Custom attributes		Unsupported
		Calculation for task and group summary rows		Unsupported
		Calculation for assignment rows		Unsupported
		Values to display		Unsupported
	Flag	Name		Unsupported
		Custom attributes		Unsupported
		Calculation for task and group summary rows		Unsupported
		Calculation for assignment rows		Unsupported
		Values to display		Unsupported
Task – Custom Fields	Number	Name		Unsupported
		Custom attributes		Unsupported
		Calculation for task and group summary rows		Unsupported
		Calculation for assignment rows		Unsupported

Top Level	Second Level	Third Level	Support Status
		Values to display	Unsupported
	Start	Name	Unsupported
		Custom attributes	Unsupported
		Calculation for task and group summary rows	Unsupported
		Calculation for assignment rows	Unsupported
		Values to display	Unsupported
	Text	Name	Unsupported
		Custom attributes	Unsupported
		Calculation for task and group summary rows	Unsupported
		Calculation for assignment rows	Unsupported
		Values to display	Unsupported
	Outline code	Name	Unsupported
		Custom attributes	Unsupported
		Calculation for task and group summary rows	Unsupported
		Calculation for assignment rows	Unsupported
		Values to display	Unsupported

PWA Settings

The table below lists the PWA Settings supported or unsupported for Project Online in IBM® Storage Protect for Cloud Microsoft™ 365:

PWA Settings

Top Level	Second Level	Third Level		Support Status
Personal settings	Manage My Alerts and Reminders	Tasks		Unsupported
		Status Reports	Unsupported	
		Queue Job Failures	Unsupported	
		Language Setting	Unsupported	
	Manage My Resources' Alerts and Reminders	My Team Members’ Tasks		Unsupported
		My Resource Requests		Unsupported
		My Resources' Status Reports		Unsupported
		Language Setting		Unsupported
	Manage Delegates	Delegation		Supported
		Filters		Supported
	Act as a Delegate			Unsupported
	My Queued Jobs			Unsupported

Top Level	Second Level	Third Level		Support Status
Look and feel	Manage Views **Note:** If the following views exist in the restore destination, the fields of the view in the backup that does not exist in destination will be added to the destination view, and the fields in the destination view that do not exist in the backup will not be removed: • **Select Tasks for Timeline** view for **Project** • **Summary** view for **Resource Assignments** • **Details** view for **My Work** • **Resource Team Assignments** view for **Team Tasks** • **My Timesheet** view for **Timesheet** • **Summary** view for **Portfolio Analyses** • **Summary** view for **Portfolio Analysis Project Selection**			Partially supported
	Grouping formats			Supported
	Gantt chart formats			Supported
	Quick launch			Supported
Workflow and Project Detail Pages	Enterprise project types	Name		Supported
		Description	Supported	
		Project ID	Supported	
		SharePoint Tasks List Project	Supported	
		Site Workflow Association **Note:** If the destination has a conflicting Enterprise project type, this setting will not be updated.	Partially supported	
Workflow and Project Detail Pages	Enterprise project types	New Project Page/Project Detail Pages **Note:** If the destination has a conflicting Enterprise project type, this setting will not be updated.		Partially supported
		Default	Supported	
		Departments	Unsupported	
		Image	Supported	
		Order	Supported	
		Site Creation	Supported	
		Synchronization	Supported	
		Site Language	Supported	
		Site Template	Supported	

Top Level	Second Level	Third Level			Support Status
		Project Plan Template		Unsupported	
		System Identification Data		Supported	
	Workflow phases	Name and Description	Name		Supported
			Description	Supported	
			System Identification Data	Supported	
	Workflow stages	Name and Description	Name		Supported
			Description	Supported	
		Description for Submit	Description (submit)		Supported
		Workflow Phase			Supported
		Workflow Stage Status Project Detail Page			Supported
		Visible Project Detail Pages			Supported
		Additional Settings for the Visible Project Detail Page			Supported
		Required Custom Fields			Supported
		Read Only Custom Fields			Supported
		Strategic Impact Behavior			Supported
		Project Check-In Required			Supported
		System Identification Data			Supported
Workflow and Project Detail Pages	Workflow Definition				Supported
	Project detail pages				Supported
Enterprise data	Enterprise custom fields and lookup tables	Enterprise Custom Fields	Name		Supported
			Description	Supported	
			Entity and Type	Supported	
			Custom Attributes	Supported	
			Department	Unsupported	
			Calculation for Summary Rows	Supported	
			Calculation for Assignment Rows	Supported	
			Values to Display	Supported	
			Behavior	Supported	
			System Identification Data	Supported	
			Last Updated	Unsupported	
			System Identification Data	Supported	

Top Level	Second Level	Third Level			Support Status
		Lookup Tables for Custom Fields **Note:** If there are conflicts, the **Type**, **Code Mask**, and **Lookup Table** fields will not be updated.	Name		Supported
			Type	Partially supported	
			Code Mask	Partially supported	
			Lookup Table	Supported	
			Last Updated	Partially supported	
	Enterprise calendars **Note:** Due to the API limitations, the Work Weeks cannot be restored.				Partially supported
Enterprise data	Resource center	Type **Note:** If there are conflicts, the **Budget,** and **Generic** fields will not be updated.		Type	Supported
				Budget	Partially supported
				Generic	Partially supported
		Identification Information		Display Name	Supported
				Email Address	Supported
				RBS	Unsupported
				Initials	Supported
				Hyperlink Name	Unsupported
				Hyperlink URL	Unsupported
				Account Status	Supported
		Assignment Attributes **Note:** If there are conflicts, the **Base Calendar**, **Timesheet Manager**, **Default Assignment Owner**, **Earliest Available**, and the **Latest Available** fields will not be updated.		Resource requires approval for all project assignments	Supported
				Resource can be leveled	Supported
				Base Calendar	Partially supported
				Default Booking Type	Supported

Top Level	Second Level	Third Level		Support Status
			Timesheet Manager	Partially supported
			Default Assignment Owner	Partially supported
			Earliest Available	Partially supported
			Latest Available	Partially supported
			Standard Rate	Unsupported
			Overtime Rate	Unsupported
			Current® Max. Units (%)	Unsupported
			Cost/Use	Unsupported
Enterprise data	Resource center	Departments		Supported
		Resource Custom Fields		Supported
		Security Groups		Supported
		Security Categories		Supported
		Global Permissions		Supported
		Group Fields	Group	Supported
			Code	Supported
			Cost Center	Supported
			Cost Type	Unsupported
		Team Details	Team Assignment Pool	Supported
			Team Name	Supported
		System Identification Data		Supported
	Reporting	Timephased Data		Supported
Time and task management	Fiscal periods	Manage Fiscal Period		Supported
		Adjust Fiscal Months	Supported	
	Time Reporting Periods	Define Bulk Period Parameters		Supported
		Define Batch Naming Convention		Supported
		Create Periods		Supported
	Line classifications	Edit, Enter Line Classification		Supported
	Timesheet Settings and Defaults	Project Web App Display		Supported
		Default Timesheet Creation Mode		Supported
		Timesheet Grid Column Units		Supported
		Default Reporting Units		Supported
		Hourly Reporting Limits		Supported
		Timesheet Policies		Supported
		Auditing		Supported
		Approval Routing		Supported
		Single Entry Mode		Supported

Top Level	Second Level	Third Level		Support Status
Time and task management	Administrative Time			Supported
	Task Settings and Display	Tracking Method		Supported
		Reporting Display		Supported
		Protect User Updates		Supported
		Define Near Future Planning Window		Supported
		Team Tasks and the Team Assignment Pool		Supported
	Manage Timesheets			Unsupported
	Timesheet Managers			Unsupported
Queue and Database Administration	Manage Queue Jobs	Filter Type		Unsupported
		Job History	Unsupported	
		Job Types	Unsupported	
		Job Completion States	Unsupported	
		Columns	Unsupported	
		Advanced Options	Unsupported	
		Jobs Grid (View, Retry, or Cancel Jobs):	Unsupported	
Operational Policies	Additional Server Settings	Project Professional Versions		Supported
		Enterprise Settings	Supported	
		Currency Settings	Supported	
		Resource Capacity Settings	Supported	
		Full-time Equivalent Calculation	Supported	
		Task Mode Settings	Supported	
		Notification Email Settings	Supported	
	Active Directory Resource Pool Synchronization	Active Directory Group **Note:** Cannot be restored to another tenant.		Partially supported
		Synchronization Status		Supported
		Sync options		Supported
Security	Manage Users	Identification Information		Supported
		User Authentication	Supported	
		Departments	Supported	
		Security Groups	Supported	
		Security Categories	Supported	
		Global Permissions	Supported	
	Manage Groups	Group Information		Supported
		Active Directory Group **Note:** Cannot be restored to another tenant.		Partially supported
		Users		Supported

Top Level	Second Level	Third Level	Support Status
		Categories	Supported
		Global Permissions	Supported
	Manage Categories	Name and Description	Supported
		Projects	Supported
		Resources	Supported
		Views	Supported
		Permissions	Supported
	Manage Security Templates	Name	Supported
		Category Permissions	Supported
		Global Permissions	Supported
	Manage User Sync Settings	Sync Options	Supported
		Sync Status	Supported
	Manage Delegates	Set Delegation Period	Supported
		Set Delegate	Supported
		Working on Behalf of	Supported

Exchange Online Data Types

The table below lists the data types supported or unsupported for Exchange Online in IBM® Storage Protect for Cloud Microsoft™ 365:

- Folder permissions are not supported.
- By default, the **Deleted Items** folder and the **Junk Emails** folder will be excluded from the backup for better performance. If you want to include the folders in your backup, contact IBM Software Support for assistance.

Learn about supported and unsupported Exchange Online for IBM® Storage Protect for Cloud Microsoft™ 365.

Data Type		Check Points	Default/Custom App Profile	Service Account (Obsolete)
Different types of Mailboxes	User’s mailbox		Supported	Supported

Data Type		Check Points	Default/Custom App Profile	Service Account (Obsolete)
	In-Place Archived Mailboxes **Note:** IBM® Storage Protect for Cloud Microsoft™ 365 also protects the archived mailboxes that have been auto-expanded. The **PersonMetadata** folder in the user’s mailbox is excluded from backup as a system folder. However, the **PersonMetadata** folder in the in-place archived mailbox is not a system folder and can be protected.		Supported	Supported
	Resource (Room and Equipment) Mailboxes		Supported	Supported
	Shared Mailboxes		Supported	Supported
Different types of Folders **Note:** The folder permissions are not supported.	Calendar	Long name, special characters, and display languages Folders in the same name Folder structure	Supported	Supported
	Contacts		Supported	Supported
	Conversation History		Supported	Supported
	Deleted Items		Supported	Supported
	Drafts		Supported	Supported
	Inbox		Supported	Supported

Data Type		Check Points	Default/Custom App Profile	Service Account (Obsolete)
	Journal **Note:** For the attachment of the Journal item that is added by the Insert pictures feature via Outlook desktop app, the attached picture cannot display after the restore. In the West Europe (Netherlands) data center, the body content of the journal in RTF format cannot display after the restore.		Supported	Supported
	Junk Email		Supported	Supported
	Notes®		Supported	Supported
	Outbox		Supported	Supported
	RSS Feeds		Supported	Supported
	Sub Folder		Supported	Supported
	Sent Items		Supported	Supported
	Tasks		Supported	Supported
Different types of Items and Item Properties	Mail	Content	Supported	Supported
		Sender	Supported	Supported
		Recipient (Including CC and BCC)	Supported	Supported
		Attachment	Supported	Supported
		Sent time	Supported	Supported
		Category	Supported	Supported
		Follow up	Supported	Supported
		Read/Unread	Supported	Supported
		Importance	Supported	Supported
		Inserted pictures or tables	Supported	Supported
		Signature	Supported	Supported
		Forward	Supported	Supported

Data Type		Check Points	Default/Custom App Profile	Service Account (Obsolete)
		Reply	Supported	Supported
		Font, art word, special character, and display languages	Supported	Supported
		Sort (by size; by conversation)	Supported	Supported
	Post	Intact content	Supported	Supported
		Post location	Supported	Supported
		Category	Supported	Supported
		Follow up	Supported	Supported
		Read/Unread	Supported	Supported
		Inserted pictures or tables	Supported	Supported
		Forward	Supported	Supported
		Reply	Supported	Supported
		Font, art word, special character, and display languages	Supported	Supported
	Appointment	Event	Supported	Supported
		Location	Supported	Supported
		Attendees	Supported	Supported
		Start time	Supported	Supported
		End time	Supported	Supported
		Duration	Supported	Supported
		Reminder	Supported	Supported
		Show as	Supported	Supported
		Repeat	Supported	Supported
		Mark as	Supported	Supported
		Online meeting	Supported	Supported
		Attachment	Supported	Supported
		Picture	Supported	Supported
		Category	Supported	Supported
		Font, art word, special character, and display languages	Supported	Supported
	Meeting	Event	Supported	Supported
		Location	Supported	Supported
		Attendees	Supported	Supported
		Start time	Supported	Supported
		End time	Supported	Supported
		Duration	Supported	Supported
		Reminder	Supported	Supported

Data Type		Check Points	Default/Custom App Profile	Service Account (Obsolete)
		Show as	Supported	Supported
		Repeat	Supported	Supported
		Mark as	Supported	Supported
		Online meeting	Supported	Supported
		Attachment	Supported	Supported
		Picture	Supported	Supported
		Category	Supported	Supported
		Font, art word, special character, and display languages	Supported	Supported
	Contact **Note:** Unsupported in GCC High environment	Name (Full name; First name; Middle name; Last name)	Supported	Supported
		Email (display as)	Supported	Supported
		Phone	Supported	Supported
		IM	Supported	Supported
		Work	Supported	Supported
		Address	Supported	Supported
		Notes®	Supported	Supported
		Other	Supported	Supported
		Picture	Supported	Supported
		Private	Supported	Supported
		Follow up	Supported	Supported
		Category	Supported	Supported
		Linked in	Supported	Supported
	Contact group **Note:** Unsupported in GCC High environment	Member	Supported	Supported
		Group Settings	Supported	Supported
	Task	Content	Supported	Supported
		Attachment	Supported	Supported
		Inserted pictures or tables	Supported	Supported
		Font, art word, special character, and display languages	Supported	Supported
		From	Supported	Supported
		Assign to	Supported	Supported
		Details	Supported	Supported

Data Type		Check Points	Default/Custom App Profile	Service Account (Obsolete)
		Recurrence	Supported	Supported
		Category	Supported	Supported
		Follow up	Supported	Supported
		Importance	Supported	Supported
		Private	Supported	Supported
		Status	Supported	Supported
		Complete	Supported	Supported
		Start date	Supported	Supported
		Due date	Supported	Supported
		Alert	Supported	Supported
	Task request	Content	Supported	Supported
		Attachment	Supported	Supported
		Inserted pictures or tables	Supported	Supported
		Font, art word, special character, and display languages	Supported	Supported
		From	Supported	Supported
		Assign to	Supported	Supported
		Details	Supported	Supported
		Recurrence	Supported	Supported
		Category	Supported	Supported
		Follow up	Supported	Supported
		Importance	Supported	Supported
		Private	Supported	Supported
		Status	Supported	Supported
		Complete	Supported	Supported
		Start date	Supported	Supported
		Due date	Supported	Supported
		Alert	Supported	Supported
	Note	Content	Supported	Supported
		Special character and display language	Supported	Supported
		Category	Supported	Supported
	Journal Entry	Type	Supported	Supported
		Subject	Supported	Supported
		Start time	Supported	Supported
		Duration	Supported	Supported
		Contact	Supported	Supported
		Category	Supported	Supported
		Content	Supported	Supported

Data Type		Check Points	Default/Custom App Profile	Service Account (Obsolete)
	Conversation	Participants	Supported	Supported
		Content	Supported	Supported
		Subject	Supported	Supported
		Modes	Supported	Supported
		Category	Supported	Supported
		Follow up	Supported	Supported
		Read/Unread	Supported	Supported
		Hyperlink	Supported	Supported
		Font, art word, special character, and display languages	Supported	Supported

Public Folders Data Types

Refer to the table below for the supported and unsupported data types of Public Folders in IBM® Storage Protect for Cloud Microsoft™ 365.

> **Note:** If the URL or the name of an object in Public Folder contains "\", "\" will be replaced by "/" on Restore overview page.

Learn about supported and unsupported Public Folders data types for IBM® Storage Protect for Cloud Microsoft™ 365.

Object Level		Check Points	Default/ Custom App Profile	Service Account (Obsolete)
Mail and Post items	Mail	Content	Supported	Supported
		Sender	Supported	Supported
		Recipient (Including CC and BCC)	Supported	Supported
		Attachment	Supported	Supported
		Sent time	Supported	Supported
		Category	Supported	Supported
		Read/Unread	Supported	Supported
		Importance	Supported	Supported
		Inserted pictures or tables	Supported	Supported
		Signature	Supported	Supported
		Forward	Supported	Supported
		Reply	Supported	Supported
Contact items	Contact	Name (Full name; First name; Middle name; Last name)	Supported	Supported
		Email (Display as)	Supported	Supported
		Phone	Supported	Supported

Object Level		Check Points	Default/ Custom App Profile	Service Account (Obsolete)
		IM	Supported	Supported
		Work	Supported	Supported
		Address	Supported	Supported
		Notes	Supported	Supported
		Other	Supported	Supported
		Picture	Supported	Supported
		Private	Supported	Supported
		Category	Supported	Supported
Info Path Form Items	Mail	Content	Supported	Supported
		Sender	Supported	Supported
		Recipient (Including CC and BCC)	Supported	Supported
		Attachment	Supported	Supported
		Sent time	Supported	Supported
		Category	Supported	Supported
		Read/Unread	Supported	Supported
		Importance	Supported	Supported
		Inserted pictures or tables	Supported	Supported
		Signature	Supported	Supported
		Forward	Supported	Supported
		Reply	Supported	Supported
Note items	Note	Content	Supported	Supported
		Category	Supported	Supported
Task items	Task request	Content	Supported	Supported
		Attachment	Supported	Supported
		Inserted pictures or tables	Supported	Supported
		From	Supported	Supported
		Assign to	Supported	Supported
		Details	Supported	Supported
		Recurrence	Supported	Supported
		Category	Supported	Supported
		Follow up	Supported	Supported
		Importance	Supported	Supported
		Private	Supported	Supported
		Status	Supported	Supported
		Complete	Supported	Supported
		Start date	Supported	Supported
		Due date	Supported	Supported
		Remember	Supported	Supported

Object Level		**Check Points**	**Default/ Custom App Profile**	**Service Account (Obsolete)**
Journal items	Journal Entry	Type	Supported	Supported
		Subject	Supported	Supported
		Start time	Supported	Supported
		Duration	Supported	Supported
		Contact	Supported	Supported
		Category	Supported	Supported
		Content	Supported	Supported
Calendar items	Appointment	Event	Supported	Supported
		Location	Supported	Supported
		Attendees	Supported	Supported
		Start time	Supported	Supported
		End time	Supported	Supported
		Duration	Supported	Supported
		Reminder	Supported	Supported
		Show as	Supported	Supported
		Repeat	Supported	Supported
		Mark as Complete	Supported	Supported
		Meeting	Supported	Supported
		Attachment	Supported	Supported
		Inserted pictures	Supported	Supported
		Category	Supported	Supported
		Font, art word, special character, and display languages	Supported	Supported
	Meeting	Event	Supported	Supported
		Location	Supported	Supported
		Attendees	Supported	Supported
		Start time	Supported	Supported
		End time	Supported	Supported
		Duration	Supported	Supported
		Reminder	Supported	Supported
		Show as	Supported	Supported
		Repeat	Supported	Supported
		Mark as	Supported	Supported
		Online meeting	Supported	Supported
		Attachment	Supported	Supported
		Inserted pictures	Supported	Supported
		Category	Supported	Supported
		Font, art word, special character, and display languages	Supported	Supported
Metadata	Enable	Enable	Supported	Supported

Object Level		Check Points	Default/ Custom App Profile	Service Account (Obsolete)
		Disable	Supported	Supported
	Folder Permission	User	Supported	Supported
		Group	Supported	Supported
	General	Name	Supported	Supported
		Path	Supported	Supported
		Total items	Supported	Supported
		Size	Supported	Supported
		Public folder mailbox	Supported	Supported
		Modified	Supported	Supported
		Maintain per-user read and unread information for this public folder	Supported	Supported
	Statistics	Associated items	Supported	Supported
		Deleted items	Supported	Supported
		Total size of associated items (MB)	Supported	Supported
		Total size of deleted items (MB)	Supported	Supported
		Owner count	Supported	Supported
		Contact count	Supported	Supported
		Last modified time	Supported	Supported
	Limits	Use organization quota defaults	Supported	Supported
		Issue warning at (MB)	Supported	Supported
		Prohibit post at (MB)	Supported	Supported
		Maximum item size: (MB)	Supported	Supported
		Use organization retention defaults	Supported	Supported
		Retain deleted items for (days)	Supported	Supported
		Use organization age limit defaults	Supported	Supported
		Age limit for folder content (days)	Supported	Supported

Microsoft™ 365 Groups Data Types

Refer to the table below for the supported and unsupported data types of Microsoft™ 365 Groups in IBM® Storage Protect for Cloud Microsoft™ 365.

> **Note:** IBM® Storage Protect for Cloud Microsoft™ 365 Groups can protect the Microsoft™ 365 Group team sites for the teams that are created in Microsoft™ Teams.

To protect Planner data in app context, you can now go to the App Management page in IBM® Storage Protect for Cloud interface to configure a Microsoft delegated app for IBM® Storage Protect for Cloud Microsoft™ 365 with the Protect Planner data option selected. The authentication user of this delegated app must have the Global administrator role and the Exchange license. When you are using app profile authentication for Auto Discovery, IBM® Storage Protect for Cloud Microsoft™ 365 will use this delegated app for the backup and restore of the Planner data.

For the support status of data types in the Microsoft™ 365 Groups team site, refer to “SharePoint Sites Data Types” on page 181.

Learn about supported and unsupported Microsoft™ 365 Groups Data Types for IBM® Storage Protect for Cloud.

Object Level			Details	Default/Custom App Profile	Service Account (Obsolete)	Note
Microsoft™ 365 Group Mailbox	Conversations (Mails)		Content	Supported	Supported	
			Sender	Supported	Supported	
			Recipient (Including CC and BCC)	Supported	Supported	
			Attachment	Supported	Supported	
			Sent time	Supported	Supported	
			Category	Supported	Supported	
			Follow up	Supported	Supported	
			Read/Unread	Supported	Supported	
			Importance	Supported	Supported	
			Inserted pictures or tables	Supported	Supported	
			Signature	Supported	Supported	
			Forward	Supported	Supported	
			Reply	Supported	Supported	
			Font, art word, special character, and display languages	Supported	Supported	
			Sort (by size; by conversation)	Supported	Supported	
	Calendar	Appointments	Event	Supported	Supported	
			Location	Supported	Supported	
			Attendees	Supported	Supported	
			Start time	Supported	Supported	
			End time	Supported	Supported	
			Duration	Supported	Supported	
			Reminder	Supported	Supported	
			Show as	Supported	Supported	
			Repeat	Supported	Supported	

Object Level		Details	Default/Custom App Profile	Service Account (Obsolete)	Note
		Mark as	Supported	Supported	
		Online meeting	Supported	Supported	
		Attachment	Supported	Supported	
		Picture	Supported	Supported	
		Category	Supported	Supported	
		Font, art word, special character, and display languages	Supported	Supported	
	Meetings	Event	Supported	Supported	
		Location	Supported	Supported	
		Attendees	Supported	Supported	
		Start time	Supported	Supported	
		End time	Supported	Supported	
		Duration	Supported	Supported	
		Reminder	Supported	Supported	
		Show as	Supported	Supported	
		Repeat	Supported	Supported	
		Mark as	Supported	Supported	
		Online meeting	Supported	Supported	
		Attachment	Supported	Supported	
		Picture	Supported	Supported	
		Category	Supported	Supported	
		Font, art word, special character, and display languages	Supported	Supported	
Group Type		Microsoft™ 365 Group	Supported	Supported	
		Distribution Group	Unsupported	Unsupported	
		Mail-enabled Security Group	Unsupported	Unsupported	
		Security Group	Unsupported	Unsupported	
Group setting		Follow in inbox	Unsupported	Unsupported	

Object Level			Details	Default/Custom App Profile	Service Account (Obsolete)	Note
Planner **Note:** Without the Delegated app configured, the planner data is unsupported in app context.	Board		Bucket	Supported	Supported	
		Task	Task Member	Supported	Supported	
			Progress	Supported	Supported	
			Start Time	Supported	Supported	
			Due Date	Supported	Supported	
			Description	Supported	Supported	
			Checklist	Supported	Supported	
			Attachment	Supported	Supported	
			Comments	Supported	Supported	
			Label	Supported	Supported	
			Priority	Supported	Supported	
	Chart		Status	Supported	Supported	
			Member	Supported	Supported	
Group Information			Name	Supported	Supported	
			Description	Supported	Supported	
			Privacy	Supported	Supported	
			Hide from my organization’s global address list	Unsupported	Unsupported	
			Aliases	Unsupported	Unsupported	
			Send copies of group conversations and events to group members’ inboxes	Unsupported	Supported	
			Let people outside the organization email the group	Unsupported	Supported	
			Language for group-related notifications	Unsupported	Unsupported	
			Manage group email setting	Unsupported	Unsupported	

Object Level	Details	Default/Custom App Profile	Service Account (Obsolete)	Note
	Send all group conversations and events to members' inboxes. They can stop following this group later if they want to	Unsupported	Supported	API limitation
Group Membership	Assigned	Supported	Supported	
	Dynamic	Supported	Supported	

Teams Data Types

For the support status of Teams data types, note the following and refer to the tables in the following sections:

- With the update of Teams API, Teams can now be protected by using app profile authentication. By leveraging App Context when connecting your Microsoft™ 365 environment to IBM® Storage Protect for Cloud, IBM® does not store any of your administrative credentials (only consent) and will not require service users to be the owners and members of your Teams in order to manage and protect them. With this update, many of the per-user throttling limits that are common with service accounts can be avoided.
- The restore of the Team's owner and members may take a couple of hours to synchronize to the destination Teams interface. In addition, the guest users in Teams cannot be restored due to API limitations.
- Private Channels in Teams can now be protected with limitations. For details, refer to "Components in Private/Shared Channels" on page 234.
- IBM® Storage Protect for Cloud Microsoft™ 365 does not support protecting Teams Chats (personal chats).
- For the support status of data types in the team's Team site, refer to "SharePoint Sites Data Types" on page 181.
- Most tab types can be created, but many cannot be configured currently through the API. For the support of tabs, the current release is designed to recover the tabs that have been deleted. The current release does not support updating existing tabs to previous settings and configurations apart from the following five tabs: Planner, Word, Excel, PowerPoint, and PDF.

> **Note:** If you have performed a restore for any tabs in one of the six types before and at that time the configurations were not being restored to the destination, you can now remove that tab from the Team and run the restore job again. The configurations can be restored properly.

Refer to the following tables:

- "Components in Teams Channel" on page 230
- "Components in Private/Shared Channels" on page 234
- "Settings and Permissions" on page 238
- "Planner Data" on page 240
- "SharePoint Sites Data Types" on page 181
- "Archived Teams" on page 240
- Microsoft Education Environment

Components in Teams Channel

Refer to the following table for the supported and unsupported status of the components in Channel, and the supported and unsupported status for the data that are added or attached to the Channel through the corresponding methods.

Conversations

Note the following for Conversations:

- Conversations can be restored as posts or to HTML files.
    - If the conversations are restored to HTML files, these restored files are stored in the **Files** tab. To open or download the attached files in the restored conversation, you can right-click the file link and select **Open in new tab** or **Open in new window**. Note that due to the API limitations, the conversation time in the restored HTML file is UTC time.
    - The restore channel conversations as posts, you must have a Microsoft Delegated app configured in your tenant. Note that the authentication user of the delegated app must have a Teams license and an Exchange Online license. A restore job to restore conversations as posts will add the authentication user to Teams members or private channel members and then automatically remove them after the restore job completes. The conversation time restored in posts will follow UTC time.
- Tab conversations will be restored with Channel conversations to HTML files or posts.
- The conversations that are generated by creating meetings will be restored with no details.
- If Teams has a new app installed, a conversation for the new app will be started. After the conversation is restored to the HTML file, there may be extra strings and lines displayed in the HTML file.

Components/Properties		**Default/Custom App Profile**		**Service Account (Obsolete)**		**Comment**
		Restore to HTML file	***Restore as Posts***	***Restore to HTML file***	***Restore as Posts***	
Format	Add subject	Supported	Supported	Supported	Supported	
	Mention/ Tag (@)	Supported	Supported	Supported	Supported	The link cannot be kept after being restored to the HTML file.
	Bold	Supported	Supported	Supported	Supported	
	Italic	Supported	Supported	Supported	Supported	
	Underline	Supported	Supported	Supported	Supported	
	Strikethrough	Supported	Supported	Supported	Supported	
	Text highlight color	Supported	Supported	Supported	Supported	
	Font color	Supported	Supported	Supported	Supported	
	Font size	Supported	Supported	Supported	Supported	
	Monospaced	Supported	Supported	Supported	Supported	
	Heading	Supported	Supported	Supported	Supported	
	Paragraph	Supported	Supported	Supported	Supported	
	Decrease indent	Supported	Supported	Supported	Supported	

Components/Properties		**Default/Custom App Profile**		**Service Account (Obsolete)**		**Comment**
		Restore to HTML file	***Restore as Posts***	***Restore to HTML file***	***Restore as Posts***	
	Increase indent	Supported	Supported	Supported	Supported	
	Bulleted list	Supported	Supported	Supported	Supported	
	Numbered list	Supported	Supported	Supported	Supported	
	Quote	Supported	Supported	Supported	Supported	
	Insert link	Partially Supported	Supported	Supported	Partially Supported	
	Code Snippet	Supported	Unsupported	Unsupported	Supported	API limitation
	Inset horizontal rule	Supported	Supported	Supported	Supported	
	Insert table	Supported	Supported	Supported	Supported	
	Mark as important	Supported	Supported	Supported	Supported	
	Show for me	Unsupported	Unsupported	Unsupported	Unsupported	API limitation
	Show for members	Unsupported	Unsupported	Unsupported	Unsupported	API limitation
Post in multiple channels		Unsupported	Unsupported	Unsupported	Unsupported	
Announcement type post's specific elements	Background	Unsupported	Unsupported	Unsupported	Supported	
	Icon	Unsupported	Unsupported	Unsupported	Supported	
	Color scheme	Unsupported	Unsupported	Unsupported	Supported	
	Subheader	Supported	Supported	Supported	Supported	
	Headline	Unsupported	Unsupported	Unsupported	Supported	
Attach: **Note:** In the restored HTML file, you can right-click the file link and then click **Open in new tab** or **Open in new window** to open or download the file.	Recent	Supported	Supported	Supported	Supported	
	Browse Teams and Channels	Supported	Supported	Supported	Supported	
	OneDrive	Supported	Supported	Supported	Supported	
	Upload from my computer	Supported	Supported	Supported	Supported	
Emoji		Supported	Supported	Supported	Supported	

Components/Properties	**Default/Custom App Profile**		**Service Account (Obsolete)**		**Comment**
	Restore to HTML file	***Restore as Posts***	***Restore to HTML file***	***Restore as Posts***	
Giphy	Supported	Supported	Supported	Supported	
Praise	Supported	Unsupported	Unsupported	Partially Supported	
Sticker	Supported	Supported	Supported	Supported	
Stream	Unsupported	Supported	Unsupported	Supported	
Form	Unsupported	Supported	Unsupported	Partially Supported	
News	Partially Supported	Supported	Partially Supported	Partially Supported	
Places	Partially Supported	Supported	Partially Supported	Partially Supported	The links in the Stocks, Weather, Places, and Wikipedia data cannot be restored, and the map in the restored Places is not available. To view the map in the restored Places, access Teams using the same browser, and then reopen the restored file.
Stocks	Unsupported	Unsupported	Unsupported	Partially Supported	
Weather	Partially Supported	Partially Supported	Partially Supported	Partially Supported	
Wikipedia Search	Partially Supported	Partially Supported	Partially Supported	Partially Supported	
YouTube	Partially Supported	Partially Supported	Partially Supported	Partially Supported	
Post	Supported	Supported	Supported	Supported	
Voice Message	Unsupported	Unsupported	Unsupported	Unsupported	
Reply	Supported	Supported	Supported	Supported	
Edit Post/Reply	Partially Supported	Unsupported	Partially Supported	Unsupported	The **Edited** status of a post or reply cannot be kept.

Components/Properties		Default/Custom App Profile		Service Account (Obsolete)		Comment
		Restore to HTML file	*Restore as Posts*	*Restore to HTML file*	*Restore as Posts*	
Delete post/Reply		Unsupported	Supported	Unsupported	Supported	The message for a post or a reply being deleted cannot be kept.
Notification		Unsupported	Unsupported	Unsupported	Unsupported	
Mark as unread		Unsupported	Unsupported	Unsupported	Unsupported	
Like/Unlike		Unsupported	Unsupported	Unsupported	Unsupported	
Copy Link		Supported	Supported	Supported	Supported	
The “Save this message” mark		Unsupported	Unsupported	Unsupported	Unsupported	
Get email address	Send email to channel	Partially supported	Unsupported	Partially supported	Unsupported	The **To information** and the **Download original email** link are not kept in the restored HTML file.

Others

Object	Component/Property		Default/Custom App Profile		Service Account	Comment
Files	New	Folder		Supported	Supported	
		Word document	Supported	Supported		
		Excel spreadsheet	Supported	Supported		
		PowerPoint presentation	Supported	Supported		
		OneNote notebook	Supported	Supported		
		Forms for Excel	Supported	Supported		
	Send email to channel			Supported	Supported	
	Upload			Supported	Supported	
	Add cloud storage	SharePoint		Unsupported	Unsupported	API limitation
		Dropbox		Unsupported	Unsupported	
		Box		Unsupported	Unsupported	

Object	Component/Property	Default/Custom App Profile	Service Account	Comment
	ShareFile	Unsupported	Unsupported	
	Google Drive	Unsupported	Unsupported	
Tab	Add a tab	Supported	Supported	Restore job supports adding your tabs back. When configuring restore settings, select **Merge** as the container level conflict resolution.
	Word Excel PowerPoint PDF Document library Planner	Supported	Supported	Supports adding the tabs back and update the tabs to the previous settings and configurations.
	Other tabs	Partially supported	Partially supported	Apart from the six tabs above, the restore for tabs now can only support adding them back. You must manually configure the tab settings to connect your data source.
Meetings	Body	Supported	Supported	
	Title	Supported	Supported	
	Location	Supported	Supported	
	Start Time	Supported	Supported	
	End Time	Supported	Supported	
	Details	Supported	Supported	
	Channel	Supported	Supported	
	Invite People	Supported	Supported	
	Organizer	Supported	Supported	

Components in Private/Shared Channels

Refer to the following table for the supported and unsupported status of the components in private or shared channels, and the supported and unsupported status for the data that is added or attached to the private/ shared channels through the corresponding methods.

Note the following for the private/shared channels:

- If you are using service account authentication for the backup of Teams' Private Channel, the service account must be the owner of the Private Channel.
- Private/shared channels can only be restored through the time-based restore wizard, and private/shared channels do not support out-of-place restore.

Conversations

Components/Properties		**App Profile**		**Service Account (Obsolete)**		**Comment**
		Restore to HTML file	**Restore as Posts**	**Restore to HTML file**	**Restore as Posts**	
Format	Add subject	Supported	Supported	Supported	Supported	
	Mention (@)	Supported	Supported	Supported	Supported	
	Bold	Supported	Supported	Supported	Supported	
	Italic	Supported	Supported	Supported	Supported	
	Underline	Supported	Supported	Supported	Supported	
	Strikethrough	Supported	Supported	Supported	Supported	
	Text highlight color	Supported	Supported	Supported	Supported	
	Font color	Supported	Supported	Supported	Supported	
	Font size	Supported	Supported	Supported	Supported	
	Monospaced	Supported	Supported	Supported	Supported	
	Heading	Supported	Supported	Supported	Supported	
	Paragraph	Supported	Supported	Supported	Supported	
	Decrease indent	Supported	Supported	Supported	Supported	
	Increase indent	Supported	Supported	Supported	Supported	
	Bulleted list	Supported	Supported	Supported	Supported	
	Numbered list	Supported	Supported	Supported	Supported	
	Quote	Supported	Supported	Supported	Supported	
	Insert link	Partially Supported	Partially Supported	Partially Supported	Partially Supported	Cannot preview the link
	Code Snippet	Supported	Supported	Supported	Supported	
	Inset horizontal rule	Supported	Supported	Supported	Supported	
	Insert table	Supported	Partially Supported	Supported	Partially Supported	

Components/Properties		**App Profile**		**Service Account (Obsolete)**		**Comment**
		Restore to HTML file	**Restore as Posts**	**Restore to HTML file**	**Restore as Posts**	
	Mark as important	Supported	Supported	Supported	Supported	
Post in multiple channels	Messages	Supported	Supported	Supported	Supported	
	Post in	Unsupported	Unsupported	Unsupported	Unsupported	
Announcement type post's specific elements	Background	Unsupported	Unsupported	Unsupported	Supported	
	Color scheme	Unsupported	Supported	Unsupported	Supported	
	Subheader	Supported	Supported	Supported	Supported	
	Headline	Unsupported	Supported	Unsupported	Supported	
Attach: **Note:** In the restored HTML file, you can right-click the file link and then click **Open in new tab** or **Open in new window** to open or download the file.	Recent	Partially Supported	Supported	Partially Supported	Supported	
	Browse Teams and Channels	Partially Supported	Supported	Partially Supported	Supported	
	OneDrive	Partially Supported	Supported	Partially Supported	Supported	
	Upload from my computer	Partially Supported	Supported	Partially Supported	Supported	
Emoji		Supported	Supported	Supported	Supported	
Giphy		Supported	Supported	Supported	Supported	
Sticker		Partially Supported	Supported	Partially Supported	Supported	
Post		Supported	Supported	Supported	Supported	
Voice Message		Unsupported	Unsupported	Unsupported	Unsupported	
Reply		Supported	Supported	Supported	Supported	
Edit Post/Reply		Partially Supported	Partially Supported	Partially Supported	Unsupported	The **Edited** status of a post or reply cannot be kept.
Delete post/Reply		Unsupported	Unsupported	Unsupported	Supported	The message for a post or a reply being deleted cannot be kept.
Mark as unread		Unsupported	Unsupported	Unsupported	Unsupported	

Components/Properties		App Profile		Service Account (Obsolete)		Comment
		Restore to HTML file	**Restore as Posts**	**Restore to HTML file**	**Restore as Posts**	
Like/Unlike		Unsupported	Unsupported	Unsupported	Unsupported	
The “Save this message” mark		Unsupported	Unsupported	Unsupported	Unsupported	
Get email address	Send email to channel	Unsupported	Unsupported	Unsupported	Unsupported	The **To** information and the **Download original email** link are not kept in the restored HTML file.
Image		Partially Supported	Supported	Partially Supported	Supported	
Recording **Note:** The Recording refers to system conversations during the recording process rather than the actual recorded file.		Unsupported	Unsupported	Unsupported	Unsupported	
Meeting		Supported	Supported	Supported	Supported	

Others

Objects	Components/Properties		App Profile	Service Account	Comment
Files	New	Folder	Supported	Supported	
		Word document	Supported	Supported	
		Excel spreadsheet	Supported	Supported	
		PowerPoint presentation	Supported	Supported	
		OneNote notebook	Supported	Supported	
	Send email to channel		Supported	Supported	
	Upload		Supported	Supported	
	Add cloud storage	SharePoint	Unsupported	Unsupported	API limitation
		Dropbox	Unsupported	Unsupported	
		Box	Unsupported	Unsupported	
		ShareFile	Unsupported	Unsupported	
		Google Drive	Unsupported	Unsupported	

Objects	Components/Properties	App Profile	Service Account	Comment
Tab	Add a tab: Excel, Word, PowerPoint, PDF, Document library	Supported	Supported	Supports adding the tabs back and update the tabs to the previous settings and configurations for the listed tabs.
Meetings	Body	Supported	Supported	
	Title	Supported	Supported	
	Location	Supported	Supported	
	Start Time	Supported	Supported	
	End Time	Supported	Supported	
	Details	Supported	Supported	
	Channel	Supported	Supported	
	Invite People	Supported	Supported	
	Organizer	Supported	Supported	

Settings and Permissions

Example

Refer to the table below for the supported and unsupported settings and permissions.

Components	Settings/Permissions			Default/Custom App Profile	Service Account (Obsolete)	Comment
Teams	Name			Supported	Supported	
	Description			Supported	Supported	
	Privacy			Partially Supported	Partially Supported	**Org-wide** cannot be restored to the destination. If the destination policy is **Org-wide**, the restore job cannot update it to other values apart from that **Private** is being restored.
	Send copies of group conversations and events to group members' inboxes			Unsupported	Supported	
	Let people outside the organization email the group			Unsupported	Supported	
	Show/Hide team What used to be **Favorite** and **Remove Favorite** is now **Show** and **Hide**.			Unsupported	Unsupported	Microsoft API limitation
	Tags			Unsupported	Unsupported	
	Hidden			Unsupported	Unsupported	
	Create a team from an existing Microsoft 365 group			Supported	Supported	
Members	Add member			Supported	Supported	The restore of the Team's owner and members may take a couple of hours to synchronize to the destination Teams interface.
	Add owner			Supported	Supported	
Channel You cannot change the user role for members in Private Channels.	Name			Supported	Supported	
	Description			Supported	Supported	
	Owner/member			Supported	Supported	
	Privacy	Standard		Supported	Supported	
		Private				
	Automatically favorite this channel for the whole team			Unsupported	Unsupported	Microsoft API limitation
	Pin			Unsupported	Unsupported	
	Notification	All activities		Unsupported	Unsupported	
		Off		Unsupported	Unsupported	
		All new posts	Banner and feed	Unsupported	Unsupported	
			Only show in feed	Unsupported	Unsupported	
			Off	Unsupported	Unsupported	
		Channel mentions	Banner and feed	Unsupported	Unsupported	
			Only show in feed	Unsupported	Unsupported	
			Off	Unsupported	Unsupported	
	Channel setting	Permission	Channel moderation	Unsupported	Unsupported	
			Who can start a new post?	Unsupported	Unsupported	
			Team member permissions	Unsupported	Unsupported	
	Show for me			Unsupported	Unsupported	Microsoft API limitation

Components	Settings/Permissions			Default/Custom App Profile	Service Account (Obsolete)	Comment
	Show for members			Unsupported	Unsupported	Microsoft API limitation
	Hidden			Unsupported	Unsupported	
Settings	Team picture			Unsupported	Unsupported	Microsoft API limitation
		Allow creating and updating channels		Supported	Supported	
	Member permissions	Allow members to delete and restore channels		Supported	Supported	
		Allow members to add and remove apps		Supported	Supported	
		Allow members to upload custom apps		Unsupported	Unsupported	Microsoft API limitation
		Allow members to create, update, and remove tabs		Supported	Supported	
		Allow members to create, update, and remove connectors		Supported	Supported	
		Give members the option to delete their messages		Supported	Supported	
		Give members the option to edit their messages		Supported	Supported	
		General Channel	Anyone can post messages	Unsupported	Unsupported	The setting will be restored to the default option: **Anyone can post messages.**
			Anyone can post; show an alert that posting will notify everyone (useful for large teams)			
			Only owners can post messages			
	Guest permissions	Allow creating and updating channels		Supported	Supported	
		Allow guests to delete channels		Supported	Supported	
	@Mentions	Allow @team or @[team name] mentions (this will send a notification to everyone on the team)		Supported	Supported	
		Allow @channel or @[channel name] mentions (this will send a notification to everyone who has favorited the channel being mentioned)		Supported	Supported	
	Team code			Unsupported	Unsupported	
	Tags > Who can add tags			Unsupported	Unsupported	
	Fun stuff	Enable Giphy for this team		Supported	Supported	
		Filter out inappro-priate content using one of the settings below	Strict	Supported	Supported	
			Allow all content	Unsupported	Unsupported	Microsoft API limitation
			Moderate	Supported	Supported	
		Enable stickers and memes		Supported	Supported	
		Enable stickers and memes		Supported	Supported	
		Allow memes to be uploaded		Supported	Supported	
Analytics				Supported	Supported	
Apps	Forms			Supported	Supported	The restore of Teams apps only supports adding the apps back to your Teams. For the apps whose data is stored outside Teams, the restore job cannot restore the apps' data. To ensure a successful backup and restore for Teams' Apps when using service account authentication, the service account must have the Team Owner role.
	OneNote			Supported	Supported	
	Planner			Supported	Supported	For the details of Planner data supported status, refer to Planner Data.
	Stream			Supported	Supported	
	Others (Go to store)			Supported	Supported	
Membership type			Assigned	Supported	Supported	
			Dynamic			

Planner Data

Refer to the table below for the supported Planner data and note the following issues for Planner backup and restore:

Authentication Method

- Planner data now supports app profile authentication.

General

- Due to limitations in the Microsoft API, Planner Premium cannot be protected.
- Microsoft™ Graph API now only allows you to create up to 200 plans in a Team or Group. Therefore, if the number of plans in the destination Microsoft™ 365 group or team reaches 200, the restore of the remaining plans that need to be created in the destination will fail.
- When restoring plans, the plan ID and plan name will be used to identify the plan. If the destination has a plan using the same ID, the backup data of the plan will be updated and merged into the destination plan. If there is no identical plan using the same ID, refer to the following:
  - If there is only one destination plan using the same name as the backup, the backup data of the plan will be updated and merged into the destination plan.
  - If there is no plan using the same name or more than one plan using the same name in the destination, the restore job will create new plans for restoring the plans in the backup.
- If you only selected plans to restore to a target channel, the plan cannot be automatically added to the Channel tabs. You must manually add the Planner app to the tab and select the restored plan to add.
- By default, the restore job will restore the Planner task's attachment link to the target. If you want to restore the latest files in the attachment of the Planner tasks, contact the IBM Software SupportIBM Support team for assistance.

Data Type			**Default/Custom App Profile**	**Service Account/ Delegated App (Obsolete)**
Plan			Supported	Supported
Board	Bucket		Supported	Supported
	Task	Task Member	Supported	Supported
		Progress	Supported	Supported
		Start Time	Supported	Supported
		Due Date	Supported	Supported
		Description	Supported	Supported
		Checklist	Supported	Supported
		Attachment	Supported	Supported
		Comments	Supported	Supported
		Label	Supported	Supported
		Priority	Supported	Supported
Chart		Status	Supported	Supported
		Members	Supported	Supported

Archived Teams

Example

Refer to the table below for the supported and unsupported status of backup and restore for the archived teams.

Note: The archived status cannot be kept after restore, and the archived teams will be restored to active. However, if the team site has been set to read-only for members, the in-place restore for the associated site will fail.

Object Type	Backup Status	Restore Status	Note
Teams mailbox	Supported	Supported	
Teams team site	Supported	Supported	
Public channels	Supported	Supported	
Private channels	Supported	Supported	
Planner	Supported	Supported	
Tabs	Supported	Supported	
Apps	Supported	Supported	

Microsoft Education Environment

Example

Refer to the table below for the supported and unsupported status of backup and restore for Teams in Microsoft Education Environment.

Object Type	Backup Status	Restore Status
Team	Supported	Supported
Team Site	Supported	Supported
Sites	Supported	Supported
List/Library	Supported	Supported
Folder	Supported	Supported
Document	Supported	Supported
Item	Supported	Supported
Apps	Supported	Supported
Team Mailbox	Supported	Supported
Folder in Mailbox	Supported	Supported
Mailbox Item	Supported	Supported
Plan	Supported	Supported
Task	Supported	Supported
Public Channel	Supported	Supported
Channel Conversation (HTML)	Supported	Supported
Channel Conversation (Post)	Supported	Supported
Channel File	Supported	Supported
Private Channel Conversation (HTML)	Supported	Supported
Private Channel Conversation (Post)	Supported	Supported
Private Channel File	Supported	Supported
Class Notebook	Supported	Supported
Assignments	Unsupported	Unsupported

Object Type	Backup Status	Restore Status
Grades	Unsupported	Unsupported
Insights	Unsupported	Unsupported
Home Page	Supported	Partially supported (The template can be restored, but the data in it cannot be restored.)
Class Notebook	Supported	Partially supported (The template can be restored, but the data in it cannot be restored.)
Classwork	Supported	Partially supported (The template can be restored, but the data in it cannot be restored.)
Assignments	Supported	Partially supported (The template can be restored, but the data in it cannot be restored.)
Grades	Supported	Partially supported (The template can be restored, but the data in it cannot be restored.)
Reflect	Supported	Supported
Insights	Supported	Supported
Parents	Supported	Supported
Plc Notebook	Supported	Partially supported (The template can be restored, but the data in it cannot be restored.)
Staff Notebook	Supported	Partially supported (The template can be restored, but the data in it cannot be restored.)
Meeting	Supported	Supported
Group Conversation	Supported	Supported

Teams Chat Data Types

Refer to the table below for the supported and unsupported data types of Teams chats.

Note the following:

- The Microsoft Teams Chat backup service can protect the 1:1 chats and the group chats in Teams.
- For the **default Microsoft Graph API**, the backup of chats started by external users is not supported, but chats started by internal users and including external users can be protected. For the **Teams Export API model B**, only plain text can be protected.
- Only the default Microsoft Graph API can be used to protect Teams Chat in GCC environments.
- Due to API limitations, the self chat in Teams cannot be protected.
- Due to API limitations and unique message formats, certain chat messages sent by apps within Microsoft Teams cannot be protected. Given the extensive range of apps in Teams, it is not feasible to maintain a comprehensive support list for all of them. Please be aware of this limitation and consider this aspect when integrating with various apps with Teams.

Components/Properties		Teams Export API	Microsoft Graph API	Comment
Format	Mention/Tag (@)	Supported	Supported	The link cannot be kept after being restored to the HTML file.
	Bold	Supported	Supported	
	Italic	Supported	Supported	
	Underline	Supported	Supported	
	Strikethrough	Supported	Supported	
	Text highlight color	Supported	Supported	
	Font color	Supported	Supported	
	Font size	Supported	Supported	
	Monospaced	Supported	Supported	
	Heading	Supported	Supported	
	Paragraph	Supported	Supported	
	Decrease indent	Supported	Supported	
	Increase indent	Supported	Supported	
	Bulleted list	Supported	Supported	
	Numbered list	Supported	Supported	
	Quote	Supported	Supported	
	Insert link	Supported	Supported	
	Code Snippet	Supported	Supported	
	Inset horizontal rule	Supported	Supported	
	Insert table	Partially Supported	Partially Supported	Only the content can be restored.
Delivery Options	Standard	Supported	Supported	
	Important	Supported	Supported	
	Urgent	Unsupported	Unsupported	
Attach File	OneDrive	Supported	Supported	
	Upload from my computer	Supported	Supported	
Loop components	Bulleted list	Unsupported	Unsupported	
	Numbered list	Unsupported	Unsupported	
	Checklist	Unsupported	Unsupported	
	Paragraph	Unsupported	Unsupported	
	Table	Unsupported	Unsupported	
	Task list	Unsupported	Unsupported	
	progress tracker	Unsupported	Unsupported	
	Q&A	Unsupported	Unsupported	
	Voting table	Unsupported	Unsupported	
Emoji		Supported	Supported	
Giphy		Supported	Supported	
Sticker		Supported	Supported	

Components/Properties		Teams Export API	Microsoft Graph API	Comment
Apps	Stream	Unsupported	Unsupported	The links in the Stocks, Weather, Places, and Wikipedia data cannot be restored, and the map in the restored Places is not available. To view the map in the restored Places, access Teams using the same browser, and then reopen the restored file.
	Update	Unsupported	Unsupported	
	Praise	Unsupported	Unsupported	
	Form	Unsupported	Unsupported	
	News	Partially Supported	Partially Supported	
	Places	Supported	Supported	
	Power BI	Unsupported	Unsupported	
	Stocks	Unsupported	Unsupported	
	Weather	Partially Supported	Partially Supported	
	Wikipedia Search	Partially Supported	Partially Supported	
Action	Post	Supported	Supported	
	Reply	Supported	Supported	
	Edit Post/Reply	Supported	Supported	
	Delete Post/Reply	Unsupported	Unsupported	
	Reaction: Like	Unsupported	Unsupported	
	The “Save this message” mark	Unsupported	Unsupported	
	Translate	Unsupported	Unsupported	
Message Type	Image (screenshot)	Supported	Supported	
	Image (attachment)	Unsupported	Unsupported	
	Voice Message	Unsupported	Unsupported	
	Recordings/Video	Unsupported	Unsupported	

Viva Engage Data Types

The table below lists the data types supported or unsupported for Viva Engage in IBM® Storage Protect for Cloud Microsoft™ 365:

Note:

- Viva Engage services currently support in place recovery only (restoring to the original location), meaning the Viva Engage community needs to be there already, as well as to export files and conversations.
- The External Network, Private Message, and Classic Viva Engage are not supported.
- Only the message content and comment are supported for the Discussions, Questions, Praise, and Poll messages. In the current release, Viva Engage messages are only available in the time-based recovery wizard and will be restored to HTML files.

Data Type		Default Viva Engage App
Internal Network	Viva Engage Group	Supported
	Viva Engage community Members	Supported
	Viva Engage community favorites status (Only in new Viva Engage view)	Unsupported

	Viva Engage Group settings	Name	Unsupported
		Description	Unsupported
		Image	Unsupported
		Who can view conversations and post messages?	Unsupported
		Default publisher type	Unsupported
		Pattern (Only in classic Viva Engage view)	Unsupported
	Mute/Unmute Viva Engage community status (Only in new Viva Engage view)		Unsupported
	Viva Engage community mute for Network status (Only in new Viva Engage view)		Unsupported
	Viva Engage community cover photo (Only in new Viva Engage view)		Unsupported
	Info		Unsupported
	Pinned		Unsupported
	Related Groups (Only in classic Viva Engage view)		Unsupported
	Discussion	Message content	Supported
		People in message	Unsupported
		Announcement	Unsupported
		Topic	Unsupported
		Attachment	Unsupported
		GIF	Unsupported
		Like	Unsupported
		Comment	Supported
		Share	Unsupported
		Conversation open/close status	Unsupported
		Pin/Unpin status	Unsupported
		Follow/Unfollow in Inbox status	Unsupported
		Feature Conversation	Unsupported
		Read/Unread property	Unsupported
	Question	Message content	Supported
		People in message	Unsupported
		Announcement	Unsupported
		Topic	Unsupported
		Attachment	Unsupported
		GIF	Unsupported
		Like	Unsupported
		Comment	Supported
		Share	Unsupported
		Conversation open/close status	Unsupported
		Pin/Unpin status	Unsupported

		Follow/Unfollow in Inbox status	Unsupported
		Feature Conversation	Unsupported
		Read/Unread property	Unsupported
	Praise	Message content	Supported
		People in message	Unsupported
		Announcement	Unsupported
		Topic	Unsupported
		Attachment	Unsupported
		GIF	Unsupported
		Like	Unsupported
		Comment	Supported
		Share	Unsupported
		Conversation open/close status	Unsupported
		Pin/Unpin status	Unsupported
		Follow/Unfollow in Inbox status	Unsupported
		Feature Conversation	Unsupported
		Read/Unread property	Unsupported
	Poll	Message content	Supported
		People in message	Unsupported
		Announcement	Unsupported
		Topic	Unsupported
		Attachment	Unsupported
		GIF	Unsupported
		Like	Unsupported
		Comment	Supported
		Share	Unsupported
		Conversation open/close status	Unsupported
		Pin/Unpin status	Unsupported
		Follow/Unfollow in Inbox status	Unsupported
		Feature Conversation	Unsupported
		Read/Unread property	Unsupported
		Question	Unsupported
		Answer	Unsupported
		Vote	Unsupported
	Events	Event details	Unsupported
		Questions in event	Supported
		Discussion in event	Supported
	Content in Viva Engage group site		Supported
	Content in Viva Engage group mailbox		Unsupported
	Planner		Supported

	Account settings	Networks	Unsupported
		My applications	Unsupported
		Notifications	Unsupported
		References	Unsupported
Private Messages	Message content		Unsupported
	GIF		Unsupported
	People in message		Unsupported
	Attachment		Unsupported
	Conversation open/close status		Unsupported
	Follow/Unfollow status		Unsupported
	Feature Conversation		Unsupported
	Read/Unread property		Unsupported
	Like		Unsupported
	Comment		Unsupported
Membership Type		Assigned	Supported
		Dynamic	Supported

OneDrive Data Types

IBM® Storage Protect for Cloud Microsoft™ 365 for OneDrive will protect the **Documents** library and will protect the **Site Assets** library as well if the site feature **Site NoteBook** is activated.

The service only protects content and permissions for OneDrive since OneDrive is the cloud service used to securely store, share, and access your files.

Backup for OneDrive now uses Microsoft Graph API for improved performance. Graph API has been more focused on protecting OneDrive content, and it has some limitations, such as it cannot protect the file versions. The file version number cannot be kept either after being restored to the destination. The restored file will use version: **1.0**.

Refer to the table below for the supported and unsupported data types in OneDrive.

Supported and unsupported data types in OneDrive

Data Types			**Default/Custom App Profile**	**Service Account (Obsolete)**
Lists/libraries	Permission	Users **Note:** Restore the users before the content.	Unsupported	Unsupported
		Role Assignments	Unsupported	Unsupported
	Versioning settings	Content Approval	Unsupported	Unsupported
	Document Version History	No versioning	Unsupported	Unsupported
		Create major versions	Unsupported	Unsupported
		Create major and minor (default) versions	Unsupported	Unsupported
	Content Types		Unsupported	Unsupported

Data Types			**Default/Custom App Profile**	**Service Account (Obsolete)**
	Columns		Unsupported	Unsupported
	List Views		Unsupported	Unsupported
Documents **Note:** Only protects the current version.	Permission	Users **Note:** Restore the users before the content.	Supported	Supported
		Role Assignments	Unsupported	Unsupported
	Column values	Author	Supported	Supported
		Editor	Supported	Supported
		Modified	Supported	Supported
		Created	Supported	Supported
		Column values on the edit and view form	Unsupported	Unsupported
		Column values for the required fields	Unsupported	Unsupported
		Other	Unsupported	Unsupported
	Content		Supported	Supported
History Version	Column values	Author	Unsupported	Unsupported
		Editor	Unsupported	Unsupported
		Modified	Unsupported	Unsupported
		Created	Supported	Supported
	Content		Unsupported	Unsupported
List view			Unsupported	Unsupported
Workflow			Unsupported	Unsupported
Term set			Unsupported	Unsupported
Site settings			Unsupported	Unsupported
Library settings			Unsupported	Unsupported
Subsites			Unsupported	Unsupported
IRM			Supported	Supported
Asset library			Unsupported	Unsupported
Other lists/libraries			Unsupported	Unsupported
Web part			Unsupported	Unsupported
Site features			Unsupported	Unsupported
Storage metrics			Unsupported	Unsupported
Region and language		Region setting	Unsupported	Unsupported
		Language setting	Unsupported	Unsupported

Document-Related Data Types

Refer to the following tables for the supported/unsupported/partially supported data types related to document restore.

The data types are grouped by the following tables: Content, Workflow, Column, and Content Type.

Content

Data Types			**Default/Custom App Profile**	**Service Account (Obsolete)**
Document	Document Properties	Checkout **Note:** The non-checkout versions of the checked-out file can be protected.	Unsupported	Unsupported
	Document Version	Major and Minor Versions	Supported	Supported
		Major Versions	Supported	Supported
Item	Item Field	Attachment	Supported	Supported
	Item Version	Item Version (not open approval)	Supported	Supported
		Item Version (open approval)	Unsupported	Supported
Page	Page Content	Embed	Supported	Supported
		Format Text	Supported	Supported
		Insert Links	Supported	Supported
		Insert Media	Supported	Supported
		Insert Tables	Supported	Supported
	Page Version	Version Page Content	Supported	Supported
SharePoint Designer Objects	Site Level Design Items	default.aspx	Supported	Supported
	Site Level Design Items	default.aspx	Supported	Supported
		GettingStarted.aspx	Supported	Supported
		newsfeed.aspx	Supported	Supported
	List/Library Level Design Folders	Forms	Supported	Supported

Data Types			Default/Custom App Profile	Service Account (Obsolete)
	List/Library Level Design Items **Note:** The **Modified By** property cannot be kept.	AllItems.aspx	Partially Supported	Supported
		Combine.aspx	Partially Supported	Supported
		DispForm.aspx	Partially Supported	Supported
		EditForm.aspx	Partially Supported	Supported
		repair.aspx	Partially Supported	Supported
		template.dotx	Partially Supported	Supported
		Thumbnails.aspx	Partially Supported	Supported
		Upload.aspx	Partially Supported	Supported
		NewForm.aspx	Partially Supported	Supported

Workflow

Note: SharePoint 2010 workflows are no longer sussported for restore as Microsoft™ no longer supports SharePoint 2010 workflows in Microsoft™ 365.

Data Types		Default/Custom App Profile	Service Account (Obsolete)
Built-in Workflow	Approval Workflow	Supported	Supported
	Collect Feedback Workflow	Supported	Supported
	Collect Signatures Workflow	Supported	Supported
	Disposition Approval Workflow	Supported	Supported
	Three-State Workflow	Supported	Supported
Designer 10 Workflow_Condition	If any _ equals _	Unsupported	Unsupported
	Else-If Branch	Unsupported	Unsupported
	The person is a valid SharePoint user	Unsupported	Unsupported
Designer 10 Workflow_Action	Core Actions	Unsupported	Unsupported
	Document Set Actions	Unsupported	Unsupported
	List Actions	Unsupported	Unsupported
	Relational Actions	Unsupported	Unsupported
	Task Actions	Unsupported	Unsupported
	Utility Actions	Unsupported	Unsupported
Designer 10 Workflow_Step	Multiple Steps	Unsupported	Unsupported
	Parallel Block	Unsupported	Unsupported
	Impersonation Step	Unsupported	Unsupported
Designer 13 Workflow_Condition	If any _ equals _	Supported	Supported
	Else Branch	Supported	Supported
	The person is a valid SharePoint user	Supported	Supported

Data Types		Default/Custom App Profile	Service Account (Obsolete)
Designer 13 Workflow_Action	Coordination Actions	Supported	Supported
	Core Actions	Supported	Supported
	List Actions	Supported	Supported
	Task Actions	Supported	Supported
	Utility Actions	Supported	Supported
Designer 13 Workflow_Stage	Multiple Stages	Supported	Supported
Designer 13 Workflow_Step	Multiple Steps	Supported	Supported
	Parallel Block	Supported	Supported
Designer 13 Workflow_Loop	Loop n Times	Supported	Supported
	Loop with Condition	Supported	Supported
Workflow level	List Content Type Workflow	Supported	Supported
	List/Library Workflow	Supported	Supported
	Site Content Type Workflow	Supported	Supported
	Site workflow	Supported	Supported
Workflow Settings	Start Options	Supported	Supported
Workflow History		Unsupported	Unsupported
Nintex Workflow for Office 365		Unsupported	Supported

Column

Data Types			Default/Custom App Profile	Service Account (Obsolete)
Site Columns	Base Columns	Append-Only Comments	Supported	Supported
		Categories	Supported	Supported
		End Date	Supported	Supported
		Language	Supported	Supported
		Start Date	Supported	Supported
		URL	Supported	Supported
		Workflow Name	Supported	Supported
	Label	Retention label	Supported	Supported
		Label applied by	Unsupported	Unsupported
		Retention label applied	Unsupported	Unsupported
		Label Settings	Unsupported	Unsupported
	Business Intelligence	Is Data	Supported	Supported
		Is Report	Supported	Supported
	Content Feedback	Number of Likes	Supported	Supported
		Number of Ratings	Supported	Supported
		Rating (0-5)	Supported	Supported

Data Types			Default/Custom App Profile	Service Account (Obsolete)
	Core Contact and Calendar Columns	Address	Supported	Supported
		Anniversary	Supported	Supported
		Assistant's Name	Supported	Supported
		Assistant's Phone	Supported	Supported
		Birthday	Supported	Supported
		Business Phone	Supported	Supported
		Business Phone 2	Supported	Supported
		Callback Number	Supported	Supported
		Car Phone	Supported	Supported
		Children's Names	Supported	Supported
		City	Supported	Supported
		Company	Supported	Supported
		Company Main Phone	Supported	Supported
		Computer Network Name	Supported	Supported
		Contact Photo	Supported	Supported
		Country/Region	Supported	Supported
		Custom ID Number	Supported	Supported
		Department	Supported	Supported
		Email	Supported	Supported
		Email 2	Supported	Supported
		Email 3	Supported	Supported
		Event Address	Supported	Supported
		Fax Number	Supported	Supported
		First Name	Supported	Supported
		FTP Site	Supported	Supported
		Full Name	Supported	Supported
		Gender	Supported	Supported
		Government ID Number	Supported	Supported
		Hobbies	Supported	Supported
		Home Address City	Supported	Supported
		Home Address Country/Region	Supported	Supported
		Home Address Postal Code	Supported	Supported
		Home Address State Or Province	Supported	Supported
		Home Address Street	Supported	Supported
		Home Fax	Supported	Supported
		Home Phone	Supported	Supported

Data Types			Default/Custom App Profile	Service Account (Obsolete)
		Home Phone 2	Supported	Supported
		IM Address	Supported	Supported
		Initials	Supported	Supported
		ISDN	Supported	Supported
		Job Title	Supported	Supported
		Location	Supported	Supported
		Manager's Name	Supported	Supported
		Middle Name	Supported	Supported
		Mobile Number	Supported	Supported
		Nickname	Supported	Supported
		Office	Supported	Supported
		Organizational ID Number	Supported	Supported
		Other Address City	Supported	Supported
		Other Address Country/Region	Supported	Supported
		Other Address Postal Code	Supported	Supported
		Other Address State Or Province	Supported	Supported
		Other Address Street	Supported	Supported
		Other Fax	Supported	Supported
		Other Phone	Supported	Supported
		Pager	Supported	Supported
		Personal Website	Supported	Supported
		Primary Phone	Supported	Supported
		Profession	Supported	Supported
		Radio Phone	Supported	Supported
		Referred By	Supported	Supported
		Spouse/Domestic Partner	Supported	Supported
	Core Document Columns	State/Province	Supported	Supported
		Suffix	Supported	Supported
		Telex	Supported	Supported
		TTY-TDD Phone	Supported	Supported
		User Field 1	Supported	Supported
		User Field 2	Supported	Supported
		User Field 3	Supported	Supported
		User Field 4	Supported	Supported
		Web Page	Supported	Supported
		ZIP/Postal Code	Supported	Supported
		Author	Supported	Supported

Data Types			Default/Custom App Profile	Service Account (Obsolete)
		Category	Supported	Supported
		Comments	Supported	Supported
		Contributor	Supported	Supported
		Copyright	Supported	Supported
		Coverage	Supported	Supported
		Date Created	Supported	Supported
		Date Modified	Supported	Supported
		Date Picture Taken	Supported	Supported
		Format	Supported	Supported
		Keywords	Supported	Supported
		Last Printed	Supported	Supported
		Publisher	Supported	Supported
		Relation	Supported	Supported
		Resource Identifier	Supported	Supported
		Resource Type	Supported	Supported
		Revision	Supported	Supported
		Rights Management	Supported	Supported
		Source	Supported	Supported
		Status	Supported	Supported
		Subject	Supported	Supported
		Version	Supported	Supported
	Core Task and Issue Columns	% Complete	Supported	Supported
		Actual Work	Supported	Supported
		Assigned To	Supported	Supported
		Billing Information	Supported	Supported
		Date Completed	Supported	Supported
		Due Date	Supported	Supported
		Mileage	Supported	Supported
		Predecessors	Supported	Supported
		Priority	Supported	Supported
		Related Company	Supported	Supported
		Role	Supported	Supported
		Task Status	Supported	Supported
		Total Work	Supported	Supported
	Custom Columns	Category Picture	Supported	Supported
		Description	Supported	Supported
		HashTags	Supported	Supported
		Task Outcome	Supported	Supported
		Wiki Categories	Supported	Supported
		WSEnabled	Supported	Supported

Data Types			Default/Custom App Profile	Service Account (Obsolete)
	Display Template Columns	Compatible Managed Properties	Supported	Supported
		Compatible Search Data Types	Supported	Supported
		Crawler XSL File	Supported	Supported
		Hidden Template	Supported	Supported
		Managed Property Mappings	Supported	Supported
		Target Control Type (Search)	Supported	Supported
		Template Level	Supported	Supported
	Document and Record Management Columns	Active	Supported	Supported
		Aliases	Supported	Supported
		Custom Router	Supported	Supported
		Description	Supported	Supported
		Priority	Supported	Supported
		Properties used in Conditions	Supported	Supported
		Property for Automatic Folder Creation	Supported	Supported
		Route To External Location	Supported	Supported
		Rule Name	Supported	Supported
		Submission Content Type	Supported	Supported
		Target Folder	Supported	Supported
		Target Library	Supported	Supported
		Target Path	Supported	Supported
	Enterprise Keywords Group	Enterprise Keywords	Supported	Supported
	Extended Columns	Company Phonetic	Supported	Supported
		First Name Phonetic	Supported	Supported
		Issue Status	Supported	Supported
		Last Name Phonetic	Supported	Supported
		Related Issues	Supported	Supported
		Task Group	Supported	Supported
		UDC Purpose	Supported	Supported
	Help Columns	Context Key	Supported	Supported
		Is On By Default	Supported	Supported
		Locale ID	Supported	Supported
		Product	Supported	Supported

Data Types			**Default/Custom App Profile**	**Service Account (Obsolete)**
		Resources	Supported	Supported
		See Also Help Topics	Supported	Supported
	JavaScript™ Display Template Columns	Hidden	Supported	Supported
		Icon	Supported	Supported
		Target Control Type	Supported	Supported
		Target List Template ID	Supported	Supported
		Target Scope	Supported	Supported
	Page Layout Columns	Byline	Supported	Supported
		Catalog-Item URL	Supported	Supported
		Image Caption	Supported	Supported
		Page Content	Unsupported	Unsupported
		Page Icon	Supported	Supported
		Page Image	Supported	Supported
		Redirect URL	Supported	Supported
		Rollup Image	Supported	Supported
		Summary Links	Supported	Supported
		Summary Links 2	Supported	Supported
	Publishing Columns	Article Date	Supported	Supported
		Browser Title	Supported	Supported
		Contact	Supported	Supported
		Contact Email Address	Supported	Supported
		Contact Name	Supported	Supported
		Contact Picture	Supported	Supported
		Hide from Internet Search Engines	Supported	Supported
		Hide physical URLs from search	Supported	Supported
		Meta Description	Supported	Supported
		Meta Keywords	Supported	Supported
		Scheduling End Date	Supported	Supported
		Scheduling Start Date	Supported	Supported
		Target Audiences	Supported	Supported
	Reports	Owner	Supported	Supported
		Report Category	Supported	Supported
		Report Description	Supported	Supported
		Report Status	Supported	Supported
		Save to report history	Supported	Supported
	Search Config	Notes®	Supported	Supported

Data Types			Default/Custom App Profile	Service Account (Obsolete)
		Scope	Supported	Supported
		Status	Supported	Supported
	Status Indicators	Auto Update	Supported	Supported
		Data Source	Supported	Supported
		Description	Supported	Supported
		Detail Link	Supported	Supported
		Display Folder	Supported	Supported
		Formatted indicator goal	Supported	Supported
		Formatted indicator value	Supported	Supported
		Formatted indicator warning	Supported	Supported
		Goal Cell	Supported	Supported
		Goal from workbook	Supported	Supported
		Goal Sheet	Supported	Supported
		Include child indicators	Supported	Supported
		Indicator	Supported	Supported
		Indicator Comments	Supported	Supported
		Indicator Goal Threshold	Supported	Supported
		Indicator Status	Supported	Supported
		Indicator Value	Supported	Supported
		Indicator Warning Threshold	Supported	Supported
		Lower values are better	Supported	Supported
		Most recent indicator data update	Supported	Supported
		Percent Expression	Supported	Supported
	Translation Columns	Trend	Supported	Supported
		Update Error	Supported	Supported
		Value Cell	Supported	Supported
		Value Expression	Supported	Supported
		Value Sheet	Supported	Supported
		View GUID	Supported	Supported
		Warning Cell	Supported	Supported
		Warning from workbook	Supported	Supported
		Warning Sheet	Supported	Supported
		Batch Id	Supported	Supported

Data Types			Default/Custom App Profile	Service Account (Obsolete)
		Download Link	Supported	Supported
		Errors	Supported	Supported
		Export Job Size	Supported	Supported
		Export Time	Supported	Supported
		Exporting User	Supported	Supported
		Job Completion Time	Supported	Supported
		List	Supported	Supported
		List Link	Supported	Supported
		Number of Items	Supported	Supported
		Site	Supported	Supported
		Submission Time	Supported	Supported
		Terms	Supported	Supported
		Translated Items	Supported	Supported
		Translation Language	Supported	Supported
		Translation Status	Supported	Supported
		Translation type	Supported	Supported
		Translator Name	Supported	Supported
		Upload Job Size	Supported	Supported
		Upload Time	Supported	Supported
		Uploading User	Supported	Supported
List Column	Column Type	Single line of text	Supported	Supported
		Multiple lines of text	Supported	Supported
		Choice	Supported	Supported
		Number	Supported	Supported
		Currency	Supported	Supported
		Date and Time	Supported	Supported
		Lookup	Supported	Supported
		Yes/No	Supported	Supported
		Person or Group	Supported	Supported
		Hyperlink or Picture	Supported	Supported
		Calculated	Supported	Supported
		Task Outcome	Supported	Supported
		External Data	Supported	Supported
		Managed Metadata	Supported	Supported

Content Type

Note: The content type applied to the list item cannot be kept after restore.

Data Types			Default/Custom App Profile	Service Account (Obsolete)
Site Content Types	Business Intelligence	Excel-based Status Indicator	Supported	Supported
		Fixed Value-based Status Indicator	Supported	Supported
		Report	Supported	Supported
		Report Document	Supported	Supported
		SharePoint List based Status Indicator	Supported	Supported
		SQL Server Analysis Services based Status	Supported	Supported
		Indicator	Supported	Supported
		Web Part Page with Status List	Supported	Supported
	Community Content Types	Category	Supported	Supported
		Community Member	Supported	Supported
		Site Membership	Supported	Supported
	Digital Asset Content Types	Audio	Supported	Supported
		Image	Supported	Supported
		Rich Media Asset	Supported	Supported
		Video	Supported	Supported
		Video Rendition	Supported	Supported
	Display Template Content-Type	Control Display Template	Supported	Supported
		Filter Display Template	Supported	Supported
		Group Display Template	Supported	Supported
		Item Display Template	Supported	Supported
		JavaScript Display Template	Supported	Supported
	Document Content Types	Basic Page	Supported	Supported
		Document	Supported	Supported
		Dublin Core Columns	Supported	Supported
		Form	Supported	Supported
		Link to a Document	Supported	Supported
		List View Style	Supported	Supported

Data Types			Default/Custom App Profile	Service Account (Obsolete)
		Master Page	Supported	Supported
		Master Page Preview	Supported	Supported
		Picture	Supported	Supported
		Web Part Page	Supported	Supported
		Wiki Page	Supported	Supported
	Document Set Content Types **Note:** Document Set Settings are not supported.	Document Set	Supported	Supported
	Duet Enterprise Content Types	OBA Report	Supported	Supported
	Folder Content Types	Discussion	Supported	Supported
		Folder	Supported	Supported
		Summary Task	Supported	Supported
	Group Work Content Types	Circulation	Supported	Supported
		Holiday	Supported	Supported
		New Word	Supported	Supported
		Official Notice	Supported	Supported
		Phone Call Memo	Supported	Supported
		Resource	Supported	Supported
		Resource Group	Supported	Supported
		Timecard	Supported	Supported
		Users	Supported	Supported
		What's New Notification	Supported	Supported
	Help Content Types	Help Category	Supported	Supported
		Help Collection	Supported	Supported
		Help Media File	Supported	Supported
		Help Topic	Supported	Supported
	List Content Types	Announcement	Supported	Supported
		Comment	Supported	Supported
		Contact	Supported	Supported
		East Asia Contact	Supported	Supported
		Event	Supported	Supported
		Issue	Supported	Supported
		Item	Supported	Supported
		Link	Supported	Supported

Data Types			Default/Custom App Profile	Service Account (Obsolete)
		Message	Supported	Supported
		Post	Supported	Supported
		Reservations	Supported	Supported
		Schedule	Supported	Supported
		Schedule and Reservations	Supported	Supported
		Task	Supported	Supported
		Workflow Task (SharePoint 2013)	Supported	Supported
	Page Layout Content Types	Article Page	Supported	Supported
		Catalog-Item Reuse	Supported	Supported
		Enterprise Wiki Page	Supported	Supported
		Error Page	Supported	Supported
		Project Page	Supported	Supported
		Redirect Page	Supported	Supported
		Welcome Page	Supported	Supported
	Project Server Approval	PSWApprovalTask	Supported	Supported
	Publishing Content Types	ASP.NET Master Page	Supported	Supported
		HTML Master Page	Supported	Supported
		HTML Page Layout	Supported	Supported
		Page	Supported	Supported
		Page Layout	Supported	Supported
	Search Config	Search Config Content Type	Supported	Supported
	Special Content Types	Unknown Document Type	Supported	Supported

Document ID

Data			Default/Custom App Profile	Service Account (Obsolete)
Library	Added by **New**	Folder	Unsupported	Unsupported
		Word document	Supported	Supported
		Excel workbook	Supported	Supported
		PowerPoint presentation	Supported	Supported
		OneNote notebook	Unsupported	Unsupported
		Link	Supported	Supported
		Text document	Supported	Supported
		Image	Supported	Supported

Data			Default/Custom App Profile	Service Account (Obsolete)
	Added by **Upload**	File	Unsupported	Unsupported
		Folder	Unsupported	Unsupported
Pages	Added by **New**	Site page	Supported	Supported
		Wikipage	Supported	Supported
		Web part page	Unsupported	Unsupported
		Link	Unsupported	Unsupported

Power BI Data Types

- IBM® Storage Protect for Cloud Microsoft™ 365 Power BI service can only protect the Power BI content in the new workspace experience. (The personal workspace is the classic workspace, which is not supported.) In addition, the IBM® Storage Protect for Cloud Power BI service now can only protect the **.pbix** Power BI files that can be downloaded.
- For the limitations on downloading a report from Power BI, refer to Limitations when downloading a report .pbix file. The downloaded .pbix file includes both the report you're downloading and the data on which the report is based, the same as the download .pbix file of “A copy of the report and data” download mode in Power BI. Note that the backup data can only be exported and downloaded.
- To use IBM® Storage Protect for Cloud Microsoft™ 365 to protect the Power BI data, you can configure an app profile for the Microsoft Delegated app with the Power BI option selected. For the list of the required permissions added to the Delegated app for Power BI, refer to “App Profile Authentication” on page 57. If you have been using a scan profile with service account authentication for Power Platform object types, the Auto discovery scan jobs and the IBM® Storage Protect for Cloudjobs can continue using the service account authentication.
- If you use service account authentication or the Delegated app to protect the Power BI data, the service account or the authentication user of the Delegated app must have a **Power BI Pro** license or **Premium Per User (PPU)** license, and have the**Fabric Administrator** role (the former **Power BI admin** role).
- Before you enable the Power BI service, ensure the Download reports feature in the tenant settings has been enabled. This feature was enabled by default. In addition, the IBM® Storage Protect for Cloud Power BI service now can only protect the .pbix Power BI files that can be downloaded. For the limitations on downloading report from Power BI, refer to Limitations when downloading a report .pbix file.
- If you use the service account authentication to protect Power BI data or the Delegated app to scan Power BI workspaces in IBM® Storage Protect for Cloud, the Auto Discovery scan job will automatically add the service account or the authentication user of the Delegated app as the workspace admin.
- Due to the API limitation, the backup job of Power BI can back up at most 200 workspaces per hour.

Power Automate Data Types

IBM® Storage Protect for Cloud Microsoft™ 365 for Power Automate only supports protecting the cloud flows. Refer to the table below for the supported attributes of flows that can be exported.

Data	Service Account	Microsoft Delegated App	Comment
Automated cloud flow	Supported	Supported	
Instant cloud flow	Supported	Supported	
Scheduled cloud flow	Supported	Supported	
Desktop flow	Unsupported	Unsupported	
Business process flow	Unsupported	Unsupported	
Flow ID	Supported	Supported	

Data	Service Account	Microsoft Delegated App	Comment
Flow name	Supported	Supported	The flows whose name contains special characters (such as ~, !, @, #, etc.) cannot be imported into Power Platform.
Description	Unsupported	Unsupported	
Flow owner	Supported	Supported	
Status	Supported	Supported	
Created time	Supported	Supported	
Modified time	Supported	Supported	
Type	Supported	Supported	
Plan	Unsupported	Unsupported	
Custom Connector	Supported	Supported	The flow will not be protected if the custom connector has not been shared to the service account or the app authentication user with sufficient permission.
Connection	Supported	Supported	
Environment information	Supported	Supported	
Connections	Supported	Supported	The flow will not be protected if the connection no longer exists.
28-day run history	Unsupported	Unsupported	
Run only users	Unsupported	Unsupported	
Share permission	Supported	Supported	

Power Apps Data Types

Power Apps service can only protect standard Canvas apps which have been published and component libraries. Note that the Restore action is unsupported and the backup data can only be exported.

Power Apps service can only protect Canvas apps which have been published and component libraries. Note that the Restore action is unsupported and the backup data can only be exported.

- To use IBM® Storage Protect for Cloud Microsoft™ 365 to protect the Power Apps data, you must configure an app profile for the Microsoft Delegated app. For the list of the required permissions added to the Delegated app for Power Apps, refer to “Required Permissions of Microsoft Delegated App” on page 63. If you have been using a scan profile with service account authentication for Power Platform object types, the Auto discovery scan jobs and the IBM® Storage Protect for Cloud jobs can continue using the service account authentication.
- If you use service account authentication or the Delegated app to protect the Power Apps data, the service account or the authentication user of the Delegated app must be the **Global Administrator** and the **Environment Admin**/**System Administrator**, and have the **Power Apps for Microsoft 365** license to proceed.
- The backup job will automatically add the service account or the authentication user of the Delegated app as the app’s co-owner and flow owner (if the app has an associated flow).

The table below lists the data types supported or unsupported for Power Apps in IBM® Storage Protect for Cloud:

Data Type			Service Account	Microsoft Delegated App
App settings	General	Name	Supported	Supported
		Description	Supported	Supported
		Icon	Supported	Supported
		Icon background fill	Supported	Supported
		Icon fill	Supported	Supported
		Auto save	Supported	Supported
		Data row limit	Supported	Supported
		Debug published app	Supported	Supported
		Automatically create environment variables when adding data sources	Supported	Supported
		Enable APP.Onstart property	Supported	Supported
	Display	Orientation	Supported	Supported
		Size	Supported	Supported
		Scale to fit	Supported	Supported
		Lock aspect ratio	Supported	Supported
		Lock orientation	Supported	Supported
	Support	Environment	Supported	Supported
		Authoring version	Unsupported	Unsupported
App detail		License designation	Supported	Supported
		Preload app for enhanced performance	Supported	Supported
		Owner	Supported	Supported
		Created Time	Supported	Supported
		Modified Time	Supported	Supported
		Web link	Supported	Supported
		Mobile QR code	Supported	Supported
		App ID	Supported	Supported
		Connections	Supported	Supported
		Flows	Supported	Supported
standard Canvas app			Supported	Supported
Component library **Note:** The data center operated by 21Vianet in China do not support component libraries, so the backup service for component libraries in such data centers is not supported as well.			Supported	Supported
Model-driven app			Unsupported	Unsupported

Website	Unsupported	Unsupported

Restore Options for Different Object Types

The table below shows the supported/unsupported restore options for different object types.

Note:

- The Project Online data, and the Apps are not supported when using the app profile only.
- Data exporting in IBM® Storage Protect for Cloud Microsoft™ 365 does not support exporting metadata.

Supported/unsupported restore options for different object types.

Object Type	Level	Restore to Original Location	Restore to Another Location (Destination)	Restore to Storage	Export
Exchange Online	Mailbox	Supported	Supported (Mailbox)	Supported	Supported
	Folder	Supported	Supported (Mailbox/ Folder)	Supported	Supported
	Mailbox Item	Supported	Supported (Folder)	Supported	Supported
Project Online	Project Online Site Collection	Supported	Supported (Site Collection)	Unsupported	Unsupported
	Subsite	Supported	Supported (Site Collection or Site)	Unsupported	Unsupported
	Project	Supported	Supported (Site Collection or Site)	Unsupported	Unsupported
	Library/List	Supported	Supported (Site Collection, Site, List, or Library)	Supported	Supported
	Folder	Supported	Supported (Library or Folder)	Supported	Supported
	Item/Document	Supported	Supported (Library or Folder)	Supported	Supported
	Apps	Supported	Supported (Site Collection or OneDrive)	Unsupported	Unsupported
Public Folder	Folder	Supported	Unsupported	Unsupported	Unsupported
	Items	Supported	Unsupported	Unsupported	Unsupported

Object Type	Level	Restore to Original Location	Restore to Another Location (Destination)	Restore to Storage	Export
Microsoft Teams Chat	User	Unsupported	Unsupported	Unsupported	Supported
	Chat	Unsupported	Unsupported	Unsupported	Supported
	Chat Message	Unsupported	Unsupported	Unsupported	Supported
Viva Engage **Note:** In the current release, Viva Engage messages are only available in the timebased recovery wizard and will be restored to HTML files.	Viva Engage Community	Supported	Supported	Unsupported	Unsupported
	Site Collection	Supported	Supported	Unsupported	Unsupported
	Site	Supported	Unsupported	Unsupported	Unsupported
	List/Library	Supported	Unsupported	Supported	Supported
	App	Supported	Unsupported	Unsupported	Unsupported
	Folder in SharePoint	Supported	Unsupported	Supported	Supported
	Document	Supported	Unsupported	Supported	Supported
	Viva Engage Conversations	Supported	Unsupported	Supported	Supported
Power BI	Workspace	Supported	Supported (Workspace)	Supported	Supported
	Report	Supported	Supported (Workspace)	Supported	Supported

SharePoint Online Restore Options

Source Object	Restore to Original Location	Restore to Storage	Export	Destination Object (Restore to Another Location)			Action
Site Collection	Supported	Unsupported	Unsupported	OneDrive			Merge
				SharePoint Site Collection			Attach/ Merge
				Group Site Collection			Attach/ Merge
				Team	Channel Site	Private Channel Site	Attach/ Merge

<table>
<tr><th>Source Object</th><th>Restore to Original Location</th><th>Restore to Storage</th><th>Export</th><th colspan="3">Destination Object (Restore to Another Location)</th><th>Action</th></tr>
<tr><td rowspan="2"></td><td rowspan="2"></td><td rowspan="2"></td><td rowspan="2"></td><td colspan="3">Shared Channel Site</td><td>Attach/ Merge</td></tr>
<tr><td colspan="3">Team Site</td><td>Attach/ Merge</td></tr>
<tr><td rowspan="6">Site</td><td rowspan="6">Supported</td><td rowspan="6">Unsupported</td><td rowspan="6">Unsupported</td><td colspan="3">OneDrive</td><td rowspan="6">Attach/ Merge</td></tr>
<tr><td colspan="3">SharePoint Site Collection/Subsite</td></tr>
<tr><td colspan="3">Group Site Collection/Subsite</td></tr>
<tr><td>Team</td><td>Channel Site</td><td>Private Channel Site / Subsite</td></tr>
<tr><td colspan="3">Shared Channel Site / Subsite</td></tr>
<tr><td colspan="3">Team Site / Subsite</td></tr>
<tr><td rowspan="12">List</td><td rowspan="12">Supported</td><td rowspan="12">Supported</td><td rowspan="12">Supported</td><td colspan="3">OneDrive</td><td>Attach</td></tr>
<tr><td colspan="3">OneDrive List</td><td>Merge</td></tr>
<tr><td colspan="3">SharePoint Site Collection/Subsite</td><td>Attach</td></tr>
<tr><td colspan="3">SharePoint Site Collection/Subsite List</td><td>Merge</td></tr>
<tr><td colspan="3">Group Site Collection/Subsite</td><td>Attach</td></tr>
<tr><td colspan="3">Group Site Collection/Subsite List</td><td>Merge</td></tr>
<tr><td>Team</td><td>Channel Site</td><td>Private Channel Site / Substrate</td><td>Attach</td></tr>
<tr><td colspan="3">Private Channel Site / Subsite List</td><td>Attach</td></tr>
<tr><td colspan="3">Shared Channel Site / Subsite</td><td>Attach</td></tr>
<tr><td colspan="3">Shared Channel Site / Subsite List</td><td>Merge</td></tr>
<tr><td colspan="2" rowspan="2">Team Site</td><td>Team Site / Subsite</td><td>Attach</td></tr>
<tr><td>Team Site / Subsite List</td><td>Merge</td></tr>
<tr><td rowspan="10">Library</td><td rowspan="10">Supported</td><td rowspan="10">Supported</td><td rowspan="10">Supported</td><td colspan="3">OneDrive</td><td>Attach</td></tr>
<tr><td colspan="3">OneDrive Library Folder</td><td>Merge</td></tr>
<tr><td colspan="3">SharePoint Site Collection/Subsite</td><td>Attach</td></tr>
<tr><td colspan="3">SharePoint Site Collection/Subsite Library</td><td>Merge</td></tr>
<tr><td colspan="3">Group Site Collection/Subsite</td><td>Attach</td></tr>
<tr><td colspan="3">Group Site Collection/Subsite Library</td><td>Merge</td></tr>
<tr><td>Team</td><td>Channel Site</td><td>Private Channel Site / Subsite</td><td>Attach</td></tr>
<tr><td colspan="3">Private Channel Site / Subsite Library</td><td>Merge</td></tr>
<tr><td colspan="3">Shared Channel Site / Subsite</td><td>Attach</td></tr>
<tr><td colspan="3">Shared Channel Site / Subsite Library</td><td>Merge</td></tr>
</table>

Source Object	Restore to Original Location	Restore to Storage	Export	Destination Object (Restore to Another Location)			Action
				Team Site		Team Site / Subsite	Attach
						Team Site / Subsite Library	Merge
Folder	Supported	Supported	Supported	OneDrive Library			Attach
				OneDrive Library Folder			Attach/ Merge
				SharePoint Library/List			Attach
				SharePoint Library/List Folder			Attach/ Merge
				Group Library/List			Attach
				Group Library/List Folder			Attach/ Merge
				Team	Channel Site	Private Channel Site / Subsite > Library/List	Attach
				Private Channel Site / Subsite > Library/List Folder			Attach/ Merge
				Shared Channel Site / Subsite > Library/List			Attach
				Shared Channel Site/ Subsite > Library /List Folder			Attach/ Merge
Document	Supported	Supported	Supported	OneDrive Library			Attach
				OneDrive Library Folder			
				SharePoint Library			
				SharePoint Library Folder			
				Group Library			
				Group Library Folder			
				Team Library	Channel Site	Private Channel Site / Subsite > Library	
				Team Library Folder			
				Private Channel Site / Subsite > Library Folder			
				Shared Channel Site / Subsite > Library			
				Shared Channel Site / Subsite > Library Folder			
				Team Site		Team Site / Subsite > Library	

Source Object	Restore to Original Location	Restore to Storage	Export	Destination Object (Restore to Another Location)			Action
						Team Site / Subsite > Library Folder	
Item & Attachment	Supported	Supported	Supported	OneDrive List			Attach
				OneDrive List Folder			
				SharePoint List			
				SharePoint List Folder			
				Group List			
				Group List Folder			
				Team	Channel Site	Private Channel Site / Subsite > List	
				Private Channel Site / Subsite > List Folder			
				Shared Channel Site / Subsite > List			
				Shared Channel Site / Subsite > List Folder			
				Team Site		Team site / Subsite > List	
						Team site / Subsite > List Folder	
Apps	Supported	Unsupported	Unsupported	OneDrive User			Attach
				SharePoint Site Collection/Subsite			
				Group Site Collection/Subsite			
				Teams Site Collection/Subsite			
				Team	Channel Site	Private Channel Site / Subsite	
				Shared Channel Site / Subsite			
				Team Site / Subsite			

OneDrive Restore Options

Summary for complex table

Source Object	Restore to Original Location	Restore to Storage	Export	Restore to Another Location (Destination)	Action	Comment
OneDrive User	Supported	Unsupported	Supported	OneDrive	Merge	
				SharePoint Site Collection	Attach/ Merge	

Source Object	Restore to Original Location	Restore to Storage	Export	Restore to Another Location (Destination)	Action	Comment
				Group Site Collection	Attach/ Merge	
				Team Site Collection	Attach/ Merge	
Library	Supported	Supported	Supported	OneDrive	Attach	
				OneDrive Library	Merge/ Attach	Only supported when one library is selected for restore.
				SharePoint Site Collection/ Subsite	Attach	
				SharePoint Library	Merge	
				Group Site Collection/ Subsite	Attach	
				Group Library	Merge	
				Team Site Collection/ Subsite	Attach	
				Team Library	Merge	
Folder	Supported	Supported	Supported	OneDrive Library	Attach	
				OneDrive Library Folder	Attach/ Merge	
				SharePoint Library	Attach	
				SharePoint Library Folder	Attach/ Merge	
				Group Site Library	Attach	
				Group Site Library Folder	Attach/ Merge	
				Team Library	Attach	
				Team Library Folder	Attach/ Merge	
Document	Supported	Supported	Supported	OneDrive Library	Attach	
				OneDrive Library Folder		

Source Object	Restore to Original Location	Restore to Storage	Export	Restore to Another Location (Destination)	Action	Comment
				SharePoint Library		
				SharePoint Library Folder		
				Group Site Library		
				Group Site Library Folder		
				Team Library		
				Team Library Folder		
				OneDrive Library		

Microsoft 365 Groups Restore Options

Summary for complex table

Table 63: Microsoft 365 Groups Restore Options

How to Find Data	Source Object	Restore to Original Location	Restore to Storage	Export	Destination Object（Restore to Another Location		Action	Comment
Object-Based Restore	Microsoft 365 Group	Supported	Unsupported	Unsupported	Microsoft 365 Group		Marge	
	Group Mailbox	Supported	Supported	Supported	Group Mailbox		Merge	Only restore Inbox and Calendar.
	Folder in Mailbox	Supported	Supported	Supported	Unsupported			
	Mailbox Item	Supported	Supported	Supported	Unsupported			
	Group Team Site	Supported	Unsupported	Unsupported	Group Team Site Collection		Merge/Attach	
					Team Site Collection			
					SharePoint Site Collection			
					OneDrive User		Merge	
	Site	Supported	Unsupported	Unsupported	Group Team Site Collection		Merge/Attach	
					Team Site Collection / Subsite			
					SharePoint Site Collection / Subsite			
					OneDrive User		Merge	
	Single List/Library	Supported	Supported	Supported	Group	Top Level Site Collection	Attach	
						Subsite		
					Team	Top Level Site List/ Library	Merge	
						Subsite List/Library		
					SharePoint	Top Level Site Collection / Subsite	Attach	
						Top Level Site / Subsite > List/ Library	Merge	
					OneDrive	Top Level Site Collection / Subsite	Attach	
						Top Level Site / Subsite > List/ Library	Merge	
	Multiple Lists & Libraries with the Same Template	Supported	Supported	Supported	Group > Top Level Site Collection / Subsite		Attach	
					Team > Top Level Site Collection / Subsite			
					SharePoint > Top Level Site Collection / Subsite			
					OneDrive User			
	Multiple Lists & Libraries	Supported	Supported	Supported	Unsupported			
	App	Supported	Unsupported	Unsupported	Group > Top Level Site Collection / Subsite		Attach	
					Team > Top Level Site Collection / Subsite			
					SharePoint > Top Level Site Collection / Subsite			
					OneDrive user			
	Plan	Supported	Unsupported	Unsupported	Microsoft 365 Group		Attach	Plan configurations and the tasks belonging to the selected plans can be restored.

How to Find Data	Source Object		Restore to Original Location	Restore to Storage	Export	Destination Object（Restore to Another Location		Action	Comment
	Task		Supported	Unsupported	Unsupported	Unsupported			
	Single Folder in SharePoint (Library Folder)		Supported	Supported	Supported	Group	Top Level Site Collection / Subsite > Library	Attach	Single or multiple list folders with the same template are unsupported to be restored to another location
							Top Level Site / Subsite > Library Folder	Merge/Attach	
						Team	Top Level Site Collection / Subsite > Library	Attach	
							Top Level Site / Subsite > Library Folder	Merge/Attach	
						SharePoint	Top Level Site Collection / Subsite > Library	Attach	
							Top Level Site / Subsite > Library Folder	Merge/Attach	
						OneDrive	Top Level Site Collection / Subsite > Library	Attacvh	
							Top Level Site / Subsite > Library Folder	Merge/Attach	
	Single Folder in SharePoint (List Folder)		Supported	Supported	Supported	Group	Top Level Site Collection / Subsite > Library	Attach	
							Top Level Site / Subsite > Library Folder	Merge/Attach	
						Team	Top Level Site Collection / Subsite > Library	Attach	
							Top Level Site / Subsite > Library Folder	Merge/Attach	
						SharePoint	Top Level Site Collection / Subsite > Library	Attach	
							Top Level Site / Subsite > Library Folder	Merge/Attach	
						OneDrive	Top Level Site Collection / Subsite > Library	Attach	
							Top Level Site / Subsite > Library Folder	Merge/Attach	
	Multiple List & Library Folders		Supported	Supported	Supported	Unsupported			It is unsupported to restore list and library folders to another location at the same time.
	Document		Supported	Supported	Supported	Group	Top Level Site Collection / Subsite > Library	Attach	
							Top Level Site / Subsite > Library Folder		
						Team	Top Level Site Collection / Subsite > Library		
							Top Level Site / Subsite > Library Folder		
						SharePoint	Top Level Site Collection / Subsite > Library		
							Top Level Site / Subsite > Library Folder		
						OneDrive	OneDrive Library		
							OneDrive Library Folder		
Time-Based Restore	Microsoft 365 Group		Supported	Unsupported	Unsupported	Microsoft 365 Group		Merge	
	Group Team Site	Group Team Site	Supported	Unsupported	Unsupported	Group Team Site Collection		Merge/Attach	
						Team Site Collection			
						SharePoint Site Collection			
						OneDrive user		Merge	
		Site	Supported	Unsupported	Unsupported	Group Team Site Collection / Subsite		Merge/Attach	The Merge and Attach actions are available when restoring a single site. If multiple sites are selected, only the Attach action is available.
						Team Site Collection / Subsite			
						SharePoint Site Collection / Subsite			
						OneDrive User		Merge	
		Single List/Library	Supported	Supported	Supported	Group	Top Level Site Collection / Subsite	Attach	
							Top Level Site Collection / Subsite > List/Library	Merge	
						Team	Top Level Site Collection / Subsite	Attach	
							Top Level Site Collection / Subsite > List/Library	Merge	
						SharePoint	Top Level Site Collection / Subsite	Attach	
							Top Level Site Collection / Subsite > List/Library	Merge	

How to Find Data	Source Object		Restore to Original Location	Restore to Storage	Export	Destination Object (Restore to Another Location		Action	Comment
						OneDrive User	Top Level Site Collection	Attach	
							Top Level Site Collection > List/ Library	Merge	
		Multiple Lists & Libraries with the Same Template	Supported	Supported	Supported	Group	Group Team Site Collection / Subsite	Attach	
						Team	Team Site Collection / Subsite		
						SharePoint	Site Collection / Subsite		
						OneDrive User	OneDrive User		
		Multiple Lists & Libraries	Supported	Supported	Supported	Unsupported			
		Single Folder in SharePoint (Library/List Folder)	Supported	Supported	Supported	Group	Top level Site Collection / Subsite > Library/List	Attach	Single or multiple list folders with the same template are unsupported to be restored to another location.
							Top level Site Collection / Subsite > Library/List Folder	Merge/Attach	
						Team	Top level Site Collection / Subsite > Library/List	Attach	
							Top level Site Collection / Subsite > Library/List Folder	Merge/Attach	
						SharePoint	Top level Site Collection / Subsite > Library/List	Attach	
							Top level Site Collection / Subsite > Library/List Folder	Merge/Attach	
						OneDrive User	Top level Site Collection / Subsite > Library/List	Attach	
							Top level Site collection / Subsite > Library/List Folder	Merge/Attach	
		Multiple List & Library Folders	Supported	Supported	Supported	Group	Top level Site Collection / Subsite > Library/List	Attach	
							Top level Site Collection / Subsite > Library/List Folder		
						Team	Top level Site Collection / Subsite > Library/List		
							Top level Site Collection / Subsite > Library/List Folder		
						SharePoint	Top level Site Collection / Subsite > Library/List		
							Top level Site Collection / Subsite > Library/List Folder		
						OneDrive User	Top level Site Collection / Subsite > Library/List		
							Top level Site collection / Subsite > Library/List Folder		
		Single or Multiple Document	Supported	Supported	Supported	Group	Top level Site Collection / Subsite > Library	Attach	
							Top level Site Collection / Subsite > Library Folder		
						Team	Top level Site Collection / Subsite > Library		
							Top level Site Collection / Subsite > Library Folder		
						SharePoint	Top level Site Collection / Subsite > Library		
							Top level Site Collection / Subsite > Library Folder		
						OneDrive User	Top level Site Collection / Subsite > Library		
							Top level Site collection / Subsite > Library Folder		
		Single or Multiple Item with Attachment	Supported	Supported	Supported	Group	Top level Site Collection / Subsite > List	Attach	
							Top level Site Collection / Subsite > List Folder		
						Team	Top level Site Collection / Subsite > List		

How to Find Data	Source Object		Restore to Original Location	Restore to Storage	Export	Destination Object (Restore to Another Location		Action	Comment
							Top level Site Collection / Subsite > List Folder		
						SharePoint	Top level Site Collection / Subsite > List		
							Top level Site Collection / Subsite > List Folder		
						OneDrive User	Top level Site Collection / Subsite > List		
							Top level Site collection / Subsite > List Folder		
		Document/Item & Folder	Supported	Supported	Supported	Unsupported			
	Planner	Plan	Supported	Unsupported	Unsupported	Microsoft 365 Group		Attach	Plan configurations and the tasks belonging to the selected plans can be restored.
		Task	Supported	Unsupported	Unsupported	Unsupported			
	Group Conversation	Group Conversation	Supported	Supported	Supported	Group Mailbox		Merge	Only restore Inbox and Calendar.
		Folder in Group Conversation	Supported	Supported	Supported	Unsupported			
		Item in Group Conversation	Supported	Supported	Supported	Unsupported			

Teams Restore Options

Summary for complex table

How to Find Data	Source Object	Restore to Original Location	Restore to Storage	Export	Destination Object (Restore to Another Location)			Action	Comment
ObjectBased Restore	Teams	Supported	Unsupported	Unsupported	Unsupported				
	Group Mailbox	Supported	Unsupported	Unsupported	Unsupported				
	Folder in Mailbox	Supported	Unsupported	Unsupported	Unsupported				
	Mailbox Item	Supported	Unsupported	Unsupported	Unsupported				
	Group Team Site	Supported	Unsupported	Unsupported	Team	Channel Site	Private Channel Site	Merge/Attach	
							Shared Channel Site		
						Team Site			
					Group	Group Team Site			
					SharePoint	Team Site			
					OneDrive	OneDrive		Merge	
	Site	Supported	Unsupported	Unsupported	Team	Channel Site	Private Channel Site	Merge/Attach	
							Shared Channel Site		
						Team Site/Subsite			
					Group	Group Team Site/Subsite			
					SharePoint	Team Site/Subsite			
					OneDrive	OneDrive		Merge	
	Single List/Library	Supported	Unsupported	Supported	Team	Channel Site	Private Channel Site/Subsite	Attach	
							Private Channel Site/Subsite > List/ Library	Merge	
							Shared Channel Site/Subsite	Attach	
							Shared Channel Site/Subsite > List/ Library	Merge	
						Team Site	Team Site/Subsite	Attach	
							Team Site/Subsite > List/Library	Merge	
					Group	Team Site/Subsite		Attach	
						Team Site/Subsite > List/Library		Merge	
					SharePoint	Team Site/Subsite		Attach	
						Team Site/Subsite > List/Library		Merge	
					OneDrive	OneDrive User		Attach	
						OneDrive User > List/Library		Merge	
	Multiple Lists & Libraries with the Same Template	Supported	Unsupported	Supported	Team	Channel Site	Private Channel Site/Subsite	Attach	
							Shared Channel Site/Subsite		
						Team Site/Subsite			
					Group	Group Team Site/Subsite			
					SharePoint	SharePoint Site/Subsite			

How to Find Data	Source Object	Restore to Original Location	Restore to Storage	Export	Destination Object (Restore to Another Location)			Action	Comment
					OneDrive	OneDrive User			
	Multiple Lists & Libraries	Supported	Unsupported	Supported	Unsupported				
	App	Supported	Unsupported	Unsupported	Team	Channel Site	Private Channel Site/Subsite	Attach	
							Shared Channel Site/Subsite		
							Team Site		
					Group	Group Team Site/Subsite			
					SharePoint	SharePoint Site/Subsite			
					OneDrive	OneDrive User			
	Plan	Supported	Unsupported	Unsupported	Teams			Attach	Plan configurations and the tasks belonging to the selected plans can be restored.
	Task	Supported	Unsupported	Unsupported	Unsupported				
	Single Folder in SharePoint (Library Folder)	Supported	Supported	Supported	Team	Channel	Private Channel	Attach	
							Shared Channel		
							Standard channel		
						Channel Site	Private Channel Site/Subsite > Library	Attach	
							Private Channel Site/Subsite > Library Folder	Merge/Attach	
							Shared Channel Site/Subsite > Library	Attach	
							Shared Channel Site/Subsite > Library Folder	Merge/Attach	
						Team Site	Team Site/Subsite > Library	Attach	
							Team Site/Subsite > Library Folder	Merge/Attach	
					Group	Group Team Site/Subsite > Library		Attach	
						Group Team Site/Subsite > Library Folder		Merge/Attach	
					SharePoint	Group Team Site/Subsite > Library		Attach	
						Group Team Site/Subsite > Library Folder		Merge/Attach	
					OneDrive	OneDrive Library		Attach	
						OneDrive Library Folder		Merge/Attach	
	Folder in SharePoint (List Folder)	Supported	Supported	Supported	Team	Channel Site	Private Channel Site/Subsite > List	Attach	
							Private Channel Site/Subsite > List Folder	Merge/Attach	
							Shared Channel Site/Subsite > List	Attach	
							Shared Channel Site/Subsite > List Folder	Merge/Attach	
						Team Site	Team Site/Subsite > List	Attach	
							Team Site/Subsite > List Folder	Merge/Attach	
					Group	Group Team Site/Subsite > List		Attach	
						Group Team Site/Subsite > List Folder		Merge/Attach	
					SharePoint	Group Team Site/Subsite > List		Attach	
						Group Team Site/Subsite > List Folder		Merge/Attach	
					OneDrive	OneDrive List		Attach	
						OneDrive List > Folder		Merge/Attach	
	Multiple List & Library Folders	Supported	Supported	Supported	Unsupported				
	Documents	Supported	Supported	Supported	Team	Channel	Private Channel	Attach	
							Shared Channel		
							Standard Channel		
						Channel Site	Private Channel Site/Subsite > Library		
							Private Channel Site/Subsite > Library Folder		
							Shared Channel Site/Subsite > Library		
							Shared Channel Site/Subsite > Library Folder		
						Team Site	Team Site/Subsite > Library		
							Team Site/Subsite > Library Folder		
					Group	Group Team Site/Subsite > Library			
						Group Team Site/Subsite > Library Folder			
					SharePoint	Group Team Site/Subsite > Library			
						Group Team Site/Subsite > Library Folder			
					OneDrive	OneDrive Library			
						OneDrive Library Folder			

Summary for complex table

How to Find Data	Source Object	Restore to Original Location	Restore to Storage	Export	Destination Object (Restore to Another Location)	Action	Comment
Time-Based Restore **Note:** The Private Channels and Shared Channels can only be restored	Teams	Supported	Unsupported	Unsupported	Unsupported		

How to Find Data	Source Object	Restore to Original Location	Restore to Storage	Export	Destination Object (Restore to Another Location)	Action	Comment
through the time-based restore wizard, and both Private Channels an							

How to Find Data	Source Object			Restore to Original Location	Restore to Storage	Export	Destination Object (Restore to Another Location)			Action	Comment
dShared Channels do not support the out-of-place restore.											
	Channel Site	Standard/ Private/Shared Channel	Standard Channel Site	Supported	Unsupported	Unsupported	Team	Channel Site	Private Channel Site	Merge/Attach	The Merge and Attach actions are available when restoring a single channel site. If multiple channel sites are selected, only the Attach action is available.
									Shared Channel Site		
								Team Site			
							Group	Group Team Site			
							SharePoint	SharePoint Site Collection			
							OneDrive	OneDrive		Merge	

How to Find Data	Source Object			Restore to Original Location	Restore to Storage	Export	Destination Object (Restore to Another Location)			Action	Comment
			Subsite	Supported	Unsupported	Unsupported	Team	Channel Site	Private Channel Site	Merge/Attach	The Merge and Attach actions are available when restoring a single subsite. If multiple subsites are selected, only the Attach action is available.
									Shared Channel Site		
								Team Site/Subsite			
							Group	Group Team Site/Subsite			
							SharePoint	SharePoint Site Collection/Subsite			
							OneDrive	OneDrive		Merge	
			Single List/ Library	Supported	Unsupported	Supported	Team	Channel Site	Private Channel Site/Subsite	Attach	
									Private Channel Site/Subsite > List/Library	Merge	
									Shared Channel Site/Subsite	Attach	
									Shared Channel Site/Subsite > List/Library	Merge	
								Team Site	Team Site/ Subsite	Attach	
									Team Site/ Subsite > List/ Library	Merge	
							Group	Group Team Site/Subsite		Attach	
								Group Team Site/Subsite > List/ Library		Merge	
							SharePoint	Team Site/Subsite		Attach	
								Team Site/Subsite > List/Library		Merge	
							OneDrive	OneDrive		Attach	
								OneDrive > List/Library		Merge	
			Multiple Lists & Libraries with the Same Template	Supported	Unsupported	Supported	Team	Channel Site	Private Channel Site/Subsite	Attach	
									Shared Channel Site/Subsite		
								Team Site/Subsite			
							Group	Group Team Site/Subsite			
							SharePoint	Team Site/Subsite			
							OneDrive	OneDrive			
			Multiple Lists & Libraries	Supported	Unsupported	Supported	Unsupported				
			Library Folder	Supported	Supported	Supported	Team	Channel	Private Channel	Attach	
									Shared Channel		
									Standard Channel		
								Channel Site	Private Channel Site/Subsite > Library	Attach	
									Private Channel Site/Subsite > Library Folder	Merge/Attach	
									Shared Channel Site/Subsite > Library	Attach	
									Shared Channel Site/Subsite > Library Folder	Merge/Attach	
								Team Site	Team Site/ Subsite > Library	Attach	
									Team Site/ Subsite > Library Folder	Merge/Attach	
							Group	Group Team Site/Subsite > Library		Attach	
								Group Team Site/Subsite > Library Folder		Merge/Attach	
							SharePoint	Team Site/Subsite > Library		Attach	
								Team Site/Subsite > Library Folder		Merge/Attach	
							OneDrive	Team Site/Subsite > Library		Attach	
								Team Site/Subsite > Library Folder		Merge/Attach	
			List Folder	Supported	Supported	Supported	Team	Channel Site	Private Channel Site/Subsite > List	Attach	
									Private Channel Site/Subsite > List Folder	Merge/Attach	
									Shared Channel Site/Subsite > List	Attach	
									Shared Channel Site/Subsite > List Folder	Merge/Attach	
								Team Site	Team Site/ Subsite > List	Attach	
									Team Site/ Subsite > List Folder	Merge/Attach	
							Group	Group Team Site/Subsite List		Attach	
								Group Team Site/Subsite List Folder		Merge/Attach	
							SharePoint	Team Site/Subsite List		Attach	
								Team Site/Subsite List Folder		OneDrive List Folder	
							OneDrive	OneDrive List		Attach	

How to Find Data	Source Object			Restore to Original Location	Restore to Storage	Export	Destination Object (Restore to Another Location)			Action	Comment
								OneDrive List Folder		OneDrive List Folder	
			Library Document	Supported	Supported	Supported	Team	Channel	Standard Channel	Attach	
									Private Channel		
									Shared Channel		
								Channel Site	Private Channel Site/Subsite Library		
									Private Channel Site/Subsite Library Folder		
									Shared Channel Site/Subsite Library		
									Shared Channel Site/Subsite Library Folder		
								Team Site	Team Site/ Subsite Library		
									Team Site/ Subsite Library Folder		
							Group	Group Team Site/Subsite Library			
								Group Team Site/Subsite Library Folder			
							SharePoint	Team Site/Subsite Library			
								Team Site/Subsite Library Folder			
							OneDrive	OneDrive Library			
								OneDrive Library Folder			
			List Item & Attachment	Supported	Supported	Supported	Team	Channel Site	Private Channel Site/Subsite List	Attach	
									Private Channel Site/Subsite List Folder		
									Shared Channel Site/Subsite List		
									Shared Channel Site/Subsite List Folder		
								Team Site	Team Site/ Subsite Lis		
									Team Site/ Subsite List Folder		
							Group	Group Team Site/Subsite List			
								Group Team Site/Subsite List Folder			
							SharePoint	Team Site/Subsite List			
								Team Site/Subsite List Folder			
							OneDrive	OneDrive List			
								OneDrive List Folder			
			App	Supported	Unsupported	Unsupported	Team	Channel Site	Private Channel Site/subsite	Attach	
									Shared Channel Site/Subsite		
								Team Site/Subsite			
							Group	Group Team Site/Subsite			
							SharePoint	SharePoint Site/Subsite			
							OneDrive	OneDrive Library Folder			
	Team Site	Team Site		Supported	Unsupported	Unsupported	Team	Channel Site	Private Channel Site	Merge/Attach	
									Shared Channel Site		
								Team Site/Subsite Library			
							Group	Group Team Site			
							SharePoint	SharePoint Site			
							OneDrive	OneDrive		Merge	
		Subsite		Supported	Unsupported	Unsupported	Team	Channel Site	Private Channel Site/subsite	Merge/Attach	The Merge and Attach actions are available when restoring a single subsite. If multiple subsites are selected, only the Attach action is available.
									Shared Channel Site/subsite		
								Team Site/Subsite			
							Group	Group Team Site/Subsite			
							SharePoint	SharePoint Site Collection/Subsite			
							OneDrive	OneDrive		Merge	
		Single List/Library		Supported	Unsupported	Unsupported	Team	Channel Site	Private Channel Site/Subsite	Attach	
									Private Channel Site/Subsite > List/Library	Merge	
									Shared Channel Site/Subsite	Attach	
									Shared Channel Site/Subsite > List/Library	Merge	
								Team Site	Team Site/ Subsite	Attach	
									Team Site/ Subsite > List/ Library	Merge	
							Group	Group Team Site/Subsite		Attach	

How to Find Data	Source Object			Restore to Original Location	Restore to Storage	Export	Destination Object (Restore to Another Location)			Action	Comment
								Group Team Site/Subsite > List/ Library		Merge	
							SharePoint	Team Site/Subsite		Attach	
								Team Site/Subsite > List/Library		Merge	
							OneDrive	OneDrive		Attach	
								OneDrive > List/Library		Merge	
		Multiple Lists & Libraries with the Same Template		Supported	Unsupported	Supported	Team	Channel Site	Private Channel Site/Subsite	Attach	
									Shared Channel Site/Subsite		
								Team Site/Subsite			
							Group	Group Team Site/Subsite			
							SharePoint	Team Site/Subsite			
							OneDrive	OneDrive			
		Multiple Lists & Libraries		Supported	Unsupported	Unsupported	Unsupported				
		Library Folder		Supported	Supported	Supported	Team	Channel	Private Channel	Attach	
									Shared Channel		
									Standard Channel		
								Channel Site	Private Channel Site Library	Attach	
									Private Channel Site Library Folder	Merge/Attach	
									Shared Channel Site Library	Attach	
									Shared Channel Site Library Folder	Merge/Attach	
								Team Site	Shared Channel Site Library	Attach	
									Shared Channel Site Library Folder	Merge/Attach	
							Group	Group Team Site/Subsite Library		Attach	
								Group Team Site/Subsite Library Folder		Merge/Attach	
							SharePoint	Team Site/Subsite Library		Attach	
								Team Site/Subsite Library Folder		Merge/Attach	
							OneDrive	OneDrive Library		Attach	
								OneDrive Library Folder		Merge/Attach	
		List Folder		Supported	Supported	Supported	Team	Channel Site	Private Channel/ Subsite List	Attach	
									Private Channel/ Subsite List Folder	Merge/Attach	
									Shared Channel/ Subsite List	Attach	
									Shared Channel/ Subsite List Folder	Merge/Attach	
								Team Site	Team Site/ Subsite List	Attach	
									Team Site/ Subsite List Folder	Merge/Attach	
							Group	Group Team Site/Subsite List		Attach	
								Group Team Site/Subsite List Folder		Merge/Attach	
							SharePoint	Team Site/Subsite List		Attach	
								Team Site/Subsite List Folder		Merge/Attach	
							OneDrive	OneDrive List		Attach	
								OneDrive List Folder		Merge/Attach	
		Library Document		Supported	Supported	Supported	Team	Channel	Private Channel	Attach	
									Shared Channel		
									Standard Channel		
								Channel Site	Private Channel Site Library		
									Private Channel Site Library Folder		
									Shared Channel Site Library		
									Shared Channel Site Library Folder		
								Team Site	Shared Channel Site Library		
									Shared Channel Site Library Folder		
							Group	Group Team Site/Subsite Library			
								Group Team Site/Subsite Library Folder			
							SharePoint	Team Site/Subsite Library			
								Team Site/Subsite Library Folder			
							OneDrive	OneDrive Library			
								OneDrive Library Folder			

How to Find Data	Source Object			Restore to Original Location	Restore to Storage	Export	Destination Object (Restore to Another Location)			Action	Comment
		List Item & Attachment		Supported	Supported	Supported	Team	Channel Site	Private Channel/ Subsite List	Attach	
									Private Channel/ Subsite List Folder		
									Shared Channel/ Subsite List		
									Shared Channel / Subsite List Folder		
								Team Site	Team Site/ Subsite List		
									Team Site/ Subsite List Folder		
							Group	Group Team Site/Subsite List			
								Group Team Site/Subsite List Folder			
							SharePoint	Team Site/Subsite List			
								Team Site/Subsite List Folder			
							OneDrive	OneDrive List			
								OneDrive List Folder			
		App		Supported	Unsupported	Unsupported	Team	Channel Site	Private Channel Site/subsite	Attach	
									Shared Channel Site/Subsite		
								Team Site/Subsite			
							Group	Group Team Site/Subsite			
							Group Team Site/Subsite	SharePoint Site/Subsite			
							OneDrive	OneDrive Library Folder			
	Meetings	Meetings Folder		Supported	Unsupported	Unsupported	Unsupported				
		Meeting Item		Supported	Unsupported	Unsupported	Unsupported				
	Channels	Standard Channel	Standard Channel	Supported	Supported	Supported	Team			Attach	
							Team	Channel	Private Channel	Attach	
									Shared Channel		
									Standard Channel		
								Channel Site	Private Channel Site Library	Attach	
									Private Channel Site Library Folder	Merge/Attach	
									Shared Channel Site Library	Attach	
									Shared Channel Site Library Folder	Merge/Attach	
								Team Site	Shared Channel Site Library	Attach	
									Shared Channel Site Library Folder	Merge/Attach	
							Group	Group Team Site/Subsite Library		Attach	
								Group Team Site/Subsite Library Folder		Merge/Attach	
							SharePoint	Team Site/Subsite Library		Attach	
								Team Site/Subsite Library Folder		Merge/Attach	
							OneDrive	OneDrive Library		Attach	
								OneDrive Library Folder		Merge/Attach	
			Folder in the Channel’s Files Folder	Supported	Supported	Supported	Team	Channel	Private Channel	Attach	
									Shared Channel		
									Standard Channel		
								Channel Site	Private Channel Site Library	Attach	
									Private Channel Site Library Folder	Merge/Attach	
									Shared Channel Site Library	Attach	
									Shared Channel Site Library Folder	Merge/Attach	
								Team Site	Shared Channel Site Library	Attach	
									Shared Channel Site Library Folder	Merge/Attach	
							Group	Group Team Site/Subsite Library		Attach	
								Group Team Site/Subsite Library Folder		Merge/Attach	
							SharePoint	Team Site/Subsite Library		Attach	
								Team Site/Subsite Library Folder		Merge/Attach	
							OneDrive	OneDrive Library		Attach	
								OneDrive Library Folder		Merge/Attach	
			Files in the Channel’s Files Folder	Supported	Supported	Supported	Team	Channel	Private Channel	Attach	
									Shared Channel		

How to Find Data	Source Object			Restore to Original Location	Restore to Storage	Export	Destination Object (Restore to Another Location)			Action	Comment
									Standard Channel		
								Channel Site	Private Channel Site Library		
									Private Channel Site Library Folder		
									Shared Channel Site Library		
									Shared Channel Site Library Folder		
								Team Site	Shared Channel Site Library		
									Shared Channel Site Library Folder		
							Group	Group Team Site/Subsite Library			
								Group Team Site/Subsite Library Folder			
							SharePoint	Team Site/Subsite Library			
								Team Site/Subsite Library Folder			
							OneDrive	OneDrive Library			
								OneDrive Library Folder			
			Conversation	Supported	Supported	Supported	Unsupported				Channel conversations can be restored as posts or to HTML files.
		Private Channel	Private Channel	Supported	Supported	Unsupported	Unsupported				
			Channel’s Files Folder	Supported	Supported	Supported	Team	Channel	Private Channel	Attach	
									Shared Channel		
									Standard Channel		
								Channel Site	Private Channel Site Library	Attach	
									Private Channel Site Library Folder	Merge/Attach	
									Shared Channel Site Library	Attach	
									Shared Channel Site Library Folder	Merge/Attach	
								Team Site	Shared Channel Site Library	Attach	
									Shared Channel Site Library Folder	Merge/Attach	
							Group	Group Team Site/Subsite Library		Attach	
								Group Team Site/Subsite Library Folder		Merge/Attach	
							SharePoint	Team Site/Subsite Library		Attach	
								Team Site/Subsite Library Folder		Merge/Attach	
							OneDrive	OneDrive Library		Attach	
								OneDrive Library Folder		Merge/Attach	
			Folder in the Channel’s Files Folder	Supported	Supported	Supported	Team	Channel	Private Channel	Attach	
									Shared Channel		
									Standard Channel		
								Channel Site	Private Channel Site Library	Attach	
									Private Channel Site Library Folder	Merge/Attach	
									Shared Channel Site Library	Attach	
									Shared Channel Site Library Folder	Merge/Attach	
								Team Site	Shared Channel Site Library	Attach	
									Shared Channel Site Library Folder	Merge/Attach	
							Group	Group Team Site/Subsite Library		Attach	
								Group Team Site/Subsite Library Folder		Merge/Attach	
							SharePoint	Team Site/Subsite Library		Attach	
								Team Site/Subsite Library Folder		Merge/Attach	
							OneDrive	OneDrive Library		Attach	
								OneDrive Library Folder		Merge/Attach	
			Files in the Channel’s Files Folder	Supported	Supported	Supported	Team	Channel	Private Channel	Attach	
									Shared Channel		
									Standard Channel		
								Channel Site	Private Channel Site Library		
									Private Channel Site Library Folder		
									Shared Channel Site Library		

How to Find Data	Source Object			Restore to Original Location	Restore to Storage	Export	Destination Object (Restore to Another Location)			Action	Comment
									Shared Channel Site Library Folder		
								Team Site	Shared Channel Site Library		
									Shared Channel Site Library Folder		
							Group	Group Team Site/Subsite Library			
								Group Team Site/Subsite Library Folder			
							SharePoint	Team Site/Subsite Library			
								Team Site/Subsite Library Folder			
							OneDrive	OneDrive Library			
								OneDrive Library Folder			
			Conversation	Supported	Supported	Supported	Unsupported				
		Shared Channel	Shared Channel	Supported	Supported	Unsupported	Unsupported				
			Channel’s Files Folder	Supported	Supported	Supported	Team	Channel	Private Channel	Attach	
									Shared Channel		
									Standard Channel		
								Channel Site	Private Channel Site Library	Attach	
									Private Channel Site Library Folder	Merge/Attach	
									Shared Channel Site Library	Attach	
									Shared Channel Site Library Folder	Merge/Attach	
							Group	Group Team Site/Subsite Library		Attach	
								Group Team Site/Subsite Library Folder		Merge/Attach	
							SharePoint	Team Site/Subsite Library		Attach	
								Team Site/Subsite Library Folder		Merge/Attach	
							OneDrive	OneDrive Library		Attach	
								OneDrive Library Folder		Merge/Attach	
			Folder in the Channel’s Files Folder	Supported	SupportedSupported	Supported	Team	Channel	Private Channel	Attach	
									Shared Channel		
									Standard Channel		
								Channel Site	Private Channel Site Library	Attach	
									Private Channel Site Library Folder	Merge/Attach	
									Shared Channel Site Library	Attach	
									Shared Channel Site Library Folder	Merge/Attach	
								Team Site	Shared Channel Site Library	Attach	
									Shared Channel Site Library Folder	Merge/Attach	
							Group	Group Team Site/Subsite Library		Attach	
								Group Team Site/Subsite Library Folder		Merge/Attach	
							SharePoint	Team Site/Subsite Library		Attach	
								Team Site/Subsite Library Folder		Merge/Attach	
							OneDrive	OneDrive Library		Attach	
								OneDrive Library Folder		Merge/Attach	
			Files in the Channel’s Files Folder	Supported		Supported	Team	Channel	Private Channel	Attach	
									Shared Channel		
									Standard Channel		
								Channel Site	Private Channel Site Library		
									Private Channel Site Library Folder		
									Shared Channel Site Library		
									Shared Channel Site Library Folder		
								Team Site	Shared Channel Site Library		
									Shared Channel Site Library Folder		
							Group	Group Team Site/Subsite Library			
								Group Team Site/Subsite Library Folder			
							SharePoint	Team Site/Subsite Library			
								Team Site/Subsite Library Folder			
							OneDrive	OneDrive Library			
								OneDrive Library Folder			

How to Find Data	Source Object			Restore to Original Location	Restore to Storage	Export	Destination Object (Restore to Another Location)	Action	Comment
			Conversation	Supported	Supported	Supported	Unsupported		Channel conversations can be restored as posts or to HTML files.
	Planner	Plan		Supported	Unsupported	Unsupported	Teams	Attach	Plan configurations and the tasks belonging to the selected plans can be restored.
		Task		Supported	Unsupported	Unsupported	Unsupported		
	Group Conversation	Group Conversation		Supported	Unsupported	Unsupported	Unsupported		
		Item in Group Conversation		Supported	Unsupported	Unsupported	Unsupported		

Restore Conflict Resolutions

Refer to the table below for the available conflict resolutions against each object type in Exchange Online, OneDrive, SharePoint Online, Project Online, Public Folders, Microsoft 365 Groups, and Teams.

Note that the data in the table below shows the supported state while HSM is disabled.

Service Type	Object Type	Container Level Conflict Resolution	Content Level Conflict Resolution	App Conflict Resolution
Exchange Online	Mailbox	Skip Merge	Skip Append Overwrite	/
	Folder	Skip Merge	Skip Append Overwrite	/
	Mailbox Item	/	Skip Append Overwrite	/
OneDrive	OneDrive User	Skip Merge Replace	Skip Overwrite Overwrite by Last Modified Time Append an “_1” to the Item/Document	/
	Library	Skip Merge Replace	Skip Overwrite Overwrite by Last Modified Time Append an “_1” to the Item/Document	/
	Folder	Skip Merge Replace	Skip Overwrite Overwrite by Last Modified Time Append an “_1” to the Item/Document	/

Service Type	Object Type	Container Level Conflict Resolution	Content Level Conflict Resolution	App Conflict Resolution
	Documentt	/	Skip Overwrite Overwrite by Last Modified Time Append an “_1” to the Item/Document	/
SharePoint Online	Site Collection	Skip Merge Replace	Skip Overwrite Overwrite by Last Modified Time Append an “_1” to the Item/Document	Skip Overwrite
	Site	Skip Merge Replace	Skip Overwrite Overwrite by Last Modified Time Append an “_1” to the Item/Document	Skip Overwrite
	List/Library	Skip Merge Replace	Skip Overwrite Overwrite by Last Modified Time Append an “_1” to the Item/Document	/
	Folder	Skip Merge Replace	Skip Overwrite Overwrite by Last Modified Time Append an “_1” to the Item/Document	/
	Item/Document	/	Skip Overwrite Overwrite by Last Modified Time Append an “_1” to the Item/Document	/
	App	Skip Merge	/	Skip Overwrite

Service Type	**Object Type**	**Container Level Conflict Resolution**	**Content Level Conflict Resolution**	**App Conflict Resolution**
Project Online	Site Collection	Skip Merge Replace	Skip Overwrite Overwrite by Last Modified Time Append an “_1” to the Item/Document	Skip Overwrite
	Site	Skip Merge Replace	Skip Overwrite Overwrite by Last Modified Time Append an “_1” to the Item/Document	Skip Overwrite
	Project	Skip Merge Replace	Skip Overwrite Overwrite by Last Modified Time Append an “_1” to the Item/Document	/
	List/Library	Skip Merge Replace	Skip Overwrite Overwrite by Last Modified Time Append an “_1” to the Item/Document	/
	Folder	Skip Merge Replace	Skip Overwrite Overwrite by Last Modified Time Append an “_1” to the Item/Document	/
	Document	/	Skip Overwrite Overwrite by Last Modified Time Append an “_1” to the Item/Document	/
	App	Skip Merge	/	Skip Overwrite
Public Folder	Folder	Skip	Skip Overwrite	/

Service Type	Object Type	Container Level Conflict Resolution	Content Level Conflict Resolution	App Conflict Resolution
	Mailbox Item	/	Skip Overwrite	/
Microsoft 365 Groups	Group	Skip Merge	Skip Overwrite Overwrite by Last Modified Time Append an “_1” to the Item/Document	Skip Overwrite
	Group Team Site	Skip Merge Replace	Skip Overwrite Overwrite by Last Modified Time Append an “_1” to the Item/Document	Skip Overwrite
	Site	Skip Merge Replace	Skip Overwrite Overwrite by Last Modified Time Append an “_1” to the Item/Document	Skip Overwrite
	List/Library	Skip Merge Replace	Skip Overwrite Overwrite by Last Modified Time Append an “_1” to the Item/Document	/
	Folder in SharePoint	Skip Merge Replace	Skip Overwrite Overwrite by Last Modified Time Append an “_1” to the Item/Document	/
	Document	/	Skip Overwrite Overwrite by Last Modified Time Append an “_1” to the Item/Document	/
	App	Skip Merge	/	Skip Overwrite

Service Type	Object Type	Container Level Conflict Resolution	Content Level Conflict Resolution	App Conflict Resolution
	Group Mailbox	/	Skip Overwrite	/
	Folder in Mailbox	/	Skip Overwrite	/
	Mailbox Item	/	Skip Overwrite	/
	Plan	/	Skip Overwrite	/
	Task	/	Skip Overwrite	/
Teams	Team	Skip Merge	Skip Overwrite Overwrite by Last Modified Time Append an "_1" to the Item/Document	Skip Overwrite
	Group Team Site	Skip Merge Replace	Skip Overwrite Overwrite by Last Modified Time Append an "_1" to the Item/Document	Skip Overwrite
	Site	Skip Merge Replace	Skip Overwrite Overwrite by Last Modified Time Append an "_1" to the Item/Document	Skip Overwrite
	List/Library	Skip Merge Replace	Skip Overwrite Overwrite by Last Modified Time Append an "_1" to the Item/Document	/
	Folder in SharePoint	Skip Merge Replace	Skip Overwrite Overwrite by Last Modified Time Append an "_1" to the Item/Document	/

Service Type	Object Type	Container Level Conflict Resolution	Content Level Conflict Resolution	App Conflict Resolution
	Document	/	Skip Overwrite Overwrite by Last Modified Time Append an "_1" to the Item/Document	/
	App	Skip Merge	/	Skip Overwrite
	Group Mailbox	/	Skip Overwrite	/
	Folder in Mailbox	/	Skip Overwrite	/
	Mailbox Item	/	Skip Overwrite	/
	Plan	/	Skip Overwrite	/
	Task	/	Skip Overwrite	/
	Public Channel	Skip Merge Replace	Skip Overwrite Overwrite by Last Modified Time Append an "_1" to the Item/Document	/
	Channel > Conversations	/	/	/
	Channel > Files	Skip Merge Replace	Skip Overwrite Overwrite by Last Modified Time Append an "_1" to the Item/Document	/
	Channel > Files > Folder	Skip Merge Replace	Skip Overwrite Overwrite by Last Modified Time Append an "_1" to the Item/Document	/

Service Type	Object Type	Container Level Conflict Resolution	Content Level Conflict Resolution	App Conflict Resolution
	Private Channel	Skip Merge Replace	Skip Overwrite Overwrite by Last Modified Time Append an "_1" to the Item/Document	/
	Private Channel > Conversations	/	/	/
	Private Channel > Files	Skip Merge Replace	Skip Overwrite Overwrite by Last Modified Time Append an "_1" to the Item/Document	/
	Private Channel > Files > Folder	Skip Merge Replace	Skip Overwrite Overwrite by Last Modified Time Append an "_1" to the Item/Document	/
	Meetings	/	Skip Overwrite	/
	Group Conversations	/	Skip Overwrite	/
Viva Engage	Viva Engage Community	Skip Merge	Skip Overwrite Overwrite by Last Modified Time Append an "_1" to the Item/Document	Skip Overwrite
	Viva Engage Messages	Skip Merge Replace	Skip Overwrite Overwrite by Last Modified Time Append an "_1" to the Item/Document	/
	Viva Engage Files	Skip Merge Replace	Skip Overwrite Overwrite by Last Modified Time Append an "_1" to the Item/Document	/

Service Type	Object Type	Container Level Conflict Resolution	Content Level Conflict Resolution	App Conflict Resolution
	Site Collection	Skip Merge Replace	Skip Overwrite Overwrite by Last Modified Time Append an "_1" to the Item/Document	Skip Overwrite
	Site	Skip Merge Replace	Skip Overwrite Overwrite by Last Modified Time Append an "_1" to the Item/Document	Skip Overwrite
	List/Library	Skip Merge Replace	Skip Overwrite Overwrite by Last Modified Time Append an "_1" to the Item/Document	/
	App	Skip Merge	/	Skip Overwrite
	Folder in SharePoint	Skip Merge Replace	Skip Overwrite Overwrite by Last Modified Time Append an "_1" to the Item/Document	/
	Document	/	Skip Overwrite Overwrite by Last Modified Time Append an "_1" to the Item/Document	/
	Plan	/	Skip Overwrite	/
	Task	/	Skip Overwrite	/
Microsoft Teams Chat	User	/	/	/
	Chat	/	/	/
	Chat Message	/	/	/

Appendix A - Accessibility features for the IBM® Storage Protect for Cloud

Accessibility features assist users who have a disability, such as restricted mobility or limited vision, to use information technology content successfully.

Overview

The IBM® Storage Protect for Cloud includes the following major accessibility features:

- Keyboard-only operation
- Operations that use a screen reader

The IBM® Storage Protect for Cloud product ensures compliance with US Section 508, Web Content Accessibility Guidelines (WCAG) 2.0, and EN 301 549. To take advantage of accessibility features, use the latest release of your screen reader and the latest web browser that is supported by the product.

The product documentation in IBM® Documentation is enabled for accessibility.

Keyboard navigation

This product uses standard navigation keys.

Interface information

User interfaces do not have content that flashes 2 - 55 times per second.

Web user interfaces rely on cascading style sheets to render content properly and to provide a usable experience. The application provides an equivalent way for low-vision users to use system display settings, including high-contrast mode. You can control font size by using the device or web browser settings.

Related accessibility information

In addition to standard IBM® help desk and support websites, IBM® has a TTY telephone service for use by deaf or hard of hearing customers to access sales and support services:
TTY service
800-IBM®-3383 (800-426-3383)
(within North America)

For more information about the commitment that IBM® has to accessibility, see IBM® Accessibility.

Notices

This information was developed for products and services offered in the US. This material might be available from IBM® in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

IBM® may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM® representative for information on the products and services currently available in your area. Any reference to an IBM® product, program, or service is not intended to state or imply that only that IBM® product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM® intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM® product, program, or service.

IBM® may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:
IBM® Director of Licensing
IBM® Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM® Intellectual Property Department in your country or send inquiries, in writing, to:
Intellectual Property Licensing
Legal and Intellectual Property Law
IBM® Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM® may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM® websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM® product and use of those websites is at your own risk.

IBM® may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:
IBM® Director of Licensing
IBM® Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM® under terms of the IBM® Customer Agreement, IBM® International Program License Agreement or any equivalent agreement between us.

The performance data discussed herein is presented as derived under specific operating conditions. Actual results may vary.

Information concerning non-IBM® products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM® has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM® products. Questions on the capabilities of non-IBM® products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM®, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM®, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM® shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work must include a copyright notice as follows: © (your company name) (year). Portions of this code are derived from IBM® Corp. Sample Programs. © Copyright IBM® Corp. _enter the year or years_.

Trademarks

IBM®, the IBM® logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM® or other companies. A current list of IBM® trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

Adobe™ is a registered trademark of Adobe™ Systems Incorporated in the United States, and/or other countries.

Linear Tape-Open™, LTO™, and Ultrium™ are trademarks of HP, IBM® Corp. and Quantum in the U.S. and other countries.

Intel™ and Itanium™ are trademarks or registered trademarks of Intel™ Corporation or its subsidiaries in the United States and other countries.

The registered trademark Linux® is used pursuant to a sublicense from the Linux® Foundation, the exclusive licensee of Linus Torvalds, owner of the mark on a worldwide basis.

Microsoft™, Windows™, and Windows NT™ are trademarks of Microsoft™ Corporation in the United States, other countries, or both.

Java™ and all Java™-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Red Hat®, OpenShift®, Ansible®, and Ceph® are trademarks or registered trademarks of Red Hat®, Inc. or its subsidiaries in the United States and other countries.

UNIX® is a registered trademark of The Open Group in the United States and other countries.

VMware, VMware vCenter Server™, and VMware vSphere™ are registered trademarks or trademarks of VMware, Inc. or its subsidiaries in the United States and/or other jurisdictions.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the IBM® website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM®.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM®.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.
IBM® reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM®, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM® MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

Privacy policy considerations

IBM® Software products, including software as a service solutions, (“Software Offerings”) may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user, or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering’s use of cookies is set forth below.

This Software Offering does not use cookies or other technologies to collect personally identifiable information.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, see IBM®’s Privacy Policy at http://www.ibm.com/privacy and IBM®’s Online Privacy Statement at http://www.ibm.com/privacy/details in the section entitled “Cookies, Web Beacons and Other Technologies,” and the “IBM® Software Products and Software-as-a-Service Privacy Statement” at http://www.ibm.com/software/info/product-privacy.

© Copyright International Business Machines Corporation 2022, 2024

US Government Users Restricted Rights - Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp