IBM Spectrum Protect Plus Online Services

Tables of Contents

IBM Spectrum Protect Plus Online Services documentation

Accessibility features for the IBM Spectrum Protect Plus Online Services

Accessibility features assist users who have a disability, such as restricted mobility or limited vision, to use information technology content successfully.

Overview

The IBM Spectrum® Protect Plus Online Services includes the following major accessibility features:

- Keyboard-only operation
- Operations that use a screen reader

The IBM Spectrum Protect Plus Online Services 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.

PDFs

The IBM Spectrum® Protect Plus Online Services product documentation is available in a collection of PDF files.

The following PDF guides are available to view or download:

- IBM Spectrum Protect Plus Online Services
- IBM Spectrum Protect Plus Online Services for Microsoft 365
- IBM Spectrum Protect Plus Online Services Web API Guide
- IBM Spectrum Protect Plus Online Services Recovery Portal Guide

IBM Spectrum Protect Plus Online Services updates

Learn about new features and updates in IBM Spectrum Protect Plus Online Services.

Release Date: July 31, 2022

New features and updates

- In **Auto Discovery**, the **Microsoft 365 User** object type and **Microsoft 365 Users** container is now available for all IBM Spectrum Protect Plus Online Services.

- For organizations that use the IBM Spectrum Protect Plus Online Services and have a working subscription for IBM Spectrum Protect Plus Online Services, the **IBM Spectrum Protect Plus Online Services Recovery Portal** portal is now available. For more information, refer to IBM Spectrum Protect Plus Online Services Recovery Portal.

The following sections of the documentation have been updated:

- Add Users
- IBM Spectrum Protect Plus Online Services Administration for Office 365
- Download a List of Reserved IP Addresses
- User Activity Report Information
- Appendix E - When Service Account and App Profile are Used

- **Updates in previous versions**

Updates in previous versions

Release Date: June 5, 2022

- German is now an available display language for IBM Spectrum® Protect Plus Online Services and the Germany West Central (Frankfurt) data center is now supported.
- If your tenant is using IBM Spectrum Protect Plus Online Services to protect Microsoft Planner data, you can now go to App Management to configure an app profile for a Microsoft delegated app with the assigned permissions. After the delegated app profile has been created, go to Auto Discovery, and add the delegated app profile to a scan profile which uses the app profile authentication method and includes Microsoft Teams in the scan scope.
- The following apps have been updated to add the Microsoft Graph API permissions that replace the Azure Active Directory API permissions:
  - IBM Spectrum Protect Plus Online Services Administrator for Office 365
  - IBM Spectrum Protect Plus Online Services Administrator for SharePoint
  - IBM Spectrum Protect Plus Online Services Administrator for Exchange
    If your tenant is using the apps above, you need to reauthorize the apps in IBM Spectrum Protect Plus Online Services > App Management.
- You can get a 30-day trial license when you sign up for IBM Spectrum Protect Plus Online Services.

The following sections of the documentation have been updated:

- Language Support
- IBM Spectrum Protect Plus Online Services Versions and Environments
- Sign Up IBM Spectrum Protect Plus Online Services
- App Profile for a Microsoft Delegated App
- Auto Discovery Notification
- Email Settings
- IBM Spectrum Protect Plus Online Services Administration for Azure
- IBM Spectrum Protect Plus Online Services Administration for Office 365
- IBM Spectrum Protect Plus Online Services Administration for SharePoint
- IBM Spectrum Protect Plus Online Services Administration for Exchange

Release Date: Mar 29, 2022

In Auto Discovery, when you configure a scan profile and the selected app profile cannot meet your data management requirements, you can add a service account profile as an additional method to manage your Microsoft 365 data. For more information, see Manage Scan Profiles.In Auto Discovery, when you configure a scan profile of the advanced mode to scan SharePoint Sites, Microsoft 365 Groups/Microsoft Teams/Yammer Communities, or Project Sites, you can now set Sensitivity Label rules to scan objects into containers.

The following sections of the documentation have been updated:

- Auto Discovery for Microsoft 365
- Appendix A - Supported Criteria in Auto Discovery Rules
- Manage Microsoft 365 Account Pool
- Download a List of Reserved IP Addresses

About IBM Spectrum Protect Plus Online Services

IBM Spectrum Protect Plus Online Services is a multi-tenant software as a service (SaaS) platform that requires no installation and minimal configuration to protect your Microsoft 365 resources. With a browser-based user interface and a fully distributed architecture, IBM Spectrum Protect Plus Online Services integrates powerful data migration, management, and protection technologies into a highly scalable solution for Microsoft 365 services such as SharePoint Online, Exchange Online, Microsoft 365 Groups, Microsoft Teams, and others.

IBM Spectrum Protect Plus Online Services serves as a central hub for the IBM Spectrum Protect Plus Online Services for Microsoft 365.

- **Language Support**
- **IBM Spectrum Protect Plus Online Services Versions and Environments**
- **Supported Browsers**

Language Support

IBM Spectrum® Protect Plus Online Services supports the following languages: English, German, and French.

IBM Spectrum Protect Plus Online Services Versions and Environments

The production version has various options based on your Microsoft 365 environment.

Microsoft 365 Environment	IBM Spectrum Protect Plus Online Services Environment
Global Microsoft 365	https://spponlineservices.ibm.com
Office 365 Germany	https://spponlineservices.ibm.com

Note: If you are using the Office 365 Germany environment, the app profile authentication method is not supported. You can use the service account authentication method.

All versions and environments are covered in this guide. The table below lists the differences.

	Commercial Production Environment
Sign-in Address	https://spponlineservices.ibm.com
Sign-in Methods	Sign in with: Local account Microsoft 365 account
Supported Data Centers	Canada Central (Toronto) East US2 (Virginia) Germany West Central (Frankfurt)

Supported Browsers

The following table provides the required browser versions.

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

The following sections provide the answers to questions you may encounter when using the IBM Spectrum® Protect Plus Online Services portal.

What If Your Tenant Does Not Allow Users to Consent to Apps?

If your Microsoft 365 tenant does not allow users to consent to apps on their behalf, Microsoft 365 users who are added as IBM Spectrum® Protect Plus Online Services users cannot sign into IBM Spectrum Protect Plus Online Services with their Microsoft 365 login IDs. Microsoft will display the **Need admin approval** page to them.

Prior to adding Microsoft 365 users as IBM Spectrum Protect Plus Online Services users, IBM Spectrum Protect Plus Online Services recommends that you check the Users can consent to apps accessing company data on their behalf option in Microsoft Azure Azure Active Directory > User settings > Enterprise applications. If the option is set to No, a Microsoft 365 Global Administrator must first consent to the IBM Spectrum Protect Plus Online Services app.

Microsoft 365 Global Administrator can consent to the **IBM Spectrum Protect Plus Online Services** app by completing the following steps:

1. Navigate to Azure Active Directory admin center > Azure Active Directory > Enterprise applications.
2. Select the IBM Spectrum Protect Plus Online Services app.
3. In the menu, click Permissions in the Security group.
4. On the Permissions page, click Grant admin consent for [Tenant name] to grant admin consent.
5. Enter the username and password of a Microsoft 365 Global Administrator account.
6. Click Sign in.

7. The required permissions of the IBM Spectrum Protect Plus Online Services app are displayed. Review the permissions and click Accept.

What is the Difference Between Service Account Profile and App Profile?

Auto Discovery requires an authentication method, either using a service account profile or an app profile. If you select a service account profile as the authentication method, the credentials of the account within the profile will be used to scan and manage Microsoft 365 objects. If you do not want to provide your account and password, or your organization uses multi-factor authentication in Microsoft 365, you must choose the app profile authentication method to use the app token to back up or manage data, and the credentials of the Microsoft 365 Global Administrator account will not be stored by Microsoft 365. Refer to Will the App Profile Method Meet Your Data Management Requirements? to help you determine if using the app profile method will satisfy your data management requirements.

How Many Accounts Should be Added into an Account Pool?

If this is the first time you are backing up objects, we recommend that the added group in the account pool contains at least 7 users for managing every 1000 objects. If it is not the first time you are backing up objects, we recommend that the added group in the account pool contain at least 3 users for managing every 2000 objects.

For example:

- If you want to back up 2000 SharePoint Online site collections for the first time with IBM Spectrum® Protect Plus Online Services for Microsoft 365, you must add at least 14 users to the account pool.
- If you want to back up 1000 SharePoint Online site collections and 2000 OneDrive for Business for the first time using IBM Spectrum Protect Plus Online Services for Microsoft 365, you must add at least 21 users to the account pool.
- If you want to back up 2000 SharePoint Online site collections after you have run the first backup job, you must add at least 3 users to the account pool.
- If you want to back up 1000 SharePoint Online site collections and 2000 OneDrive for Business after you have run the first backup job, you must add at least 4 users to the account pool.

What Services Can Use a Microsoft 365 Account Pool?

The following service will use the Microsoft 365 account pool when the service account authentication method is used in the corresponding scan profile:

IBM Spectrum® Protect Plus Online Services for Microsoft 365
: The backup for SharePoint sites, Project sites, OneDrive for Business, Microsoft 365 Group team sites, and Exchange public folders.

What Should I Do If My Organization Uses Multi-Factor Authentication (MFA) in Microsoft 365?

If your organization uses multi-factor authentication (MFA) in Microsoft 365, to get started in IBM Spectrum® Protect Plus Online Services, refer to the following to configure the Microsoft 365 MFA Service Account Profile, the App Profile for Microsoft 365, Auto Discovery, and the Microsoft 365 Account Pool containing MFA users.

Microsoft 365 MFA Service Account Profile
: Microsoft 365 service account profile is used to connect Microsoft 365 to IBM Spectrum Protect Plus Online Services. When creating a Microsoft 365 service account profile, enable MFA and provide the app password of the Microsoft 365 account. For more details, refer to Create a Service Account Profile. However, Microsoft 365 MFA Service Account Profile cannot be used in Auto Discovery to scan objects or be used to invite Microsoft 365 users/groups as IBM Spectrum Protect Plus Online Services users, so App Profile for Microsoft 365 is required.

App Profile for Microsoft 365
: App Profile for Microsoft 365 is required if one of the following circumstances are met:

  - You want to add Microsoft 365 users or groups as IBM Spectrum Protect Plus Online Services users.
  - You use Auto Discovery to scan Microsoft 365 objects.

  For more information, refer to Create an App Profile for Microsoft 365.

Auto Discovery
: When configuring a scan profile to scan Microsoft 365 objects, you must choose the **Use an app profile** authentication method and select a Microsoft 365 Service Account Profile with MFA enabled. For more information, refer to Manage Auto Discovery.
  Note the following:

  - Some Microsoft 365 services are not supported by the app profile authentication method with Microsoft 365 MFA service account. For more information, refer to Appendix E - When Service Account and App Profile are Used.
  - Refer to Will the App Profile Method Meet Your Data Management Requirements? to help you determine if using the app profile method will satisfy your data management requirements.

Microsoft 365 Account Pool
: SharePoint Online has a built-in throttling feature that prevents one account from processing several requests simultaneously. To avoid getting throttled or blocked in SharePoint Online, you can configure the account pool in IBM Spectrum Protect Plus Online Services. The account pool contains multiple

Microsoft 365 accounts. When configuring the account pool, enable MFA and provide the app passwords of the Microsoft 365 accounts. For more information, refer to Manage Microsoft 365 Account Pool.

Does IBM Spectrum Protect Plus Online Services Support Microsoft 365 Tenants with Multi-Geo Licenses?

With Microsoft 365 Multi-Geo, your organization can expand its Microsoft 365 presence to multiple geographic regions and/or countries within your existing tenant. You can provision and store data at rest in the geo locations that you have chosen to meet data residency requirements, and at the same time, unlock your global rollout of modern productivity experiences to your workforce.

If your Microsoft 365 tenant has a Microsoft 365 Multi-Geo , you can pair this with a similar license for IBM Spectrum Protect Plus Online Services for Microsoft 365.
Note: While you can use a standard IBM Spectrum Protect Plus Online Services for Microsoft 365 license to support a multi-geo Microsoft 365 tenant with no changes, all data will be protected and stored centrally in a single IBM Spectrum Protect Plus Online Services tenant. To take advantage of our global network, you will need to purchase a license from IBM Spectrum Protect Plus Online Services to leverage our multi-geo infrastructure described below.
Because your tenant will be supported by IBM Spectrum Protect Plus Online Services data centers around the world, we want to make sure that you are familiar with which data centers will be supporting you.

Start by going to **Data Center Mappings** and reviewing the list of geo locations from your Microsoft 365 tenant that are detected and the supporting data centers from IBM Spectrum Protect Plus Online Services. For more information, refer to Manage Data Center Mappings.

Next, in **Auto Discovery**, ensure that you are using the filters provided in the advanced scan mode to separate mailboxes, OneDrives, sites, and other Microsoft 365 content by their preferred data locations. These boundaries are used to help distribute the management for each of these containers around the world. For more information, refer to Advanced Mode.

Finally, you can create separate administrators for each geo location using delegated administration in **User Management**, which maintains segregation among geo locations. For more information, refer to Manage Users.

How Do I Select the Right Conditions?

When you configure rules for an advanced mode scan profile in **Auto Discovery**, refer to the information below to select a proper condition from **Equals**, **Contains**, and **Matches**:

Equals
: Use this condition to scan Microsoft 365 objects whose property values are equal to the entered value.

Contains
: Use this condition to scan Microsoft 365 objects whose property values contain the entered value.

Matches
: Use this condition to scan Microsoft 365 objects whose property values match the entered value and wildcards.

For example, when you scan SharePoint sites by the **URL** criterion, you can refer to the following to configure conditions:

- If you want to scan the SharePoint site whose URL is **https://contoso.sharepoint.com/sites/site1**, choose the **Equals** condition and set the value to the desired SharePoint site URL.
- If you want to scan the SharePoint sites whose URLs contain **site1**, choose the **Contains** condition and set the value to **site1**.
- If you want to scan the SharePoint sites whose URLs begin with **https://contoso.sharepoint.com/sites/**, choose the **Matches** condition and set the value to **https://contoso.sharepoint.com/sites/***.

Will the App Profile Method Meet Your Data Management Requirements?

To back up or manage your Microsoft 365 data in services for Microsoft 365, you must first use IBM Spectrum® Protect Plus Online Services Auto Discovery to scan or add Microsoft 365 objects. Auto Discovery provides the service account profile and app profile authentication methods to scan objects. The easiest way to work with your environment is by registering an app profile. This ensures that all jobs that run in your environment are tagged as IBM Spectrum Protect Plus Online Services activities, and also ensures that we do not need to store any service accounts or passwords. When you use the app profile authentication method to scan objects, the app token within the app profile will be used to back up or manage data, and the credentials of the Microsoft 365 Global Administrator account will not be stored by IBM Spectrum Protect Plus Online Services — only the consent of your administrator is recorded and this consent can be monitored in your Azure AD and can be revoked at any time from your environment. While using the app profile method is suggested, there are specific instances when this method is not recommended. Refer to the information in the links below to help you determine if using the app profile method will satisfy your data management requirements.

- IBM Spectrum Protect Plus Online Services for Microsoft 365
  - SharePoint Sites Data Types
  - Exchange Online Data Types
  - Public Folders Data Types
  - Microsoft 365 Groups Data Types
  - Teams Data Types
  - Modern Team Site Data Types
  - Document-Related Data Types

Why Admin Consent is Required to Use the IBM Spectrum Protect Plus Online Services App?

According to the Microsoft's standard Azure app consent process, when adding an app to your Microsoft 365 environment, consent is required by your Global Admin since it is necessary for the Global Admin to review the permissions required by the apps. For more information about admin consent, refer to the Microsoft technical article: Who has permission to add applications to my Azure AD instance?

Note the following:

- The Global Admin account is not stored by IBM Spectrum Protect Plus Online Services. The consent process is managed by Microsoft, so your username and password are never shared with IBM Spectrum Protect Plus Online Services during the consent process.
- Admin consent does not grant admin privileges to the IBM Spectrum Protect Plus Online Services apps. For a list of the permissions that IBM Spectrum Protect Plus Online Services apps request, refer to Permissions for Microsoft App Authorization. For instructions on creating app profiles for installing the aSpps, refer to the Manage App Profiles section.

Get Started

Refer to the following sections to get started in IBM Spectrum® Protect Plus Online Services.

- **Sign Up IBM Spectrum Protect Plus Online Services**
  IBM Spectrum Protect Plus Online Services provides new tenants with a 30-day trial license for each online service.
- **Sign into IBM Spectrum Protect Plus Online Services**
- **Use the Quick Start Wizard**
  IBM Spectrum Protect Plus Online Services provides a wizard with the following steps to help you get started.
- **Manage Your Services**
  The Home page provides the following views:
- **IBM Spectrum Protect Plus Online Services User Roles**
  In IBM Spectrum Protect Plus Online Services, different user roles can perform different actions. There are three main user roles: Tenant Owner, Service Administrator, and Tenant User.
- **Manage Users**
  To manage IBM Spectrum Protect Plus Online Services users, navigate to Management > User Management. On the User Management page, the Tenant Owner, Service Administrators, and Application Administrators can use the following views to manage users and permissions:
- **Required Permissions**
  Refer to the sections below for the required permissions for authorizing IBM Spectrum Protect Plus Online Services apps and using IBM Spectrum Protect Plus Online Services for Microsoft 365 properly.

Sign Up IBM Spectrum Protect Plus Online Services

IBM Spectrum Protect Plus Online Services provides new tenants with a 30-day trial license for each online service.

Procedure

Go to IBM Spectrum Protect Plus Online Services - Free Trial and complete the steps below:

1. Select your data center – Select the data center closest to your Microsoft 365 tenant for the best performance. After the signup is finished, you cannot change the data center. Click Next.
   Note: For the services which have not been supported in your data center, you can also select your interested services to receive the notification email once they are supported.
2. Select your services – From the services that are available in your data center, select the services you want to use. Click Next.
3. Provide your information – Complete the required fields, Terms and Conditions and Privacy Policy, and Communication Preferences settings. Click Submit.
4. The **Check Email to Activate Your Account** page appears, and a confirmation email is sent to your corporate email address. If you have not received the confirmation email, click the Resend a Confirmation Email button on the bottom of the **Check Email to Activate Your Account page**. Once you receive the email, click the supplied link to activate your account within 30 days. The link will be active for 30 days.

Sign into IBM Spectrum Protect Plus Online Services

Access the following addresses according to the environment you are using.

- The production environment for commercial use https://spponlineservices.ibm.com

On the IBM Spectrum Protect Plus Online Services sign-in page, choose the following sign-in method:

- Sign in with a Local Account
- Sign in with a Microsoft 365 Account

- **Sign in with a Local Account**
  To sign in with an IBM Spectrum Protect Plus Online Services local account, complete the following steps:

- **Sign in with a Microsoft 365 Account**
  To sign in with a Microsoft 365 account, complete the following steps:

Sign in with a Local Account

To sign in with an IBM Spectrum® Protect Plus Online Services local account, complete the following steps:

Procedure

On the sign-in page, enter your login information:

1. Login ID – Enter the email address used as your IBM Spectrum Protect Plus Online Services local account.
2. Password – Enter your password.
   Note: If the password is entered incorrectly three consecutive times, your account will be locked. After an hour, it will automatically unlock. You can also refer to the instructions in Reset Your Local Account Password to retrieve and reset your password.

- **Reset Your Local Account Password**
  You can reset the password of your IBM Spectrum Protect Plus Online Services local account.

Reset Your Local Account Password

You can reset the password of your IBM Spectrum® Protect Plus Online Services local account.

Procedure

Complete the following steps:

1. Navigate to the IBM Spectrum Protect Plus Online Services sign-in page.
2. Click the Forgot Password link under the Sign In button.
3. Enter the following information:
   - **Username** – Enter the email address used as your IBM Spectrum Protect Plus Online Services username.
   - **Verification Code** – Enter the verification code. Click Refresh to refresh the verification graphic if no image is displayed.
4. 4. Click Reset Password to set a new password. A verification email is sent to the email address you specified. Retrieve the email message and click the supplied link to set a new password. After clicking the link, you will be redirected to the Reset Your Password page. Enter the following information on this page:
   - **New Password** – Enter a new password.
   - **Confirm Password** – Enter the new password again for confirmation.
   - **Verification Code** – Enter the verification code. Click Refresh to refresh the verification graphic if no image is displayed.
5. After setting up the new password, click Reset Password to save your new password, and then click OK in the pop-up window. You are redirected to the sign-in page. You can sign into IBM Spectrum Protect Plus Online Services with the new password.
   Note: The link in the verification email for resetting a new password will expire in 24 hours. If you do not reset the password within 24 hours, repeat the steps above to finish resetting your password.

Sign in with a Microsoft 365 Account

To sign in with a Microsoft 365 account, complete the following steps:

Procedure

1. On the sign-in page, click Sign in with Microsoft.
   Note: If you are using the Microsoft 365 account to sign into another app on the same browser, you will be automatically signed into IBM Spectrum® Protect Plus Online Services.
2. On the Microsoft 365 authentication page, enter an existing Microsoft 365 login ID and password.
3. Click Sign in.
4. If it is the first time that this Microsoft 365 account is signing into IBM Spectrum Protect Plus Online Services, the required permissions are displayed. Review the permissions and click Accept. The IBM Spectrum Protect Plus Online Services app is generated in My apps on Microsoft 365. You can click the app to access IBM Spectrum Protect Plus Online Services within Microsoft 365. The app will remember your credentials when you sign in through it.
   Note: If the Need admin approval page appears, it indicates that your tenant does not allow users to consent to apps and you must contact your Microsoft 365 Global Administrator to consent to the IBM Spectrum Protect Plus Online Services app first. For details of consenting to the IBM Spectrum Protect Plus Online Services app by Microsoft 365 Global Administrator, refer to What If Your Tenant Does Not Allow Users to Consent to Apps?.
   Note: If your Microsoft 365 account does not exist but your tenant exists in IBM Spectrum Protect Plus Online Services, the Join IBM Spectrum Protect Plus Online Services page will appear. If you would like to request to join the existing tenant, you can contact your Service Administrator to invite you into IBM Spectrum Protect Plus Online Services.

Use the Quick Start Wizard

IBM Spectrum® Protect Plus Online Services provides a wizard with the following steps to help you get started.

Procedure

1. Accept License Agreements – The Tenant Owner can click License Agreement to view and accept license agreements for services. After you finish, go to the next step in this wizard.
2. Register the IBM Spectrum Protect Plus Online Services App – The app that ensures IBM Spectrum Protect Plus Online Services functionality work in your Microsoft 365 environment is generated by an app profile. Registering an app profile ensures that all IBM Spectrum Protect Plus Online Services activities in your environment will be tagged and also ensures that IBM Spectrum Protect Plus Online Services will not store any service accounts or passwords. To create an app profile, select an app for the app profile, configure the corresponding settings, and then click Create an App Profile to proceed. For more information about creating app profiles, refer to Manage App Profiles. After you finish, go to the next step in the wizard. You can also click Back to view the previous step.
3. Map Your Data Locations – If your Microsoft 365 tenant has been enabled for Multi-Geo support (Microsoft 365 Multi-Geo) and will be supported by IBM Spectrum Protect Plus Online Services instances around the world, this step will appear in the wizard. In Data Center Mappings, default mappings are provided for you to review which IBM Spectrum Protect Plus Online Services data centers will be supporting your Microsoft 365 geo locations. Since you cannot separate these geo locations later, we want to make sure you review and make any changes before you start. For more information about data center mappings, refer to Manage Data Center Mappings. After you finish, go to the next step in the wizard. You can also click Back to view the previous step.
4. Discover Content – If you have services that need to scan objects from your Microsoft 365 environment to IBM Spectrum Protect Plus Online Services, this step will appear to help you discover content in your environment. Read the introductions for Express® Mode and Advanced Mode, and select one mode to create a scan profile. Click Create a Scan Profile to open a new tab and create one. For more information about scan profiles, refer to the Manage Scan Profiles section in Manage Auto Discovery. After you finish, go to the next step in the wizard. You can also click Back to view the previous step.
5. Protect Your Data – You can apply encryption profiles to encrypt backup data and sensitive tenant information using Azure Key Vault. To create an encryption profile using your own Azure Key Vault, you can click Create an Encryption Profile to open a new tab and create one. If you want to use the IBM Spectrum Protect Plus Online Services default encryption profile, select IBM Spectrum Protect Plus Online Services Managed Encryption and click Next to proceed. For information about creating custom encryption profiles, refer to Create an Encryption Profile. After you finish, go to the next step in the wizard. You can also click Back to view the previous step.
6. Manage Users – If you want to invite users from your organization to IBM Spectrum Protect Plus Online Services, or want to leverage single sign-on with your corporate identity, click Invite Users to open a new tab to proceed. For more information about adding users, refer to Add Users. After you finish this step, click Finish. The wizard is completed.

Manage Your Services

The Home page provides the following views:

- My Favorite Apps – This view displays the services you selected as favorites. Click a service name to access that service.

You can click the heart button to remove a service from your favorites.

- All Apps – This view displays all services that your tenant has purchased or for which it has started the trial. Click a service name to access that service.
  - You can click the heart button to add a service to the My Favorite Apps view.
  - If the licenses of one or more services have expired, you can select the Hide expired services from the All Apps view check box, and you will not see the expired services under this view.
- Store – This view displays all services within the IBM Spectrum® Protect Plus Online Services platform. You can start a trial for services that were not selected when your tenant signed up for IBM Spectrum Protect Plus Online Services. For details, refer to Start Trial of Additional Services.

IBM Spectrum Protect Plus Online Services can be used in two ways, either by obtaining a full license or with a free trial. The license for each online service is calculated in Greenwich Mean Time (GMT 0:00). Even if the available license duration is less than 24 hours, it is calculated as one day.

- **Activate Your Services**
  Prior to inviting users to use a service, as a Tenant Owner, you must accept the service license agreement to activate the service.
- **Obtain a Full License**
  To obtain a full license for any of the IBM Spectrum Protect Plus Online Services, contact IBM Software Support.
- **Start Trial of Additional Services**
  If your tenant wants to start a trial for services that were not selected when your tenant signed up for IBM Spectrum Protect Plus Online Services, the Tenant Owner and Service Administrators can start a trial on the Home page. Refer to the section below to obtain the trial licenses of services.

Activate Your Services

Prior to inviting users to use a service, as a Tenant Owner, you must accept the service license agreement to activate the service.

Click the service in the My Favorite Apps or All Apps view, A pop-up window appears displaying the license agreement. Read the terms in the agreement, and then click Accept.

Note: If your tenant license type or license agreement of a service has changed, you must click the service and accept the new license agreement.

Obtain a Full License

To obtain a full license for any of the IBM Spectrum® Protect Plus Online Services, contact IBM Software Support.

IBM Spectrum Protect Plus Online Services charge licenses for certain Microsoft 365 subscriptions. For more information, refer to Licensing Information.

Start Trial of Additional Services

If your tenant wants to start a trial for services that were not selected when your tenant signed up for IBM Spectrum® Protect Plus Online Services, the Tenant Owner and Service Administrators can start a trial on the Home page. Refer to the section below to obtain the trial licenses of services.

IBM Spectrum Protect Plus Online Services for Microsoft 365 Trial

On the Store tab, navigate to IBM Spectrum Protect Plus Online Services for Microsoft 365 and click START TRIAL to get a 30-day trial license. A pop-up window appears with the license agreement of the trial license displayed. Read the terms in the agreement, and then you must click Accept to start the trial.

Then, you can click IBM Spectrum Protect Plus Online Services for Microsoft 365 in the All Apps view to access it. For detailed instructions on using IBM Spectrum Protect Plus Online Services, refer to the IBM Spectrum Protect Plus Online Services for Microsoft 365 User Guide .

IBM Spectrum Protect Plus Online Services User Roles

In IBM Spectrum Protect Plus Online Services, different user roles can perform different actions. There are three main user roles: Tenant Owner, Service Administrator, and Tenant User.

- Tenant Owner – This is the user whose account is used to sign up for IBM Spectrum Protect Plus Online Services. There is only one Tenant Owner per IBM Spectrum Protect Plus Online Services tenant. A Tenant Owner can perform the following actions:
  - Access online services (if there are available licenses)
  - View license information
  - Apply promotional codes
  - Manage users
  - Manage app profiles
  - Manage service account profiles
  - Manage Auto Discovery
  - Manage encryption profiles
  - Enable report data collection
  - Export the user activity report
  - Configure notification and email settings
  - Enable integration with SCOM
  - Enable trusted IP address settings
  - Configure the security policy
  - Configure session timeout duration
  - Download a list of reserved IP addresses
  - Submit feedback
  - Edit personal profile information
- Service Administrator – The Tenant Owner or another Service Administrator can add Service Administrators to IBM Spectrum Protect Plus Online Services. Service Administrators can perform the same actions as the Tenant Owner.
- Tenant User – The Tenant Owner and Service Administrators can add Tenant Users to IBM Spectrum Protect Plus Online Services. Tenant Users can be Standard Users or Application Administrators.
  - Standard Users can perform the following actions in IBM Spectrum Protect Plus Online Services:
    - Access online services (if there are available licenses)
    - Submit feedback
    - Edit personal profile information
  - Application Administrators can:
    - Access online services (if there are available licenses)
    - Add Tenant Users and assign services to them. They can only assign the services for which they are Application Administrators.
    - Edit Tenant Users to change available services for them. They can only select the services for which they are Application Administrators.
    - Submit feedback
    - Edit personal profile information

The role permissions for specific services vary by service, to learn more go to Add Users for information that is specific to your service.

Manage Users

To manage IBM Spectrum® Protect Plus Online Services users, navigate to Management > User Management. On the User Management page, the Tenant Owner, Service Administrators, and Application Administrators can use the following views to manage users and permissions:

- User-based View – This view displays all IBM Spectrum Protect Plus Online Services users based on the user ID. The viewer will see the user ID, user role, sign-in method, available products, and status.
- Product-based View – This view displays all IBM Spectrum Protect Plus Online Services users based on the product name, together with the user status. Note: In this view, only Tenant Users and the products that they can access are visible.
- Geo Location-based View - This view displays all IBM Spectrum Protect Plus Online Services for Microsoft 365 users based on the geo locations, together with the user status.

Note: This view is only available when your tenant has Multi-Geo Capabilities in IBM Spectrum Protect Plus Online Services for Microsoft 365 service.
The Tenant Owner and Service Administrators can perform the following actions:

- User-based View
  - Add Users - In User-based View, Product-based View, or Geo Location-based View, click Add Users on the ribbon. Then, refer to the instructions in Add Users.
  - Edit – Select one user and click Edit on the ribbon. Then, refer to the instructions in Edit User Permissions.
  - Set as Tenant Owner – If you want to set an activated Service Administrator as the Tenant Owner, select the user and click Set as Tenant Owner on the ribbon. A pop-up window appears asking for your confirmation. Click OK to confirm your change. The notification email will be sent to the new Tenant Owner and the original Tenant Owner.
  - Activate – Select one or more users with the status of Deactivated or Not Activated. Then, click **Activate** on the ribbon.
  - Deactivate – Select one or more users with the status of Activated. Then, click Deactivate on the ribbon. Deactivated users are not removed from the portal but are restricted from accessing the portal.
  - Unlock – If a user enters an incorrect password consecutively for more than three times, the user account will be locked in an hour. Instead of waiting for the system to automatically unlock the account after an hour, you can manually unlock the account.
    Select the locked account. Then, click Unlock on the ribbon.
  - Delete – Select one or more users and click Delete on the ribbon. A pop-up window appears asking for your confirmation. Click OK to confirm your deletion. All the selected user profiles and system information will be deleted.
- Product-based View – In this view, Tenant Owner and Service Administrators can add users by clicking Add Users on the ribbon. For details, refer to the instructions in Add Users.
- **Geo Location-based View** (used by IBM Spectrum Protect Plus Online Services for Microsoft 365 with Multi-Geo Capabilities) – In this view, Tenant Owner and Service Administrators can add users by clicking Add Users on the ribbon. For details, refer to the instructions in Add Users.

Note: Logged-in Tenant Owner and Service Administrators cannot edit, deactivate, or delete their own accounts.
Application Administrators can perform the following actions:

- User-based View
  - Add Users – In this view, Application Administrators can click Add Users on the ribbon, and then refer to the instructions in Add Users.
    Note: Application Administrators can only add Tenant Users and assign the services for which they are Application Administrators.
- Edit – Select one user and click Edit on the ribbon and then refer to the instructions in Edit User Permissions.
  Note: Application Administrators can only change available services for Tenant Users, and they can only select the services for which they are Application Administrators.
- Product-based View or Geo Location-based View – In this view Application Administrators can click Add Users on the ribbon, and then refer to the instructions in Add Users.
  Note: Application Administrators can only add Tenant Users and assign the services for which they are Application Administrators.

Note: Logged-in Application Administrators cannot edit their own accounts.

- **Add Users**
  To add users and grant user permissions to IBM Spectrum Protect Plus Online Services and other services, click Add Users on the ribbon, and then configure the following settings:
- **Edit User Permissions**

Add Users

To add users and grant user permissions to IBM Spectrum® Protect Plus Online Services and other services, click Add Users on the ribbon, and then configure the following settings:

Procedure

1. Sign-in Method – Select the sign-in method from the drop-down list.
   - Local User – The local system will check the user credentials.
   - Microsoft 365 User/Group – Microsoft 365 users and groups will become IBM Spectrum Protect Plus Online Services users. They can use their Microsoft 365 login IDs to log into IBM Spectrum Protect Plus Online Services.
     Note: To allow added users and group users to sign in to IBM Spectrum Protect Plus Online Services for Microsoft 365 login IDs, IBM Spectrum Protect Plus Online Services recommends that the Microsoft 365 Global Administrator check the Enterprise applications configuration in Microsoft Azure > Azure Active Directory > User settings. If the Users can consent to apps accessing company data on their behalf option is set to No, the Microsoft 365 Global Administrator must consent to the IBM Spectrum Protect Plus Online Services app first. For details on consenting to the app by the Microsoft 365 Global Administrator, refer to What If Your Tenant Does Not Allow Users to Consent to Apps?
2. The following options appear according to the sign-in method you have selected:
   - **Microsoft 365 Tenant** – This option only appears if **Microsoft 365 User/Group** is selected as the sign-in method. Select a tenant from the drop-down list. The tenant is retrieved from the previously configured app profile or Microsoft 365 service account profile. If no profile has been configured, click **New App Profile**. For more information, refer to Manage App Profiles.
3. **Add Users** – Specify the users that you are about to add into IBM Spectrum Protect Plus Online Services.
   - For Local User, enter valid email addresses in the format of someone@example.com.
   - For Microsoft 365 User/Group, you can enter the following:
     - **Microsoft 365 User/Group**
       - The username of Microsoft 365 users in the format of **someone@example.com**.
       - The aliases of Microsoft 365 users.
       - The names of Microsoft 365 Groups, mail-enabled security groups, distribution groups, and security groups.

     Note: If the Microsoft 365 username, alias, or group name begins with a special character, you cannot add them to IBM Spectrum Protect Plus Online Services.
     Then, click the check button to check whether the users or groups are valid.

You can also click the browse button to view the users or groups within the selected tenant, and then select your desired users or groups.

- To search for a specific Microsoft 365 user, enter the keywords of the user username, first name, or last name.
- To search for a specific group, enter the keywords of the group display name.

Then, click the search button.

Note the following:

- If you select **Microsoft 365 User/Group** as the sign-in method, you can enter or select Everyone. Everyone refers to all available users (excluding external users) in your Microsoft 365 tenant Azure AD. If you add Everyone as IBM Spectrum Protect Plus Online Services users, all available users can sign into IBM Spectrum Protect Plus Online Services and perform the corresponding actions according to the assigned role and available products.
- When you add a security group, distribution group, or mail-enabled security group to IBM Spectrum Protect Plus Online Services, the following users cannot sign into IBM Spectrum Protect Plus Online Services:
  - 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 Spectrum Protect Plus Online Services, the nested group owner cannot sign into IBM Spectrum Protect Plus Online Services.

4. **Role** – Select the user role. If you select **Tenant User**, proceed to the next step. If you select **Service Administrator**, go directly to step 8.
   Note: For more details about the user roles, refer to IBM Spectrum Protect Plus Online Services User Roles.
5. Available Product – Select the services that the user should be able to access and then select the permissions for the users. The services available for selection depend on your license. If your license for a specific service has expired, the service is unavailable for selection.

Product	User Type
IBM Spectrum Protect Plus Online Services for Microsoft 365	**Standard User** In IBM Spectrum Protect Plus Online Services, Standard Users can configure restore settings, perform restores, and view activity reports. Additionally, Standard Users that are added to the Administrators group in IBM Spectrum Protect Plus Online Services can also configure backup settings and perform backups.
	Application Administrator The application administrator can configure backup and restore settings, perform backup and restore operations, view activity reports, etc.
IBM Spectrum Protect Plus Online Services Recovery Portal (for Microsoft 365) Note: If you want to grant permissions to a large number of users, it is recommended to grant permissions to Microsoft 365 Groups instead of Microsoft 365 users.	**Standard User** Standard Users can access the IBM Spectrum Protect Plus Online Services Recovery Portal, run jobs to recover Microsoft 365 data, and view job reports.
	Application Administrator Application Administrators can use all the functionalities in IBM Spectrum Protect Plus Online Services Recovery Portal and manage access to IBM Spectrum Protect Plus Online Services Recovery Portal for Standard Users.

6. If your tenant has Multi-Geo Capabilities in IBM Spectrum Protect Plus Online Services for Microsoft 365, the Available Geo Location field will appear when you select Microsoft 365 in the Available Product field. To maintain segregation among geo locations, select one or more geo locations that will be available to the users.
7. Send email notifications to the newly added users (for Microsoft 365 User/Group) – If you want to send email notifications to newly added users, select this check box.
8. Click Save to save your configurations. Users with the sign-in method of Local User will receive invitation emails. They must activate the user IDs first by clicking the link provided in the emails, and then use the user ID and password in the invitation emails to sign intoIBM Spectrum Protect Plus Online Services.

Edit User Permissions

Procedure

To edit user permissions, select one user and click Edit on the ribbon. Then, configure the following settings:

1. Sign-in Method - Select a sign-in method. After the changes have been saved, the user sign-in method cannot be changed again.
   Note: This option is only available if Local User is selected as the sign-in method when a Microsoft 365 account is added.
2. Role - Choose the user role Tenant User or Service Administrator.
3. If you choose Tenant User, you can further configure the following settings:

   Available Product
   : Choose the available products for the users. For more information about how to select the available products, refer to Available Product.

   Available Geo Location
   : This field only appears when your tenant has Multi-Geo Capabilities in IBM Spectrum® Protect Plus Online Services, and this service is available to the selected user. Select one or more regions that are available to the user.

4. Status- Choose the status for the selected user Activated or Deactivated.
5. Click Save to save your changes, or click Cancel on the ribbon to cancel your changes.

Required Permissions

Refer to the sections below for the required permissions for authorizing IBM Spectrum® Protect Plus Online Services apps and using IBM Spectrum Protect Plus Online Services for Microsoft 365 properly.

- **Permissions for Microsoft App Authorization**
  Refer to the following sections based on the types of tenants for which the app is created.
- **Permissions for Using IBM Spectrum Protect Plus Online Services for Microsoft 365**
  To use IBM Spectrum Protect Plus Online Services for Microsoft 365, an app profile or a Microsoft 365 service account profile is required for authentication. If you do not want to use the apps that IBM Spectrum Protect Plus Online Services will create in your Azure Active Directory, you can create a custom app in your Azure AD and create a custom Azure app profile.

Permissions for Microsoft App Authorization

Refer to the following sections based on the types of tenants for which the app is created.

When you create an app profile for Microsoft 365, Microsoft Azure AD, Sandbox, the corresponding app will be automatically created. For details on the permissions requested by these apps, refer to the sections below.

Note the following:

- The Microsoft 365 account used to consent the app must have the Global Administrator role, which is a requirement from Microsoft. For details about this role, refer to the Microsoft article About Microsoft 365 admin roles.
- If you want to create a custom Azure app to connect IBM Spectrum® Protect Plus Online Services to your Microsoft 365 tenant and use IBM Spectrum Protect Plus Online Services for Microsoft 365, you can refer to Permissions for Using IBM Spectrum Protect Plus Online Services for Microsoft 365 and add the API permissions to your custom app.
- If your organization uses IBM Spectrum Protect Plus Online Services for Microsoft 365 and scans Teams with the service account authentication method scan profiles in Auto Discovery, to restore channel conversations as posts, click the Delegated tab and create an app profile for a Microsoft Delegated app. For details about the permissions requested by this app, refer to IBM Spectrum Protect Plus Online Services Administration (for Microsoft Delegated App).

- **IBM Spectrum Protect Plus Online Services Administration for Office 365**
  If you grant All Permissions to the Microsoft 365 app profile, the IBM Spectrum Protect Plus Online Services Administration for Office 365 app will be generated accordingly in your Azure AD.
- **IBM Spectrum Protect Plus Online Services Administration for SharePoint**
  If you grant SharePoint Online Permissions to the Microsoft 365 app profile, the IBM Spectrum Protect Plus Online Services Administration for SharePoint app will be generated accordingly in your Azure AD.
- **IBM Spectrum Protect Plus Online Services Administration for Exchange**
  If you grant Exchange Online Permissions to the Microsoft 365 app profile, the IBM Spectrum Protect Plus Online Services Administration for Exchange app will be generated accordingly in your Azure AD.
- **IBM Spectrum Protect Plus Online Services Administration for Azure**
  The table below lists the permissions that should be accepted when you authorize the IBM Spectrum Protect Plus Online Services Administration for Azure app.
- **IBM Spectrum Protect Plus Online Services Administration (for Microsoft Delegated App)**
  The table below lists the delegated permissions that should be accepted when you authorize the IBM Spectrum Protect Plus Online Services Administration app.

IBM Spectrum Protect Plus Online Services Administration for Office 365

If you grant All Permissions to the Microsoft 365 app profile, the IBM Spectrum Protect Plus Online Services Administration for Office 365 app will be generated accordingly in your Azure AD.

The table below lists the permissions that should be accepted when you authorize the IBM Spectrum Protect Plus Online Services Administration for Office 365 app.

API	Permission	Type	Why we need it?
SharePoint	Sites.FullControl.All (Have full control of all site collections)	Application	Retrieve information of SharePoint Online site collections that are scanned by Auto Discovery.
	User.ReadWrite.All (Read and write user profiles)	Application	Retrieve information of Microsoft 365 user profiles related to OneDrive for Business that are scanned by Auto Discovery.
	TermStore.ReadWrite.All (Read and write managed metadata)	Application	Back up and restore Managed Metadata Service of SharePoint Online site collections and Microsoft 365 Group team sites.
Office 365 Exchange Online	full_access_as_app (Use Exchange Web Services with full access to all mailboxes)	Application	Retrieve information of Exchange Online mailboxes and Microsoft 365 Group mailboxes that are scanned by Auto Discovery.
Microsoft Graph	Channel.ReadBasic.All (Read the names and descriptions of all channels)	Application	Scan Microsoft Teams via Auto Discovery.
	User.Read (Sign in and read user profile)	Delegated	Support signing into IBM Spectrum Protect Plus Online Services with Microsoft 365 accounts.
	Group. ReadWrite.All	Application	Scan Microsoft 365 Groups and Microsoft Teams via Auto Discovery.

API	Permission	Type	Why we need it?
	(Read and write all groups)		Back up and restore Microsoft Teams and Microsoft 365 Groups data.
	Directory.Read.All (Read directory data)	Application	Retrieve your Microsoft 365 tenant information.
	Sites.ReadWrite.All (Read and write items in all site collections [preview])	Application	Back up and restore Microsoft Teams and Microsoft 365 Groups data.
	Sites.Read.All (Read items in all site collections [preview])	Application	Back up and restore Microsoft Teams and Microsoft 365 Groups data.
	Reports.Read.All (Read all usage reports)	Application	IBM Spectrum Protect Plus Online Services for Microsoft 365 can retrieve data size directly, which improves the efficiency of the License Consumption Report.
	ChannelMember.ReadWrite.All (Add and remove members from all channels)	Application	Back up and restore the members and messages of Teams private channels.
	ChannelMessage.Read.All (Read all channel messages)	Application	Back up and restore the members and messages of Teams private channels.
	ChannelSettings.ReadWrite.All (Read and write the names, descriptions, and settings of all channels)	Application	Required by the restore jobs of Teams service.
	TeamSettings.ReadWrite.All (Read and change all teams' settings)	Application	IBM Spectrum Protect Plus Online Services for Microsoft 365 uses it to back up and restore teams' settings.
	Files.Read.All (Read files in all site collections)	Application	Retrieve URLs of channels in Teams.
	TeamMember.ReadWrite.All (Add and remove members from teams)	Application	IBM Spectrum Protect Plus Online Services for Microsoft 365 uses it to back up and restore teams' members.
	TeamsTab.ReadWrite.All (Read and write tabs in Microsoft Teams)	Application	IBM Spectrum Protect Plus Online Services for Microsoft 365uses it to back up and restore teams' tabs.
	Team.Create (Create teams)	Application	IBM Spectrum Protect Plus Online Services for Microsoft 365 uses it to restore teams.
	TeamsAppInstallation.ReadWriteForTeam.All (Manage Teams apps for all teams)	Application	IBM Spectrum Protect Plus Online Services for Microsoft 365 uses it to back up and restore teams' apps.
	Channel.Create (Create channels)	Application	IBM Spectrum Protect Plus Online Services for Microsoft 365 uses it to restore teams' channels.
	Chat.Read.All (Read all chat messages)	Application	IBM Spectrum Protect Plus Online Services for Microsoft 365 uses it to back up Microsoft Teams Chat.

IBM Spectrum Protect Plus Online Services Administration for SharePoint

If you grant SharePoint Online Permissions to the Microsoft 365 app profile, the IBM Spectrum Protect Plus Online Services Administration for SharePoint app will be generated accordingly in your Azure AD.

The table below lists the permissions that should be accepted when you authorize the IBM Spectrum Protect Plus Online Services Administration for SharePoint app.

API	Permission	Type	Why we need it?
SharePoint	Sites.FullControl.All (Have full control of all site collections)	Application	Retrieve information of SharePoint Online site collections that are scanned by Auto Discovery.
	User.ReadWrite.All (Read and write user profiles)	Application	Retrieve information of Microsoft 365 user profiles related to OneDrive for Business that are scanned by Auto Discovery.
	TermStore.ReadWrite.All (Read and write managed metadata)	Application	Back up and restore Managed Metadata Service of SharePoint Online site collections and Microsoft 365 Group team sites.

API	Permission	Type	Why we need it?
Microsoft Graph	User.Read (Sign in and read user profile)	Delegated	Support signing into IBM Spectrum Protect Plus Online Services with Microsoft 365 accounts.
	Reports.Read.All (Read all usage reports)	Application	IBM Spectrum Protect Plus Online Services for Microsoft 365 can retrieve data size directly, which improves the efficiency of the License Consumption Report.
	Directory.Read.All (Read directory data)	Application	Retrieve your Microsoft 365 tenant information.

IBM Spectrum Protect Plus Online Services Administration for Exchange

If you grant Exchange Online Permissions to the Microsoft 365 app profile, the IBM Spectrum Protect Plus Online Services Administration for Exchange app will be generated accordingly in your Azure AD.

The table below lists the permissions that should be accepted when you authorize the IBM Spectrum Protect Plus Online Services Administration for Exchange app.

API	Permission	Type	Why we need it?
Office 365 Exchange Online	full_access_as_app (Use Exchange Web Services with full access to all mailboxes)	Application	Retrieve information of Exchange Online mailboxes and Microsoft 365 Group mailboxes that are scanned by Auto Discovery.
Microsoft Graph	User.Read (Sign in and read user profile)	Delegated	Support signing into IBM Spectrum Protect Plus Online Services with Microsoft 365 accounts.
	Reports.Read.All (Read all usage reports)	Application	IBM Spectrum Protect Plus Online Services for Microsoft 365 can retrieve data size directly, which improves the efficiency of the License Consumption Report.
	Directory.Read.All (Read directory data)	Application	Retrieve your Microsoft 365 tenant information.

IBM Spectrum Protect Plus Online Services Administration for Azure

The table below lists the permissions that should be accepted when you authorize the IBM Spectrum® Protect Plus Online Services Administration for Azure app.

API	Permission	Type	Why we need it?
Microsoft Graph	User.ReadWrite.All (Read and write all users' full profiles)	Application	Identity Manager uses it to search for users and display them on the interface, as well as invite guest users to organizations.
	User.Invite.All (Invite guest users to the organization)	Delegated	Identity Manager uses it to invite guest users to organizations.
	Directory.AccessAsUser.All (Access directory as the signed-in user)	Delegated	Identity Manager uses it to manage licenses, users, roles, groups, and applications that can be accessed by users.
	Directory.ReadWrite.All (Read and write directory data)	Application	Identity Manager uses it to manage licenses, users, roles, groups, and applications that can be accessed by users.
	Domain.ReadWrite.All (Read and write domains)	Application	Identity Manager uses it to manage users and groups.
	User.Read (Sign in and read user profile)	Delegated	Identity Manager uses it to retrieve tenant display name, and display the name on the interface.

IBM Spectrum Protect Plus Online Services Administration (for Microsoft Delegated App)

The table below lists the delegated permissions that should be accepted when you authorize the IBM Spectrum Protect Plus Online Services Administration app.

Service	API	Permission	Why we need it?

Service	API	Permission	Why we need it?
IBM Spectrum Protect Plus Online Services for Microsoft 365	Microsoft Graph	Group.ReadWrite.All (Read and write all groups)	Retrieves tabs information from Microsoft Teams.
		ChannelMessage.Send (Send channel messages)	Sends messages to channels in Microsoft Teams.
		TeamMember.ReadWrite.All (Add and remove members from teams)	Adds members to Microsoft Teams.
		ChannelMember.ReadWrite.All (Add and remove members from channels)	Adds members to channels in Microsoft Teams.

Permissions for Using IBM Spectrum Protect Plus Online Services for Microsoft 365

To use IBM Spectrum Protect Plus Online Services for Microsoft 365, an app profile or a Microsoft 365 service account profile is required for authentication. If you do not want to use the apps that IBM Spectrum Protect Plus Online Services will create in your Azure Active Directory, you can create a custom app in your Azure AD and create a custom Azure app profile.

For the custom app created in your Azure AD, to ensure it is available for common features in IBM Spectrum Protect Plus Online Services for Microsoft 365, refer to the table below to assign the required permissions accordingly.

API	Permission	Type	Why we need it?
Microsoft Graph	Directory.Read.All (Read directory data)	Application	Scan mailboxes, invite users, count user seats, and check the status of app profiles.
	Group.ReadWrite.All (Read and write all groups)	Application	Scan Microsoft 365 Groups, Teams, and Yammer communities. Add the service account as the owner of scanned Microsoft 365 Groups and Teams.
	Group.Read.All (Read all groups)	Application	Invite users and groups in User Management.
SharePoint	Sites.FullControl.All	Application	Scan SharePoint Online site collections, Project Online site collections, OneDrive for Business, and Microsoft 365 Group team sites.
	User.ReadWrite.All	Application	Scan OneDrive for Business to retrieve the OneDrive URL of each user from SharePoint user profiles.
Office 365 Exchange Online	full_access_as_app	Application	Scan Exchange Online public folders and in-place archived mailboxes (if necessary).

The IBM Spectrum Protect Plus Online Services for Microsoft 365 supports using a custom Azure app for authentication. The permissions of the custom app and Microsoft 365 service account vary with different cloud services your tenant is using.

To view the required permissions of your services, refer to IBM Spectrum Protect Plus Online Services for Microsoft 365.

View License Information

On the **Home** page, the Tenant Owner and Service Administrators can view the license expiration date of each available service. The license expiration date is displayed below the service name.

Your service may have the information icon on the upper-right corner in the tile if:

- The number of assigned licenses in Microsoft 365 has exceeded the licensed user seats for IBM Spectrum® Protect Plus Online Services for Microsoft 365.
- The IBM Spectrum Protect Plus Online Services for Microsoft 365 license you purchased does not provide enough capacity for all protected Microsoft 365 objects.

To ensure you can use the services without any interruption, you must contact IBM Software Support to purchase more user seats. For IBM Spectrum Protect Plus Online Services for Microsoft 365, to increase the capacity, contact your Sales representative. To decrease the consumed capacity, modify the backup scope that has been protected by this service.

Note: IBM Spectrum Protect Plus Online Services charge licenses for certain Microsoft 365 subscriptions. For more information, refer to Licensing Information.
To view the detailed information of the license for each available service, navigate to License > License Information on the left pane. The **License Information** page displays the purchased module, license type, license status, and expiration date of each service. Click a service name to view more details about your license for this service, including license type, the number of purchased user seats, license expiration date, license status, license agreement, and purchased storage (for the IBM Spectrum Protect Plus Online Services for Microsoft 365 only).

To obtain a full license for any of the IBM Spectrum Protect Plus Online Services, contact IBM Software Support.

Manage Your Profile Information

To view or change your account information or to reset your password, click the current login ID on the upper-right corner, and then select **My Profile** from the drop-down list.
Note: **My Profile** is only available to local users and Microsoft 365 Service Administrators.
In **My Profile**, you can edit the following information:

- **Contact Information** – This tab displays your user ID and contact information. Edit the information in any of the available fields. Click Save to save your changes, or click **Cancel**.
- **Reset Password** – This tab allows you to reset a new password for your IBM Spectrum® Protect Plus Online Services account when you're logged in. Enter the Old Password, New Password, and Confirm Password in the corresponding text boxes. Click Save to save your changes, or click Cancel.

Note: The Reset Password tab is only available to local users.
After you reset your password, a password change confirmation email will be sent to your email inbox to confirm the change.

Manage Service Account Profiles

A Microsoft 365 service account profile contains a Microsoft 365 Global Administrator, SharePoint Administrator, or Exchange Administrator account. With the credentials of this account, you can invite Microsoft 365 users or groups as IBM Spectrum® Protect Plus Online Services users. Auto Discovery also uses the credentials to scan Microsoft 365 objects. For an overview about when IBM Spectrum Protect Plus Online Services needs your Microsoft 365 account, see Appendix E - When Service Account and App Profile are Used.

The Tenant Owner and Service Administrators can manage service account profiles by navigating to Management > Service Account. From this menu, you can perform the following actions:

- **Create** – Click Create on the ribbon. Then, refer to the instructions in Create a Service Account Profile.
- **Edit** – Select a service account profile and click Edit on the ribbon.
  Note: If the user role of the service account has been changed, an exclamation icon will appear in front of the user role name, and you will be prompted to edit the service account profile and save it again to update the user role. If IBM Spectrum Protect Plus Online Services fails to connect to the Microsoft 365 environment via the service account, an exclamation icon will appear in front of the status, and you will be prompted to edit the service account profile and save it again to connect to Microsoft 365.
- **Delete** – Select one or more service account profiles and click Delete on the ribbon. A pop-up window appears asking for your confirmation. Click OK to confirm your deletion.
- **Create a Service Account Profile**

Create a Service Account Profile

Before you begin

Make sure that you have created a service account in the Microsoft Azure Active Directory.
Azure AD allows you to configure the service accounts in the following ways:

- Service account without MFA
- Service account with MFA application password
- Service account with MFA conditional access

For more information about creating a service account, refer to Service Account MFA Configuration.

About this task

To create a service account profile, click Create on the ribbon, and then configure the following settings on the **Create Service Account Profile** page.
Note: A Microsoft 365 tenant can only be managed in a single IBM Spectrum® Protect Plus Online Services tenant. Therefore, IBM Spectrum Protect Plus Online Services only allows one service account profile to be created for a single Microsoft 365 tenant.

Procedure

1. **Profile Name** – Enter a name for the service account profile.
2. **Description** – Enter an optional description.
3. **Enable MFA** – If your organization uses multi-factor authentication in Microsoft 365, select the **Our organization uses multi-factor authentication** checkbox.
   Note the following:
   - With MFA enabled, this service account profile cannot be used to invite Microsoft 365 users/groups as IBM Spectrum Protect Plus Online Services users.
   - With MFA enabled, if your organization selects Block access for the Apps that don't use modern authentication setting in the SharePoint admin center, this service account profile cannot be used for the Ghost Guest Users rule in Identity Manager.

   Note: Microsoft Azure AD allows you to configure the service accounts in the following ways:
   - Service account without MFA

- Service account with MFA application password
- Service account with MFA conditional access

For more information about creating the service accounts in Azure AD, refer to Service Account MFA Configuration.

4. **Username** – With the Enable MFA option selected, you must enter the login ID of a Microsoft 365 Global Administrator account or SharePoint Administrator account. If the option is deselected, you must enter the login ID of a Global Administrator account, SharePoint Administrator account, Exchange Administrator account.
   Note: IBM Spectrum Protect Plus Online Services does not recommend that a personal active user account be used as the service account. It is suggested that you use a separate service account to handle all administration.
   The IBM Spectrum Protect Plus Online Services for Microsoft 365 supports using a Microsoft 365 service account for authentication. The permissions of the Microsoft 365 service account vary with the different cloud services your tenant is using. To prepare a Microsoft 365 account and assign the required role to this account, refer to IBM Spectrum Protect Plus Online Services for Microsoft 365.

5. **Password** – If your Microsoft 365 tenant does not have multi-factor authentication (MFA) enabled, enter the login password of the account above. If MFA is enabled, enter the app password of the account above. For more information about app passwords, refer to the Microsoft technical article Manage app passwords for two-step verification.
6. Click Validation Test to validate the information above. The user role will be automatically displayed in the User Role field.
   Note: The password is validated via Microsoft 365 API. Due to a Microsoft 365 API limitation, you may encounter the following issue: the password is checked as invalid here, but you can use this password to log into Microsoft 365 successfully. To resolve the issue, you must change your password in Microsoft 365, and then enter the new password here. For details about the password limitations and requirements, refer to Appendix D - Password Limitations and Requirements of Microsoft 365 Accounts.
7. In **Advanced Settings**, you need to configure a **SharePoint Online Admin Center URL**. If your organization uses the default SharePoint Online admin center URL in Microsoft 365, select the Our organization uses the default SharePoint Online admin center URL option; if your organization uses a custom SharePoint Online admin center URL in Microsoft 365, select the Our organization uses a custom SharePoint Online admin center URL option, and enter the admin center URL in the text box.
   Note: If the **Our organization uses multi-factor authentication** checkbox is selected, you must manually enter the SharePoint Online admin center URL in the text box.
8. Click Save to save your configurations, or click Cancel to go back to the **Service Account** page without saving any configurations.

Manage Microsoft 365 Account Pool

SharePoint Online has a built-in throttling feature that prevents one account from processing several requests simultaneously. To avoid getting throttled or blocked in SharePoint Online, you can configure an account pool that contains multiple Microsoft 365 accounts. When IBM Spectrum® Protect Plus Online Services registers SharePoint Online site collections and OneDrive for Business, IBM Spectrum Protect Plus Online Services grants the site collection administrator permission to the group set in the account pool for **SharePoint Sites/OneDrive for Business/Microsoft 365 Group Team Sites**, and the Microsoft 365 accounts in the account pool will inherit the site collection administrator permission from the group.

About this task

With the credentials of these accounts, IBM Spectrum Protect Plus Online Services can work smoothly. For example, IBM Spectrum Protect Plus Online Services for Microsoft 365 can manage a large amount of data simultaneously. For an overview of what services can use a Microsoft 365 account pool, refer to What Services Can Use a Microsoft 365 Account Pool?

To build an account pool in IBM Spectrum Protect Plus Online Services, create a group in Microsoft 365 first. The group type can be Microsoft 365 Group, mail-enabled security group, or security group. This group should contain a certain number of users, and these users can be unlicensed in Microsoft 365.

The table below lists the required information for each object type.

Object Type	Need Account Pool?	Need Username?	Need Password?	Need SharePoint Administrator Role?	Need License?	
SharePoint Online Site Collection	Yes	Yes	Yes	No	No	
OneDrive for Business	Yes	Yes	Yes	No	No	
Microsoft 365 Group Team Sites	Yes	Yes	Yes	No	No	
Exchange Online Mailboxes	Yes	Yes	Yes	No	No	
Microsoft 365 Group Mailboxes	Yes	Yes	Yes	No	No	
Microsoft 365 Groups	Yes	Yes	Yes	No	Yes	Have the SharePoint Online and Exchange Online product licenses assigned in Microsoft 365.
Microsoft Teams	Yes	Yes	Yes	No	Yes	Have the Exchange Online and Microsoft Teams product licenses assigned in Microsoft 365.
Project Online Site Collections	Yes	Yes	Yes	No	Yes	Have one of the following Project Online product licenses assigned in Microsoft 365: **Essentials**, **Professionals**, or **Premium**.
Exchange Online Public Folders	Yes	Yes	No	No	Yes	Have the Exchange Online product license assigned in Microsoft 365.
Microsoft 365 Users	Yes	Yes	Yes	No	Yes	Have one of the following Azure Active Directory product licenses assigned in Microsoft 365: **Premium P1** or **Premium P2**.

Object Type	Need Account Pool?	Need Username?	Need Password?	Need SharePoint Administrator Role?	Need License?
Yammer Community	No				

Note: For SharePoint Online site collections, OneDrive for Business, and Microsoft 365 Group team sites, the SharePoint Administrator role is required by Cloud Management > **Administrator** functionalities.

Procedure

The Tenant Owner and Service Administrators can then manage the account pool by navigating to Management > Service Account Pool, and the Manage Account Pool page appears. On the Manage Account Pool page, configure the following settings:

1. Select a Tenant – Select a tenant from the drop-down list. The tenant is retrieved from the previously configured app profile or Microsoft 365 service account profile.
   Note: If you want to add more tenants, click the Microsoft 365 Service Account or App Management link to go to the corresponding page and create new profiles. Then, the tenants can be retrieved here.
2. Configure the account pool for SharePoint Sites/OneDrive for Business/Microsoft 365 Group Team Sites, Project Sites, or Exchange Public Folders according to the objects you will back up or manage via services for Microsoft 365. Click a tab and configure the following settings:
   a. Group – Enter the name of the group you prepared.
   b. Click Validate next to the group name. Group members will be displayed in the **Group Users** field. For the minimum number of users who must be included in the group, refer to the instructions in How Many Accounts Should be Added into an Account Pool?.

      Note the following:
      - If a user account exists in a service account profile, this service account will be used for managing operations in your IBM Spectrum Protect Plus Online Services tenant and will not be used to execute application-level jobs.
      - For backing up Exchange Online public folders, you do not need to provide the password of the account because of the impersonation technology. For more information about impersonation, see Impersonation and EWS in Exchange.
      - If the account of a user has multi-factor authentication (MFA) enabled in Microsoft 365, click the turn on button to enable MFA, and then enter the app password of this account.
      - To protect Planner data, the account must be both owner and member of the scanned Microsoft 365 Groups and Teams.
      - If the account of a user has multi-factor authentication enabled through a conditional access policy configured in Azure Active Directory, the account cannot be added to the account pool.

   c. Custom SharePoint Online Admin Center URL – If you enable MFA for one or more accounts, you must enter your SharePoint Online admin center URL in the text box.
3. When you finish the configurations for all desired account pools, click Save to save your configurations. If you want to remove the group from the account pool, click Clear next to the group name, and then click Save.
   Note: : After an account pool for a tenant is saved, the account pool will take effect on the next scan job.
   If you edit the account pool to change the group, a pop-up window will appear recommending you rerun the scan for Auto Discovery. Select scan profiles and click Rerun to make the changes take effect immediately. If you click Cancel, your changes will be saved but will not take effect until the next scan completes.

   If all app profiles and service account profiles are deleted, IBM Spectrum Protect Plus Online Services cannot connect to your tenant, and there will be a Delete All Account Pools button on the Manage Account Pool page. You can click Delete All Account Pools to remove the account pool configurations, or navigate to App Management or Microsoft 365 Service Account to create a new profile to retrieve an available tenant.

Manage App Profiles

IBM Spectrum® Protect Plus Online Services for Microsoft 365 can connect to your Microsoft 365, Microsoft Azure Active Directory or Yammer via an app profile.

- **App Profile for Microsoft 365**
  In order to back up, restore, and manage your data in Microsoft 365, IBM Spectrum Protect Plus Online Services needs to connect to your Microsoft 365 tenant. The connection can be built via creating an app profile for Microsoft 365, and an app will be created in your Azure Active Directory.
- **App Profile for a Custom Azure App**
  In order to use IBM Spectrum Protect Plus Online Services and Microsoft Azure Active Directory management, IBM Spectrum Protect Plus Online Services needs to connect to your Microsoft 365 tenant.The connection can be built via creating an App profile for a custom Azure app.
- **App Profile for a Microsoft Delegated App**
  In order to manage your data in Microsoft 365 via an app with delegated permissions, the Tenant Owner and Service Administrators can create an app profile for a Microsoft Delegated app. After creating an app profile, the IBM Spectrum Protect Plus Online Services Administration app will be automatically created.
- **App Profile for Yammer**
  If you want to enable the integration between IBM Spectrum Protect Plus Online Services Cloud Governance and Yammer, IBM Spectrum Protect Plus Online Services, as the service platform of IBM Spectrum Protect Plus Online Services Cloud Governance, needs to connect to your Yammer environment.

App Profile for Microsoft 365

In order to back up, restore, and manage your data in Microsoft 365, IBM Spectrum® Protect Plus Online Services needs to connect to your Microsoft 365 tenant. The connection can be built via creating an app profile for Microsoft 365, and an app will be created in your Azure Active Directory.

An app profile for Microsoft 365 is required if one of the following circumstances are met:

- Your organization uses multi-factor authentication (MFA) in Microsoft 365, and you want to add Microsoft 365 users or groups as IBM Spectrum Protect Plus Online Services users.
- Your organization uses MFA in Microsoft 365, and you have to choose **Use an app profile** as the authentication method when creating a scan profile in IBM Spectrum Protect Plus Online Services.

For an overview about when IBM Spectrum Protect Plus Online Services needs an app profile for Microsoft 365 and Microsoft 365 service account, see Appendix E - When Service Account and App Profile are Used.

- **Create an App Profile for Microsoft 365**
  The Tenant Owner and Service Administrators can create an app profile in App Management.
- **Re-authorize the App for Microsoft 365**
  The apps generated by Microsoft 365 app profiles need to be authorized. The app profiles whose statuses are **App Authorization Expired** must be re-authorized. You can also re-authorize the app for an active app profile if you want to change the account used to authorize the app.
- **Edit or Delete an App Profile for Microsoft 365**

Create an App Profile for Microsoft 365

The Tenant Owner and Service Administrators can create an app profile in App Management.

Procedure

To create an app profile for Microsoft 365, complete the following steps:

Note: A Microsoft 365 tenant can only be managed in a single IBM Spectrum® Protect Plus Online Services tenant. Therefore, IBM Spectrum Protect Plus Online Services only allows you to create Microsoft 365 app profiles with different permissions for a single Microsoft 365 tenant.

1. Click Create on the **App Management** page.
2. In the pop-up window, choose Microsoft 365.
3. **Choose a version** - Select one from the options below:
   - Commercial Microsoft 365 (your Microsoft login URL ends with .com)
4. **Grant permissions to the app profile** – Choose one of the following options to grant permissions to the app profile you are about to create.
   - **All permissions** – Select this option to grant all permissions, including SharePoint Online permissions, Exchange Online permissions, and Management API permissions, to the app profile. When the app profile is created in IBM Spectrum Protect Plus Online Services, the IBM Spectrum Protect Plus Online Services Administration for Office 365 app is created accordingly in your Azure Active Directory.
   - **SharePoint Online permissions** – Select this option to grant SharePoint Online permissions to the app profile. When the app profile is created in IBM Spectrum Protect Plus Online Services, the IBM Spectrum Protect Plus Online Services Administration for SharePoint app is created accordingly in your Azure Active Directory.
   - **Exchange Online permissions** – Select this option to grant Exchange Online permissions to the app profile. When the app profile is created in IBM Spectrum Protect Plus Online Services, the IBM Spectrum Protect Plus Online Services Administration for Exchange app is created accordingly in your Azure Active Directory.

   Note: Different types of objects that can be scanned by scan profiles require different permissions. For more information, refer to Permissions for App Authorization.
5. Creating an app profile for Microsoft 365 requires a Microsoft 365 Global Administrator account. For more information on why a Microsoft 365 Global Administrator account is required, refer to Why Admin Consent is Required to Use the IBM Spectrum Protect Plus Online Services App?.
6. Click OK.
7. On the Microsoft 365 sign-in page, sign in with a Microsoft 365 Global Administrator account.
   Note: This account will be added as a Service Administrator of IBM Spectrum Protect Plus Online Services if the account does not already exist in any existing IBM Spectrum Protect Plus Online Services tenant.
8. On the **Permissions requested** page, review the permissions required for IBM Spectrum Protect Plus Online Services and click Accept to continue
   The **App Management** page appears, and the app profile is created successfully.

- **Additional Action for Custom SharePoint Online Admin Center URL**
  If your Microsoft 365 tenant has a custom SharePoint Online admin center URL, to ensure your tenant users can use IBM Spectrum Protect Plus Online Services for Microsoft 365 for SharePoint management, you must set your SharePoint Online admin center URL in the app profile.

Additional Action for Custom SharePoint Online Admin Center URL

If your Microsoft 365 tenant has a custom SharePoint Online admin center URL, to ensure your tenant users can use IBM Spectrum® Protect Plus Online Services for Microsoft 365 for SharePoint management, you must set your SharePoint Online admin center URL in the app profile.

Procedure

1. On the **App Management** page, click the profile name of a Microsoft 365 app profile with **All Permissions** or **SharePoint Online Permissions**.
2. The SharePoint Online admin center URL displayed in the app profile details is constructed based on the default SharePoint Online admin center URL rule. Click Edit next to the admin center URL, and then edit your SharePoint Online admin center URL in the text box.
3. Click Save to save the change.

Re-authorize the App for Microsoft 365

The apps generated by Microsoft 365 app profiles need to be authorized. The app profiles whose statuses are **App Authorization Expired** must be re-authorized. You can also re-authorize the app for an active app profile if you want to change the account used to authorize the app.

Procedure

Complete the steps below to re-authorize the following app for a Microsoft 365 app profile:

- IBM Spectrum® Protect Plus Online Services Administration for Office 365
- IBM Spectrum Protect Plus Online Services Administration for SharePoint
- IBM Spectrum Protect Plus Online Services Administration for Exchange

1. Select an app profile for Microsoft 365 and click Re-authorize App on the ribbon.
2. The **Re-authorize App** action requires a Microsoft 365 Global Administrator account.
   Note: If your tenant is using or needs to use IBM Spectrum Protect Plus Online Services for Microsoft 365 to back up Exchange Online mailboxes or Microsoft 365 Groups, this account must have the license for Exchange Online assigned.
3. Click OK.
4. On the Microsoft 365 sign-in page, sign in with a Microsoft 365 Global Administrator account.
   Note: This account will be added as a Service Administrator of IBM Spectrum Protect Plus Online Services if the account does not already exist in any existing IBM Spectrum Protect Plus Online Services tenant.
5. On the **Permissions requested** page, review the permissions required for IBM Spectrum Protect Plus Online Services and click Accept to continue.
   The **App Management** page appears, and the app is successfully re-authorized for the selected tenant.

Edit or Delete an App Profile for Microsoft 365

On the **App Management** page, you can edit or delete an app profile for Microsoft 365.

- **Edit** – You can edit the name and description of an app profile. Click the app profile name, and the profile information is displayed. Click Edit to go to the edit page. Modify the profile name and/or description, and then click Save to save your changes.
- **Delete** – Select one or more app profiles and click Delete on the ribbon. A pop-up window appears asking for your confirmation. Click OK to confirm your deletion.

App Profile for a Custom Azure App

In order to use IBM Spectrum® Protect Plus Online Services and Microsoft Azure Active Directory management, IBM Spectrum Protect Plus Online Services needs to connect to your Microsoft 365 tenant.The connection can be built via creating an App profile for a custom Azure app.

- **Create an App Profile for a Custom Azure App**
  The Tenant Owner and Service Administrators can create an app profile by navigating to Management > App Management.
- **Re-authorize the Custom Azure App**
  The apps generated by the Custom Azure app profiles need to be authorized. The app profiles whose statuses are **App Authorization Expired** must be re-authorized. You can also re-authorize the app for an active app profile if you want to change the account used to authorize the app.
- **Edit or Delete an App Profile for a Custom Azure App**

Create an App Profile for a Custom Azure App

The Tenant Owner and Service Administrators can create an app profile by navigating to Management > App Management.

Before you begin

Before creating an app profile for the custom Azure app, you must first manually create an application in Azure Active Directory. For details about how to create an application and the required permissions, refer to Create Custom Azure Applications.

Procedure

After creating the application in Azure, you can create an app profile for the application by completing the following steps:

1. Click Create on the **App Management** page.
2. In the pop-up window, choose Custom Azure App.
3. **App Profile Name** – Enter a name for the profile.
4. **Application ID – Enter the application ID of the application that has been created in Azure.**
5. **Certificate File (.pfx)** – Click Browse and select your app's private certificate (the .pfx file).
   Note: If your organization does not have any certificates, you can refer to Appendix H - Prepare a Certificate for the Custom Azure App to prepare one.
6. **Certificate Password** – Enter the password of the certificate.
7. **Connect to Your Microsoft 365 Tenant** – Enter the username of a user in your Microsoft 365 tenant. This user will be used to identify your Microsoft 365 tenant ID for creating the app profile. If you want to back up and restore Exchange Online public folders, this user must have an Exchange Online product license assigned in Microsoft 365.
8. **Permissions Granted to the App** – Select Microsoft 365 or Azure AD according to the permissions you have granted to the custom Azure app. If you select Microsoft 365, choose one of the following permissions:

- **All permissions** – If the app has been granted all permissions, including SharePoint Online permissions, Exchange Online permissions, and Management API permissions, select this option.
- **SharePoint Online permissions** – If the app has been granted SharePoint Online permissions, select this option.
- **Exchange Online permissions** – If the app has been granted Exchange Online permissions, select this option.
  Note: When you want to use custom Azure apps with different permissions, you can create multiple app profiles for different custom Azure apps.

9. Click OK to create the app profile.
   The **App Management** page appears, and the app profile is created successfully.

- **Create Custom Azure Applications**

Create Custom Azure Applications

Procedure

To create the custom Azure applications, complete the following steps:

1. To create applications in Microsoft Azure, log in to Azure Portal.
2. Navigate to Azure Active Directory > App registrations > New registration.
3. On the **Register an application** page, enter your application registration information:
   - **Name** – Enter a name for the custom application.
   - **Supported account types** – Select which accounts you would like this application to support.
4. Click Register to create the custom application.
5. Click API permissions.
   The permissions that you need to grant to the custom app vary with the different cloud services your tenant is using. Click the link below to view the required permissions of your services.

   App Profile Authentication

6. The application uses certificate authentication. Complete the following steps to upload your organization's public certificate (the .cer file):
   - Locate your organization certificate and export the certificate as a .cer file.
   - Go to Azure Portal, select the application and click Certificate & secrets.
   - In the Certificates section, click Upload certificate.
   - Select the .cer file and click Add.
   - After the certificate file is successfully uploaded, it will be listed in the Certificates section.

   Note: If your organization does not have any certificates, you can refer to Appendix H - Prepare a Certificate for the Custom Azure App to prepare one.

Re-authorize the Custom Azure App

The apps generated by the Custom Azure app profiles need to be authorized. The app profiles whose statuses are **App Authorization Expired** must be re-authorized. You can also re-authorize the app for an active app profile if you want to change the account used to authorize the app.

About this task

Re-authorize the custom Azure app if:

- you want to change the custom Azure app that connects IBM Spectrum® Protect Plus Online Services to your Microsoft 365 tenant.
- the certificate file of the custom Azure app has been changed.
- the permissions of the custom Azure app have been changed.

Procedure

Complete the following steps to re-authorize the custom Azure app:

1. Select an app profile for the custom Azure app and click Re-authorize App on the ribbon.
2. **Application ID** – Enter the application ID of the application that has been created in Azure.
3. **Certificate File (.pfx)** – Click Browse and select the exported .pfx file of your app's certificate.
4. **Certificate Password** – Enter the password of the certificate.
5. **Connect to Your Microsoft 365 Tenant** – Enter the username of a user in your Microsoft 365 tenant. This user will be used to identify your Microsoft 365 tenant ID for re-authorizing the app. If you want to back up and restore Exchange Online public folders, this user must have an Exchange Online product license assigned in Microsoft 365.
6. **Permissions Granted to the App** – Select Microsoft 365 or Azure AD according to the permissions you have granted to the custom Azure app. If you select **Microsoft 365**, choose one of the following permissions:
   - All permissions – If the app has been granted all permissions, including SharePoint Online permissions, Exchange Online permissions, and Management API permissions, select this option.
   - SharePoint Online permissions – If the app has been granted SharePoint Online permissions, select this option.
   - Exchange Online permissions – If the app has been granted Exchange Online permissions, select this option.

   Note: When you want to use custom Azure apps with different permissions, you can create multiple app profiles for different custom Azure apps.
7. Click OK to re-authorize the app.
   The **App Management** page appears, and the custom Azure app is successfully re-authorized for the selected tenant.

Edit or Delete an App Profile for a Custom Azure App

On the **App Management** page, you can edit or delete an app profile for a custom Azure app.

- **Edit** – You can edit the name and description of an app profile. Click the app profile name, and the profile information is displayed. Click Edit to go to the edit page. Modify the profile name and/or description, and then click Save to save your changes.
- **Delete** – Select one or more app profiles and click Delete on the ribbon. A pop-up window appears asking for your confirmation. Click OK to confirm your deletion.

App Profile for a Microsoft Delegated App

In order to manage your data in Microsoft 365 via an app with delegated permissions, the Tenant Owner and Service Administrators can create an app profile for a Microsoft Delegated app. After creating an app profile, the IBM Spectrum® Protect Plus Online Services Administration app will be automatically created.

- **Create an App Profile for a Microsoft Delegated App**
- **Re-authorize the Microsoft Delegated App**
  The apps generated by app profiles need to be authorized. The app profiles whose statuses are App Authorization Expired must be re-authorized. You can also re-authorize the app for an active app profile if you want to change the account used to authorize the app.
- **Edit or Delete an App Profile for a Microsoft Delegated App**

Create an App Profile for a Microsoft Delegated App

Procedure

In Management > App Management, to create an app profile for a Microsoft Delegated app, complete the following steps:

1. Click Create on the **App Management** page.
2. In the pop-up window, select the Delegated tab.
3. Select check boxes next to the services that will use this app.
4. View the delegated permissions that will be added to this app, and click OK.
5. On the Microsoft 365 sign-in page, sign in with a Microsoft 365 Global Administrator account.
   Note: If the IBM Spectrum® Protect Plus Online Services for Microsoft 365 will use this delegated app to restore the channel conversations as posts, the authentication user of the delegated app must have a Teams license. If the IBM Spectrum Protect Plus Online Services for Microsoft 365 will use this app to protect the Planner data, the authentication user must have an Exchange license.
6. On the **Permissions requested** page, review the requested permissions and click Accept to continue.
7. The **App Management** page appears, and the app profile is created successfully.

Re-authorize the Microsoft Delegated App

The apps generated by app profiles need to be authorized. The app profiles whose statuses are App Authorization Expired must be re-authorized. You can also re-authorize the app for an active app profile if you want to change the account used to authorize the app.

Procedure

Complete the following steps to re-authorize the **IBM Spectrum® Protect Plus Online Services Administration** app:

1. Select an app profile for Microsoft Delegated App and click Re-authorize App on the ribbon.
2. In the pop-up window, you can select services that will use this app and view the required permissions. Then, click OK.
3. On the Microsoft 365 sign-in page, sign in with a Microsoft 365 Global Administrator account.
   Note: If the IBM Spectrum Protect Plus Online Services for Microsoft 365 uses this delegated app, the authentication user of the delegated app must have a Teams license assigned. If the IBM Spectrum Protect Plus Online Services for Microsoft 365 will use this app to protect the Planner data, the authentication user must have an Exchange license.
4. On the **Permissions requested** page, review the requested permissions and click Accept to continue.
5. The **App Management** page appears, and the app profile is successfully re-authorized.

Edit or Delete an App Profile for a Microsoft Delegated App

On the **App Management** page, you can edit or delete an app profile for a Microsoft Delegated app.

- **Edit** – You can edit the name and description of an app profile. Click the app profile name, and the profile information is displayed. Click Edit to go to the edit page. Modify the profile name and/or description, and then click Save to save your changes.
- **Delete** – Select one or more app profiles and click Delete on the ribbon. A pop-up window appears asking for your confirmation. Click OK to confirm your deletion.

App Profile for Yammer

If you want to enable the integration between IBM Spectrum® Protect Plus Online Services Cloud Governance and Yammer, IBM Spectrum Protect Plus Online Services, as the service platform of IBM Spectrum Protect Plus Online Services Cloud Governance, needs to connect to your Yammer environment.

The connection can be built via creating an app profile for Yammer. You can use the default app IBM Spectrum Protect Plus Online Services Administration provided by IBM® or use a custom app that you have registered in Yammer.

- **Create an App Profile for Yammer**
  The Tenant Owner and Service Administrators can create an app profile by navigating to Management > App Management.
- **Re-authorize the App for Yammer**
  The app used by the Yammer app profile needs to be authorized. The app profile whose status is **App Authorization Expired** must be re-authorized. You can also re-authorize the app for an active app profile if you want to change the account used to authorize the app, switch between the default app and the custom app, and change the custom app used for authorization.
- **Edit or Delete an App Profile for Yammer**

Create an App Profile for Yammer

The Tenant Owner and Service Administrators can create an app profile by navigating to Management > App Management.

- **Use a Custom Yammer App**
  To create an app profile for Yammer by using a custom app, you must register an app in Yammer.

Use a Custom Yammer App

To create an app profile for Yammer by using a custom app, you must register an app in Yammer.

Procedure

1. Navigate to https://www.yammer.com/client_applications and click Register New App.
2. Refer to the instructions in App Registration to configure the fields.
3. When configuring the **Redirect URI** field, enter following redirect URI.
   - Commercial production environment: https://spponlineservices.ibm.com/AuthManagement/YammerAuthCallBack
4. After the app registration is finished, copy the client ID and client secret. You need to provide the client ID and client secret when creating the app profile in IBM Spectrum® Protect Plus Online Services.
5. Navigate to IBM Spectrum Protect Plus Online Services> Management > App Management
6. Click Create on the **App Management** page.
7. In the pop-up window, choose Yammer and choose Use a custom Yammer app.
8. Complete the following fields:
   - **Profile Name** – Enter a name for the profile.
   - **Client ID** – Enter the client ID of your custom app.
   - **Client Secret** – Enter the client secret of your custom app.
9. Click OK.
10. On the Yammer login page, log in with an account that has the Verified Admin privileges.
11. Click Allow to proceed.
    The **App Management** page appears, and the app profile is created successfully.

Re-authorize the App for Yammer

The app used by the Yammer app profile needs to be authorized. The app profile whose status is **App Authorization Expired** must be re-authorized. You can also re-authorize the app for an active app profile if you want to change the account used to authorize the app, switch between the default app and the custom app, and change the custom app used for authorization.

Procedure

Complete the following steps to re-authorize the app:

1. Select the app profile for Yammer and click Re-authorize App on the ribbon.
2. In the pop-up window, choose Use the default Yammer app or Use a custom Yammer app.
   - If you choose to use the default app, click OK and proceed to the next step.
   - If you choose the use a custom app, enter the Client ID and Client Secret of your custom app. Click OK and proceed to the next step
3. On the Yammer login page, log in with an account that has the Verified Admin privileges.
4. Click Allow to proceed.
   The **App Management** page appears, and the app registered for IBM Spectrum® Protect Plus Online Services is successfully re-authorized for the selected tenant.

Edit or Delete an App Profile for Yammer

On the **App Management** page, you can edit or delete an app profile for Yammer.

- **Edit** – You can edit the name and description of an app profile. Click the app profile name, and the profile information is displayed. Click Edit to go to the edit page. Modify the profile name and/or description, and then click Save to save your changes.
- **Delete** – Select one or more app profiles and click Delete on the ribbon. A pop-up window appears asking for your confirmation. Click OK to confirm your deletion.

Manage Auto Discovery

Refer to the sections below to manage Auto Discovery for Microsoft 365 environments.

- **Auto Discovery for Microsoft 365**

Auto Discovery for Microsoft 365

The Auto Discovery feature automatically registers the following objects in your Microsoft 365 environment:

- SharePoint Online site collections
- OneDrive for Business
- Exchange Online mailboxes
- Microsoft 365 Groups/Microsoft Teams/Yammer communities (including group team sites and group mailboxes)
- Project Online site collections
- Exchange Online public folders
- Microsoft 365 users
- Security and Distribution Group (including Security Groups, Mail-enabled Security Groups, and Distribution Groups)

Note:

- For each Microsoft 365 tenant, an object type can only be included in one scan profile.
- For the SharePoint sites which have already been created before being connected to Microsoft 365 Groups, these SharePoint sites will be kept in both **SharePoint Sites** containers and **Groups/Teams/Yammer Communities** containers.
- For the SharePoint team sites which are created with Microsoft 365 Groups at the same time, these SharePoint team sites can only be scanned as the Microsoft 365 Group object type into **Groups/Teams/Yammer Communities** containers.

The detected objects will appear in your cloud services' environments. IBM Spectrum® Protect Plus Online Services will automatically monitor for updates, creation, and deletion of these objects.

In **Auto Discovery** on the left pane, you can manage the following items:

- **Data Center Mappings** – If your Microsoft 365 tenant has a Multi-Geo license (Microsoft 365 Multi-Geo), and you have paired a similar license for IBM Spectrum Protect Plus Online Services for Microsoft 365, this setting is provided for you to review and confirm which IBM Spectrum Protect Plus Online Services for Microsoft 365 data centers will support your Microsoft 365 geo locations. After you configure an app profile or service account, prior to starting the Auto Discovery, you must configure mappings between your Microsoft 365 geo locations and IBM Spectrum Protect Plus Online Services data centers. Click Data Center Mappings in the left pane. Then, refer to the instructions in Manage Data Center Mappings.
- **Scan Profiles** – Click Scan Profiles in the left pane. Then, refer to the instructions in Manage Scan Profiles.
- **Rules** – After rules are created in scan profiles, you can manage these rules. Click Rules in the left pane. Then, refer to the instructions in Manage Rules.
- **Containers** – After containers are created in scan profiles, you can manage these containers and the objects within the containers. Click Containers in the left pane. Then, refer to the instructions in Manage Containers.

- **Manage Scan Profiles**
- **Manage Rules**
- **Manage Containers**
- **Manage Data Center Mappings**

Manage Scan Profiles

On the Scan Profiles page, you can perform the following actions:

- Create
  To create a scan profile, click Create on the ribbon. Choose a scan mode first, **Express Mode** or **Advanced Mode**.
  - The advanced mode provides rules, which allow you to define how Microsoft 365 objects are detected and grouped in online services. This can make the management of those objects a lot easier. For organizations with over 300 users, you can use this mode to register your Microsoft 365 objects dynamically to custom containers. For details about advanced mode settings, refer to Advanced Mode.
  - If you do not have a lot of Microsoft 365 objects, you can use the express mode, where all objects are clustered within their default containers. For details about express mode settings, refer to Express Mode.

  Note: For each Microsoft 365 tenant, an object type can only be included in one scan profile.

- View Scan History
  To view the scan history of a scan profile, select the profile and click Scan History on the ribbon. The View Scan History page appears.
  In the "What's New" Report field, you can click Download Daily Report and Download Weekly Report to view the conclusion report of this scan profile's scan results. If you want to use emails to send conclusion reports of all scan profiles' updates to specific recipients, you can enable the "what's new" digest setting in Notification Settings > Advanced Settings > Notification & Email Settings > Notification Settings > Auto Discovery Notification. For more details, refer to Notification Settings.
  You can click Export Scan History to export a report about the detailed scan results. You can also click Delete Scan History to delete the selected scan job, including the basic job information and detailed scan results.
  If a scan job is not successfully completed, the Comment field will display the corresponding error message. For some error messages containing error codes, you can refer to the solutions provided in Appendix F - Helpful Notes When Auto Discovery Scan Results Return Error Codes.

- Edit
  Select a profile and click Edit on the ribbon. Then, edit the profile settings.

  Note: When you are editing a container, and you click Remove on the right pane, the container is just removed from the current profile, and it is not deleted. If you want to delete the container or remove objects from the container, navigate to Auto Discovery > Containers. For detailed instructions, refer to Manage Containers

- Delete
  Select one or more profiles and click Delete on the ribbon. A pop-up window appears, providing the following options from which you can choose a resolution for the containers that are related to the selected profiles:

  - Delete the containers along with the profile. They will be removed from IBM Spectrum® Protect Plus Online Services products.
  - Keep these containers registered in the system. They will continue to appear in your IBM Spectrum Protect Plus Online Services. No new objects will be added.

  Choose one of the options above and click Delete to confirm your deletion.

  Note: If you choose to keep the containers and you do not manually remove the objects from the containers via Auto Discovery > Containers, once you use the same Microsoft 365 credentials to create a new scan profile, the scan result of these objects will be Need to Remove.

- Run
  To run a scan profile, select the profile and click Run on the ribbon. A pop-up window appears prompting you that the scan profile cannot be edited when it is in the running process. To confirm your action and run the scan profile immediately, click Run in the pop-up window.

- Stop
  You can stop the scan process for a scan profile in the Scanning status. Select one or more profiles with the status of Scanning, and click Stop on the ribbon. A pop-up window appears asking for your confirmation. Click Stop to confirm.

  Note: The stop does not affect any objects that have already been scanned and registered.

- View Scan Settings
  To view detailed scan settings of a scan profile, click View Scan Settings under the Action column of a profile. The View Auto Discovery Settings page appears.
  On the View Auto Discovery Settings page, you can also click Edit to edit the profile or click View Scan History to view the scan history of this profile.

  Note: If the following message is displayed, it indicates that some objects need to be removed:
  Due to changes in this scan profile, some objects no longer meet the container's criteria. View and manage these objects?

  Click the View and manage these objects link, and a pop-up window appears displaying the objects that need to be removed. You can select one or more objects and click Remove on the ribbon. You can also click Remove All to remove all of these objects from the corresponding containers.

Express Mode

Procedure

Refer to the instructions below to configure express mode settings:

1. Select one or more object types that you want to scan.
   Note: Microsoft uses throttling to manage Microsoft 365 operations. The throttling limits can affect the scan of Exchange Online public folders and result in slow performance or failed scan jobs. If you select Exchange Online Public Folder, to avoid slow performance and failed scan jobs, you can contact Microsoft Support to adjust the Exchange parameter below to significantly reduce throttling in Microsoft 365:
   EWSMaxConcurrency: highest limit

2. Click Next.
3. Profile Name – Enter a name for the profile.
4. Description – Enter an optional description for the profile.
5. Authentication Method to Scan/Manage Data – Microsoft 365 service account profile and app profile can both be used to scan and manage Microsoft 365 objects.
   Based on the object types you have selected to scan and the cloud services your tenant is using, the supported authentication method and required permissions can be various. You can click the link below to view the details before choosing the authentication method.
   - IBM Spectrum Protect Plus Online Services for Microsoft 365

   Choose one of the following authentication methods:
   - Use an app profile – If you do not want to provide your account and password, you can choose the app profile authentication method.
     Note: If your organization uses multi-factor authentication in Microsoft 365, you must choose this method.

However, the app profile authentication method cannot scan Project Online site collections.

If you choose the app profile authentication method, you may need to configure the following settings:

- Scan in-place archived mailboxes – If Mailboxes are included in the scan scope, and you want to scan in-place archived mailboxes, select this checkbox. Note that using an app profile to scan in-place archived mailboxes may have an effect on the efficiency of the scan.
- Add service account profile as an additional method - If the app profile authentication method cannot meet your data management requirements, select this checkbox and select a service account profile from the drop-down list. For more information about the data management requirements of cloud services, refer to Will the App Profile Method Meet Your Data Management Requirements?
  In this situation, IBM Spectrum® Protect Plus Online Services for Microsoft 365 will use the app token within the app profile to back up Exchange Online mailboxes, Microsoft 365 Group/Teams mailboxes, and Exchange Online public folders, and use the service account with MFA enabled to back up Project Online site collections. For SharePoint Online site collections and Microsoft 365 Group team sites, we will use the app profile to back up and use the service account to back up the data types that are unsupported in the app context.

- Add delegated app profile to protect Microsoft Planner data - If your tenant is using the IBM Spectrum Protect Plus Online Services for Microsoft 365, has created an app profile for a Microsoft delegated app to protect Planner data, and has added Microsoft 365 Groups/Microsoft Teams/Yammer Communities to the scan scope, you can select this checkbox and select a corresponding delegated app profile from the drop-down list.
  With the above checkbox selected, you can choose whether to **Automatically add the authentication user of the delegated app as both owner and member of all scanned Microsoft 365 Groups and Teams**. If you change the option to No, ensure the authentication user of the delegated app will be manually added as both owner and member of the scanned objects.

- Impersonation Account – When Exchange Online public folders are included in the scan scope, you must configure this setting. This is a Microsoft 365 user that will be used to invoke the Exchange Web Services API, and this user must have an Exchange Online product license assigned in Microsoft 365. If you want to scan and protect Exchange Online public folders, this user also needs to be in the owner group of the public folders.
  Enter the username of a Microsoft 365 user as the impersonation account, and click Validation Test to validate this user.

- Use a service account profile (without MFA enabled) – If the app profile limitations are not acceptable, you can choose this method.
  If you want to back up and restore Microsoft Teams and Planner, configure Advanced options for backup and restore of Microsoft Teams and Planner. To protect Teams and Planner, the service account must be added as both owner and member of the following scanned objects:

  - Teams – For backup and restore of Teams only.
  - Microsoft 365 Groups and Teams – For backup and restore of Planner or both Teams and Planner.

  According to your scenario, choose to either automatically or manually add the service account as both owner and member of the scanned objects. If you select Yes, the Auto Discovery job will ensure the service account to be added as both owner and member for all scanned groups and teams.

  By default, the option of the Automatically add the service account as the owner of private channels in all scanned Teams setting is No. You can select Yes to enable this setting if necessary.

6. Update Schedule – If you want to run a scheduled scan, select the Set up a daily scan schedule checkbox, and then select the time for IBM Spectrum Protect Plus Online Services to scan and update your Microsoft 365 objects.
   Note: The selected time follows the time zone of your local computer.
7. Automatic Actions – Objects will be automatically moved to other containers when they match the containers' rules. You can select the Send an email notification to the following recipients when objects are moved to other containers or removed from any containers checkbox, and then select the email recipients from the drop-down list. Whenever objects are moved to other containers or removed from IBM Spectrum Protect Plus Online Services containers, the configured email recipients will receive email notifications. If there is no email recipient list, click New Email Recipient List to create one. For more instructions on configuring email recipient lists, refer to Email Settings.
8. How would you like to handle locked objects? - To scan objects in OneDrive for Business, SharePoint Online site collections, Microsoft 365 Groups/Microsoft Teams/Yammer communities, or Project Online site collections, you can choose to Ignore the locked objects when updating the job status. With this option selected, the scan results of locked objects will still be **Failed** in detailed reports, but the scan results will not affect the status of the scan job.
9. Choose to run the scan profile immediately or based on the configured schedule:
   - If you want to run the scan profile immediately, click Save and Run.
   - If you want to run the scan profile based on the configured schedule, click Save. The profile is created successfully. When the scheduled time arrives, IBM Spectrum Protect Plus Online Services will start the scan process.

   The whole process will be divided into multiple partial scans, so that you can manage and monitor the registered objects flexibly, rather than waiting for the whole process to complete. When a partial scan is finished, the detected objects will appear in your service environment. You can also find them in the Scan History.

Advanced Mode

Procedure

Refer to the instructions below to configure the advanced mode settings:

1. Select object types that you want to scan and configure containers and scan rules for them respectively by following the instructions below.
   Note: Microsoft uses throttling to manage Microsoft 365 operations. The throttling limits can affect the scan of Exchange Online public folders and result in slow performance or failed scan jobs. If you select Exchange Public Folders, to avoid slow performance and failed scan jobs, you can contact Microsoft Support to adjust the Exchange parameter below to significantly reduce throttling in Microsoft 365:
   EWSMaxConcurrency: highest limit

2. Choose one of the following methods to scan objects: Scan all objects and place them in one container or Scan objects according to dynamic rules.
   - If you choose the Scan all objects and place them in one container option, enter a container name in the text box. You can also click the select container button and select an existing container in the pop-up window.
   - If you choose the Scan objects according to dynamic rules option, define containers for desired Microsoft 365 object types. Click the title for an object type, click New Container, and then configure the following settings:
     - Container Name – Enter a name for this object container.

- Rule Name – Enter a name for the rule that will be used to filter objects.
  Configure rule settings by selecting a criterion, selecting a condition, and selecting or entering a value. For more information about supported criteria, refer to Appendix A - Supported Criteria in Auto Discovery Rules.
  Note: You can click Copy from Existing Rules to reuse rule settings. In the pop-up window, all rules are displayed. Click Copy Criteria or Copy Criteria and Values.
- You can click the add button to add another criterion. With multiple criteria, you must select the logic option And or Or.

  And
  The objects that meet all criteria will be filtered to be included.
  Or
  The objects that meet any one of the criteria will be filtered to be included.

- Click Save to save this container. The container settings are collapsed. You can click the blank area next to the container name to edit the container settings or click Remove to remove the container from the profile.
- You can click New Container and repeat the steps above to create another container.
- If you define multiple containers, set a container's priority by selecting a number from the Priority drop-down list.

If there is any object that does not meet the criteria in your rules, the object will not be registered to the containers you defined. Select a resolution for the object:

- Do not add them to any containers
- Add them to system default containers
- Add them to a custom container
  If you choose the custom container option, enter either an existing container name or a non-existing container name. You can also click the select button to select an existing container. If you enter a non-existing container name, IBM Spectrum® Protect Plus Online Services will automatically create the container.

3. Click Next.
4. Profile Name – Enter a name for the profile.
5. Description – Enter an optional description for the profile.
6. Authentication Method to Scan/Manage Data – The Microsoft 365 service account profile and app profile can both be used to scan and manage Microsoft 365 objects.
   Based on the object types you have selected to scan and the cloud services your tenant is using, the supported authentication method and required permissions can be various. You can click the link below to view the details before choosing the authentication method.

   - IBM Spectrum Protect Plus Online Services for Microsoft 365

   Choose one of the following authentication methods:
   - Use an app profile – If you do not want to provide your account and password, you can choose the app profile authentication method.
     Note: If your organization uses multi-factor authentication in Microsoft 365, you must choose this method.
     However, the app profile authentication method has the following limitations:
     - Unable to filter mailboxes by the Mailbox Type rule.
     - The app profile authentication method cannot scan Project Online site collections.

     If you choose the app profile authentication method, you may need to configure the following settings:
     - Scan in-place archived mailboxes – If Mailboxes are included in the scan scope, and you want to scan in-place archived mailboxes, select this checkbox. Note that using an app profile to scan in place archived mailboxes may have an effect on the efficiency of the scan.
     - Add service account profile as an additional method – If the app profile authentication method cannot meet your data management requirements, select this checkbox and select a service account profile from the drop-down list. For more information about the data management requirements of cloud services, refer to Will the App Profile Method Meet Your Data Management Requirements?
       In this situation, IBM Spectrum Protect Plus Online Services for Microsoft 365 will use the app token within the app profile to back up Exchange Online mailboxes, Microsoft 365 Group/Teams mailboxes, and Exchange Online public folders, and use the service account with MFA enabled to back up Project Online site collections, SharePoint Online site collections and Microsoft 365 Group team sites.

     - Add delegated app profile to protect Microsoft Planner data - If your tenant is using the IBM Spectrum Protect Plus Online Services for Microsoft 365, has created an app profile for a Microsoft delegated app to protect Planner data, and has added Microsoft 365 Groups/Microsoft Teams/Yammer Communities to the scan scope, you can select this checkbox and select a corresponding delegated app profile from the drop-down list.
       With the above checkbox selected, you can choose whether to **Automatically add the authentication user of the delegated app as both owner and member of all scanned Microsoft 365 Groups and Teams**. If you change the option to **No**, ensure the authentication user of the delegated app will be manually added as both owner and member of the scanned objects.

     - MFA service account profile – If your organization uses multi-factor authentication in Microsoft 365, select this checkbox and select a service account profile with MFA enabled from the drop-down list. In this situation, IBM Spectrum Protect Plus Online Services for Microsoft 365 will use the app token within the app profile to back up Exchange Online mailboxes, Microsoft 365 Group mailboxes, and Exchange Online public folders, and use the service account with MFA enabled to back up SharePoint Online site collections, Project Online site collections, and Microsoft 365 Group team sites.
     - Impersonation Account – When Exchange Online public folders are included in the scan scope, you must configure this setting. This is a Microsoft 365 user that will be used to invoke the Exchange Web Services API, and this user must have an Exchange Online product license assigned in Microsoft 365. If you want to scan and protect Exchange Online public folders, this user also needs to be in the owner group of the public folders.
       Enter the username of a Microsoft 365 user as the impersonation account, and click Validation Test to validate this user.

   - Use a service account profile (without MFA enabled) – If the app profile limitations are not acceptable, you can choose this method.
     If you want to back up and restore Microsoft Teams and Planner, configure Advanced options for backup and restore of Microsoft Teams and Planner.
     To protect Teams and Planner, the service account must be added as both owner and member of the following scanned objects:

     - Teams – For backup and restore of Teams only.
     - Microsoft 365 Groups and Teams – For backup and restore of Planner or both Teams and Planner.

   According to your scenario, choose to either automatically or manually add the service account as both owner and member of the scanned objects. If you select Yes, the Auto Discovery job will ensure that the service account is added as both owner and member for all scanned groups and teams.

By default, the option of the Automatically add the service account as the owner of private channels in all scanned Teams setting is No. You can select Yes to enable this setting if necessary.

7. Update Schedule – If you want to run a scheduled scan, select the Set up a daily scan schedule checkbox, and then select the time for IBM Spectrum Protect Plus Online Services to scan and update your Microsoft 365 objects.
   Note: The selected time follows the time zone of your local computer.
8. Automatic Actions – Objects will be automatically moved to other containers when they match the containers' rules. You can select the Send an email notification to the following recipients when objects are moved to other containers or removed from any containers checkbox, and then select the email recipients from the drop-down list. Whenever objects are moved to other containers, the configured email recipients will receive email notifications. If you choose the Do not add them to any containers option in the previous step, the recipients will also receive email notifications when objects no longer meet the rule of any containers, and the objects are removed from IBM Spectrum Protect Plus Online Services containers. If there is no email recipient list, click New Email Recipient List to create one. For more instructions on configuring email recipient lists, refer to Email Settings.
9. How would you like to handle locked objects? - To scan objects in OneDrive for Business, SharePoint Online site collections, Microsoft 365 Groups/Microsoft Teams/Yammer communities, or Project Online site collections, you can choose to Ignore the locked objects when updating the job status. With this option selected, the scan results of locked objects will still be **Failed** in detailed reports, but the scan results will not affect the status of the scan job.
10. Choose to run the scan profile immediately or based on the configured schedule:
    - If you want to run the scan profile immediately, click Save and Run.
    - If you want to run the scan profile based on the configured schedule, click Save. The profile is created successfully. When the scheduled time arrives, IBM Spectrum Protect Plus Online Services will start the scan process.

    The whole process will be divided into multiple partial scans, so that you can manage and monitor the registered objects flexibly, rather than waiting for the whole process to complete. When a partial scan is finished, the detected objects will appear in your service environment. You can also find them in the Scan History.

Manage Rules

Click Rules in the left pane; the Rules page appears. You can edit or delete rules.

- Edit
  To edit the settings of a rule, select the rule and click Edit on the ribbon.
- Delete
  To delete one or more rules, select the rules and click Delete on the ribbon. A pop-up window appears asking for your confirmation. Click OK to confirm your deletion.

Manage Containers

Click Containers in the left pane; the Containers page appears. You can perform the following actions:

- View By
  You can choose to view containers by Container Name or Geo Location.
  Note: The Geo Location view is only available when your tenant has Multi-Geo Capabilities in IBM Spectrum® Protect Plus Online Services for Microsoft 365
- View Details
  You can view details of scan profiles and rules that are applied to custom containers. Click View Details next to a custom container name. A pop-up window appears displaying the scan profile name and rule details.
- Batch Import
  To batch import objects into a container, complete the following steps:

  1. Click the title of a Microsoft 365 object type to import objects into the containers for this type of object.
  2. Select the container where the objects will be imported.
  3. Click Batch Import on the ribbon, and a pop-up window appears. Then, refer to the instructions in Import Objects in Batch.
- Delete Container
  To delete one or more custom containers, select the containers and click Delete on the ribbon. A pop-up window appears asking for your confirmation. Click OK to confirm your deletion. When the containers are deleted, the objects within the containers are removed from the groups.
- Remove Objects
  To remove one or more objects from their containers, expand the container name, select the objects, and click Delete on the ribbon. A pop-up window appears asking for your confirmation. Click OK to confirm your action.
- Remove Objects Only
  To only remove the objects from one or more containers, select the containers and click Remove Objects Only on the ribbon. A pop-up window appears asking for your confirmation. Click OK to confirm your action.
- **Import Objects in Batch**
  You can use a batch job to import objects.

Import Objects in Batch

You can use a batch job to import objects.

Procedure

In the pop-up window for importing objects in batch, configure the following settings:

1. Download an object list template by clicking the Download the Object List Template link.
2. In the downloaded Excel file, enter the information about the objects you are about to import.
3. Click Browse to upload the configured object list.
   Note: You can only upload one object list at a time. The previously uploaded object list will be replaced by the newly uploaded one.
4. Provide a Microsoft 365 account to connect to your Microsoft 365 environment in the Microsoft 365 Account Information field. Select one of the following methods:
   Note: The method determines the types of objects that can be imported. For more information, refer to Appendix B - Objects Supported by Batch Import.
   - Retrieve from a service account profile – Select this option to retrieve Microsoft 365 account information from a service account profile. Select a service account profile from the drop-down list. If you have not created any service account profiles, you can select the New Service Account Profile option from the drop-down list, and the Create Service Account Profile page will appear in a new tab. For details of creating a service account profile, refer to Create a Service Account Profile. After creating a new service account profile, go back to the Manage Containers page, and click the refresh button next to the corresponding drop-down list to get the latest profile.
   - Retrieve from an app profile – Select this option to retrieve a Microsoft 365 account information from an app profile. Select an app profile from the drop-down list. If you have not created any app profiles, you can select the New App Profile option from the drop-down list, and the App Management page will appear in a new tab. For details of creating an app profile, refer to Create an App Profile for Microsoft 365. After creating a new app profile, go back to the Container page, and click the refresh button next to the corresponding drop-down list to get the latest profile.
5. Options for Microsoft 365 Users – If you batch import Microsoft 365 users, configure the following additional options:

   - How would you like to handle the imported Microsoft 365 users in Auto Discovery scan jobs?
     The default setting is Ignore the scan rules and keep the imported users in their original containers. With this setting selected, when the batch imported Microsoft 365 users meet the criterion in scan rules, they will not be moved to other containers by scan jobs. If you want to disable this setting, deselect this checkbox.

   - How would you like to handle the imported Microsoft 365 users in Batch Import jobs?
     The default setting is Move the imported users from the original containers to the new containers. With this checkbox selected, the Microsoft 365 users existing in containers will be moved to the new containers which are provided in Batch Import jobs. If you want to disable this setting, deselect this checkbox.

6. If you want to configure Notification for batch import, select the Send an email to the following recipients after the batch import is finished checkbox, and select a recipient list in the drop-down list. You can also create New Email Recipient List to create a new list. For details of configuring an email recipient list, refer to Email Settings.
7. Click Import to import the objects into the selected container in batch, or click Cancel to close the pop-up window without importing any objects.
   Note: When Yammer communities are imported to containers, the Yammer community IDs are not retrieved. During the scan process, the community IDs will be retrieved. If you use an advanced mode scan profile, the community IDs can be retrieved only when the communities meet the scan rules.

Manage Data Center Mappings

When you navigate to Data Center Mappings to configure mappings for the first time, you will see the pop-up window below.

Your organization's backup data is now stored in the central IBM Spectrum® Protect Plus Online Services location where your primary tenant initially signed up.

- To keep the backup data of your Microsoft 365 geo locations in the central IBM Spectrum Protect Plus Online Services location, you can click **Map Microsoft 365 geo locations to the central IBM Spectrum Protect Plus Online Services location** and select geo locations. The selected geo locations will be mapped to the central location, and the rest of the geo locations will be automatically mapped to other data centers.
- IBM Spectrum Protect Plus Online Services
- If you disable the option, all geo locations will be automatically mapped to different IBM Spectrum Protect Plus Online Services data centers. IBM Spectrum Protect Plus Online Services for Microsoft 365 will back up the data of these geo locations once again, and the backup data will be stored in different IBM Spectrum Protect Plus Online Services data centers according to the mappings.

Click Confirm to confirm your selection.

On the Data Center Mappings page, under the Multi-Geo Data Centers tab, you will see the default mappings between your Microsoft 365 geo locations and IBM Spectrum Protect Plus Online Services data centers. You can also configure storage locations for your geo locations.

In the following scenarios, you can select a desired data center from the drop-down list:

- IBM Spectrum Protect Plus Online Services has more than one data center corresponding to a Microsoft 365 geo location.
- The data center corresponding to a Microsoft 365 geo location has not been supported in IBM Spectrum Protect Plus Online Services yet.

In the following scenarios, you can configure storage locations for your organization’s geo locations by selecting **IBM Spectrum Protect Plus Online Services Storage** or Bring Your Own Storage.

- New geo locations are added, and your organization uses IBM Spectrum Protect Plus Online Services storage.
- Your organization signs up for IBM Spectrum Protect Plus Online Services and uses IBM Spectrum Protect Plus Online Services storage.
  Note: The Storage Location can only be configured once for each geo location.

Click Save to save the mappings.

Note: These mappings will be used to create boundaries between different geo locations in your environment, and the saved mappings cannot be changed. Under the Central IBM Spectrum Protect Plus Online Services Location tab, you can view the data center where your primary IBM Spectrum Protect Plus Online Services tenant initially signed up. All data managed prior to your multi-geo license or data related to other services will be stored here. Note that the data is not

shared with multi-geo tenants, even in the same data center.

Manage Encryption Profiles

Encryption profiles allow you to use Azure Key Vault to encrypt backup data and tenant-sensitive information (Microsoft 365 usernames, passwords, etc.).

The Tenant Owner and Service Administrators can manage encryption profiles in Encryption Management. From this menu, you can perform the following actions:

- Create
  Click Create on the ribbon. Then, refer to the instructions in Create an Encryption Profile.
- Apply
  To make the key vault in an encryption profile take effect, you must apply the encryption profile. Select the profile and click Apply on the ribbon. A pop-up window appears asking for your confirmation. Click OK to confirm. The Being Applied label is displayed next to the profile name. When the key vault in the profile is successfully applied, the Being Applied status is changed to Being Used.
- Edit
  Select an encryption profile and click Edit on the ribbon.
  If you want to change your key vault used in an encryption profile, refer to the details in What Should I Do If I Need to Change My Azure Key Vault or Keys? to see in which scenario you need to edit an encryption profile.
  Note: The Default Encryption Profile cannot be edited.
- Delete
  Select one or more encryption profiles and click Delete on the ribbon. A pop-up window appears asking for your confirmation. Click OK to confirm your deletion.
  If you want to change the key used in an encryption profile, refer to the details in What Should I Do If I Need to Change My Azure Key Vault or Keys? to see when an encryption profile and the key specified in the profile can be deleted.

Note: IBM Spectrum Protect Plus Online Services provides a default encryption profile. You can also create a custom encryption profile and apply it.

- **Preparations**
  Before creating an encryption profile, make sure you have a key vault in Azure. If you do not have any key vaults, refer to the instructions in Appendix C - Create a Key Vault in Azure.
- **Create an Encryption Profile**
  To create an encryption profile, click Create on the ribbon. Make sure you have finished the Preparations, and then configure the following settings on the Create Encryption Profile page.
- **What Should I Do If I Need to Change My Azure Key Vault or Keys?**
  The IBM Spectrum Protect Plus Online Services encryption profile uses Azure Key Vault to encrypt your backup data and tenant-sensitive information (Microsoft 365 usernames, passwords, etc.). When you use a custom key vault for data encryption, you provide your key vault information in an encryption profile.
- **What Should I Do If My Key Vault Has been Permanently Deleted in Azure?**
  The IBM Spectrum Protect Plus Online Services encryption profile uses Azure Key Vault to encrypt your backup data and tenant-sensitive information (Microsoft 365 usernames, passwords, etc.). When you use a custom key vault for data encryption, you provide your key vault information in an encryption profile.

Preparations

Before creating an encryption profile, make sure you have a key vault in Azure. If you do not have any key vaults, refer to the instructions in Appendix C - Create a Key Vault in Azure.

Procedure

Then, perform the following pre-check on the key vault:

1. Log in to Azure Portal.
2. Navigate to Key vaults.
3. Click the key vault you prepared and click Access policies on the middle pane.
4. Locate the application that is used for your key vault.
5. In the Key permissions drop-down list, make sure that at least the following operations are selected: Get, Encrypt, and Decrypt.
6. Navigate to the pane for key vault settings and click Keys.
7. Click a key and click a version of the key.
8. In the Permitted operations section, make sure that at least Encrypt and Decrypt are selected.
9. Copy the key identifier that resides in the Properties section. When you create an encryption profile in IBM Spectrum® Protect Plus Online Services, you will need to provide this key identifier.
   Apart from the pre-checking above, ensure that you back up the key in case that the key is deleted accidentally. If a key has been applied to IBM Spectrum Protect Plus Online Services encryption profile to encrypt data, and the key is deleted with no backup, the encrypted data will be damaged and IBM Spectrum Protect Plus Online Services cannot work for you smoothly.

Create an Encryption Profile

To create an encryption profile, click Create on the ribbon. Make sure you have finished the Preparations, and then configure the following settings on the Create Encryption Profile page.

1. Profile Name
   Enter a name for the encryption profile.
2. Description
   Enter an optional description.
3. Key Identifier
   Enter the key identifier of your key vault.
4. Client ID
   Enter the application ID of the application you prepared for the key vault.
5. Client Secret
   Enter the application key of the application above.
6. Click Validation Test to validate your key vault information.
7. Expiration Date
   Since the encryption profile cannot continue to work once the client secret expires, you can choose to Add a reminder for the Key Vault's client secret expiration date. After checking the client secret's expiration date in Microsoft Azure, click the calendar button and select a date.
8. Send an email notification to the following recipients 15 days before the expiration date
   If you want to receive the notification before the client's secret expiration date, select this checkbox and select an email recipient list from the drop-down list.
9. Click Save to save your configurations, or click Cancel to go back to the Encryption Management page without saving any configurations.

What Should I Do If I Need to Change My Azure Key Vault or Keys?

The IBM Spectrum® Protect Plus Online Services encryption profile uses Azure Key Vault to encrypt your backup data and tenant-sensitive information (Microsoft 365 usernames, passwords, etc.). When you use a custom key vault for data encryption, you provide your key vault information in an encryption profile.

You may need to change your key vault or keys in the Azure Key Vault due to your organization's key rotation requirements or other reasons. If you need to change the key vault or keys in the Azure Key Vault, to ensure IBM Spectrum Protect Plus Online Services functionality works well and your data is still protected, you must follow the procedures in the scenarios below.

- **I Need to Change the Key Used for Data Encryption**
  If you need to change the key that is used to encrypt your backup data and tenant sensitive information (Microsoft 365 usernames, passwords, etc.), follow the procedure below:
- **I Need to Change My Key Vault**
  If you need to change your key vault settings, but do not change the associated application or key, your IBM Spectrum Protect Plus Online Services encryption profile does not require any changes.
- **I Need to Use a New Key Vault**
  You can apply a new key vault to replace the original key vault.

I Need to Change the Key Used for Data Encryption

If you need to change the key that is used to encrypt your backup data and tenant sensitive information (Microsoft 365 usernames, passwords, etc.), follow the procedure below:

Procedure

1. In the Azure Key Vault, create a new key or create a new version for the key that is used in the IBM Spectrum® Protect Plus Online Services encryption profile.
   Note: Skip this step if you already prepared a key.
2. Navigate to IBM Spectrum Protect Plus Online Services > Encryption Management, and create a new encryption profile. For details, see Create an Encryption Profile.
3. On the Encryption Management page, select the newly created profile and click Apply on the ribbon to switch from the old key to the new key.
   Note: After you click Apply, IBM Spectrum Protect Plus Online Services starts applying the key, and the Being Applied label is displayed next to the new profile name. When IBM Spectrum Protect Plus Online Services is applying the key in the new profile to re-encrypt your data, the key in the old profile is still being used. To ensure IBM Spectrum Protect Plus Online Services works well and your data is still protected, do not delete the old profile or the old key in the Azure Key Vault when the key is being applied. The old profile and the old key must still be available before the backend re-encryption process is completed.
4. When the new encryption profile status is changed from Being Applied to Being Used, it indicates that the key in the new profile is successfully applied. Many organizations are required to keep the old keys for a period of time according to their key retention policy, but if you need to delete the key used in the old encryption profile or delete the old encryption profile, you may delete it now.

I Need to Change My Key Vault

If you need to change your key vault settings, but do not change the associated application or key, your IBM Spectrum® Protect Plus Online Services encryption profile does not require any changes.

Procedure

If you need to change the application associated with your key vault in the Azure Key Vault, but do not change the associated key, follow the procedures below:

1. In the Azure Portal, create a new application.
   Note: Skip this step if you want to use an existing application.
2. Copy the client ID of the application.
3. Add a client secret for the application.
   Note: Skip this step if you want to use an existing application that already has a valid client secret.
4. Copy the client secret.
   Note: You can only copy the client secret upon the client secret generation. The client secret will be hidden after you perform another operation or leave the page.
5. Edit your key vault's access policies and add a new access policy for the application.
6. Navigate to IBM Spectrum Protect Plus Online Services > Encryption Management, edit your custom encryption profile and update the client ID and client secret.

I Need to Use a New Key Vault

You can apply a new key vault to replace the original key vault.

Procedure

1. In the Azure Portal, create a new key vault. For details, see Appendix C - Create a Key Vault in Azure.
2. Navigate to IBM Spectrum® Protect Plus Online Services > Encryption Management, and create a new encryption profile. For details, see Create an Encryption Profile.
3. On the **Encryption Management** page, select the newly created profile and click **Apply** on the ribbon to switch from the old key vault to the new key vault.
   Note: After you click Apply, IBM Spectrum Protect Plus Online Services starts applying the key vault, and the Being Applied label is displayed next to the new profile name. When IBM Spectrum Protect Plus Online Services is applying the key in the new profile to re-encrypt your data, the key in the old profile is still being used. To ensure IBM Spectrum Protect Plus Online Services works well and your data is still protected, do not delete the old profile, the old key vault, or the old key in the Azure Key Vault when the key is being applied. The old profile and the old key must still be available before the backend re-encryption process is completed.
4. When the new encryption profile status is changed from Being Applied to Being Used, it indicates that the key in the new profile is successfully applied. Many organizations are required to keep the old keys for a period of time according to their key retention policy, but if you need to delete the key used in the old encryption profile, delete the old key vault, or delete the old encryption profile, you may delete it now.

What Should I Do If My Key Vault Has been Permanently Deleted in Azure?

The IBM Spectrum® Protect Plus Online Services encryption profile uses Azure Key Vault to encrypt your backup data and tenant-sensitive information (Microsoft 365 usernames, passwords, etc.). When you use a custom key vault for data encryption, you provide your key vault information in an encryption profile.

If the key vault was deleted in Azure, your data cannot be encrypted in IBM Spectrum Protect Plus Online Services. IBM Spectrum Protect Plus Online Services recommends you first contact Microsoft Support to recover your key vault.

The table below shows the influence of the key vault deletion on IBM Spectrum Protect Plus Online Services and other cloud services.

Service	Influence
IBM Spectrum Protect Plus Online Services	You cannot use some of the IBM Spectrum Protect Plus Online Services features.
IBM Spectrum Protect Plus Online Services for Microsoft 365	The data previously protected by IBM Spectrum Protect Plus Online Services for Microsoft 365 cannot be restored.

If the key vault cannot be recovered in Azure, you can recover your tenant in IBM Spectrum Protect Plus Online Services to make sure IBM Spectrum Protect Plus Online Services and your cloud services work well. Refer to the steps below:

1. In the Azure Portal, create a new key vault. For details, see Appendix C - Create a Key Vault in Azure.
2. Navigate to IBM Spectrum Protect Plus Online Services > Encryption Management, and create a new encryption profile. For details, see Create an Encryption Profile.
3. Contact the IBM Software Support team to apply the new encryption profile to your IBM Spectrum Protect Plus Online Services tenant.
   Note: It takes a while to apply the new encryption profile to your tenant. During this time, no additional operations should be taken in both your IBM Spectrum Protect Plus Online Services tenant and IBM Spectrum Protect Plus Online Services environments until the new encryption profile is successfully applied.
4. IBM Spectrum Protect Plus Online Services cannot decrypt your data that was encrypted before. Once the new encryption profile is successfully applied to your tenant, you need to perform the following actions if your tenant has configured the corresponding settings:
   - Edit your service account profile
   - Re-authorize your app profile
   - Edit the service account pool
   - Edit the System Center Operations Manager settings in Advanced Settings > Integration with SCOM

Enable Report Data Collection

You can enable report data collection for Microsoft 365.

Data in Microsoft 365

Note:

- To collect data, make sure the **Audit log search** is turned on in the compliance center. For instructions, see How to turn on audit log search.
- When you enable the **Report Data Collection** for the first time, IBM Spectrum® Protect Plus Online Services first collects data for six days after you enable the option, and then collects data daily.
- To avoid 429 throttling issues, Cloud Management Report Center supports using Office 365 Management Activity APIs to read user activities for Auditor Reports. To use Office 365 Management Activity APIs, you must enable data collection on this page and select the **Use Office 365 Management Activity API, configured through Report Data Collection in IBM Spectrum Protect Plus Online Services interface (Recommended)** option in the Report Center > Global Settings interface.

Complete the following steps to enable the report data collection:

1. Click Report Data Collection on the left pane.
2. On the **Report Data Collection** page, click the Data in Microsoft 365 tab and select the Enable data collection checkbox.
3. You can set Account Filter, which can be useful for filtering out service accounts to improve the quality and accuracy of reports. Enter one or more accounts in the following format: **someone@example.com**.
4. **Exclude activities of Microsoft 365 Service Accounts and IBM Spectrum Protect Plus Online Services Account Pool users** – If you use the service account profile authentication method to scan Microsoft 365 objects, you can select this option to filter out activities of Microsoft 365 service accounts and account pool users whose accounts are used to register objects into IBM Spectrum Protect Plus Online Services, since the action records caused by scan jobs may affect the collected data and the analysis results.
5. **Filter out data with the default URL components** – Select this checkbox if you want to filter out data using the URL components displayed in the **Customize URL components to filter out view activities on the pages** text box. If you want to customize URL components to filter out data, deselect this checkbox and enter the custom URL components in the text box. If you want to filter out all activities, select the **Filter out all activities on pages that contain the URL components above** checkbox.
6. **Notification about Failed Data Collection** – IBM Spectrum Protect Plus Online Services collects data every day. You can choose whether to **Send an email notification if no data is collected in the past _ days**. If you enable the notification, enter a number between 1 and 7 and select the email recipients.
    - **Send an email notification to Service Administrators** – If no data is collected in the defined time, an email notification will be sent to Service Administrators.
    - **Send an email notification to the following recipients** – If you select the checkbox, select an email recipient list from the drop-down list. The recipients in the list will receive an email notification if no data is collected in the defined time. If there is no email recipient list, refer to the Email Settings section to create one.
7. **Tenant Scope** – Set the scope for the tenants whose data will be displayed on reports. Select **All tenants** or **Specific tenants**. If you select **Specific tenants**, select at least one tenant from the drop-down list.
8. **Storage Configuration** – Configure the storage for storing Microsoft 365 activity data.
    - Select a storage type:
        - **Default storage** – Select this if you want to continue to use the default Azure storage provided by IBM Spectrum Protect Plus Online Services.
        - **Custom storage** – Select this if you want to create custom storage (only Azure Blob Storage is supported), and finish the configurations below.
            - **Account name** – Enter an account name of Azure Blob Storage.
            - **Account password** – Enter the password of the account above.
            - **Container name** – Enter the container name of the storage. If the container is removed from the storage, IBM Spectrum Protect Plus Online Services will create a new container using the same name when collecting storage for the next time.
              Note: If you want to use custom storage, note the following:
                - Before adding the storage account to the IBM Spectrum Protect Plus Online Services interface, ensure IBM Spectrum Protect Plus Online Services agents have access to your storage. For details, refer to Allow IBM Spectrum Protect Plus Online Services Agent Servers to Access Your Storage Account.
                - Once the configuration is saved, old data in the default storage will be cleared up but won't be moved to the new custom storage, and you cannot switch to the default storage anymore.
                - If you want to change to another custom storage device, manually move the data from the old custom storage to the new one. IBM Spectrum Protect Plus Online Services does not have the permission to clear up data from the old custom storage.
            - **Enable email notification about failed connection** (for **Custom storage** only) – Select this if you want to send an email notification to all active Service Administrators when the custom storage connection fails. The email notification will be sent at 00:00 UTC every day if the connection continues to fail.
9. **Export Microsoft 365 Activity Data** – Choose whether to **Export Microsoft 365 tenant activity data to Azure SQL database**. The data will be exported to your Azure SQL database every hour. If you enable this option, provide the following information:
    - **Server name** – Enter the name of the SQL server where the SQL database is located.
    - **Database name** – Enter the name of the SQL database you prepared.
    - **Username** – Enter the username of an account that has the **db_owner** role to the database.
    - **Password** – Enter the password of the account above.
10. Click Save to save your selections, or click Cancel to go back to the homepage without saving any selections.

Activities in Microsoft 365

Enable data collection for the service that monitors the Microsoft Activity API and provides auditing reports/alerts for IBM Spectrum Protect Plus Online Services products.

- **Allow IBM Spectrum Protect Plus Online Services 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.

Allow IBM Spectrum Protect Plus Online Services 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 Spectrum Protect Plus Online Services can access your storage, complete the settings as required in the following conditions:
Note: If you are using a trial license and the storage account you want to use in the trial has a firewall enabled, read the conditions below and contact IBM Software Support for the corresponding reserved IP addresses or ARM VNet IDs.

- If you are using a storage type other than Microsoft Azure 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.
- 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 Spectrum Protect Plus Online Services or your storage account is in its paired region**, you must add the Azure Resource Manager (ARM) vNet subnets where the IBM Spectrum Protect Plus Online Services agents are running on to your storage networking. You can find additional details in this Microsoft article: Grant access from a virtual network, and contact the IBM Software Support team to get the subnet ID of IBM Spectrum Protect Plus Online Services for your data center. 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** section below.

Add Reserved IP Addresses

You can add reserved IP addresses by following the procedure.

1. Navigate to **IBM Spectrum Protect Plus Online Services** interface and click Advanced Settings > Reserved IP Addresses to download the list of reserved IP addresses of IBM Spectrum Protect Plus Online Services. For details, refer to Download a List of Reserved IP Addresses.
2. Go to the storage account that you want to secure.
3. Select Networking on the menu.
4. Check that you've selected to allow access from Selected networks.
5. Enter the IP address or address range under Firewall > Address Range.
6. Select Save to apply your changes.

Add ARM Virtual Networks

To grant access to a subnet in a virtual network belonging to another tenant, use PowerShell, a command-line interface, or a REST API.

```
## Contact IBM Software Support team to get the IBM Spectrum Protect Plus  Online Services network subnet resource ID
$SUBNETID="/subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-
yyyyyyyyyyyy/resourceGroups/ResrouceGroupName/providers/Microsoft.Network/virtualNetworks/VIrtualNetworkName/subnets/Subn
etName"

$DESTRG="customer_resource_group_name"
$DESTSTA="customer_storage_accont_name"


####
##    Use the Azure cli tool (https://docs.microsoft.com/en-us/cli/azure/install-azure-cli?view=azure-cli-latest)
##
## Add the firewall virtual network rule to grant access to IBM Spectrum Protect Plus  Online Services
az storage account network-rule add --resource-group $DESTRG --account-name $DESTSTA --subnet $SUBNETID
az storage account network-rule list --resource-group $DESTRG --account-name $DESTSTA --query virtualNetworkRules
## (Optional) Disable the public access to storage account
az storage account update --resource-group $DESTRG --name $DESTSTA --default-action Deny
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)
##
Add-AzStorageAccountNetworkRule -ResourceGroupName $DESTRG -Name $DESTSTA -VirtualNetworkResourceId $SUBNETID
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 the message.

Configure Advanced Settings

In **Advanced Settings**, the Tenant Owner and Service Administrators can configure notification and email settings, integration with SCOM, trusted IP address settings, the security policy, and the session timeout setting. Refer to the instructions in the sections below.

- **Configure Notification and Email Settings**
  In Notification and Email Settings, you can configure notification settings, email recipient lists, email date format, and email language.

- **Enable Integration with SCOM**
  You can integrate IBM Spectrum Protect Plus Online Services and System Center Operations Manager (SCOM).
- **Enable Trusted IP Address Settings**
  You can enable trusted IP address settings to only allow users to access IBM Spectrum Protect Plus Online Services from certain IP addresses or IP address ranges.Only IPv4 addresses are supported.
- **Configure the Security Policy**
- **Configure Session Settings**
- **Download a List of Reserved IP Addresses**
  If your tenant has the enterprise license for any service offered by IBM Spectrum® Protect Plus Online Services the Tenant Owner and Service Administrators can download a list of reserved IP addresses.

Configure Notification and Email Settings

In Notification and Email Settings, you can configure notification settings, email recipient lists, email date format, and email language.

- **Notification Settings**
- **Email Settings**

Notification Settings

Under the **Notification Settings** tab, you can configure authentication notifications, Auto Discovery notifications, and license notifications.

To monitor your authentication statuses, you can enable the app authorization notification and Microsoft 365 service account and service account pool authentication notification.

- **Authentication Notification**
  To monitor your authentication statuses, you can enable the app authorization notification and Microsoft 365 service account & service account pool authentication notification.
- **Auto Discovery Notification**
  To monitor your Auto Discovery scan job, you can enable the email notification and “What’s new” report, which summarizes changes to your Auto Discovery.
- **License Notification**
  By default, the license notifications (including license extension, license expiration, and out-of-policy notifications) will be sent to the Tenant Owner and all Service Administrators in IBM Spectrum Protect Plus Online Services.
- **Announcement Notification**
  To ensure important announcements can be received when they are published, IBM Spectrum Protect Plus Online Services enabled the announcement notification.

Authentication Notification

To monitor your authentication statuses, you can enable the app authorization notification and Microsoft 365 service account & service account pool authentication notification.

- **Enable app authorization notification** – If you enable the notification, select the email notification recipients:
  - **Send an email notification to Service Administrators** – Select the checkbox and an email notification will be sent to Service Administrators if any app profile is in the status of **App Authorization Expired**.
  - **Send an email notification to the following recipients** – If you select the checkbox, select an email recipient list from the drop-down list. The recipients in the list will receive an email notification if any app profile is in the status of **App Authorization Expired**. If there is no email recipient list, click New Email Recipient List to create one. For more instructions on configuring email recipient lists, refer to Email Settings.
- **Enable Microsoft 365 service account & service account pool authentication notification** – If you enable the notification, select the email notification recipients:
  - **Send an email notification to Service Administrators** – Select the checkbox and an email notification will be sent to Service Administrators if any Microsoft 365 account being used in a service account profile or service account pool fails to connect to the Microsoft 365 tenant.
  - **Send an email notification to the following recipients** – If you select the checkbox, select an email recipient list from the drop-down list. The recipients in the list will receive an email notification if any Microsoft 365 account being used in a service account profile or service account pool fails to connect to the Microsoft 365 tenant. If there is no email recipient list, click New Email Recipient List to create one. For more instructions on configuring email recipient lists, refer to Email Settings.

The failed connection occurs when the configured account is deleted from Microsoft 365, or when the account’s password is changed. The email notification will be sent every day if the connection continues to fail.
Note: Once you configure the email notification for the Microsoft 365 service account and service account pool here, the notification settings you configured in **Service Account**/**Service Account Pool** will be invalid.
Click Save to save your configurations.

Auto Discovery Notification

To monitor your Auto Discovery scan job, you can enable the email notification and “What’s new” report, which summarizes changes to your Auto Discovery.

- **Enable email notification** – Select this checkbox to enable sending job email notifications, and then complete the following settings:
  1. **Send an email if any scan job completes with the following status** – Select the checkbox of your desired status.
  2. **Select an Email Recipient List** – Select an email recipient list from the drop-down list. The recipients in the list will receive the job notifications. If there is no email recipient list, click New Email Recipient List to create one. For more information on the email recipient list, refer to Email Settings.
- **Enable "What's New" digest that summarizes changes to your Auto Discovery** – Select this checkbox, and IBM Spectrum® Protect Plus Online Services will automatically send scheduled conclusion reports of Auto Discovery updates to recipients. Complete the following settings:
  - **Frequency** – Select Daily or Weekly as your desired frequency.
  - **Select an Email Recipient List** – Select an email recipient list from the drop-down list. The recipients in the list will receive the email notifications. If there is no email recipient list, click New Email Recipient List to create one. For more information on the email recipient list, refer to Email Settings.
  - **Skip notifications if there are no changes in Auto Discovery** – With this option selected, IBM Spectrum Protect Plus Online Services will not send notifications to the recipients when there are no changes in Auto Discovery.

Click Save to save your configurations.

License Notification

By default, the license notifications (including license extension, license expiration, and out-of-policy notifications) will be sent to the Tenant Owner and all Service Administrators in IBM Spectrum Protect Plus Online Services.

The Tenant Owner and Service Administrators can select the following recipients:

- **Tenant Owner in IBM Spectrum® Protect Plus Online Services**
- **All Service Administrators in IBM Spectrum Protect Plus Online Services**
- **Custom recipients (select an email profile)**
  If you select this option, select an email recipient list or click **New Email Recipient List** from the drop-down list to create one. For details about managing email recipient lists, refer to Email Settings.

Click Save to save your configurations.

Announcement Notification

To ensure important announcements can be received when they are published, IBM Spectrum Protect Plus Online Services enabled the announcement notification.

When IBM Spectrum Protect Plus Online Services publishes an announcement related to service interruption or additional required configurations, the Tenant Owner and all Service Administrators will receive a notification email.

You can select the announcement categories to decide what announcement notifications your tenant will receive, as well as select your desired email recipients:

- **Send email notifications when there are new announcements with the following categories:**
  - **Service interruption**
  - **Environment updates (product releases)**
  - **Additional configurations required**
  - **Informational (new features)**
- **Select email recipients:**
  - **Tenant Owner in IBM Spectrum® Protect Plus Online Services**
  - **All Service Administrators in IBM Spectrum Protect Plus Online Services**
  - **Custom recipients (select an email profile)**
    If you select the custom recipients option, select an email recipient list or click **New Email Recipient List** from the drop-down list to create one. For details about managing email recipient lists, refer to Email Settings.

  Click Save to save your configurations.

Email Settings

Refer to the instructions below to configure email related settings such as email recipient list, email date format, and email language:

- **Email Recipient List** – You can configure email recipient lists to customize recipients who will receive the email notifications. Then, in other settings providing email notifications, you can select a recipient list to receive the specific notifications.

You can perform the following actions to manage email recipient lists:

- **Create** – Click Create on the ribbon to create an email recipient list. On the **Create an Email Recipient List** page, configure the following fields:
  - **List Name** – Enter a list name.
  - **Description** – Enter an optional description if necessary.
  - **Email Addresses** – Enter email addresses of recipients, and separate each email address with a semicolon (**;**).

Click Save to save the configuration.

- **Edit** – Select an email recipient list, and click Edit on the ribbon to edit its settings. Click Save to save the configuration.
- **Delete** – Select one or multiple email recipient lists, and click Delete on the ribbon. Click OK to confirm your deletion.
- **Date Format** – You can select a date format for the date displayed in the notification emails.

- **Email Language** – By default, the display language of notification email content is set according to the country or region you've selected while signing up for IBM Spectrum Protect Plus Online Services. You can select a language preference from English, German, and French.

The following table lists the default email language mappings.

Language	Country/Region
French	Benin
	Burundi
	Canada
	Central African Republic
	Chad
	Comoros
	Democratic Republic of the Congo
	Djibouti
	Equatorial Guinea
	France
	French Guiana
	French Polynesia
	Gabon
	Guernsey
	Guinea
	Haiti
	Ivory Coast
	Madagascar
	Mali
	Mauritania
	Monaco
	Niger
	Republic of the Congo
	Senegal
	Togo
German	Austria
	Germany

Note: For the countries or regions that are not listed in the table, the email language has been mapped to English.

Enable Integration with SCOM

You can integrate IBM Spectrum Protect Plus Online Services and System Center Operations Manager (SCOM).

Procedure

With the integration enabled, you can monitor IBM Spectrum Protect Plus Online Services, IBM Spectrum Protect Plus Online Services for Microsoft 365, and activities in System Center Operations Manager.

Note: The integration supports System Center Operations Manager 2012 R2 and System Center Operations Manager 2016.
Complete the following steps to enable the integration:

1. Navigate to Advanced Settings > Integration with SCOM on the left pane.
2. Select the Enable integration with System Center Operations Manager checkbox.
3. Configure the following settings:
   - **SCOM Server** – Enter the IP address of the server where the System Center Operations Manager is installed.
   - **Domain** – Enter the name of the domain where the SCOM server resides.
   - **Username** – Enter the username of an account that has the Operations Manager Administrators user role in SCOM.
   - **Password** – Enter the password of the account above.
4. Click Validation Test to validate the information above.
5. Click Save to save your configurations, or click Cancel to go back to the homepage without saving any configurations.

Enable Trusted IP Address Settings

You can enable trusted IP address settings to only allow users to access IBM Spectrum Protect Plus Online Services from certain IP addresses or IP address ranges.Only IPv4 addresses are supported.

Procedure

Complete the following steps to enable trusted IP address settings:

1. Navigate to Advanced Settings > Trusted IP Address Settings on the left pane.
2. Select the Enable trusted IP address settings checkbox.
    - If you want to set specific IP addresses as trusted, enter the IP address in the Trusted IP Address text box. You can enter multiple IP addresses by separating them with commas (,).
    - If you want to set the IP address range as trusted, click New IP Address Range in the Trusted IP Address Range field. Then, enter the IP address range and click the save button. You can set multiple IP address ranges.
3. Click Save to save your configurations, or click Cancel to go back to the homepage without saving any configurations.

Configure the Security Policy

On the Security Policy page, you can enable the password policy and temporary support account.

Password Policy

Enable the password policy for IBM Spectrum® Protect Plus Online Services local users. Local users will be asked to change their account passwords regularly for the security of their accounts.
Note: Microsoft 365 users follow the related systems' password policies.
Complete the following steps to enable the password policy:

- Navigate to Advanced Settings > Password Policy on the left pane.
- Select the Enable password rotation for local accounts checkbox.
- Select 30, 60, 90, or 180 days as the lifespan of the passwords.
- Click Save to save your configurations or click Cancel to go back to the homepage without saving any configurations.

Once you enable the password policy, email notifications will be sent to local users 15 days before their password expiration dates. Users can click the link in the emails to change their passwords. The link will expire in 15 days. If users do not change their passwords before the password expiration date, they can still sign in using their previous passwords. However, they must set new passwords before they can perform any actions in IBM Spectrum Protect Plus Online Services.

Temporary Support Account

By default, the Allow temporary account creation for IBM Software Support option is enabled. When the Tenant Owner, Service Administrators, or Application Administrators invite support for assistance, the IBM Software Support team members can use the accounts to access the IBM Spectrum Protect Plus Online Services environments to help resolve the issues. You may need to disable temporary support accounts due to your organization's security policy.
Note: If you disable the option, temporary support accounts can no longer be created. If your tenant has any active support accounts, they will be deactivated immediately and you can navigate to User Management to delete them. When you need the IBM Software Support team to access your IBM Spectrum Protect Plus Online Services or other IBM Spectrum Protect Plus Online Services environments to help resolve issues, you must contact IBM Software Support to enable the option again.

Configure Session Settings

IBM Spectrum® Protect Plus Online Services has the following default session settings:

- An account will be automatically signed out if there is no activity for 15 minutes. The user can sign in again to start a new session.
- An account can be used to sign into IBM Spectrum Protect Plus Online Services in multiple locations at the same time.

If you have the following requirements, you can configure the session settings:

- You want to extend the session timeout duration to be longer than 15 minutes.
- Your organization does not allow concurrent sign-ins at multiple locations for the same account. For example, Bob has used an account to sign into IBM Spectrum Protect Plus Online Services and John uses the same account to sign in at a different location. Upon John's sign-in, Bob will be automatically signed out.

Complete the following steps to configure the session settings:

1. Navigate to Advanced Settings > Session Settings on the left pane.
2. Configure the following settings based on your scenario:
    - If you want to extend the session timeout duration, select the Session Timeout Setting tab and complete the followings:
        - Select the Configure session timeout setting checkbox.
        - Enter a number in the text boxes before hours and/or minutes.
          Note: The duration cannot be less than 15 minutes.
    - If your organization does not allow concurrent sign-ins, select the Concurrent Sign-in Setting tab and deselect the Allow concurrent sign-ins from multiple locations for the same account checkbox. Click Save to save your configurations or click Cancel to go back to the homepage without saving any configurations.

Download a List of Reserved IP Addresses

If your tenant has the enterprise license for any service offered by IBM Spectrum® Protect Plus Online Services the Tenant Owner and Service Administrators can download a list of reserved IP addresses.

About this task

The reserved IP addresses can be added to your Microsoft 365 firewall to ensure IBM Spectrum Protect Plus Online Services and IBM Spectrum Protect Plus Online Services for Microsoft 365 can operate on your environment. IBM Spectrum Protect Plus Online Services is the entry for all IBM Spectrum Protect Plus Online Services. Apart from adding the IP addresses of the IBM Spectrum Protect Plus Online Services you want to use, make sure the IP addresses of IBM Spectrum Protect Plus Online Services are also added to the allow list in your environment.

Procedure

Complete the following steps to download a list of reserved IP addresses:

1. Navigate to Advanced Settings > Firewalls and Virtual Networks on the left pane.
2. Select the Reserved IP Addresses tab.
3. Click Download a List of Reserved IP Addresses.
4. Select a location to save the file.
   Note: The downloaded file contains IP addresses of all data centers. When your organization's users need to access IBM Spectrum Protect Plus Online Services from other data centers, you can now add the corresponding IP addresses to the trusted list in your environment.
   For details on adding reserved IP addresses, refer to Add Reserved IP Addresses.

   Note: If your organization enabled the Continuous Access Evaluation (CAE) feature in Azure Active Directory > Conditional Access policies, the reserved IP addresses must be excluded from the Conditional Access policies based on CAE. Otherwise, the usage of Microsoft 365 service accounts or app profiles will be affected. For more information about the CAE feature, refer to in the Microsoft article.

Export the User Activity Report

The Tenant Owner and Service Administrators can export reports of their tenant's user activities in IBM Spectrum® Protect Plus Online Services By default, the user activity logs will be retained for three years.

Procedure

If you want to change the retention time of user activity audit logs or export user activity reports, refer to the following steps:

1. Click User Activity Report on the left pane.
2. Specify the options that meet your business requirements:

   Retention Setting
   Complete the steps below to change the retention time of the activity logs:
   - In the Retain user activity logs for field, select Years or Months from the drop-down list, and then enter a number in the nearby text box.
   - Click Save to save your changes.

   Export Report
   Complete the steps below to export user activity reports:
   - Click the calendar button and respectively select the Start Time and End Time.
   - Click Export and select a location to save the User_Activity_Report (.xlsx). The report contains information about user activities within the selected time range. The information includes the summary of actions, the login ID of the users who performed the actions, the operation time, etc.

- **User Activity Report Information**

User Activity Report Information

The table below lists the information that can be recorded in the **User Activity Report**.

Section	Information
Common	Sign In/Out
	Session Timeout
	Hide/Show Expired Services from the All Apps View
	Accept License Agreement
	Start Trial for IBM Spectrum® Protect Plus Online Services for Microsoft 365
	Download License Report
	Access IBM Spectrum Protect Plus Online Services for Microsoft 365
	Submit Invite Support Request
	Reset Password

Section	Information
App Management	Create/Updated/Delete/Re-authorize/Edit App Profile
Service Account	SharePoint Online Admin Center URL
Service Account Pool	Create/Edit/Delete Service Account Profile
	Validate Administrator Account for Service Account Profile
	Save Service Account Pool
	Validate Group for Service Account Pool
	Validate User Account for Service Account Pool
User Management	Add/Edit/Delete/Activate/Deactivate/Unlock User
Encryption Management	Create/Edit/Delete/Apply Encryption Profile
	Validate Key Vault Information for Encryption Profile
Auto Discovery	Create/Edit/Delete Container
	Change Container Name
	Remove Container from Scan Profile
	Add/Edit/Delete Scan Rule
	Remove Objects from Container
	Download the "What's New" Weekly Report for Auto Discovery
	Download the "What's New" Daily Report for Auto Discovery
	Save/Edit/Delete Scan Profile
	Save Scan Profile and Run Scan Job
	Stop Scan Job
	Export Scan History
	Batch Import
	Save Data Center Mappings
Report Data Collection	Enable/Disable Report Data Collection
User Activity Report	Configure Retention Setting for User Activity Report
	Export User Activity Report
Advanced Settings	Create/Edit/Delete Email Recipient List
	Configure Date Format in Notification & Email Settings
	Configure Email Language
	Saved Email Notification Settings
	Enable/Disable Integration with SCOM
	Enable/Disable Trusted IP Address Settings
	Enable/Disable Password Policy
	Create/Delete/Disable Temporary Support Account
	Enable/Disable Session Timeout Setting
	Allow/Block Concurrent Sign-ins from Multiple Locations for the Same Account
	Download the List of Reserved IP Addresses

View Announcements

In Announcement Center on the left pane, you can view current and previous announcements.

Current Announcements

To view current announcements, click Current Announcements. The Current Announcements page appears with all the current announcements. You can click Subscribe to These Announcements by Email to configure announcement notifications via email. For more instructions, refer to the Announcement Notification in the Notification Settings section.

Announcement History

To view previous announcements, click Announcement History. The Announcement History page appears, and you can view all services' previous announcements here.

Submit Feedback

IBM Spectrum® Protect Plus Online Services provides a platform to collect feedback where you can provide suggestions for service features from your IBM Spectrum Protect Plus Online Services experience.

Procedure

Complete the following steps to submit feedback:

1. Click the submit feedback button in the upper-right corner.
2. On the Submit Feedback page, configure the following settings:

   Rate Your IBM Spectrum Protect Plus Online Services Experience
   : Click the stars to evaluate your IBM Spectrum Protect Plus Online Services experience.

   Your Suggestion
   : Enter your suggestions about IBM Spectrum Protect Plus Online Services features.

3. Click Submit to submit your feedback, or click Cancel to return to the IBM Spectrum Protect Plus Online Services homepage without submitting your feedback.

Appendices

The following table details the appendices included in this document:

Appendix	Description
Appendix A - Supported Criteria in Auto Discovery Rules	Lists the criteria that are supported in Auto Discovery advanced mode rules.
Appendix B - Objects Supported by Batch Import	Lists the objects that can be and cannot be registered via Batch Import.
Appendix C - Create a Key Vault in Azure	Details how to create an Azure Key Vault.
Appendix D - Password Limitations and Requirements of Microsoft 365 Accounts	Details the password limitations and requirements of Microsoft 365 accounts.
Appendix E - When Service Account and App Profile are Used	Details when Service Account, Microsoft 365 MFA Service Account, and App Profile for Microsoft 365 are used.
Appendix F - Helpful Notes When Auto Discovery Scan Results Return Error Codes	Details solutions for some scan error messages in Auto Discovery.
Appendix G - Events Monitored by SCOM	Lists the IBM Spectrum Protect Plus Online Services events that can be monitored by System Center Operations Manager.
Appendix H - Prepare a Certificate for the Custom Azure App	Details how to prepare a certificate for the custom Azure app.
Appendix I - IBM Spectrum Plus Online Services App Registrations	Details how to register, update, and delete IBM Spectrum Protect Plus Online Services apps that can be used to leverage resources of IBM Spectrum Protect Plus Online Services for Microsoft 365.

- **Appendix A - Supported Criteria in Auto Discovery Rules**
- **Appendix B - Objects Supported by Batch Import**
  The table below lists the objects that can be and cannot be registered via Batch Import.
- **Appendix C - Create a Key Vault in Azure**
  You can create a key vault in Azure.
- **Appendix D - Password Limitations and Requirements of Microsoft 365 Accounts**
  The table below details the password limitations and requirements of Microsoft 365 accounts. Note that the password limitations and requirements are from Microsoft 365.
- **Appendix E - When Service Account and App Profile are Used**
  The following table details when Service Account, Microsoft 365 MFA Service Account, App Profile for Microsoft 365 are used.
- **Appendix F - Helpful Notes When Auto Discovery Scan Results Return Error Codes**
  The table below lists Auto Discovery scan jobs' error messages and related error codes. You can click the error code links to view the helpful notes.
- **Appendix G - Events Monitored by SCOM**
  Refer to the table below for IBM Spectrum Protect Plus Online Services events that can be monitored by System Center Operations Manager.
- **Appendix H - Prepare a Certificate for the Custom Azure App**
  Before preparing a certificate, make sure you have a key vault in Azure.
- **Appendix I - IBM Spectrum Plus Online Services App Registrations**
  If you need to leverage the resources of IBM Spectrum Protect Plus Online Services Services, you can register an app in IBM Spectrum Protect Plus Online Servicess and grant permissions to the app.

Appendix A - Supported Criteria in Auto Discovery Rules

The table below lists the criteria that are supported in Auto Discovery advanced mode rules.
Note: For details of how to select conditions, refer to How Do I Select the Right Conditions?

Exchange Online Mailbox

Criteria	Condition
City	Contains
	Does Not Contain
	Equals
	Does Not Equal
	Matches
	Does Not Match
Company	Contains
	Does Not Contain
	Equals
	Does Not Equal
	Matches
	Does Not Match
Country or Region	Equals
	Does Not Equal
Custom Attribute	Contains
	Does Not Contain
	Equals
	Does Not Equal
	Matches
	Does Not Match
Department	Contains
	Does Not Contain
	Equals
	Does Not Equal
	Matches
	Does Not Match
Display Name	Contains
	Does Not Contain
	Equals
	Does Not Equal
	Matches
	Does Not Match
Email Address	Contains
	Does Not Contain
	Equals
	Does Not Equal
	Matches
	Does Not Match
Group Membership	Contains
	Does Not Contain
	Equals
	Does Not Equal
Job Title	Contains
	Does Not Contain
	Equals
	Does Not Equal
	Matches
	Does Not Match
Mailbox Type	Equals
	Does Not Equal
Office	Contains
	Does Not Contain

Criteria	Condition
	Equals
	Does Not Equal
	Matches
	Does Not Match
Microsoft 365 Subscription Name	Contains
	Does Not Contain
	Equals
	Does Not Equal
Geo Location*	Equals
	Does Not Equal
State or Province	Contains
	Does Not Contain
	Equals
	Does Not Equal
	Matches
	Does Not Match
User ID	Contains
	Does Not Contain
	Equals
	Does Not Equal
	Matches
	Does Not Match
ZIP/Postal Code	Contains
	Does Not Contain
	Equals
	Does Not Equal
	Matches
	Does Not Match
Sign-in Status	Equals

Note the following:

- **Mailbox Type** – This criterion only takes effect when a service account profile is selected as the authentication method in the scan profile. After selecting Custom Attribute, select an attribute number, which is retrieved from Exchange Online.
- **Geo Location** – This criterion corresponds to the **Preferred Data Location** property in a multi-geo Microsoft 365 tenant, and the criterion is only available when your tenant has the Multi-Geo Capabilities in IBM Spectrum® Protect Plus Online Services for Microsoft 365.
- **Group Membership** – This criterion allows you to scan mailboxes of users in a specific group.
  - If users are in a security group, enter the group name.
  - If users are in a Microsoft 365 group, distribution group, shared mailbox, or mail-enabled security group, enter the group ID before domain '@'.
  - If the group you entered has nested groups, IBM Spectrum Protect Plus Online Services will scan mailboxes for users in the first five layers of groups.

OneDrive for Business

Criteria		Condition
Site Collection Property	Created Time	Before
		After
		On
		Within
		Older Than
	Custom Property: Date and Time	Before
		After
		On
		Within
		Older Than
	Custom Property: Number	>=
		<=
		=
	Custom Property: Text	Contains
		Does Not Contain
		Equals
		Does Not Equal
		Matches
		Does Not Match
	Custom Property: Yes/No	Equals
		Does Not Equal

	Criteria	Condition
	Primary Administrator	Contains
		Equals
	Size	>=
		<=
	URL	Contains
		Does Not Contain
		Equals
		Does Not Equal
		Matches
		Does Not Match
Basic User Information	City	Contains
		Does Not Contain
		Equals
		Does Not Equal
		Matches
		Does Not Match
	Company	Contains
		Does Not Contain
		Equals
		Does Not Equal
		Matches
		Does Not Match
	Country or Region	Contains
		Does Not Contain
		Equals
		Does Not Equal
		Matches
		Does Not Match
	Custom Attribute	Contains
		Does Not Contain
		Equals
		Does Not Equal
		Does Not Match
	Department	Contains
		Does Not Contain
		Equals
		Does Not Equal
		Matches
		Does Not Match
	Group Membership	Contains
		Does Not Contain
		Equals
		Does Not Equal
	Job Title	Contains
		Does Not Contain
		Equals
		Does Not Equal
		Matches
		Does Not Match
	Office	Contains
		Does Not Contain
		Equals
		Does Not Equal
		Matches
		Does Not Match
	Sign-in Status	Equals
		Does Not Equal
	Microsoft 365 Subscription Name	Contains
		Does Not Contain
		Equals
		Does Not Equal
	Geo Location*	Equals
		Does Not Equal
	Username	Contains

	Criteria	Condition
		Does Not Contain
		Equals
		Does Not Equal
		Matches
		Does Not Match
	Usage Location	Equals
		Does Not Equal
User Profile Property	Boolean	Equals
		Does Not Equal
User Profile Property	Date	Before
		After
		On
		Within
		Older Than
	Date Time	Before
		After
		On
		Within
		Older Than
	Email	Contains
		Does Not Contain
		Equals
		Does Not Equal
		Matches
		Does Not Match
	Person	Contains
		Does Not Contain
		Equals
		Does Not Equal
		Matches
		Does Not Match
	String (Single Value)	Contains
		Does Not Contain
		Equals
		Does Not Equal
		Matches
		Does Not Match
	URL	Contains
		Does Not Contain
		Equals
		Does Not Equal
		Matches
		Does Not Match

Note: Geo Location – This criterion corresponds to the Preferred Data Location property in a multi-geo Microsoft 365 tenant, and the criterion is only available when your tenant has the Multi-Geo Capabilities in IBM Spectrum® Protect Plus Online Services for Microsoft 365.

SharePoint Online Site Collection

Criteria	Condition
Created Time	Before
	After
	On
	Within
	Older Than
Creator	Contains
	Does Not Contain
	Equals
	Does Not Equal
	Matches
	Does Not Match
Custom Property: Date and Time	Before
	After
	On

Criteria	Condition
	Within
	Older Than
Custom Property: Number	>=
	<=
	=
Custom Property: Text	Contains
	Does Not Contain
	Equals
	Does Not Equal
	Matches
	Does Not Match
Custom Property: Yes/No	Equals
	Does Not Equal
External Sharing: Anyone New and Existing Guests	Equals
Existing Guests Only Only People in Your Organization	Does Not Equal
Primary Administrator	Contains
	Equals
Sensitivity Label	Contains
	Does Not Contain
	Equals
	Does Not Equal
	Matches
	Does Not Match
Site Classification	Contains
	Does Not Contain
	Equals
	Does Not Equal
	Matches
	Does Not Match
Geo Location*	Equals
	Does Not Equal
Size	>=
	<=
Template Name*	Contains
	Does Not Contain
	Equals
	Does Not Equal
	Matches
	Does Not Match
Template Title*	Contains
	Equals
Title	Contains
	Does Not Contain
	Equals
	Does Not Equal
	Matches
	Does Not Match
URL	Contains
	Does Not Contain
	Equals
	Does Not Equal
	Matches
	Does Not Match

Note the following:

- An example for Template Name: STS#0
- An example for Template Title: Team Site
- **Geo Location** – This criterion corresponds to the Preferred Data Location property in a multi-geo Microsoft 365 tenant, and the criterion is only available when your tenant has the Multi-Geo Capabilities in IBM Spectrum® Protect Plus Online Services for Microsoft 365.

Microsoft 365 Groups/Microsoft Teams/Yammer Communities

Criteria		Condition
Group/Team/Yammer Community Property	Type	Equals
		Does Not Equal
	Display Name	Contains
		Does Not Contain
		Equals
		Does Not Equal
		Matches
		Does Not Match
	Creator: Department Azure AD Attribute Usage Location	Contains
		Does Not Contain
		Equals
		Does Not Equal
		Matches
		Does Not Match
	Custom Property: Number*	>=
		<=
		=
	Custom Property: Text*	Contains
		Does Not Contain
		Equals
		Does Not Equal
		Matches
		Does Not Match
	Classification	Contains
		Does Not Contain
		Equals
		Does Not Equal
		Matches
		Does Not Match
	Primary Email Address	Contains
		Does Not Contain
		Equals
		Does Not Equal
		Matches
		Does Not Match
	Owner	Contains
		Does Not Contain
		Equals
		Does Not Equal
		Matches
		Does Not Match
		Is Not Empty
		Is a Member of the Group*
		Domain is
	Member	Contains
		Does Not Contain
		Is Not Empty
	Privacy	Equals
		Does Not Equal
	Geo Location*	Equals
		Does Not Equal
Group Team Site Property	Created Time	Before
		After
		On
		Within
		Older Than
	Custom Property: Date and Time	Before
		After
		On
		Within
		Older Than

Criteria		Condition
	Custom Property: Number	>=
		<=
		=
	Custom Property: Text	Contains
		Does Not Contain
		Equals
		Does Not Equal
		Matches
		Does Not Match
	Custom Property: Yes/No	Equals
		Does Not Equal
	External Sharing: Anyone New and Existing Guests Existing Guests Only Only People in Your Organization	Equals
		Does Not Equal
	Sensitivity Label	Contains
		Does Not Contain
		Equals
		Does Not Equal
		Matches
		Does Not Match
	Size	>=
		<=
	Title	Contains
		Does Not Contain
		Equals
		Does Not Equal
		Matches
		Does Not Match
	URL	Contains
		Does Not Contain
		Equals
		Does Not Equal
		Matches
		Does Not Match

Note the following:

- **Owner**
  - **Equals** - If you use this condition to scan a Microsoft 365 Group which has more than one owner, you can add each owner's user ID using the **Equals** condition and apply the **Or** logic option to these **Equals** conditions.
  - **Equals/Does Not Equal/Contains/Does Not Contain/Matches/Does Not Match** – If you use any of these conditions to scan Microsoft 365 Groups, enter the full user ID before domain '@'.
  - **Is a Member of the Group** – This condition allows you to scan all Microsoft 365 Groups whose owner or at least one of their owners is a member of a group in Microsoft 365.
    - If the owner is in a security group, enter the group name.
    - If the owner is in a Microsoft 365 Group, distribution group, shared mailbox, or mail-enabled security group, enter the group ID before domain '@'.
    - If the group you entered has nested groups, IBM Spectrum® Protect Plus Online Services will search members from the first five layers.
  - **Member** - If you use the Contains or Does Not Contain condition to scan Microsoft 365 Groups, enter the full user ID before domain '@'.
  - **Geo Location** – This criterion corresponds to the **Preferred Data Location** property in a multi-geo Microsoft 365 tenant, and the criterion is only available when your tenant has the Multi-Geo Capabilities in IBM Spectrum Protect Plus Online Services for Microsoft 365.
  - **Custom Property: Number** and **Custom Property: Text** – For more information about extended properties, refer to Add custom data to groups using schema extensions.

Project Online Site Collection

Criteria	Condition
Created Time	Before
	After
	On
	Within
	Older Than
Custom Property: Date and Time	Before

Criteria	Condition
	After
	On
	Within
	Older Than
Custom Property: Number	>=
	<=
	=
Custom Property: Text	Contains
	Does Not Contain
	Equals
	Does Not Equal
	Matches
	Does Not Match
Custom Property: Yes/No	Equals
	Does Not Equal
Primary Administrator	Contains
	Equals
Sensitivity Label	Contains
	Does Not Contain
	Equals
	Does Not Equal
	Matches
	Does Not Match
Geo Location*	Equals
	Does Not Equal
Size	>=
	<=
Template Name	Contains
	Does Not Contain
	Equals
	Does Not Equal
	Matches
	Does Not Match
Template Title	Contains
	Equals
Title	Contains
	Does Not Contain
	Equals
	Does Not Equal
	Matches
	Does Not Match
URL	Contains
	Does Not Contain
	Equals
	Does Not Equal
	Matches
	Does Not Match

Note:
The Geo Location criterion corresponds to the Preferred Data Location property in a multi-geo Microsoft 365 tenant, and this criterion is only available when your tenant has the Multi-Geo Capabilities in IBM Spectrum® Protect Plus Online Services for Microsoft 365.

Exchange Online Public Folder

Criteria	Condition
Display Name	Contains
	Does Not Contain
	Equals
	Does Not Equal
	Matches
	Does Not Match
Path	Is Under
	Is Not Under

Microsoft 365 Users

Criteria	Condition
City	Contains
	Does Not Contain
	Equals
	Does Not Equal
	Matches
	Does Not Match
Company	Contains
	Does Not Contain
	Equals
	Does Not Equal
	Matches
	Does Not Match
Country or Region	Equals
	Does Not Equal
Department	Contains
	Does Not Contain
	Equals
	Does Not Equal
	Matches
	Does Not Match
Display Name	Contains
	Does Not Contain
	Equals
	Does Not Equal
	Matches
	Does Not Match
Domain	Equals
	Does Not Equal
Email Address	Contains
	Does Not Contain
	Equals
	Does Not Equal
	Matches
	Does Not Match
Group Membership	Contains
	Does Not Contain
	Equals
	Does Not Equal
Job Title	Contains
	Does Not Contain
	Equals
	Does Not Equal
	Matches
	Does Not Match
Microsoft 365 Subscription Name	Contains
	Does Not Contain
	Equals
	Does Not Equal
Office	Contains
	Does Not Contain
	Equals
	Does Not Equal
	Matches
	Does Not Match
Primary Email Domain	Equals
	Does Not Equal
Sign-in Status	Equals
	Does Not Equal
State or Province	Contains
	Does Not Contain
	Equals

Criteria	Condition
	Does Not Equal
	Matches
	Does Not Match
User ID	Contains
	Does Not Contain
	Equals
	Does Not Equal
	Matches
	Does Not Match
ZIP/Postal Code	Contains
	Does Not Contain
	Equals
	Does Not Equal
	Matches
	Does Not Match

Security and Distribution Group

Criteria	Condition
Group Type: Security Group Mail-enabled Security Group	Equals
  Distribution List Dynamic Distribution List	Does Not Equal
Display Name	Contains
	Does Not Contain
	Equals
	Does Not Equal
	Matches
	Does Not Match
Owner	Contains
	Does Not Contain
	Equals
	Does Not Equal
	Matches
	Does Not Match
Member	Contains
	Does Not Contain
	Is Not Empty
Primary Email Address	Contains
	Does Not Contain
	Equals
	Does Not Equal
	Matches
	Does Not Match
Created Time	Before
	After
	On
	Within
	Older Than
Custom Attribute	Contains
	Does Not Contain
	Equals
	Does Not Equal
	Matches
	Does Not Match
Custom Property: Number	>=
	<=
	=
Custom Property: Text	Contains
	Does Not Contain

Criteria	Condition
	Equals
	Does Not Equal
	Matches
	Does Not Match

Note:

- **Owner**
  - **Equals** – If you use this condition to scan a group which has more than one owner, you can add each owner's user ID using the **Equals** condition and apply the **Or** logic option to these **Equals** conditions.
  - **Equals/Does Not Equal/Contains/Does Not Contain/Matches/Does Not Match** – If you use any of these conditions to scan groups, enter the full user ID before domain '@'.
  - **Is a Member of the Group** – This condition allows you to scan all groups whose owner or at least one of their owners is a member of a group in Microsoft 365.
    - If the owner is in a security group, enter the group name.
    - If the owner is in a distribution group or mail-enabled security group, enter the group ID before domain '@'.
    - If the group you entered has nested groups, IBM Spectrum® Protect Plus Online Services will search members from the first five layers.
- **Member** – If you use the **Contains** or **Does Not Contain** condition to scan groups, enter the full user ID before domain '@'.
- **Custom Property: Number and Custom Property: Text** – For more information about extended properties, refer to Add custom data to groups using schema extensions.

Shared Drive

Criteria	Condition
Created Date	After
	Before
	Older Than
Member	Contains
	Does Not Contain
Name	Contains
	Does Not Contain
	Equals
	Does Not Equal
	Matches
	Does Not Match

Appendix B - Objects Supported by Batch Import

The table below lists the objects that can be and cannot be registered via Batch Import.

Retrieve Credentials from		SharePoint Online Site Collection	Exchange Online Mailbox	OneDrive for Business	Microsoft 365 Groups/Microsoft Teams/Yammer Communities	Project Online Site Collection	Exchange Online Public Folder	Microsoft 365 User
Microsoft 365 Service Account Profile	Global Administrator	Supported	Supported	Supported	Supported	Supported	Unsupported	Supported
	SharePoint Administrator	Supported	Unsupported	Supported	Unsupported	Supported	Unsupported	Unsupported
	Exchange Administrator	Un-supported	Supported	Supported	Supported	Unsupported	Unsupported	Unsupported
App Profile (for Microsoft 365)	All Permissions	Supported	Supported	Unsupported	Supported	Supported	Unsupported	Supported
	SharePoint Online Permissions	Supported	Supported	Unsupported	Supported	Supported	Unsupported	Unsupported
	Exchange Online Permissions	Unsupported	Supported	Unsupported	Supported	Unsupported	Unsupported	Unsupported

Appendix C - Create a Key Vault in Azure

You can create a key vault in Azure.

Procedure

Make sure you have an Azure subscription that contains Azure Key Vault. Then follow the instructions below:

1. Create an application. This application is only used for Azure Key Vault. IBM Spectrum® Protect Plus Online Servicesencryption profile will access the key vault via the application.
    a. In the Azure Portal, navigate to Azure Active Directory > App registrations.
    b. Click New registration on the ribbon.
    c. On the Register an application page, configure the application settings.
    d. Click Register to create your application.
    e. After the application is created successfully, copy the application ID. The application ID is the client ID that will be used in the encryption profile.
2. Add a client secret for the application. The client secret will be used in the IBM Spectrum Protect Plus Online Services encryption profile.
    a. After creating the application, click Certificates & secrets in the left menu.
    b. In the Client secrets field, click New client secret.
    c. In the Add a client secret pane, enter a description for the client secret and select a duration.
    d. Click Add. The value of the client secret is automatically generated and displayed.
    e. Copy the client secret value. You will need to provide the value when configuring the encryption profile.

    Note: The value will be hidden after you leave or refresh the page.
3. Create a key vault.
    a. In Azure Portal, enter Key vaults in the search box on the top, and then select the first result to access the Key vaults page.
    b. Click Add. The Create key vault page appears.
    c. In the Basics tab, provide the basic information for the key vault, and then click the Access policy tab.
    d. Click Add Access Policy.
    e. On the Add access policy page, select the following Key permissions from the drop-down list.
        - In the Key Management Operations field, select Get.
        - In the Cryptographic Operations field, select Decrypt and Encrypt.
    f. Click the select button in the Select principal field.
    g. In the Principal pane, enter the application name or application ID in the search box.
    h. Select the application and click Select at the bottom.
    i. Click Add to add the access policy.
    j. Click the Networking tab.
    k. Select Public endpoint (all networks) which allows all networks to connect to this key vault.
    Note: If you only allow the IBM Spectrum Protect Plus Online Services and the IBM Spectrum Protect Plus Online Services for Microsoft 365 that you are using to connect to this key vault, you can edit the key vault's firewall settings after the key vault provisioning.
    l. Click the Tags tab and you can add tags to categorize your key vault.
    m. Click Review + create to review all of your configurations first, and then click Create at the bottom to create the key vault.
    Note: If you need to change some settings before creating the key vault, you can click the Previous button to change previous settings.
4. Create a key.
    a. On the Key vaults page, click the newly created key vault.
    b. Click Keys in Settings. In the Keys pane, click Generate/Import on the ribbon and create a key.
    c. In the Keys pane, click the key name, and then click the current version. The key properties are displayed.
    d. Copy the key identifier. You will need to provide the key identifier when configuring the encryption profile.
5. If you only allow the IBM Spectrum Protect Plus Online Services and the IBM Spectrum Protect Plus Online Services for Microsoft 365 that you are using to connect to the key vault, complete the following steps to edit the key vault's firewall:
    a. On the Key vaults page, click the name of the key vault you created, and then click Networking in Settings.
    b. In the Firewalls and virtual networks tab, select Private endpoint and selected networks.
    c. In the Firewall field, enter the IP addresses of the IBM Spectrum Protect Plus Online Services and the IBM Spectrum Protect Plus Online Services for Microsoft 365 you are using in the text boxes.
    Note: To get the IP addresses, sign in to IBM Spectrum Protect Plus Online Services and navigate to Advanced Settings > Reserved IP Address.
    d. Click Save to save your configurations.

Appendix D - Password Limitations and Requirements of Microsoft 365 Accounts

The table below details the password limitations and requirements of Microsoft 365 accounts. Note that the password limitations and requirements are from Microsoft 365.

Property	Requirements
Characters Allowed	• A-Z • a-z • 0-9 • @ # $ % ^ & * - _ ! + = [] {} | \ : ' , . ? / ` ~ " () ;
Characters Not Allowed	• Unicode characters • Spaces • Strong passwords only: Cannot contain a dot character (.) immediately preceding the @ symbol.

Password Restrictions	• Eight (8) characters is the minimum and sixteen (16) characters is the maximum
	• **Strong passwords only**: Three of the following are required:
	  ◦ Lowercase characters
	  ◦ Uppercase characters
	  ◦ Numbers (0-9)
	  ◦ Symbols (see the symbols listed in **Characters Allowed** above)

Password Expiry	By default, password expiry is enabled. If you want to disable it, navigate to Microsoft 365 > Admin center > Settings > Security & privacy > Password policy, click Edit, and then click the Off button.

Property	Requirements
Password Expiry Duration	By default, a password will expire in **90** days. If you want to change the duration, navigate to Microsoft 365 > Admin center > Settings > Security & privacy > Password policy, click Edit, and then modify the number in the Days before passwords expire field.
Password Expiry Notification	By default, a password expiry notification will be sent to users **14** days before the password expires. If you want to change the notification time, navigate to Microsoft 365 > Admin center > Settings > Security & privacy > Password policy, click Edit, and then modify the number in the Days before a user is notified about expiration field.

Appendix E - When Service Account and App Profile are Used

The following table details when Service Account, Microsoft 365 MFA Service Account, App Profile for Microsoft 365 are used.

Service	App Profile	Service Account	App Profile + MFA Service Account	App Profile Type
Microsoft 365 General Services: Licensing, Manage Users, Retrieve Microsoft 365 Tenant	Supported (and preferred)	Supported	Supported Note: MFA Service Account does not support these services.	Microsoft 365
SharePoint Management	Supported with limitations	Supported	Supported	Microsoft 365
OneDrive for Business Management	Supported with limitations	Supported	Supported	Microsoft 365
Exchange Management	Supported (and preferred)	Supported	Supported	Microsoft 365
Project Management	Unsupported	Supported	Supported	Microsoft 365
Microsoft 365 Groups Management	Supported with limitations	Supported	Supported	Microsoft 365
Microsoft Teams Management	Supported	Supported	Supported	Microsoft 365 Note: Microsoft delegated app profile is required in the following scenario:IBM Spectrum® Protect Plus Online Services for Microsoft 365 uses it to restore Microsoft Teams channel conversations as posts and protect Planner data.
Microsoft Planner Management	Supported	Supported	Supported	Microsoft Delegated App

Note: Service account profile and app profile can both be used to scan objects in Auto Discovery, but the methods and required permissions vary with object types and the IBM Spectrum Protect Plus Online Services for Microsoft 365 your tenant is using. For details, refer to Required Permissions.
Note: Refer to Will the App Profile Method Meet Your Data Management Requirements? to help you determine if using the app profile method will satisfy your data management requirements.

Appendix F - Helpful Notes When Auto Discovery Scan Results Return Error Codes

The table below lists Auto Discovery scan jobs' error messages and related error codes. You can click the error code links to view the helpful notes.

Error Message	Error Code
SharePoint Online has throttled requests from this scan job.	cs0000001
The SharePoint Online environment is temporarily unavailable.	cs0000002
The number of simultaneous PowerShell Sessions a user can open to Exchange Online has reached its limit.	cs0000003
The Group team sites of some Microsoft 365 Groups and Microsoft Teams cannot be retrieved.	cs0000004
The service account has multi-factor authentication enabled, but MFA has not been configured in the service account profile.	cs0000005

cs0000001

SharePoint Online has a throttling policy that prevents too many simultaneous requests (SharePoint Online returns HTTP status code 429). To avoid getting throttled in SharePoint Online, choose the following solutions based on your scenario:

- Use the app profile authentication method to rerun the scan job. For more information about app profile, refer to What is the Difference Between Service Account Profile and App Profile?
- When the app profile authentication method cannot meet your data management requirements and you still want to use the service account method, try the following solutions and rerun the scan job:
  - Configure a Microsoft 365 service account pool and add enough users to the account pool. Note that the scan profile's service account cannot be added to the account pool. For more details, refer to Manage Microsoft 365 Account Pool and How Many Accounts Should be Added into an Account Pool?
  - Check the scan profile's **Update Schedule** setting, ensuring that scan jobs will not run when there are other services sending a lot of requests to SharePoint Online. Change the scan profile's scan schedule if necessary.

cs0000002

SharePoint Online has a throttling policy when the environment is too busy (SharePoint Online returns HTTP status code 503). To avoid getting throttled in SharePoint Online, choose the following solutions based on your scenario:

- Use the app profile authentication method to rerun the scan job. For more information about app profile, refer to Manage Microsoft 365 Account Pool and What is the Difference Between Service Account Profile and App Profile?.
- When the app profile authentication method cannot meet your data management requirements and you still want to use the service account method, you can try to rerun the scan job or change the scan profile's **Update Schedule** setting. Ensure that scan jobs will not run when there are other services sending a lot of requests to SharePoint Online. For more information about audit logs, see this Microsoft document. If your SharePoint Online environment has been unavailable for a long time, we suggest you contact Microsoft for help.

cs0000003

Exchange Online PowerShell has a limit for the number of simultaneous sessions a user can open. This error occurs when the number of sessions exceeds the limit.

To avoid this error, try the following methods based on your scenario:

- Make sure that you are not connecting to Exchange Online PowerShell when a scan job is running.
- If you need to connect to Exchange Online PowerShell for other services, try contacting Microsoft to modify the limits for your Microsoft 365 tenant.

If the error still exists after you followed the methods above, contact IBM Software Support for help.

cs0000004

Auto Discovery uses Microsoft PowerShell to scan Microsoft 365 Groups and Microsoft Teams, and the Group team sites will be scanned as the Microsoft 365 Groups' properties. Sometimes, even if a Group team site already exists, the property needs to be initialized in Microsoft 365 Outlook.

The scan result of these Group team sites is **Partially Scanned**. To initialize them, sign in to Outlook, find them under the Group tab, and then click Files.

cs0000005

For organizations that use multi-factor authentication in Microsoft 365, it is useful to enable the app profile authentication method for the scan profiles in Auto Discovery. For more information, refer to What Should I Do If My Organization Uses Multi-Factor Authentication (MFA) in Microsoft 365?

When the app profile method cannot meet your data management requirements, choose one of the following solutions based on your scenario:

- Modify the scan profile to select another service account without MFA enabled.
- If you still want to use this service account in the scan profile, disable MFA for this account.

Appendix G - Events Monitored by SCOM

Refer to the table below for IBM Spectrum® Protect Plus Online Services events that can be monitored by System Center Operations Manager.

Event ID	Event	Function
1000	A user signed in.	
1001	A user signed out.	
1002	A user updated an app profile for Microsoft 365.	App Management
1003	A user deleted an app profile.	
1005	A user updated an app profile for Yammer.	
1006	A user clicked **START TRIAL**.	Store
1007	A user successfully started a trial for a service.	
1008	A user reset a password.	My Profile
1009	A user updated contact information.	
1100	A user updated a scan profile.	Auto Discovery
1101	A user clicked **Edit** in **Scan Profile**.	
1102	A user viewed scan history.	
1103	A user deleted a scan profile.	
1104	A user edited a rule.	
1105	A user exported a job's scan history.	
1106	A user deleted one or more rules.	
1107	A user deleted a job's scan history.	
1108	A user deleted one or more containers.	
1109	A user removed one or more objects from a container.	
1110	The objects that no longer meet scan rules were removed from a container.	
1111	A user clicked **Edit**.	Service Account
1112	A user deleted a Service Account profile.	
1113	A user created a Service Account profile.	
1114	A user edited a Service Account profile and saved the edits.	
1200	One or more users were added to the IBM Spectrum Plus Online Services system.	User Management
1201	One or more users were deleted.	
1202	A user's permission information was updated.	
1203	One or more users were activated.	
1204	A user was unlocked.	

Event ID	Event	Function
1206	One or more users were deactivated.	
1301	A user's login session timed out.	
1302	A user's login session ended with a forced timeout.	

Appendix H - Prepare a Certificate for the Custom Azure App

Before preparing a certificate, make sure you have a key vault in Azure.

Procedure

If you do not have any key vaults, refer to the instructions in Appendix C - Create a Key Vault in Azure. Then follow the instructions below to prepare the certificate.

1. In the Azure Portal, navigate to Key vaults.
2. On the Key vaults page, select a key vault and then select Certificates in the left menu.
3. In the Certificates panel, click Generate/Import and complete the required fields. The screenshot below is a sample certificate.

Note: In the Content Type field, select PKCS #12.

4. Click Create and wait for the Status of the certificate to become Enabled. You can click Refresh to update the status if needed.
5. Click the name of the certificate, and then select the current version of the certificate.
6. Click Download in CER format and Download in PFX/PEM format to download the certificate files to your local machine.
7. When you have the certificate (.pfx file), you must set a password to protect the certificate.
   a. Open Windows PowerShell and paste the following script to Windows PowerShell. Replace [`Full Path of your pfx certificatefile`] with the full path of the certificate (.pfx file) in your local machine.

```
$pfxPath=[Full Path of your pfx certificatefile]
  # This command will popup a window, and it will ask you to input a password to protect the certificate.
  $credential=Get-Credential -Message "Enter a password to protect the certificate." -UserName "any"
  $pfxdata=Get-PfxData -FilePath $pfxPath
  Export-PfxCertificate -FilePath $pfxPath -Password $credential.Password -PFXData $pfxdata
```

   b. Press Enter to execute the script.

After completing the steps above, you will get two certificate files. The .cer file can be used to Create Custom Azure Applications in Azure Active Directory and the .pfx file can be used to Create an App Profile for a Custom Azure App in IBM Spectrum® Protect Plus Online Services.

Appendix I - IBM Spectrum Plus Online Services App Registrations

If you need to leverage the resources of IBM Spectrum® Protect Plus Online Services Services, you can register an app in IBM Spectrum Protect Plus Online Servicess and grant permissions to the app.

About this task

With the registered app, you can use the generated application (client) ID for authentication. The table below lists the services that can use the registered app.

IBM Spectrum Protect Plus Online Services	Usage
IBM Spectrum Protect Plus Online Services	Utilize APIs of Auto Discovery to use a batch job to create scan profiles for Microsoft 365 users.

Contact IBM Software Support to acquire the link to the page where you can register IBM Spectrum Protect Plus Online Services apps and then refer to the sections below for more instructions:

Register an App

Procedure

Follow the steps below to register an app:

1. Sign into IBM Spectrum Protect Plus Online Services, and then use the link to open the IBM Spectrum Protect Plus Online Services App Registration page.
2. On the page, click Create.
3. On the Register an Application page, complete the following steps:
   a. Enter a name for the app.
   b. Select the services and corresponding permissions that you need to grant to this app.
   c. Upload a certificate (.cer file) as credentials that allow your application to authenticate as itself, requiring no interaction from a user at runtime. You can refer to Appendix H - Prepare a Certificate for the Custom Azure App to prepare a certificate.
   d. Click Save to save your configurations.
   When you finish the registration, click the app name and you can copy the generated application (client) ID on the app details page. You can use the client ID for authentication when leveraging the resources of IBM Spectrum Protect Plus Online Services for Microsoft 365.

Edit an App

You can edit an app in IBM Spectrum Protect Plus Online Services.

Procedure

1. On the IBM Spectrum Protect Plus Online Services App Registration page, select the app you want to edit and click Edit.
2. On the Edit an app page, you can update the app name, permissions, or certificate. You can refer to the instructions in the **Register an App** section above.

Delete Apps

You can delete an app in IBM Spectrum Protect Plus Online Services.

Procedure

1. On the IBM Spectrum Protect Plus Online Services App Registration page, select the apps and click Delete on the ribbon.
2. A pop-up window appears asking for your confirmation.
3. Click OK to delete the selected apps.

IBM Spectrum Protect Plus Online Services for Microsoft 365

IBM Spectrum Protect Plus Online Services for Microsoft 365 updates

Learn about new features and updates in IBM Spectrum Protect Plus Online Services for Microsoft 365.

Release Date: July 31, 2022

New features and updates

- IBM Spectrum Protect Plus Online Services Recovery Portal for Microsoft 365 is now available to the end users in your organization to perform data recovery for their own OneDrive for Business and Exchange mailbox content using the backup data generated by IBM Spectrum Protect Plus Online Services for Microsoft 365. For details, refer to Recovery Portal for End Users.
- On the End-User Restore Settings page of IBM Spectrum Protect Plus Online Services for Microsoft 365 interface, your application administrator or service provider can choose to allow IBM Spectrum Protect Plus Online Services Recovery Portal users to restore backup data stored at the archive tier of Azure Blob storage.
- The Microsoft Teams Chat service is now available in IBM Spectrum Protect Plus Online Services for Microsoft 365 interface to protect the Teams chat messages of Microsoft 365 users. In the current release, Teams chat messages can only be exported to HTML files for data recovery.
- SSO (Single Sign-on) is now supported. When you access IBM Spectrum Protect Plus Online Services for Microsoft 365 via the direct URL, you do not need to provide user credentials to sign in once it is detected that you have signed into IBM Spectrum Protect Plus Online Services.
- To avoid any accidental deletion of backup data, you can contact IBM Software Support to disable the GDPR-related features (Data Subject Access Requests and the Manually Delete Backup Data function) for your tenant.
- You can now store your data to IBM Cloud Object Storage by using IBM Spectrum Protect Plus Online Services for Microsoft 365. For more information about configuring IBM COS, refer to IBM Cloud Object Storage

The following sections of the documentation have been updated or added:

- Added Recovery Portal for End Users
- Updated List of On-Demand Features
- Added Use Case - Want to Restore Teams Chat Messages?
- Updated FAQs
- Updated Authentications in Auto Discovery and Hybrid Approach
- Updated App Profile Authentication
- Updated Configuring Super Users
- Updated Amazon S3
- Added Export Teams Chat Messages
- Updated Data Subject Access Requests
- Updated View Subscription Consumption Report
- Added Teams Chat Data Types
- Updated Restore Options for Different Object Types
- Added Restore Conflict Resolutions

- **Updates in previous versions**

Updates in previous versions

Release Date: June 5, 2022

- German is now an available display language for IBM Spectrum® Protect Plus Online Services for Microsoft 365 and the Germany West Central (Frankfurt) data center is now supported.
- Microsoft Delegated app can now be used to protect Planner data. If you have a Microsoft Delegated app for restoring Teams channel conversations as posts, the authentication user of the Microsoft Delegated app will now be automatically deleted from the Team members and private channel members after the restore completes.
- Long-running backup performance has been improved. Full backup jobs that have been running for a long time will not be split off or paused until they are finished. Scheduled backup jobs to protect incremental changes will run in parallel with the full.
- You can now protect Planner data with a Delegated app when using app profile authentication for Auto Discovery. To protect Planner data in app context, you can go to the App Management page in the IBM Spectrum Protect Plus Online Services interface to configure a delegated app for IBM Spectrum Protect Plus Online Services for Microsoft 365 with the Protect Planner data option selected. The authentication user must have the Global administrator role and an Exchange license.
- Added the following error codes to the job report to help with troubleshooting: **SP-IRMProtectedFileFailed** and **SP-SkipBackupRecordingFolder**.

The following sections of the documentation have been updated or added:

- Updated Split-Off and Pause Backups.
- Added Authentications in Auto Discovery and Hybrid Approach.
- Updated Amazon S3.
- Added Export OneDrive for Business Data
- Updated Microsoft 365 Groups Data Types.
- Updated Planner Data.
- Added SP-IRMProtectedFileFailed, and SP-SkipBackupRecordingsFolder.

Release Date: Mar 29, 2022

- IBM Spectrum Protect Plus Online Services for Microsoft 365 now supports configuring a data retention period that is less than one year.

- When you are restoring a site collection (of SharePoint Online, Microsoft 365 Groups, Teams, or Yammer), a group, a team, or a community, you can now choose to restore the hub site connection for the site. Note that this feature does not support cross-tenant restores.
- The Microsoft 365 Unusual Activities Analysis Report is now available to show the unusual activities detected in your OneDrive for Business backups. This report requires OneDrive accounts to have at least 12 days of incremental backups with changes. The report displays an overview of the unusual activities tracked over the last 30 days and provides a Restore option on that page to directly recover the OneDrive account to a safe state.
- By default, IBM Spectrum Protect Plus Online Services for Microsoft 365 uses V2 authentication to access your Amazon S3 Compatible storage. If you want to use V4 authentication, add **SignatureVersion=V4** as an extended parameter when providing the storage information.

The following sections of the documentation have been updated or added:

- Updated About IBM Spectrum Protect Plus Online Services for Microsoft 365.
- Added Features unavailable in trial license.
- Updated Backup and Restore.
- Added Use Case – Want the Ability to Detect a Potential Ransomware Attack and Safely Recover Encrypted Files?
- Updated Amazon S3-Compatible Storage.
- Updated Configure Retention Policy.
- Added Use Microsoft 365 Unusual Activities Analysis Report.
- Updated Restore Options for Different Object Types.

About IBM Spectrum Protect Plus Online Services for Microsoft 365

IBM Spectrum Protect Plus Online Services for 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 Spectrum Protect Plus Online Services for Microsoft 365 offers backup capabilities for all Microsoft 365 instances, such as Exchange Online, OneDrive for Business, SharePoint Online, Microsoft 365 Groups, Teams, Project Online, and Public Folders, to protect your data. These object types are backed up and restored independently of one another.

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

- SharePoint Sites Data Types
- Modern Team Site Data Types
- Project Online Data Types
- Exchange Online Data Types
- Public Folders Data Types
- Microsoft 365 Groups Data Types
- Teams Data Types
- OneDrive for Business Data Types
- Document-Related Data Types

Note the following:

Yammer service:

- To protect Yammer data, you must have a Yammer app connected to your tenant, and the authentication user of this Yammer app must have the Verified Admin role. For details on configuring a Yammer app, refer to App Profile for Yammer. Yammer service currently supports in place restore only (restoring to the original location), meaning the Yammer community needs to already be there, as well as the ability to export files and conversations. Note that the Microsoft 365 services in GCC High data center and the data center operated by 21Vianet in China do not support Yammer, so the Yammer backup service in such data centers is not supported as well.
- If you have Microsoft 365 connected Yammer communities protected under Microsoft 365 Groups service, once the Yammer service is enabled, the connected groups will be removed from Microsoft 365 Groups service and can only be protected in Yammer even if you disable the Yammer service again. IBM Spectrum Protect Plus Online Services for Microsoft 365 job will start a new backup cycle for these Yammer communities, but their former backup data as Microsoft Groups will not be deleted until the data expires retention period.

SharePoint Online, OneDrive for Business, and Project Online:

- 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 Spectrum Protect Plus Online Services for Microsoft 365 will run a full backup for SharePoint Online sites and OneDrive for Business objects with new URLs.
- IBM Spectrum Protect Plus Online Services for Microsoft 365 for OneDrive for Business 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 for Business since OneDrive for Business is the cloud service used to help securely store, share, and access your files.

- As Microsoft 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 Spectrum Protect Plus Online Services for 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 for Business, 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 you would like to filter the folders to protect a **OneDrive for Business** service or **Exchange Online** service, or filter the folders 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.
- 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.
- 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 Spectrum Protect Plus Online Services for 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.
- **Preservation Hold** library is not protected by IBM Spectrum Protect Plus Online Services for Microsoft 365.
- IBM Spectrum Protect Plus Online Services for Microsoft 365 for SharePoint Online also supports protecting **Communication Sites**. When restoring a deleted Communication Site to its original location, IBM Spectrum Protect Plus Online Services for 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.
- IBM Spectrum Protect Plus Online Services for Microsoft 365 for Project Online supports restoring **Project Permission Mode** features. Project Online data cannot be protected in the app context (using app profile authentication), and 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.

Exchange Online and Public Folders:

- If you would like to filter the folders to protect a **OneDrive for Business** service or **Exchange Online** service, or filter the folders 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.
- The service for **Public Folders** only supports restoring content, permissions, and metadata of Public Folders to the original location. Note that the Public Folders service does not support protecting Public Folder metadata in the app context.
- 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 Spectrum Protect Plus Online Services for 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.

Microsoft 365 Groups and Teams

- IBM Spectrum Protect Plus Online Services for Microsoft 365 can 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' **Private Channel**, the service account must be the owner of the Private Channel.
- If you are using custom app authentication, ensure your app has access to the protected APIs of Microsoft Teams. Otherwise, the public and private channels' conversations cannot be protected. To request access to the protected APIs, refer to the Microsoft article: Protected APIs in Microsoft Teams.

Microsoft Teams Chat

- To use the Microsoft Teams Chat service to protect Teams chat messages, you can register the **All permissions** type app profile for Microsoft 365 for Auto Discovery and backup, or you can use a hybrid approach (using service account authentication for Auto Discovery while also having an app profile configured for your tenant). You can also choose to use a custom app. For details on the required permissions for custom app, refer to App Profile Authentication.
- Microsoft Teams Chat service in IBM Spectrum Protect Plus Online Services for Microsoft 365 currently uses the Teams Export API of Microsoft Graph to export Teams chat messages to an HTML file. Currently, we are using Export API model A to protect the chats of Microsoft 365 users with any of the following licenses:
  - Microsoft 365 A5 for Faculty
  - Microsoft 365 E5
  - Microsoft 365 E5 Compliance
  - Microsoft 365 E5 Security
  - Microsoft 365 E5 without Audio Conferencing
- The Export API may charge the app creator for messages consumed beyond the seeded capacity. Therefore, if you are using an IBM Spectrum Protect Plus Online Services default app for Microsoft 365, you may incur charges from IBM Spectrum Protect Plus Online Services as Microsoft begins charging for this API. If you are using a custom app, to request access to Export APIs, read the Prerequisites and complete the request form.
- Microsoft Teams Chat backup service does not support GCC tenants. For more details on the supported data types, refer to Teams Chat Data Types.

Single Sign-On

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

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.

IBM Spectrum Protect Plus Online Services for Microsoft 365 provides a backup frequency of 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 that if there is a backup job in progress, the automatic backup job scheduled to run will be skipped.

Backup jobs can also be run manually if there is data that failed to be backed up during the last backup job. For detailed instructions on manually running backup jobs, refer to Manually Run a Backup.

Storage Location

You can choose to store the backup data to the default storage location provided by IBM Spectrum Protect Plus Online Services for Microsoft 365 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 license 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 five storage types: **Amazon S3**, **Dropbox**, **FTP**, **Microsoft Azure Blob Storage**, and **SFTP**. 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 license 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 toRestore Options for Different Object Types and Restore and Recover Your Data.

Note: If your device is **Microsoft Azure Blob Storage**, IBM Spectrum Protect Plus Online Services will automatically store your backup data to a cool tier to help conserve storage costs. The supported Azure account kinds are **StorageV2** and **BlobStorage** of the **Standard** performance type.
You may have some old backup data stored to the archive tier, the most cost-effective manner of using Azure blob storage. But for a successful restore, IBM Spectrum Protect Plus Online Services recommends keeping the index database in the online tier (hot or cool).

When Azure Blob Storage users perform a restore job, they can choose to allow the restore job to automatically rehydrate data from the archive tier, or they must manually change the access tier of the backup data in storage.

The restore job will first rehydrate the data sets in the archive tier, and this restore job may take longer than previously. The restore job also supports restoring the archive tier backup data to your own storage. If you are using IBM Spectrum Protect Plus Online Services default storage, the restore job will automatically rehydrate data.

The export job also supports automatically rehydrating backup data in the archive tier if you are using IBM Spectrum Protect Plus Online Services default storage. This feature has not been supported yet for customers using BYOS.

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.

Retention

If you use your own storage device and have purchased an unlimited data retention agreement, you can customize the data retention period for each service type. Prior to any data deletion, IBM Spectrum Protect Plus Online Services for 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).

Reporting

By monitoring the license consumptions, jobs operations, and all user activities, 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 details, you can refer to:

- Generate and Download a Job Report
- View Subscription Consumption Report
- Use the Job Analytics Report
- Audit User Activities in System Auditor

- **Recoverable Items Mailboxes**
  The Exchange Online service of IBM Spectrum Protect Plus Online Services for Microsoft 365 supports backup and restore for only the Recoverable Items folder in the User's mailboxes, Resource (room and equip) mailboxes, In Place Archive mailboxes, and Shared mailboxes.
- **Multi-Geo License**
  IBM Spectrum Protect Plus Online Services for Microsoft 365 supports protecting your Microsoft 365 tenant that has the Multi-Geo license.
- **Recovery Portal for End Users**
- **Split-Off and Pause Backups**
  If an incremental backup job for **SharePoint Online**/**OneDrive for Business**/**Project Online**/**Exchange Online**/**Teams/Groups** running has been running for 2 days, 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. For any content we've already finished protecting, we'll mark this job as "**Partially Finished**" in the backup dashboard in order 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 in order to maintain the best SLA.
- **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 Spectrum Protect Plus Online Services for Microsoft 365 is deployed on the Microsoft Azure framework to make outbound Microsoft API calls and internal communications over HTTPS/TLS 1.2 encrypted channels. Certificate-based authentication is used for internal communications.
- **List of On-Demand Features**
  IBM Spectrum Protect Plus Online Services for Microsoft 365 has several features to be delivered or enabled on your demand.
- **Microsoft Graph API Beta Version in Use**
  Refer to the table below for the beta version API methods of Microsoft Graph that we use in IBM Spectrum Protect Plus Online Services for Microsoft 365.

Recoverable Items Mailboxes

The Exchange Online service of IBM Spectrum® Protect Plus Online Services for Microsoft 365 supports backup and restore for only the Recoverable Items folder in the User's mailboxes, Resource (room and equip) mailboxes, In Place Archive mailboxes, and Shared mailboxes.

You can contact the IBM Software Support team to enable this feature.

With this feature enabled, the IBM Spectrum Protect Plus Online Services Auto Discovery job will only scan and register the Recoverable Items Mailboxes to the containers, and the Exchange Online service in IBM Spectrum Protect Plus Online Services for Microsoft 365 will only display the Recoverable Items Mailboxes in the backup scope.

After an in-place restore job, you can find the restored items through **Recover Deleted Items** in the Outlook desktop app.

Note the following:

- Currently, IBM Spectrum Protect Plus Online Services only support the Deletion subfolder in the Recoverable Items. For more information about Recoverable Items, refer to this Microsoft article: Recoverable Items folder in Exchange Online.
- The in-place restore (restore to original location), restore to storage, and export functions are supported, but the out-of-place restore (restore to another location) is unsupported.
- If you have backup data of mailboxes before this feature is enabled, the backup data will be moved to the unprotected scope, and will be deleted on time.

The section below will show you how to get this feature enabled in different scenarios:

Scenario 1: New to IBM Spectrum Protect Plus Online Services and do not have an Exchange Online scan profile in Auto Discovery.

1. Go to IBM Spectrum Protect Plus Online Services for Microsoft 365 to initialize the instance but do not configure the scan profile in this step.
2. Contact IBM Software Support to enable this feature for your tenant.
3. Configure an Exchange Online scan profile in Auto Discovery, run the scan job, and then wait five to ten minutes after the scan job completes.
4. Go to theIBM Spectrum Protect Plus Online Services for Microsoft 365 interface to check whether the Recoverable Items Mailboxes are displayed in the backup scope (The backup data tree should only display the Recoverable Items Mailboxes).
5. Enable the Exchange Online backup service if the backup scope is correct.

Scenario 2: Exchange Online scan profile has been configured in Auto Discovery, but Exchange Online backup service has not been enabled.

1. If you have not yet accessed IBM Spectrum Protect Plus Online Services for Microsoft 365, go to the IBM Spectrum Protect Plus Online Services for Microsoft 365 interface to initialize the instance; if you have, skip this step.
2. Contact IBM Software Support to enable this feature for your tenant.
3. Run the Exchange Online scan profile in Auto Discovery and wait five to ten minutes after the scan job completes.
4. Go to the IBM Spectrum Protect Plus Online Services for Microsoft 365 interface to check whether the Recoverable Items Mailboxes are displayed in the backup scope (The backup data tree should only display the Recoverable Items Mailboxes).
5. Enable the Exchange Online backup service if the backup scope is correct.

Scenario 3: Exchange Online service has been enabled in IBM Spectrum Protect Plus Online Services for Microsoft 365.

1. Contact IBM Software Support to enable this feature for your tenant.
2. This feature will take effect after your next scheduled scan job completes five to ten minutes later.
3. Go to the IBM Spectrum Protect Plus Online Services for Microsoft 365 interface to check whether the Recoverable Items Mailboxes are displayed in the backup scope (The backup data tree should only display the Recoverable Items Mailboxes).

Note: Your backup data of mailboxes before this feature has been enabled will be moved to the unprotected scope for deletion.

Multi-Geo License

IBM Spectrum® Protect Plus Online Services for Microsoft 365 supports protecting your Microsoft 365 tenant that has the Multi-Geo license.

For more information, see Microsoft 365 Multi-Geo.

For details on how it should be configured through the IBM Spectrum Protect Plus Online Services platform and how it is protected in the IBM Spectrum Protect Plus Online Services for Microsoft 365 app, refer to Does IBM Spectrum Protect Plus Online Services Support Microsoft 365 Tenants with Multi-Geo Licenses?

You can start using the Multi-Geo license by going to Manage Data Center Mappings to review and map the list of geo locations from your Microsoft 365 tenant that we have detected 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 Spectrum Protect Plus Online Services for Microsoft 365 interface. Users with only one region will be automatically redirected to the regional Cloud Backup 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 Spectrum Protect Plus Online Services for 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 Spectrum Protect Plus Online Services Auto Discovery and get protected by IBM Spectrum Protect Plus Online Services for Microsoft 365. This means, in the IBM Spectrum Protect Plus Online Services for 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 license)
    - 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 for Business/SharePoint sites – If the OneDrive for Business library or SharePoint site existed before your tenant enabled Multi-Geo, the OneDrive for Business 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 for Business/SharePoint site geo move of approximately 4-6 hours, depending on site contents. During the move, the OneDrive for Business library/SharePoint site will continue being protected in the IBM Spectrum Protect Plus Online Services for Microsoft 365 instance for the former region. After the move is completed and the site is registered as new through IBM Spectrum Protect Plus Online Services Auto Discovery, the site will be protected in the IBM Spectrum Protect Plus Online Services for 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, consider configuring a custom app profile. The Directory.ReadWrite.All permission is not automatically consented to the default app profile, but this permission 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.
- 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 Spectrum Protect Plus Online Services storage with a Multi-Geo license, IBM Spectrum Protect Plus Online Services for 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 Spectrum Protect Plus Online Services storage.
- The **License Consumption Report** is only available to the IBM Spectrum Protect Plus Online Services 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 the Multi-Geo license. 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.

Recovery Portal for End Users

Recovery portal is a data recovery center designed to connect end users in your organization to their lost OneDrive for Business and Exchange mailbox content. 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 Spectrum® Protect Plus Online Services> 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 IBM Spectrum Protect Plus Online Services Recovery Portal.

Split-Off and Pause Backups

If an incremental backup job for **SharePoint Online**/**OneDrive for Business**/**Project Online**/**Exchange Online**/**Teams/Groups** running has been running for 2 days, 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. For any content we've already finished protecting, we'll mark this job as "**Partially Finished**" in the backup dashboard in order 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 in order 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 2 days (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 go 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 SharePoint Online/Project Online/OneDrive for the Business backup job hasn't been completed after running for another 14 days, it will be paused. 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 Spectrum® Protect Plus Online Services 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 Spectrum® Protect Plus Online Services for Microsoft 365 is deployed on the Microsoft Azure framework to make outbound Microsoft API calls and internal communications over HTTPS/TLS 1.2 encrypted channels. Certificate-based authentication is used for internal communications.

For data storage encryption, IBM Spectrum Protect Plus Online Services for 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 Spectrum® Protect Plus Online Services for 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:

- 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, the successful item level objects will not be included in the job report. If you want to view the successful item level objects in the job report, contact IBM Software Support for assistance.
- If you would like to filter the folders to protect the **OneDrive for Business** service or **Exchange Online** service or filter the folders 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.
- 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.
- The Exchange Online service of IBM Spectrum Protect Plus Online Services for Microsoft 365 can support the backup and restore for only the **Recoverable Items** folder in the User's mailboxes, Resource (room and equip) mailboxes, In Place Archive mailboxes, and Shared mailboxes. You can contact the IBM Software Support team to enable this feature. For details, refer to Recoverable Items Mailboxes.
- 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.
- Auto archive for BYOS Azure storage – If you are using your own Azure storage with longer retention policies, you can contact the IBM Software Support team to enable the automatic archive to keep your legacy backup data in the archive tier to save cost. Your legacy backup data will be moved to the archive tier in the next archive job.
- The Export Encryption Key feature is by default not available to users who are using default storage hosted by IBM Spectrum Protect Plus Online Services. You can contact the IBM Software Support if needed. For details on exporting encryption keys, refer to Export Encryption Key.
- The data recovery job can use the Migration API to improve the speed of large-scale recoveries. If you are interested in this method, contact the IBM Software Support team to help you enable it. The High-Speed Migration (HSM) restore method supports SharePoint Online, OneDrive for Business, Microsoft 365 Groups, and Teams 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 High Speed Migration (HSM) Restore Method.
- 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 more details, refer to Remove Unprotected Data.
- 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.

Microsoft Graph API Beta Version in Use

Refer to the table below for the beta version API methods of Microsoft Graph that we use in IBM Spectrum® Protect Plus Online Services for 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.
Channel message	Get all channel messages	Yes	These methods in the 1.0 version currently do not support either the **Application** permission type or the **Delegated** permission type.
	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 Spectrum® Protect Plus Online Services for 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 Spectrum® Protect Plus Online Services for Microsoft 365 Account Management feature is a security trimming solution for restore operations. It provides a built-in Administrator group with full control permission to IBM Spectrum Protect Plus Online Services for Microsoft 365. Administrators can add groups through Account 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 Spectrum® Protect Plus Online Services for 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 Spectrum Protect Plus Online Services for 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 Spectrum Protect Plus Online Services for 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.

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 Spectrum® Protect Plus Online Services for 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 Spectrum Protect Plus Online Services for 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 Spectrum Protect Plus Online Services for Microsoft 365, refer to Get Started. For more information on restoring SharePoint Online data, refer to Restore SharePoint Online Data.

Use Case - Want to Restore OneDrive for Business Data?

Event:

Tom left the company six months ago. Tom stored many business documents in his personal OneDrive for Business site. Bob, Tom's boss, would like access to one of Tom's OneDrive for Business 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 for Business library to Bob's OneDrive for Business site.

Problem:

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

Resolution:

You have an IBM Spectrum® Protect Plus Online Services for Microsoft 365 account and have the OneDrive for Business backup service enabled for the backup of this OneDrive for the Business site. You log into IBM Spectrum Protect Plus Online Services for Microsoft 365 to recover Tom's deleted library. You select Tom's username for OneDrive for Business 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 for Business site.

To get started with IBM Spectrum Protect Plus Online Services for Microsoft 365 services, refer to Get Started. For more information on restoring OneDrive for Business data, refer to Restore OneDrive for Business Data.

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 Spectrum® Protect Plus Online Services for 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 Spectrum Protect Plus Online Services for 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 Spectrum Protect Plus Online Services for 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 Spectrum Protect Plus Online Services for Microsoft 365, refer to Get Started. For more information on restoring Microsoft 365 Groups data, refer to Restore Microsoft 365 Groups Data.

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 Spectrum® Protect Plus Online Services for 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 Spectrum Protect Plus Online Services for 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 Spectrum Protect Plus Online Services for Microsoft 365, refer to Get Started. For more information on restoring Project Online data, refer to Restore Project Online Data.

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 Spectrum® Protect Plus Online Services for 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 Spectrum Protect Plus Online Services for 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 Spectrum Protect Plus Online Services for 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 Spectrum Protect Plus Online Services for Microsoft 365, refer to Get Started. For more information on restoring Public Folders data, refer to Restore Public Folder Data.

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 Spectrum® Protect Plus Online Services for 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 Spectrum Protect Plus Online Services for 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 Spectrum Protect Plus Online Services for Microsoft 365, refer to Get Started. For more information on restoring teams, refer to Restore Teams Data.

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 Spectrum® Protect Plus Online Services for 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 Spectrum Protect Plus Online Services for Microsoft 365, refer to Get Started. For more information on restoring teams, refer to Export Teams Chat Messages.

Use Case - Want to Restore Yammer Data

Event:

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

Problem:

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

Resolution:

You have a IBM Spectrum® Protect Plus Online Services for Microsoft 365 account and already have the Yammer backup service enabled for the backup of the Yammer community. You can use the Yammer service to restore or export Yammer messages. To locate the Yammer 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 Spectrum Protect Plus Online Services for Microsoft 365, refer to Get Started. For more information on restoring teams, refer to Restore Yammer Data.

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 the ability to have early detection in place along with options for a safe restore in the event of an attack. You have a IBM Spectrum® Protect Plus Online Services for Microsoft 365 account in place with OneDrive already set up to be protected with regular backups in place. Plus, IBM Spectrum Protect Plus Online Services for Microsoft 365provides 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 Microsoft 365 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 Case - Want to Obtain a Better Understanding of Your License Consumption?

Event:

Your organization uses IBM Spectrum® Protect Plus Online Services for Microsoft 365 to protect your Microsoft 365 tenant. The IT team wants the ability to fully monitor the license consumption, from the application level down to an individual object level such as a site collection, mailbox, OneDrive for a Business object, group, or team, in order to understand and identify trends in utilization.

Resolution:

The License Consumption Report provides a complete breakdown of license utilization and consumption. The report includes the following components: a dashboard which provides full license 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 license of each protected object along with the ranking in its service type in the Utilization tab. The reports are also downloadable in CSV format.

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

Event:

You may have used IBM Spectrum® Protect Plus Online Services 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 license or have been using default IBM Spectrum Protect Plus Online Services storage with an unlimited retention license, 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.

Supported Browsers

The table below outlines the required browser versions to support IBM Spectrum® Protect Plus Online Services for Microsoft 365.

Table 1.

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**
- **Security and Integrity**
- **Public APIs**
- **Backup and Restore**
- **Storage**

License and Subscription

If a user's Microsoft 365 license expires, will their data become unprotected?

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 backup data of the object be moved to the unprotected scope for deletion and detected by the **Remove Unprotected Data** report. For details, refer to Remove Unprotected Data. By default, the Remove Unprotected Data feature does not support BYOS customers or trial licenses.

Table 1.

Service Type	Reactions
Exchange Online	Service account authentication cannot detect the users' mailboxes if their license expired, and the backup data of these mailboxes will be kept until the data retention date is reached. App profile authentication will continue protecting the mailboxes in this case if they are in the backup scope.
OneDrive for Business	If the user's My Site has been deleted permanently from Microsoft 365 (compared to soft-delete state), this site will be no longer discoverable to IBM Spectrum Protect Plus Online Services, and its backup data will be kept until the data retention date is reached.
Project Online	License expiration does not affect the Auto Discovery but will fail the backup.

I am currently using IBM Spectrum Protect Plus Online Services default storage to store backup data. If I end my subscription, would I ever be able to recover the backup data from IBM Spectrum Protect Plus Online Services?

When a subscription ends, IBM Spectrum Protect Plus Online Services will retain the backup data in IBM Spectrum Protect Plus Online Services storage for 15 days, subject to the terms of your service agreement. The backup data in IBM Spectrum Protect Plus Online Services 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 Spectrum Protect Plus Online Services storage. If you have the BYOS (bring your own storage) license, 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 Spectrum Protect Plus Online Services 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 Spectrum Protect Plus Online Services for Microsoft 365interface once your subscription has ended. For details on exporting encryption keys, refer to Export Encryption Key.

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

Features unavailable in trial license

The following features are unavailable to trial users:

- Change backup scope
- Remove Unprotected Data
- Storage Consumption Report

Security and Integrity

Does IBM Spectrum Protect Plus Online Services for Microsoft 365 Support Data Deduplication and Compression?

IBM Spectrum® Protect Plus Online Services for Microsoft 365 applies standard .zip compression to data. Though our DAT files can support deduplication algorithms, we currently do not support deduplication on Blob storage as this necessitates a physical/virtual storage system that is not as cost-effective as Azure Cool 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 Spectrum Protect Plus Online Services for 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 Spectrum Protect Plus Online Services for 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 more details, you can refer to Customer Key Overview from the Microsoft website.

Public APIs

I am using a backup reporting software. May I pull the daily job information into that software to monitor my IBM Spectrum Protect Plus Online Services for Microsoft 365?

Yes. You can use the public APIs that IBM Spectrum® Protect Plus Online Services provide to get the audit records, subscription consumption, and job information of IBM Spectrum Protect Plus Online Services for Microsoft 365. For details, refer to IBM Spectrum Protect Plus Online Services Web API.

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 Spectrum® Protect Plus Online Services for Microsoft 365 using service accounts support modern authentication.

type:

How to add permissions to an admin role in the Exchange admin center?

If you are using a service account in Auto Discovery to scan Exchange Online mailboxes, you must ensure the **ApplicationImpersonation** permission has been added to the admin role of this service account via the Exchange admin center. Otherwise, the destination data tree for restoring the mailbox items to another location may not show any items.

Follow the steps blew to add permissions to an admin role in the Exchange admin center:

1. In the Exchange admin center, go to Roles > Admin roles on the quick launch panel.
2. Click the admin role group of the service account. The details of the role group are displayed in the right panel.
3. Click the Permissions tab.
4. Scroll down the list and select the checkbox ahead of ApplicationImpersonation permission.
5. Click Save to save your changes.

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 Spectrum Protect Plus Online Services for 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 Spectrum Protect Plus Online Services for 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 SharePoint domain name has been changed after backup?

You can change the SharePoint domain name for your organization in Microsoft as introduced in this Microsoft article: Rename your SharePoint domain. This change will affect the SharePoint sites, Team/Group team site, and OneDrive for Business.

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 Spectrum Protect Plus Online Services for 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.

To restore the wiki data, the following requirements must be met:

- Enable High Speed Migration (HSM).
- The Wiki tab still exists, and only the sections or pages in Wiki are deleted or updated.
- You have not yet restored the wiki list (channelID_wiki) before the HSM is enabled.

Follow the steps below to restore the wiki list:

1. Select the wiki list (channelID_wiki) in the backup data of the Team's team site to restore.
2. Use the **Merge** or **Skip** as the container level conflict resolution and use **Overwrite** as the content level conflict resolution.
3. For more details on restoring Teams data, refer to Restore Teams 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 Spectrum Protect Plus Online Services for 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 Spectrum Protect Plus Online Services will keep it in both the **SharePoint Sites** container and the **Microsoft 365 Groups** container. IBM Spectrum Protect Plus Online Services for 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 Spectrum Protect Plus Online Services for Microsoft 365 protect the mailboxes on Litigation Hold?

IBM Spectrum Protect Plus Online Services for 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 Spectrum Protect Plus Online Services for 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 Azure AD, 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 global term store data, select any site collection in your tenant and use Skip as the conflict resolution for all to perform a restore job.
- If you want to restore local term store data for a site collection, select that site collection to restore and use Skip as the conflict resolution for all to perform a restore job.

How does IBM Spectrum Protect Plus Online Services for 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 Spectrum Protect Plus Online Services for Microsoft 365 cannot protect the history versions of OneNote files.

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 Spectrum® Protect Plus Online Services automatically stores your backup data to the cool tier to help conserve storage costs. The supported Azure storage account types are **StorageV2** and **BlobStorage** of **Standard** performance type. To use your Azure blob storage in the most cost-effective manner, you can also store the backup data to the archive tier. Contact IBM Software Supportto help you move your older backup data to the archive tier. Note that you may experience a slower restore when restoring backup data from the archive tier.

Hot Tier	Cool Tier	Archive Tier
Index database	The backup job stores backup data to the cool tier automatically from the July 2020 release and will always keep at least a full backup cycle in the cool tier.	Older backup data can be moved to the archive tier.

Does IBM Spectrum Protect Plus Online Services for Microsoft 365 use HTTPS (SSL) for Amazon S3 communication?

Yes. IBM Spectrum Protect Plus Online Services for Microsoft 365 uses HTTPS (SSL) instead of HTTP to access Amazon S3 by default. For details on Amazon S3 storage configuration, refer to Amazon S3.

Best Practices

Backup Scheduling

Microsoft has recently implemented tighter throttling limits on background apps, including content migration, data loss prevention, and backup solutions for SharePoint Online and OneDrive for Business, during weekday daytime hours. You should expect that these 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. Consider implementing the following scheduling practices to help 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. For more information on the app profile, Auto Discovery, and how to set up an Auto Discovery Profile, refer to Manage Auto Discovery.
Note: IBM Spectrum® Protect Plus Online Services for Microsoft 365 can also apply a hybrid approach for the backup and restore of the Exchange Online, Exchange Public Folders, OneDrive for Business, SharePoint Online, Microsoft Teams, and Microsoft 365 Groups when you use a service account for Auto Discovery and have an app profile with proper permissions granted in your tenant. For more details, refer to Configure Auto Discovery.

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

Before you start using IBM Spectrum® Protect Plus Online Services for Microsoft 365, you must obtain a full license to IBM Spectrum Protect Plus Online Services for Microsoft 365 and configure the Auto Discovery profile to scan the objects you want to protect.

- To find out how IBM® charges for licenses for IBM Spectrum Protect Plus Online Services for Microsoft 365, refer to Licensing Information.
- If your Microsoft 365 tenant has a Microsoft 365 Multi-Geo, you can start by going to the Manage Data Center Mappings in IBM Spectrum Protect Plus Online Services to review and map the list of geo locations from your Microsoft 365 tenant we've detected and the supporting data centers.
  Note: The mapping for SharePoint Online sites depends on the region of the SharePoint Administrator.
- Use Auto Discovery to scan and register the objects that you want to protect into containers. For details, refer to Configure Auto Discovery. By leveraging Auto Discovery, objects that are added or modified to your environment after your initial backup will be included in all subsequent backups. If your administrator has blocked access from apps that don't use modern authentication, Cloud Backup jobs using a service account will now use modern authentication for the backup and restore.
  Note: If your tenant is Multi-Geo, you will want to ensure you are using the filters provided in the advanced scan mode to separate the mailboxes, OneDrives, 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 around the world.

When you log into IBM Spectrum Protect Plus Online Services for Microsoft 365 for the first time, you will be prompted to select the objects you want to back up. The backup cycle is one year.

- **Configure Auto Discovery**
- **Centralized Account Management**
  Account Management provides centralized management of groups and securities. Administrators can add and manage groups for security control of what users can restore in IBM Spectrum Protect Plus Online Services for Microsoft 365. Security group allows you to organize users in IBM Spectrum Protect Plus Online Services for 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.
- **Select the Objects You Want to Back Up**
  When you log into IBM Spectrum Protect Plus Online Services for Microsoft 365 for the first time, the Backup Objects Selection page will appear to ask you to select the objects to back up.

Configure Auto Discovery

Prior to running backup jobs in IBM Spectrum® Protect Plus Online Services for Microsoft 365, you must register the objects below that you want to protect in the Auto Discovery of IBM Spectrum Protect Plus Online Services.

- Exchange Online mailboxes
- OneDrive for Business
- SharePoint Online site collections
- Microsoft 365 Groups (including group team sites, group mailboxes) and Microsoft Teams
- Project Online site collections
- Exchange Online public folders (For Multi-Geo license, the public folders can only be protected in the Central IBM Spectrum Protect Plus Online Services Location)

To increase security for your Microsoft 365 tenant and avoid throttling during your backup jobs, IBM® 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 Auto Discovery for Microsoft 365.

The detected objects will be grouped into default or custom containers and will appear in your IBM Spectrum Protect Plus Online Services for Microsoft 365 environment. IBM Spectrum Protect Plus Online Services will automatically monitor for object updates, creation, and deletion. It will take a few minutes to synchronize objects from IBM Spectrum Protect Plus Online Services to IBM Spectrum Protect Plus Online Services for Microsoft 365 when you log into IBM Spectrum Protect Plus Online Services for Microsoft 365 for the first time.

Read the following for additional notes:

If a SharePoint site is connected to a Microsoft 365 Group (a groupified site), IBM Spectrum Protect Plus Online Services will keep it in both the **SharePoint Sites** container and the **Microsoft 365 Groups** container. IBM Spectrum Protect Plus Online Services for Microsoft 365 for Microsoft 365 will protect this site in the corresponding container separately as you selected.
In the IBM Spectrum Protect Plus Online Services Manage Scan Profiles, you can now 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 Spectrum Protect Plus Online Services for Microsoft 365 can back up and restore this type of mailbox via app profile.

- **Authentications in Auto Discovery and Hybrid Approach**

Authentications in Auto Discovery and Hybrid Approach

The Auto Discovery in IBM Spectrum® Protect Plus Online Services allows you to choose the following methods to scan and register the objects in your tenant for data protection or management.

- Default app profile (For permissions authorized by default, refer to IBM Spectrum Protect Plus Online Services Administration for Office 365).
- Custom app profile (For permissions that you must manually add, refer to the table in App Profile Authentication).
- Service account profile (For the required permissions for the service account and account pool user, refer to Service Account Authentication).

Note: If your tenant enabled MFA, Auto Discovery requires using an app profile with an MFA service account. For more details, refer to What Should I Do If My Organization Uses Multi-Factor Authentication (MFA) in Microsoft 365?.
After you have registered the objects in the IBM Spectrum Protect Plus Online Services platform, you can access IBM Spectrum Protect Plus Online Services for Microsoft 365 for data protection.

Before you start the backup cycle, you need to know how the app profiles and service account profiles you configured in IBM Spectrum Protect Plus Online Services will affect the backup and restore jobs in IBM Spectrum Protect Plus Online Services for Microsoft 365.

If you are using a service account for Auto Discovery and also have app profiles with proper permissions in your tenant, IBM Spectrum Protect Plus Online Services for Microsoft 365 will apply a hybrid approach in the backup and restore.

The hybrid approach means that Cloud Backup jobs will use app profile by default for the backup and restore and use service account authentication automatically for the data types that are unsupported by app profile authentication.

Note: Project Online service only supports service account authentication.
Refer to the authentication methods recommended for each service type:

Table 1.

Service Type	Recommended Method
Exchange Online	App profile only is the best practice
OneDrive for Business	App profile recommended
SharePoint Online	App profile recommended You can refer to the data types listed in SharePoint Sites Data Types for their support status in app profile authentication and service account authentication to decide upon your own condition.
Project Online	Service account Project Online service does not support app profile authentication.
Microsoft 365 Groups/Teams	App profile recommended. IBM Spectrum Protect Plus Online Services recommends you configure the app profile for Microsoft 365 for Auto Discovery and configure an additional Delegated app to protect the planner data. Note: • If you use a service account for Auto Discovery, IBM Spectrum Protect Plus Online Services for Microsoft 365will use the service account to protect the Planner data regardless of whether that Delegated app is in place. • If you want to protect the Planner data in an MFA-enabled tenant with service account authentication for Auto Discovery, we recommend using a service account that does not have MFA enabled when configuring the Authentication Method to Scan/Manage Data field. Note: If you want to restore the Teams channel conversations as new posts to the channel, you must use service account authentication to scan Teams and configure a Microsoft Delegated app in your tenant. For details, refer to App Profile for a Microsoft Delegated App. Note that the authentication user of the delegated app must have the Teams license.. Note: If you are using a hybrid approach for backup and restore, the Private Channels' sites will be protected in the app context. Note: If you are using a multi-geo tenant, we recommend configuring a custom app profile. The Directory.ReadWrite.All permission is not automatically consented to the default app profile, but this permission 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.

Service Type	Recommended Method
Microsoft Teams Chat	Only app profile authentication is supported. You can register an IBM Spectrum Protect Plus Online Servicesdefault app for Microsoft 365 All permissions type for your tenant or you can configure a custom app. Microsoft Teams Chat service uses the Microsoft Graph Teams Export API to retrieve chat messages. If you are using your own custom app, you must request access to the Teams protected APIs and you will be billed for API consumption if the usage exceeds Microsoft's seeded capacity. Therefore, if you are using the IBM Spectrum Protect Plus Online Services default app, you may incur charges from IBM Spectrum Protect Plus Online Services as Microsoft begins charging for this API. For details, refer to this Microsoft article.
Public Folders	If you do not want to protect the metadata, app profile only is the best practice. Otherwise, we recommend the hybrid approach (use a service account for Auto Discovery and configure an app profile with proper permission in your tenant.) For the best practice of using app profile authentication to scan Public Folders, we recommend you configure the service account pool for Exchange Public Folders. IBM Spectrum Protect Plus Online Services for Microsoft 365 will automatically use these account pool users to run the backup.
Yammer	Only app profile authentication is supported. If you have protected the Microsoft 365 connected Yammer communities under Microsoft 365 Groups service, to protect them using the Yammer service, you need to have a Yammer app connected to your tenant. If your Yammer app is newly created, rerun the scan job to update the registration information for Yammer communities, and then go to the IBM Spectrum Protect Plus Online Services for Microsoft 365 to enable the Yammer backup service. Note: The authentication user for the Yammer app must have the Verified Admin role. The IBM Spectrum Protect Plus Online Services for Microsoft 365 job will start a new backup cycle for these Yammer communities in Yammer service, and their former backup data as Microsoft 365 Groups will not be removed as unprotected data. IBM Spectrum Protect Plus Online Services for Microsoft 365 will only delete this backup data until it expires the retention period.

- **Service Account Authentication**
  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.
- **App Profile Authentication**
  The easiest way to work with your environment is by registering an app profile. You can register the default IBM Spectrum Protect Plus Online Services app or use a custom app, which ensures that all Auto Discovery and IBM Spectrum Protect Plus Online Services for 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 Azure AD and can be revoked at any time.

Service Account Authentication

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.

To avoid getting throttled or blocked, you can configure an account pool. For details, refer to Manage the Account Pool.

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.

The Hybrid approach in IBM Spectrum Protect Plus Online Services for Microsoft 365 backup and restore jobs can be automatically triggered if you use service account authentication for Auto Discovery and have an app profile with proper permissions configured in your tenant.

Note: The hybrid approach requires using service account authentication for Auto Discovery.
In hybrid mode, IBM Spectrum Protect Plus Online Services for 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.

- **Manage the Account Pool**
  If you want to use the Microsoft 365 service account profile to scan objects in Auto Discovery and you have more than one Microsoft 365 service account, it is recommended that you configure account pools for all tenants in IBM Spectrum Protect Plus Online Services prior to running any backup jobs in IBM Spectrum Protect Plus Online Services for Microsoft 365.
- **Required Permissions of Service Account**
  When backing up and restoring the registered objects, make sure the accounts have the corresponding permissions.

Manage the Account Pool

If you want to use the Microsoft 365 service account profile to scan objects in Auto Discovery and you have more than one Microsoft 365 service account, it is recommended that you configure account pools for all tenants in IBM Spectrum® Protect Plus Online Services prior to running any backup jobs in IBM Spectrum Protect Plus Online Services for Microsoft 365.

About this task

An account pool can contain multiple Microsoft 365 accounts. With these accounts, IBM Spectrum Protect Plus Online Services for Microsoft 365 can back up a large amount of data simultaneously without causing throttling issues, and these accounts will be dynamically distributed when performing a backup job. If the

throttling issue occurs, the backup job will retrieve a new user from the account pool to continue with the backup. If the number of accounts does not satisfy the actual need, you can add users to the account pool. The users added to the account pool will be automatically distributed within 15 minutes.

Procedure

If you configured account pool for backup, ensure the Language Preference of all users in the account pool is the same as that of the service account:

1. Locate the users in Account Pool through the IBM Spectrum Protect Plus Online Services interface.
2. Go to SharePoint Admin > User profiles > Manage User Profile and find these users.
3. Select a user and then click Edit My Profile to update its **Language Preference**. Repeat the same operation for all users in the Account Pool and for the service account.
   For more instructions on managing an account pool, refer to Manage Microsoft 365 Account Pool.
   Note the following for how IBM Spectrum Protect Plus Online Services for Microsoft 365 leverages the service account and account pool, users

   - If the account pools are configured, IBM Spectrum Protect Plus Online Services grants the Site Collection Administrator permission to the group configured in the account pool when IBM Spectrum Protect Plus Online Services registers OneDrive for Business, SharePoint Online site collections, and Project Online site collections.
     Note: The account pool users used to protect the **Project Online** data must also have one of the following Project Online licenses: **Essentials**, **Project Plan 3** (formerly, **Professionals**), or **Project Plan 5** (formerly, **Premium**).
     If you are using app profile authentication to scan public folders and have a configured service account pool for Exchange Public Folders, the IBM Spectrum Protect Plus Online Services for Microsoft 365 job can automatically use the service account pool users to run the backup. The Exchange Online mailboxes and Microsoft 365 group mailboxes will be backed up and restored by the account that is used in the object registration.
   - If the account pools are not configured, the account that is used in the object registration will be used to back up and restore the SharePoint Online site collections, Project Online site collections, OneDrive for Business, Exchange Online mailboxes, and Microsoft 365 Groups.

Required Permissions of Service Account

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

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 for Business**	**SharePoint Administrator** role for object registration Note: The account pool users used to protect the Project Online data must have one of the following Project Online licenses: Essentials, Project Plan 3 (formerly, Professionals), or Project Plan 5 (formerly, Premium).	The backup and restore jobs only use the **Site Collection Administrator** permission for backing up and restoring the SharePoint Online site collections, Project Online site collection, and OneDrive for Business. If you want to restore the Managed Metadata Service, you must also ensure that the Term Store Administrator permission is in place. For details, refer to Restore Managed Metadata Service.
Exchange Online mailboxes	**Exchange Administrator** role	If your tenant has blocked access from apps that don't use modern authentication, you must also assign the **ApplicationImpersonation** permission manually to the role through the Exchange admin center. For details, refer to How to add permissions to an admin role in the Exchange admin center?
Public Folders	The 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 Editor** permission can assign **Reviewer** permission to others but cannot assign **Owner** permission to others.
Microsoft 365 Groups	The 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 backup and restore of the Microsoft 365 group team site only requires the **Site Collection Administrator** permission.
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.

App Profile Authentication

The easiest way to work with your environment is by registering an app profile. You can register the default IBM Spectrum® Protect Plus Online Services app or use a custom app, which ensures that all Auto Discovery and IBM Spectrum Protect Plus Online Services for 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 Azure AD and can be revoked at any time.

The **Microsoft Teams Chat** service is now available in the IBM Spectrum Protect Plus Online Services for Microsoft 365 interface to protect Teams chat messages for your tenant users. If you have a Microsoft 365 app with All permissions configured, you can re-authorize this app to update the permissions. For details, refer to Re-authorize the App for Microsoft 365; if you are using a custom app profile, you must manually update the permissions of your custom app in your Microsoft 365 tenant. For details on the required custom app permissions for Microsoft Teams Chat service, refer to the table in Required Permissions of Microsoft 365 App Profile.

If you use IBM Spectrum Protect Plus Online Services for **SharePoint Online**, **OneDrive for Business**, **Project Online**, **Exchange Online**, **Public Folders**, **Microsoft 365 Groups**, **Teams** or **MicrosoftTeams Chat** service, you need a Microsoft 365 app connected to your tenant. If you use the **Yammer** service, you need an app profile for Yammer.

The authentication user for the Yammer app must have the **Verified Admin** role; for the permissions required by Microsoft 365 app, refer to Required Permissions of Microsoft 365 App Profile.

Note: If you are using a multi-geo tenant, we recommend configuring a custom app profile. The Directory.ReadWrite.All permission is not automatically consented to the default app profile, but this permission 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.
To view the lists of data types that are supported or unsupported for each service type, refer to Appendices. For the permission requirements of an app profile for a specific service type, refer to the section below.

Required Permissions of App Profile

Refer to the table below for the API permission requirement. They are the API permissions that are automatically granted to the **IBM Spectrum Protect Plus Online Services Administration for Office 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 Spectrum Protect Plus Online Services for Microsoft 365services to protect different data types in your tenant.

If you are using custom app authentication, ensure your app has access to the protected APIs of Microsoft Teams. Otherwise, the public and private channels' 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 the IBM Spectrum Protect Plus Online Services Administration for Office 365.

Note: If your service contains not only the Microsoft 365 Groups or Teams, you will notice that the permissions required for Microsoft 365 Groups or Teams are sufficient to protect the SharePoint Online, OneDrive for Business, 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/OneDrive for Business	SharePoint Online	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 for Business, Groups, and Teams.
			Application Permission: TermStore.ReadWrite.All (Read and write managed metadata)	Back up and restore Managed Metadata Service.
		Microsoft Graph	Application Permission: Files.Read.All (Read files in all site collections)	Exclude the backup of the **Recordings** folder in OneDrive for Business.
Exchange Online/Public Folder	Exchange Online	Exchange	Application Permission: full_access_as_app (Use Exchange Web Services with full access to all mailboxes)	Back up and restore mailboxes.
Microsoft 365 Groups/Teams	All Permissions	SharePoint	Application Permission: Sites.FullControl.All (Have full control of all site collections)	Back up and restore site collections.

Service Type	App Profile Type	APIs	Permission	Why You Need
			Application Permission: User.ReadWrite.All (Read and write user profiles)	Back up and restore Microsoft 365 user profiles related information in OneDrive for Business, 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.
Microsoft 365 Groups/Teams	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	All Permissions	Microsoft Graph	Application Permission: Directory.ReadWrite.All (Read and write directory data)	Restore the region information of the Microsoft 365 Group or Team in a multi-geo tenant. Currently, the default app profile does not have this permission to consent. If you are using a multi-geo tenant, please configure a custom app profile.
			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.
			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	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 License Consumption Report.
			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.

Service Type	App Profile Type	APIs	Permission	Why You Need
			Application Permission: Files.Read.All (Read files in all site collections)	Back up teams' files.
			Application Permission: TeamsAppInstallation.ReadWriteForTeam.All (Manage Teams apps for all teams)	Back up and restore teams' apps.
			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.
Microsoft Teams Chat	All permissions	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.

Centralized Account Management

Account Management provides centralized management of groups and securities. Administrators can add and manage groups for security control of what users can restore in IBM Spectrum® Protect Plus Online Services for Microsoft 365. Security group allows you to organize users in IBM Spectrum Protect Plus Online Services for 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 Spectrum Protect Plus Online Services for Microsoft 365. You cannot remove this group or update its permissions. The security groups you created will be listed on the Account Management page. You can click the View button to view the details of a group, click the Edit button to update the group information and permissions, or click the Delete button to remove the group.

Note: The users who have been designated as service administrators of IBM Spectrum Protect Plus Online Services for Microsoft 365 will be automatically synchronized to the Administrators group. If the user is demoted from the IBM Spectrum Protect Plus Online Services for Microsoft 365 application administrator to a standard user, IBM Spectrum Protect Plus Online Services for Microsoft 365 will automatically remove this user from the Administrators group as well. If service administrators contain groups, you must manually add the groups into the Administrators group.

- **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.
- **Add Users to an Existing Group**
  You can directly add a set of users to an existing group to authorize the permissions that the group has been granted in IBM Spectrum Protect Plus Online Services for 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. In the Account Management interface, 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 box. The users and groups you grant permissions to must exist in your tenant and have license and permissions to access IBM Spectrum® Protect Plus Online Services for Microsoft 365.
4. In the Grant Permissions section, all service types are displayed in the list.
   a. Hover the mouse over the service type, and then click the Select Scope button.

b. Select the containers for the selected service type. To select all containers for this service type, select the Container option in the column header.
c. Click Save to save the permission scope for the service type; click Cancel to go back without saving.
The containers you selected will be displayed in the Permission Scope column for the selected service type.

5. Select the services that you want to grant restore permissions to. The users of this group can run restore jobs for the containers in the permission scope of the selected services.
6. Click Save to save your configurations; click Cancel to exit the creation.

Add Users to an Existing Group

You can directly add a set of users to an existing group to authorize the permissions that the group has been granted in IBM Spectrum® Protect Plus Online Services for Microsoft 365.

Procedure

1. In the Account Management interface, click Grant User Permissions.
2. In the right pane for granting user permissions, enter users and groups that you want to grant permissions to in IBM Spectrum Protect Plus Online Services for Microsoft 365. The users and groups you grant permissions to must exist in your tenant and have license and permissions to access IBM Spectrum Protect Plus Online Services for Microsoft 365.
3. Select an existing group that you want to add the users to from the Select Group list. The services and permission scopes of the selected group will be automatically displayed in the table.
4. Click Save to save your configurations; click Cancel to exit without saving.

Select the Objects You Want to Back Up

When you log into IBM Spectrum® Protect Plus Online Services for Microsoft 365 for the first time, the Backup Objects Selection page will appear to ask you to select the objects to back up.

About this task

Note: If your organization has a Multi-Geo license, the users assigned to multiple regions in IBM Spectrum Protect Plus Online Services will need to select a region. The users with only one region will be automatically redirected to that regional IBM Spectrum Protect Plus Online Services for Microsoft 365 instance.
Note: With the trial license, you can only enable or disable the backup service for each object type. The backup scope cannot be changed with the backup service enabled. To update your license, you can contact IBM Software Support.

Procedure

1. n the Backup Objects Selection page, click Mailbox, OneDrive for Business, Site Collection, Microsoft 365 Group, Teams, Project Online, and Public Folders to navigate through all backup object types and define the backup scope for each object type. By default, the backup service for each object type is enabled. You can disable the backup service by turning off the switch.
2. With the backup service enabled, select the containers that you want to back up. Select the Select All option to select all containers in the backup scope, which will automatically include the objects registered later.
   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.

   Note the following:
   - IBM Spectrum Protect Plus Online Services for Microsoft 365 only protects the published workflow definitions. The running workflows will not be restarted once the restore is complete.
   - The first backup job that starts a new backup cycle for SharePoint Online site collections, Project Online site collections, OneDrive for Business objects, and Microsoft 365 group team sites will include the last 50 versions for the items or documents in the backup; the other backup jobs will include the last 10 versions for the items or documents in the backup.
   - If a site collection URL has been changed after the backup, IBM Spectrum Protect Plus Online Services for Microsoft 365 will perform a full backup on this site collection as it will be regarded as a new site, and the previous backup data can only be used for an out of place restore. For details, refer to What if my site collection URL has been updated after backup?

3. When you finish selecting the objects to back up, you can:
   - Click Save and Run Now to save the configurations and start the backup jobs, if you are using a default storage location.
   - Click the Next button, if you have a custom storage location. The Storage Location Configuration page appears. Configure the storage information and click Validation Test to test whether the entered information is valid. If successful, click Save and Run Now to save the configurations and start the backup jobs.
     Note: If you purchased the backup service from a partner, first turn on the Use my own storage button, and then configure your custom storage location.
     If you are about to use your own Microsoft Azure storage account, you need to first add the IBM Spectrum Protect Plus Online Services IP addresses to your Azure storage account firewall and configure the firewall to allow IBM Spectrum Protect Plus Online Services agent servers to run on a dedicated ARM Vnet subnet to access your storage location. For details, refer to Allow IBM Spectrum Protect Plus Online Services Agent Servers to Access Your Storage Account.

Note: After you click Save and Run Now, the backup job for an object type will not start if the backup service for this object type is disabled.

Monitor Your Backup

On the **Home** page, you can view the backup or restore details through the **MORE DETAILS** link for each object type. The **Backup Details** will display the last four backup records, the number of successful, skipped, and failed objects in each job, and the progress of the running backup or the time to run the next backup. You can click the **View Details** link in **Job Summary** to go to the **Job Monitor** page to generate and download the job report.

Procedure

To view backup job details and generate a backup job report, follow the steps below:

1. Go to the **Home** page, click the MORE DETAILS link in the **Exchange Online**, **OneDrive for Business**, **SharePoint Online**, **Microsoft 365 Groups**, **Teams**, **Project Online**, or **Public Folders** section. A pane that displays the backup and restore details appears.
   Note: If a Warning icon appears, which indicates your last backup job for an object type meets one of the scenarios listed in this note, you need to pay attention, and you can choose to manually run a backup.
2. In the **Backup Details** tab, the last four backup jobs are listed.
   Note: If a backup job is currently running, you can click Details on the tile. The **Backup Job In Progress** pane will open on the right, and you can view the job progress and the backup status of objects in the backup scope. If the job is not completed within 24 hours, a message bar will appear on the top of this pane. Click the link in the message to go to the **Job Analytics** page to view the detailed job progress. For details, refer to Use the Job Analytics Report.
3. Click the status of the job to view its summary. The **Job Summary** displays the total number of objects that are backed up in this job and the number of successful, skipped, and failed objects. Click View Details to navigate to the **Job Monitor** page for generating and downloading the job report. For detailed instructions on generating and downloading a job report, refer to Generate and Download a Job Report.
   Note: The backup job will not back up the SharePoint Online site collections that have not had any changes made since the last backup.
   Note: The failed objects in the backup job for OneDrive for Business, SharePoint 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. If the backup for the failed objects continues to fail in the next two incremental backup jobs, they will not be backed up again; the failed objects in the backup job for Exchange Online 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 failed objects have been modified before the next incremental backup job, they will not be regarded as the failed objects and will be included in the next incremental backup job.
4. On the right pane of the **Backup Details** tab, the information about the running backup or the next backup will be displayed.
   - If there is a running backup job, **Progress of the Running Job** shows the progress of the job that is running. Click View Details to navigate to the **Job Monitor** page, and then click Expand All to view the detailed information about this job.
   - If there is not a running backup job, the time to run the next backup job is displayed.

Manually Run a Backup

The backup jobs for Exchange Online, OneDrive for Business, SharePoint Online, Microsoft 365 Groups, Teams, Project Online, and Public Folders can be run manually in case some of the data failed to be backed up in the last backup job.

Procedure

To run a backup manually, follow the steps below:

1. Click the MORE DETAILS link in the object section with a Warning icon. A pane that displays the backup and restore details appears.
   Note: The Warning icon appears when the last backup job for an object type meets one of the following scenarios:
   - A top container-level object fails to be backed up, including the site collection in SharePoint Online, Project Online, and OneDrive for Business, mailbox in Exchange Online, group team site, and group mailbox in Microsoft 365 Groups/Teams, and the public folders.
   - More than 5% of objects of a container level apart from the top container level objects fail to be backed up.
   - More than 10% of objects of a content level fail to be backed up.
   - The last backup job's status is **Failed**.
2. Click start a new backup again to start a new backup job to protect your data. You can view the details about the backup job in progress by clicking Details in this object section.

Configure Alerts

With IBM Spectrum® Protect Plus Online Services for Microsoft 365, you can define certain statuses of backup and restore jobs (including data exporting) which will trigger alerts.

Procedure

To configure alert settings, follow the steps below:

1. In the left pane, click Notification Settings. The **Notification Settings** page will be displayed on the right pane.
2. 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 Spectrum Protect Plus Online Services for Microsoft 365.

b. **Send the email notifications for the jobs in the following status** – Select the job status (Finished, Finished with exception, or Failed), which will trigger the notification. When the job completes with the selected status, the email notification will be sent to the email addresses that you configured in the last step.

3. If you have a separate team to manage the export and restore jobs, you can select the **Customize the notification for the restore and export jobs** option and then configure the recipients who will receive the email notification, particularly for the restore and export jobs of specific statuses.
4. Click Reset if you want to reset the settings.
5. Click Apply when finished configuring the settings. The notification settings will take effect immediately.

Change the Backup Scope

After you get started, you can make changes to the objects you want to back up for Exchange Online, OneDrive for Business, SharePoint Online, Microsoft 365 Groups, Teams, Project Online, and Public Folders. 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.

Before you begin

The backup scope cannot be changed with the trial license. To update your license, you can contact IBM Software Support.

Procedure

To change the backup scope, follow the steps below:

1. Click the Settings button in the upper-right corner of the **Exchange Online**, **OneDrive for Business**, **SharePoint Online**, **Microsoft 365 Groups**, **Teams**, **Project Online**, or **Public Folders** section of the **Home** page, and then click Change Backup Scope from the drop-down list. The **Change Backup Scope** pane appears.
2. With the backup service enabled, select the containers that you want to back up. You can select the Select All option to select all containers in the backup scope, which will automatically include the objects registered later.
   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.

3. Click Apply 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 **Home** page without saving any changes.
   Note: 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.
   Note: 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 Spectrum® Protect Plus Online Services for 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.

Procedure

1. Click the Settings button in the upper-right corner of the **Exchange Online**, **OneDrive for Business**, **SharePoint Online**, **Microsoft 365 Groups**, **Teams**, **Project Online**, or **Public Folders** section of the **Home** page, and then click **Edit Backup Frequency** from the drop-down list. The **Backup Frequency** pane appears.
2. Select a number from the How many backup jobs would you like to run per day? list. IBM Spectrum Protect Plus Online Services for Microsoft 365 will automatically provide the job schedule according to the frequency you selected.
3. You can change the start time for the first backup job. The rest of the schedules will be automatically calculated and displayed.
4. Click Apply 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 **Home** page without saving any changes.

Manage Your General Settings

In **General Settings**, you can configure the settings for the backup job and restore job, as well as view and manage the storage settings. If you have purchased the license to use your own storage, you can update the default storage provided by IBM Spectrum® Protect Plus Online Services to your own storage in the **Storage Location** tab.
Note: The default storage location information cannot be modified, and the custom storage path cannot be changed once saved.

- **Configure Additional Backup Settings**
- **About the Restore Thread**
- **Manage Your Storage**
- **Configure Retention Policy**
  Either using the IBM Spectrum Protect Plus Online Services default storage or your own storage, the data retention settings can be applied to your backup data to help save your storage costs.
- **Disable a Backup**
  The backup service for Exchange Online, OneDrive for Business, SharePoint Online, Microsoft 365 Groups, Teams, Project Online, or Public Folders 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.
- **Export Encryption Key**
  This feature is only available for administrators of the IBM Spectrum Protect Plus Online Services tenant. The Support account that you established for troubleshooting will not be able to access the **Encryption Key** tab.
- **Configure End-User Restore Settings**
  If you have a BYOS subscription and are using Azure storage, you can go to Settings > > End-User Restore Settings page to configure to allow end users of IBM Spectrum Protect Plus Online Services Recovery Portal in your tenant to restore the backup data in the archive tier. The **End-User Restore Settings** feature is only available to your application administrators or the service provider.

Configure Additional Backup Settings

The **Backup Settings** tab displays the encryption profile that is used to encrypt the backup data, and you can configure the following:

Include specific mailbox folders (Deleted Items and Junk Email)

Select the special mailbox folders that you want to back up for the mailboxes. You can select the Deleted Items option and the Junk Email option to include these folders in the backup. Keeping these options unchecked can help to improve job performance.

Back up Private Channels

Select whether to back up private channels in Microsoft Teams. You can configure an app profile to connect your tenant for a successful backup of private channels, or the service account you use must be an **owner** of all current and future private channels. The Auto Discovery scan job can 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 Manage Scan Profile.

Back up item and file versions

Select whether to back up the item and file version. 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. To limit the number of backup versions, deselect the **Back up item and file versions** option. With this option selected, the backup job will include the most recent 10 versions by default.

Back up Recordings folder

As updated by Microsoft for Microsoft Teams, all new Teams meeting recordings will be saved to OneDrive for Business and Share Point. (The change from using Microsoft Stream to OneDrive for Business 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 for Business (user's *OneDrive for Business/Recordings*) or the Recordings folder in the Documents library of the Teams channel (*Teams channel site/Documents/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 license 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 for Business, to exclude the **Recordings** folder from the OneDrive for Business 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 Spectrum® Protect Plus Online Services for Microsoft 365.
- Deleting a public channel from Teams will not delete the connected site. The backup service cannot identify these kinds of sites as they were connected to the deleted public channels. Therefore, even if you deselected the **Back up Recordings folder** option, the backup job will still include the Recordings folder in the backup.

- (API limitation) In the app context (using app profile authentication or the hybrid mode), the backup service for OneDrive for Business 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 with the following message: The recordings created after you disable this option won't be captured.

Back up Public Folder Metadata (Every two weeks)

Select whether to back up Public Folder metadata. If you select the **Back up Public Folder Metadata** checkbox, the job that backs up metadata will run every two weeks, and the job details will be displayed in **Job Monitor**.

Public Folder metadata refers to the settings in the following categories: **general**, **statistics**, **limits**, **general mail properties**, **email address**, **member of**, **delivery options**, and **mail flow settings**. For details, go to **Microsoft 365 Exchange Online admin center -public folders**.

Enable super users to decrypt the files protected by Information Rights Management (IRM)

Select whether to enable super users who have access to the Information Rights Management (IRM) protected files to encrypt these files in the backup.

- With super user configured, these files will be decrypted during the backup, and the decrypted files will be restored without protection enabled, accessible to anyone with access rights to the destination. To use this feature, you must at first create a new service principal for connecting the Azure Rights Management service. You will get the **AppPrincipalId** and **Symmetric Key** and then add the service principal to the super user list. For detailed instructions, refer to Configuring Super Users.
- If the **Enable super users to decrypt the files protected by Information Rights Management (IRM)** option is not selected, these files will not be decrypted during the backup, and the files restored to the destination will still be protected by IRM and only accessible to the users who have permissions to the files in the source.

- **Configuring Super Users**
  You can create a service principal and configure the service principal as a super user.

Configuring Super Users

You can create a service principal and configure the service principal as a super user.

Procedure

1. To create a service principal from the MSOnline PowerShell module for Azure Active Directory, complete the steps below:
   a. Locate and right-click Windows PowerShell on your server.
   b. Select Run as administrator.
   c. If the MSOnline PowerShell module is not installed on your server, enter **`Install-Module MSOnline`** and then press Enter.
   Note: Go to the next step directly if the MSOnline PowerShell module is installed on your server.
   d. Enter **`Connect-MsolService`** and then press Enter to connect to Azure Active Directory. A pop-up window appears.
   e. Enter the credentials of your Azure Active Directory tenant administrator in the pop-up window. Typically, use an account that is a global administrator for Azure Active Directory or Microsoft 365.
   f. Enter `New-MsolServicePrincipal -DisplayName AzureRMSProtectionServicePrincipal -AppPrincipalId 'GUID'` and then press Enter to create a service principal. Replace **GUID** with a GUID that has not been used as the App principal ID. You can also replace the **`AzureRMSProtectionServicePrincipal`** with a display name you like, if necessary.
   Note: Do not use the **`New-AzureADServicePrincipal`** command to create the service principal since the Azure Rights Management service doesn't support **`New-AzureADServicePrincipal`**.
   g. The symmetric key (in the first line), App principal ID, and the other information are displayed.
   h. Take a note of the symmetric key and App principal ID that will be used later.
   Note: If you forget the symmetric key and App principal ID later, you have to create a service principal again.
2. To configure the service principal as a super user, complete the steps below:
   Note: If the Rights Management administration module is not installed on your server, refer to Installing the AIPService PowerShell module to install the module.
   a. Locate and right-click Windows PowerShell on your server.
   b. Select Run as administrator.
   c. Enter **`Install-Module -Name AIPService`** and then press Enter to install the AIPService module
   d. Enter **`Connect-AipService`** and then press Enter to connect to the Azure Information Protectionservice. A pop-up window appears.
   e. Enter the credentials of your Azure Active Directory tenant administrator in the pop-up window. Typically, use an account that is a global administrator for Azure Active Directory or Microsoft 365.
   f. Enter **`Enable-AipServiceSuperUserFeature`** and then press Enter to enable the super user feature for your organization's Azure Information Protection service.
   g. Enter **`Add-AipServiceSuperUser -ServicePrincipalId ID`** and then press Enter to add the service principal to the super user list for your organization. Replace the ID with the App principal ID retrieved in step 1.
   h. Enter **`(Get-AipServiceConfiguration).BPOSId`** and then press Enter to get the tenant ID.
   i. The tenant ID is displayed. Take a note of the tenant ID.

About the Restore Thread

Restore jobs automatically use multiple threads to help optimize job performance.

Multiple threads can improve the performance, but the following issue requires your attention:

- The **Modified** and **Modified By** properties will be lost for the major versions if the latest version to restore is a minor version.

Manage Your Storage

In the **Storage Location** tab, 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 by purchasing an extended retention period under your license agreement.

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

- Default storage location – The default storage location is hosted by IBM Spectrum® Protect Plus Online Services for Microsoft 365 Azure Blob Storage and cannot be modified. If you want to use your own storage, contact IBM Software Support to update your license. The default storage location resides in the same Azure Data Center that was selected during your registration to IBM Spectrum Protect Plus Online Services for Microsoft 365. For Multi-Geo license customers, the default storage locations are distributed according to the data center mappings.
  Note: If you are using default storage for Multi-Geo and you want to apply custom storage for only a few regions, while others are still using default storage, you can change the storage information once for each region. After you have updated the default storage to your own storage, you cannot change the storage to another device anymore or change it back to the default storage.
- Custom storage location – If your license has BYOS enabled, you can configure a custom storage location for all service types or configure separate storage for each service type to store your data, in accordance to your license agreement.
  The storage information, apart from its path information, can be modified.

- Click Validation Test to test whether the entered information is valid after modifying the information. If successful, click **Apply** to apply the storage settings.

  If you are using your own Microsoft Azure storage account, note the following:
  - 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 Spectrum Protect Plus Online Services for Microsoft 365 tenant for the best network performance.
  - Before you add the Azure storage account to the IBM Spectrum Protect Plus Online Services for Microsoft 365, you must first add the IBM Spectrum Protect Plus Online Services IP addresses to your Azure storage account firewall and configure the firewall to allow IBM Spectrum Protect Plus Online Services agent servers running on a dedicated ARM Vnet subnet to access your storage location. For details, refer to Allow IBM Spectrum Protect Plus Online Services agent servers to Access Your Storage Account.
  - IBM Spectrum Protect Plus Online Services for Microsoft 365 can automatically store your backup data to the Azure storage cool tier to help conserve storage costs. The supported Azure account kinds are **StorageV2** and **BlobStorage** of **Standard** performance type.
  - 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 Spectrum Protect Plus Online Services for Microsoft 365. Currently, you can only append one additional storage account, and this is only available for BYOS customers on Azure. After saving the new storage location, the new storage will be used to store backup data for the further incremental backup jobs and restore jobs. Cloud Backup services will no longer write to the legacy storage location.

- **Allow IBM Spectrum Protect Plus Online Services 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.
- **Change Storage Location**
- **Storage Information**

Allow IBM Spectrum Protect Plus Online Services 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.

About this task

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 Spectrum Protect Plus Online Services for Microsoft 365 can access your storage, complete the settings as required in the following conditions:
Note: If you are using a trial license and the storage account you want to use in the trial has a firewall enabled, read the conditions below and contact IBM Software Support for the corresponding reserved IP addresses or ARM VNet IDs.

- If you are using a storage type other than Microsoft Azure 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.
- 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 Spectrum Protect Plus Online Services or your storage account is in its** paired region, you must add the Azure Resource Manager (ARM) vNet subnets where the IBM Spectrum Protect Plus Online Services agents are running on to your storage networking. You can find additional details in this Microsoft article: Grant access from a virtual network, and contact the IBM Software Support to get the subnet ID of IBM Spectrum Protect Plus Online Services for Microsoft 365 products for your data center. For detailed instructions, refer to Step 7.
  - **Other than the condition above**, you need to add all the reserved IP addresses to the Azure storage firewall. For details, refer to below steps.

Procedure

To add reserved IP addresses and ARM virtual networks, complete the following steps:

1. Navigate to **IBM Spectrum Protect Plus Online Services for Microsoft 365** interface > Advanced Settings > Reserved IP Addresses to download the list of reserved IP addresses of IBM Spectrum Protect Plus Online Services. For details, refer to Download a List of Reserved IP Addresses.
2. Go to the storage account that you want to secure.
3. Select Networking on the menu.
4. Check that you've selected to allow access from Selected networks.
5. Enter the IP address or address range under Firewall > Address Range.
6. Select Save to apply your changes.
7. To grant access to a subnet in a virtual network belonging to another tenant, use PowerShell, CLI, or REST API.

```
## Contact IBM Software Support team to get the IBM Spectrum Protect Plus Online Services for Microsoft 365 products
network subnet resource ID
$SUBNETID="/subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-
yyyyyyyyyyyy/resourceGroups/ResrouceGroupName/providers/Microsoft.Network/virtualNetworks/VIrtualNetworkName/subnets
/SubnetName"

$DESTRG="customer_resource_group_name"
$DESTSTA="customer_storage_accont_name"


####
## Use the Azure cli tool (https://docs.microsoft.com/en-us/cli/azure/install-azure-cli?view=azure-cli-latest)
##
## Add the firewall virtual network rule to grant access to IBM Spectrum Protect Plus Online Services for Microsoft
365
az storage account network-rule add --resource-group $DESTRG --account-name $DESTSTA --subnet $SUBNETID
az storage account network-rule list --resource-group $DESTRG --account-name $DESTSTA --query virtualNetworkRules
## (Optional) Disable the public access to storage account
az storage account update --resource-group $DESTRG --name $DESTSTA --default-action Deny
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)
##
Add-AzStorageAccountNetworkRule -ResourceGroupName $DESTRG -Name $DESTSTA -VirtualNetworkResourceId $SUBNETID
Get-AzStorageAccountNetworkRuleSet -ResourceGroupName $DESTRG -AccountName $DESTSTA
```

You will see the virtual network rules in Azure Portal. 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.

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 license and then complete the following steps. Otherwise, IBM Spectrum® Protect Plus Online Services for Microsoft 365 will continue to store data to the IBM Spectrum Protect Plus Online Services-hosted default storage.

Procedure

1. In the **Storage Location** tab, 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 Spectrum Protect Plus Online Services storage until the retention time expires** – The backup data in the default storage location will be retained until the retention time expires. 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 Spectrum Protect Plus Online Services 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 your license 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.
   - 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 Location** tab will display the configurations.
   - If you are using the Microsoft Azure Blob storage and facing the upper limit of your storage account, you can now append an additional storage account of Microsoft Azure Blob Storage for backup and restore.

   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 Spectrum Protect Plus Online Services for Microsoft 365 will no longer write to the legacy storage location. For details on storage configuration, refer to Microsoft Azure Blob Storage.

4. Configure the storage information. For details of configuring storage information, refer to Storage Information. Click Validation Test to test whether or not 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 Spectrum Protect Plus Online Services 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 license 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 Spectrum Protect Plus Online Services 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.
   - If your license 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 Spectrum® Protect Plus Online Services will store your backup data to the S3 Standard storage class automatically. You can move the backup data from S3 Standard to S3 Standard-IA®, S3 One Zone-IA, or S3 Intelligent-Tiering, and IBM Spectrum Protect Plus Online Services for 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 Spectrum Protect Plus Online Services for Microsoft 365 cannot access the archived data in your Amazon S3 storage.
- **Amazon S3-Compatible Storage**
  You can configure Amazon S3-compatible storage.
- **IBM Cloud Object Storage**
  You can configure IBM Cloud® Object Storage.
- **IBM Spectrum Protect Server S3**
  You can configure IBM Spectrum Protect Server S3 storage.
- **Microsoft Azure Blob Storage**
  You can configure Microsoft Azure Blob Storage.
- **FTP**
  You can configure File Transfer Protocol (FTP) storage.
- **SFTP**
  You can configure Secure File Transfer Protocol (SFTP) storage.
- **Dropbox**
  You can configure storage on the Dropbox file hosting service.

Amazon S3

IBM Spectrum® Protect Plus Online Services will store your backup data to the S3 Standard storage class automatically. You can move the backup data from S3 Standard to S3 Standard-IA®, S3 One Zone-IA, or S3 Intelligent-Tiering, and IBM Spectrum Protect Plus Online Services for 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 Spectrum Protect Plus Online Services for 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: 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.
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 West (Oregon)
   - EU (Frankfurt)
   - Asia Pacific (Tokyo)
   - Asia Pacific (Mumbai)
   - US East (Ohio)
   - Canada (Central)
   - EU (London)

- Asia Pacific (Sydney)
- South America (Sao Paulo)
- US West (Northern California)
- EU (Ireland)
- Asia Pacific (Singapore)
- Asia Pacific (Seoul)

6. **Advanced** – Enter the following extended parameters in **Advanced** 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.
   - **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 2147483646. For example, RetryCount=6 represents when the network connection is interrupted, it can reconnect at most 6 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.
   - **enablessl=true** – Configure to enable SSL for the backups stored on this physical device. By default, IBM Spectrum Protect Plus Online Services for Microsoft 365 will use HTTPS communication to access Amazon S3 storage if you have not configured this parameter yet.
   - **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.
7. **Retain the Data for** – Configure the number of years for data retention. Enter a number into the box.
8. Click Validation Test to verify that the information you entered is correct.

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.
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. **Advanced** – Enter the following extended parameters in **Advanced** 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.
   - **SignatureVersion** – By default, IBM Spectrum® Protect Plus Online Services for 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.
   - **RetryCount** – Customize the reconnection times after the network connection is interrupted. Enter any positive integer between 0 and 2147483646. For example, RetryCount=6 represents when the network connection is interrupted, it can reconnect at most 6 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.
7. **Retain the Data for** – Configure the number of years for data retention. Enter a number into the box.
8. Click Validation Test to verify that the information you entered is correct.

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 `Bucket name` must consist of only lowercase letters.
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. **Advanced** – Enter the following extended parameters in **Advanced** 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.
   - **SignatureVersion** – By default, IBM Spectrum® Protect Plus Online Services for 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.
   - **RetryCount** – Customize the reconnection times after the network connection is interrupted. Enter any positive integer between 0 and 2147483646. For example, RetryCount=6 represents when the network connection is interrupted, it can reconnect at most 6 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.
7. **Retain the Data for** – Configure the number of years for data retention. Enter a number into the box.
8. Click Validation Test to verify that the information you entered is correct.

IBM Spectrum Protect Server S3

You can configure IBM Spectrum Protect Server S3 storage.

Procedure

Follow the instructions below:

1. **Storage Type** – Select IBM Spectrum Protect Server S3 from the drop-down list.
2. **Bucket name** – Enter the bucket name you wish to access.
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. **Advanced** – Enter the following extended parameters in **Advanced** 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.
   - **SignatureVersion** – 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.
   - **RetryCount** – Customize the reconnection times after the network connection is interrupted. Enter any positive integer between 0 and 2147483646. For example, RetryCount=6 represents when the network connection is interrupted, it can reconnect at most 6 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.
7. **Retain the Data for** – Configure the number of years for data retention. Enter a number into the box.
8. Click Validation Test to verify that the information you entered is correct.

Related information

- IBM Spectrum Protect server S3 agent

Microsoft Azure Blob Storage

You can configure Microsoft Azure Blob Storage.

Before you begin

Before adding the storage account to the IBM Spectrum® Protect Plus Online Services for Microsoft 365 interface, ensure IBM Spectrum Protect Plus Online Services agents have access to your storage. For details, refer to Allow IBM Spectrum Protect Plus Online Services Agent Servers to Access Your Storage Account.

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. **Advanced** – Enter the following extended parameters in **Advanced** 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.
   - **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 2147483646. For example, RetryCount=10 represents when the network connection is interrupted, it can reconnect at most 10 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.
8. **Retain the Data for** – Configure the number of years for data retention. Enter a number into the box.
9. Click Validation Test to verify that the information you entered is correct.

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 Spectrum Protect Plus Online Services for 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 Spectrum Protect Plus Online Services for 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. **Advanced** – Enter the following extended parameters in advanced settings 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:
   - **FtpType=win03** – Whether or not the FTP is the FTP in the Windows 2003 operating system.
   - **IsRetry** – Whether or not to try again when Cloud Backup failed to write the data in the physical device.
     - If you enter **IsRetry=true**, it will try again when Cloud Backup failed to write the data in the physical device.
     - If you enter **IsRetry=false**, it will not try again when Cloud Backup 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.

- **RetryCount** – Customize the reconnection times after the network connection is interrupted. You are allowed to enter any positive integer between 0 and 2147483646. For example, RetryCount=60 represents when the network connection is interrupted, it can reconnect at most 60 times.
  If you do not configure this parameter, the value is 6 by default.

7. **Retain the Data for** – Configure the number of years for data retention. Enter a number into the box.
8. Click Validation Test to verify that the information you entered is correct.

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. **Password** – Enter the corresponding password of the user used to access the root folder.
7. **Private key file** – If the SFTP server supports the private key file, click Browse to upload a private key file.
8. **Private key file password** – Enter the corresponding password of the uploaded private key file.
9. **Advanced**– Enter the following extended parameters in advanced settings 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:
   - **FtpType=win03** – Whether or not the FTP is the FTP in the Windows 2003 operating system.
   - **IsRetry** – Whether or not to try again when Cloud Backup failed to write the data in the physical device.
     - If you enter **IsRetry=true**, it will try again when Cloud Backup failed to write the data in the physical device.
     - If you enter **IsRetry=false**, it will not try again when Cloud Backup 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.
   - **RetryCount**– Customize the reconnection times after the network connection is interrupted. You are allowed to enter any positive integer between 0 and 2147483646. For example, RetryCount=60 represents when the network connection is interrupted, it can reconnect at most 60 times.
     Note: If you do not configure this parameter, the value is 6 by default.
10. **Retain the Data for** – Configure the number of years for data retention. Enter a number into the box.
11. Click Validation Test to verify that the information you entered is correct.

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. **Advanced -** Enter the following extended parameters in advanced 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.
   - **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 2147483646. For example, RetryCount=10 represents when the network connection is interrupted, it can reconnect at most 10 times.
     If you do not configure this parameter, the value is 6 by default.

5. **Retain the Data for** – Configure the number of years for data retention. Enter a number into the box.
6. Click Validation Test to verify that the information you entered is correct.

Configure Retention Policy

Either using the IBM Spectrum® Protect Plus Online Services 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

Once there is backup data approaching the retention period, your administrator group or partner's 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 your IBM Spectrum Protect Plus Online Services Account Manager to update your license 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 Spectrum Protect Plus Online Services 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 the Data Export Service.
- If your license 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.

If you changed storage from the default IBM Spectrum Protect Plus Online Services 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 license or the default IBM Spectrum Protect Plus Online Services storage with an unlimited retention license, the retention policy supports being configured at container level for each service type. Note that the default retention period for BYOS license 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.

From March 2022 release, you can configure a retention period that is less than one year (from 30 to 365). To enable the day unit retention policy, contact IBM Software Support for assistance.
Note:

- The day unit retention policy currently does not support customization at the container level and is not applicable to SharePoint apps, the channel conversations and settings in Teams, and the Yammer messages.
- 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.
- 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 license. You need to go to the IBM Spectrum Protect Plus Online Services for 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 > General Settings > Retention Policy.
2. You can update the number in the **Retain the data for _ years** field to apply a default retention period for your backup data of all service types. If you would like to customize the retention policy for each service, select the Use a custom retention policy for each service option.
   Note: If your data retention in the purchased license is between 2 to 10 years, the retention period you can set for the retention policy is up to your purchased retention years. For example, if your data retention in the license is 3 years, you can select 1, 2, or 3 from the drop-down list of this field as the retention period.
3. With the Use a custom retention policy for each service option selected, all the enabled service types are displayed.
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.
6. You can update the default retention period for the service type and update the number under the **Retention Period** column in the table for a specific container. **20** is now an available option.
7. Click Apply 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 **Retention Policy** page to update the settings.

Disable a Backup

The backup service for Exchange Online, OneDrive for Business, SharePoint Online, Microsoft 365 Groups, Teams, Project Online, or Public Folders 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. On the **Home** page, click the settings button and click Change Backup Scope from the drop-down list in the Exchange Online, OneDrive for Business, SharePoint Online, Microsoft 365 Groups, Teams, Project Online, or Public Folders section. The Change Backup Scope pane appears.
2. Turn off the switch to disable the backup service.
3. Click Apply and click OK to confirm your operation.

Export Encryption Key

This feature is only available for administrators of the IBM Spectrum® Protect Plus Online Services tenant. The Support account that you established for troubleshooting will not be able to access the **Encryption Key** tab.

By default, this page is not available to the users who are using default storage hosted by IBM Spectrum Protect Plus Online Services. You can contact the IBM Software Support team to enable this feature if needed.

The backup data generated by IBM Spectrum Protect Plus Online Services for Microsoft 365 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 Spectrum Protect Plus Online Services for Microsoft 365 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.

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 after the last time you generate the key, click Regenerate to regenerate the key for the updated backup data and download the file again.

Configure End-User Restore Settings

If you have a BYOS subscription and are using Azure storage, you can go to Settings > > End-User Restore Settings page to configure to allow end users of IBM Spectrum® Protect Plus Online Services Recovery Portal in your tenant to restore the backup data in the archive tier. The **End-User Restore Settings** feature is only available to your application administrators or the service provider.

By default, the switch is off. To allow all IBM Spectrum Protect Plus Online Services Recovery Portal users to restore backup data in the archive tier, turn this switch on. The restore job will at first rehydrate the backup data sets in archive tier for restore. Therefore, the restore job may take longer and you may notice an additional charge. For more details, refer to this Microsoft article: Azure Blob storage: hot, cool, and archive access tiers .

Note: If your subscription was updated to use IBM Spectrum Protect Plus Online Services 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 Spectrum Protect Plus Online Services for Microsoft 365 interface instead.

Export and Download Your Data

IBM Spectrum® Protect Plus Online Services for Microsoft 365 helps you export and download your backup data for Exchange Online, SharePoint Online, OneDrive for Business, Microsoft 365 Groups, Project Online, Public Folders, and Teams.

After you export your data, you can go to the Job Monitor to download the exported data to a local location. By default, you can export up to **100 GB of data per month for all services in total**. The exported data must be downloaded within seven days; otherwise, the data will be removed. This quota limitation also applies to the BYOS license.

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.

You can export data from Azure archive storage if you are using IBM Spectrum Protect Plus Online Services default storage.

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 Alerts.

- **Export Exchange Online Data**
  With IBM Spectrum Protect Plus Online Services for 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.
- **Export SharePoint Online Data**
  With IBM Spectrum Protect Plus Online Services for Microsoft 365, you can export the backup data for SharePoint Online lists, libraries, folders, documents, and items.
- **Export OneDrive for Business Data**
  With IBM Spectrum Protect Plus Online Services for Microsoft 365, you can export the backup data for the OneDrive for Business libraries, folders, and documents.
- **Export Microsoft 365 Groups Data**
  With IBM Spectrum Protect Plus Online Services for 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.
- **Export Project Online Data**
  With IBM Spectrum Protect Plus Online Services for Microsoft 365, you can export the backup data of projects, libraries, lists, folders, items, and documents in a Project Online site.
- **Export Teams Data**
  With IBM Spectrum Protect Plus Online Services for Microsoft 365, you can export the backup data of Teams files or conversations.
- **Export Teams Chat Messages**
- **Export Yammer Data**
  You can export folders and files from the Yammer site and export the Yammer messages. You can only find the Yammer messages through time-based

restore wizard (drill down a backup job). For detailed information on supported data types, refer to Restore Options for Different Object Types.

- **Download the Exported Data**
- **Get Password**
  You can get a password to extract downloaded content. Only the user who started the export job and the email recipients designated for the restore and export job can get the password through Job Monitor.

Export Exchange Online Data

With IBM Spectrum® Protect Plus Online Services for 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.

Procedure

Complete the steps below to export Exchange Online backup data:

1. Click the Restore tab on the left pane, and then click the Exchange Online button.
2. Select the items that you want to export. You can choose one of the following methods to find the data to export:
   - Define a mailbox as the search scope and then use the Advanced Search feature to search for the items within the mailbox. Refer to the steps below:
     - 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.
     - To change the search conditions, click Advanced Search to expand this field.
     - 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.
     - 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.
     - 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.
     - 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.
   - 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.
     - Click the Find the items in the specific backup job link or the Next button.
     - In the calendar, all Exchange 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.
     - Select a backup job. All backup data of Exchange 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.
     - 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 SharePoint Online Data

With IBM Spectrum® Protect Plus Online Services for 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. Click the Restore tab on the left pane, and then click the SharePoint Online button.
2. Select the items that you want to export. You can choose one of the following methods to find the data to export:
   - Define a SharePoint Online site collection as the search scope and then use the **Advanced Search** feature 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:
     - 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.
     - To change the search conditions, click Advanced Search to expand this field.
     - 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.
     - 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**.
    - 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.
    - 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.
  - 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.
    - Click the Find the items in the specific backup job link or the Next button.
    - In the calendar, all SharePoint 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.
    - Select a backup job. All backup data of SharePoint 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.
    - 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 for Business Data

With IBM Spectrum® Protect Plus Online Services for Microsoft 365, you can export the backup data for the OneDrive for Business libraries, folders, and documents.

Before you begin

Note: When you select OneDrive for Business 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 for Business:

1. Click the Restore tab on the left pane, and then click Search by Service Type.
2. Click the OneDrive for Business button.
3. Select the items that you want to export. You can choose one of the following methods to find the data to export:
   - Define a OneDrive for Business address as the search scope and then use the Advanced Search feature 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:
     - In the Name field, enter or select a OneDrive for Business address. The default search condition is to search the backup data for that OneDrive for Business Address within the last backup cycle.
     - To change the search conditions, click Advanced Search to expand this field.
     - 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.
     - Select OneDrive for Business 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 for Business 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 configure the following search conditions: **Document Name**, **Created Date**, **Created By**, **Modified By**, or **Document Size**.
     - 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.
     - 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.
   - 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.
     - Click the Find the items in a specific backup job link or the Next button.
     - In the calendar, all OneDrive for Business 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.
     - Select a backup job. All backup data for OneDrive for Business 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.
     - You can enter keywords to search the items that you can click the backup data to browse the items you want to export.
4. 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 Spectrum® Protect Plus Online Services for 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. Click the Restore tab on the left pane, and then click the Microsoft 365 Groups button.
2. Select the items that you want to export. You can choose one of the following methods to find the data to export:
   - Define a Microsoft 365 Group as the search scope and then use Advanced Search feature to search for the items within the scope.
     Refer to the steps below:
     - 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.
     - To change the search conditions, click Advanced Search to expand this field.
     - 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.
     - 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.
     - 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.
     - 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.
   - 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.
     - Click the Find the items in the specific backup job link or the Next button.
     - 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.
     - 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) option to only show the data backed up in the selected backup job.
     - 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 Spectrum® Protect Plus Online Services for 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. Click the Restore tab on the left pane, and then click the Project Online button.
2. Select the items that you want to export. You can choose one of the following methods to find the data to export:
   - Define a Project Online site collection as the search scope and then use the Advanced Search feature 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:
     - 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.
     - To change the search conditions, click Advanced Search to expand this field.
     - 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.
     - 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.
     - 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.
     - 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.
   - 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.
     - Click the Find the items in the specific backup job link or the Next button.
     - 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.
     - 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.
     - 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 Teams Data

With IBM Spectrum® Protect Plus Online Services for Microsoft 365, you can export the backup data of Teams files or conversations.

Procedure

Complete the steps below to export Teams backup data:

1. Click the Restore tab on the left pane, and then click the Teams button.
2. 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 Teams 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.
    c. Select a backup job. All backup data of Teams is 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.
    d. 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 go 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 more details on the supported and unsupported data types of Teams Chat Message, refer to Teams Chat Data Types.
Note: When you select users to export, you can only select up to 10 users at once.

Procedure

Complete the steps below to export Teams Chat messages:

1. Click the Restore tab on the left pane, and then click Search by Service Type.
2. Click the Microsoft Teams Chat button.
3. Select the items that you want to export. You can choose one of the following methods to find the data to export.
    - Define the search scope and then use the Advanced Search feature to search for the items within the scope. Refer to the steps below:
        - 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.
        - To change the search conditions, click Advanced Search to expand this field.
        - 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.
        - 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.
        - 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.
    - 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.
        - Click the Find the items in a specific backup job link or the Next button.
        - 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.
        - Select a backup job. All backup data 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.
        - You can enter keywords to search the items, or you can click the backup data to browse the items you want to restore.
4. Select a node, and then click Export.
5. An export job for Teams will start, and you can go to Job Monitor to view the job status and download the exported data.

Export Yammer Data

You can export folders and files from the Yammer site and export the Yammer messages. You can only find the Yammer messages through time-based restore wizard (drill down a backup job). For detailed information on supported data types, refer to Restore Options for Different Object Types.

Procedure

Complete the steps below to export Yammer backup data:

1. Click the Restore tab on the left pane, and then click Search by Service Type.
2. Click the Yammer button.
3. Select the items that you want to export. You can choose one of the following methods to find the data to export.
    - Define a Yammer community as the search scope and then use the Advanced Search feature to search for the items within the scope. Refer to the steps below:
        - In the Name field, enter or select a Yammer community. The default search condition is to search the backup data within the last backup cycle.
        - To change the search conditions, click Advanced Search to expand this field.
        - 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.
        - Select Yammer 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 Yammer Community. You can leave the search conditions empty.
        - 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.
    - 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.
        - Click the Find the items in a specific backup job link or the Next button.
        - In the calendar, all backup jobs of Yammer are displayed. You can select whether to display the finished with an exception or failed jobs in the 102 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.
        - 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.
        - You can enter keywords to search the items, or you can click the backup data to browse the items you want to restore.
4. Select a node, and then click Export.
5. An export job for Yammer will start, and you can go to Job Monitor to view the job status and download the exported data.

Download the Exported Data

In Job Monitor, find the job record after the job is finished and click the Download Content button to save the exported data to your desired location.

If a job exported the data of multiple mailboxes/sites, a **Download Content** window will appear. 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**, the exported data will also be split for downloading.

Get Password

You can get a password to extract downloaded content. Only the user who started the export job and the email recipients designated for the restore and export job can get the password through Job Monitor.

About this task

Note: If the recipients are added after the export job has started, the recipients will not have access to the password of this export job.

Procedure

Follow the steps below to get the password through Job Monitor:

1. Go to the Job Monitor and select Export from the Job Type filter.
2. Find your export job, and then click the Get Password button on the right.
3. Click Copy to copy the password to your clipboard.
4. Use this password for extracting the downloaded content.

Restore and Recover Your Data

IBM Spectrum® Protect Plus Online Services for Microsoft 365 helps you quickly restore and recover your data from Exchange Online, SharePoint Online, OneDrive for Business, Microsoft 365 Groups, Teams, Project Online, and Public Folders. You can restore the backup data to its original location or restore data to a different location. If you have an additional license, you can restore backup data to a custom storage location.

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.

Note: If you use the app token to register SharePoint Online sites, Microsoft 365 Groups, and Teams, you must follow the steps in Restore Managed Metadata Service to ensure that the Term Store Administrator permission is in place so that the managed metadata can be successfully restored.

The Restore wizard provides two separate entries for you to find the data that you want to restore:

- Search for the items via keywords in properties
- Target the backup job to restore the items at that recovery point

- **High Speed Migration (HSM) Restore Method**
  The High Speed Migration (HSM) restore supports SharePoint Online, OneDrive for Business, Microsoft 365 Groups, and Teams in both app profile authentication and service account authentication, and now HSM restore jobs can support restoring content larger than 15 GB.
- **Restore Exchange Online Data**
  With IBM Spectrum Protect Plus Online Services for 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.
- **Restore SharePoint Online Data**
  With IBM Spectrum Protect Plus Online Services for Microsoft 365, you can browse or search for SharePoint Online backup jobs or data to restore items to its original location in SharePoint Online, to another location in SharePoint Online, or to a separate, customer-defined storage location. Additionally, you can select the OneDrive for Business containers as the destination to restore the SharePoint Online backup data.
- **Restore OneDrive for Business Data**
  You can browse or search for OneDrive for Business backup jobs or data to its original location in OneDrive for Business, to another location in OneDrive for Business, or to a separate, customer-defined storage location. Besides, you can select the SharePoint Online containers as the destination to restore the OneDrive for Business backup data.
- **Restore Microsoft 365 Groups Data**
  You can use IBM Spectrum Protect Plus Online Services for Microsoft 365 to restore Microsoft 365 Groups data, including soft-deleted groups. You can restore a soft-deleted group from the Microsoft 365 recycle bin to its last known good state.
- **Restore Project Online Data**
  With IBM Spectrum Protect Plus Online Services for 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.
- **Restore Public Folder Data**
  With IBM Spectrum Protect Plus Online Services for Microsoft 365, you can restore Public Folder backup data to its original location.
- **Restore Teams Data**
  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.
- **Restore Yammer Data**
- **Restore Managed Metadata Service**
  To restore the Managed Metadata Service, you must first ensure that the Term Store Administrator permission is in place. Refer to the instructions below for the different scenarios.
- **Monitor Your Restore**
  On the Home page, you can view the backup or restore details through the MORE DETAILS link for each object type. The Restore Details will display the number of items restored at each level in a specific time range and display the last restore record. You can click the View Details link under the Last Restore History to go to the Job Monitor page to generate and download the job report of the last restore job.

High Speed Migration (HSM) Restore Method

The High Speed Migration (HSM) restore supports SharePoint Online, OneDrive for Business, Microsoft 365 Groups, and Teams in both app profile authentication and service account authentication, and now HSM restore jobs can support restoring content larger than 15 GB.

Refer to the following for the scenarios of HSM data recoveries:

- Select sites, subsites, document libraries, custom lists, or folders to restore.
  Note: If your selection for restore contains files or items, HSM restore is not applicable; HSM restore does not support apps either.
- Restore destination must be a container in SharePoint Online site or user's OneDrive for Business.

Note the following known issues:

- Restore settings, such as restoring the security-only or restoring the sharing link permissions, are not supported.
- 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 Spectrum® Protect Plus Online Services for 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.

About this task

IBM Spectrum Protect Plus Online Services for 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 Spectrum Protect Plus Online Services cannot be the destination of the restore.

Procedure

Complete the steps below to restore Exchange Online data:

1. Click the Restore tab on the left pane, and then click the Exchange Online button to restore the Exchange Online data.
2. Select the items that you want to restore. You can choose one of the following methods to find the data to restore.
   - Define a mailbox as the search scope at first and then use the Advanced Search feature to search for the items within the mailbox. Refer to the steps below:
     - 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.
     - To change the search conditions, click Advanced Search to expand this field.
     - 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.
     - 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.
     - 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.
     - Find and select the item you want to restore 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 restore. 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.
     - Go to step 3 to continue with the Restore settings.
   - 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.
     - Click the Find the items in the specific backup job link or the Next button.
     - 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.
     - Select a backup job. All backup data of Exchange 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.
     - 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 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.
     - Go to step 3 to continue with the Restore settings.
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 the restore destination. The items that can be selected as the restore destination are listed under the Search a Restore Destination box. You can click the page number or enter the page number to go to a specific page to view the items on that page. 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; Merge will add the contents to the destination node.

   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 Spectrum Protect Plus Online Services.

5. Select how to handle the conflicts in the restore job.
   - Container level – 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 – 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.

6. Select Yes or No for 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 license type. For IBM Spectrum Protect Plus Online Services 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.
7. Click Next to view the restore summary.
8. Click Restore to restore the selected items.

Restore SharePoint Online Data

With IBM Spectrum® Protect Plus Online Services for Microsoft 365, you can browse or search for SharePoint Online backup jobs or data to restore items to its original location in SharePoint Online, to another location in SharePoint Online, or to a separate, customer-defined storage location. Additionally, you can select the OneDrive for Business containers as the destination to restore the SharePoint Online backup data.

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 Spectrum Protect Plus Online Services 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.
Note: If you use the app token to register objects and run backup and restore jobs, you must follow the steps in Restore Managed Metadata Service to ensure that the Term Store Administrator permission is in place so that the managed metadata can be successfully restored.

Procedure

Complete the steps below to restore Sharepoint Online data:

1. Click the Restore tab on the left pane, and then click the SharePoint Online button to restore the SharePoint Online data.
2. Select the items that you want to restore. You can choose one of the following methods to find the data to restore.
   - Define a SharePoint Online site collection as the search scope at first and then use the Advanced Search feature 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.
   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 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.
   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 500 items. You can edit the search conditions and click Search to adjust the search results.
   f. Find and select the item you want to restore 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 restore. 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.
   g. Go to step 3 to continue with the Restore settings.

   - 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 the specific backup job link or the Next button.
   b. 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.
   c. Select a backup job. All backup data of SharePoint 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.
   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. 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 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. Go to step 3 to continue with the Restore settings.
3. If necessary, you can enter your comments 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 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.
   Restriction: SharePoint Online site collections, sites, and apps can be restored only to the original location in SharePoint or to another location in SharePoint.

   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:

     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.

     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.

Select a destination object type
: Select whether to restore the backup data to SharePoint Online or OneDrive for Business. You can enter keywords to search the restore destination. The items that can be selected as the restore destination are listed under the Search a Restore Destination box.
Note: If you choose to restore to OneDrive for Business, 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.

You can click the page number or enter the page number to go to a specific page to view the items on that page.

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.

Restore the data to your storage
: Restore the backup data to your own configured storage location. 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 destination conflicting container will be retained in the destination.

     Merge
     : The source container settings and the content will be merged to the destination conflicting container.

     Replace
     : The settings of the destination conflicting 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 destination conflicting content is earlier than that of the source content, the destination conflicting 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 destination conflicting content is the same, the restore will be skipped; if the last modified time is different, the destination conflicting 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 destination conflicting app and AppData will be retained in the destination, and the backup data of the conflicting content will not be restored.

     Overwrite
     : The destination conflicting 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. Choose how you would like to restore the version history. 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 Spectrum Protect Plus Online Services for Microsoft 365 can restore up to **20** versions for one document. For the best performance and simplest experience, IBM Spectrum Protect Plus Online Services recommends restoring only the latest version.
   Note: 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.
   Note: This restore setting is not available when restoring security only.
8. Select if you would like to restore the sharing permissions. This feature only works for the sharing of items to specific people inside or outside your organization. The restore job will restore the permissions for the users who have accessed the sharing link. During the restore process, email notifications will be triggered and sent to each user who has accessed the sharing link.
   Note: The Sharing setting is a tenant-level setting, and IBM Spectrum Protect Plus Online Services for 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.
9. Select Yes or No for 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 license type. For IBM Spectrum Protect Plus Online Services default storage, the restore job will automatically rehydrate data.
   Note: IBM Spectrum Protect Plus Online Services recommends not storing the index database to the Azure archive storage tier.
10. Select Yes or No for whether to restore the subsites. This option is only available when you select site collections or sites to restore.
11. Click Next to view the restore summary.

12. Click Restore to restore the selected items. After the job has started, you can go to the Job Monitor to view more job details. For details, refer to Generate and Download a Job Report.

Restore OneDrive for Business Data

You can browse or search for OneDrive for Business backup jobs or data to its original location in OneDrive for Business, to another location in OneDrive for Business, or to a separate, customer-defined storage location. Besides, you can select the SharePoint Online containers as the destination to restore the OneDrive for Business backup data.

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 Spectrum® Protect Plus Online Services cannot be the destination of the restore. Additionally, the OneDrive for Business site collections and sites do not support being restored to a custom storage location.

Procedure

Complete the steps below to restore OneDrive for Business data:

1. Click the Restore tab on the left pane, and then click the OneDrive for Business button to restore the OneDrive for Business data.
2. Select the items that you want to restore. You can choose one of the following methods to find the data to restore.
   - Define a OneDrive for Business address as the search scope at first and then use the Advanced Search feature 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 for Business address. The default search condition is to search the backup data for that OneDrive for Business address 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 OneDrive for Business 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 for Business 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 configure the following search conditions: Document Name, Created Date, Created By, Modified By, or Document Size.
   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 500 items. You can edit the search conditions and click Search to adjust the search results.
   f. Find and select the item you want to restore 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 restore. 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 of the selected items.
   g. Go to step 3 to continue with the Restore settings.

   - 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 the specific backup job link or the Next button.
   b. In the calendar, all backup jobs of OneDrive for Business 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 for OneDrive for Business 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. 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 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. Go to step 3 to continue with the Restore settings.
3. If necessary, you can enter your comments 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 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 for Business site collections and sites can be restored only to the original OneDrive for Business location or another location in OneDrive for Business.

   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:

     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.

     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.

Select a destination object type
: Select whether to restore the backup data to SharePoint Online or OneDrive for Business. You can enter keywords to search the restore destination. The items that can be selected as the restore destination are listed under the Search a Restore Destination box.
Note: If you choose to restore to OneDrive for Business, 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.

You can click the page number or enter the page number to go to a specific page to view the items on that page.

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.

Restore the data to your storage
: Restore the backup data to your own configured storage location. This option is not available if the default storage location is used.
Note: The OneDrive for Business 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 destination conflicting container will be retained in the destination.

     Merge
     : The source container settings and the content will be merged to the destination conflicting container.

     Replace
     : The settings of the destination conflicting 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 destination conflicting content is earlier than that of the source content, the destination conflicting 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 destination conflicting content is the same, the restore will be skipped; if the last modified time is different, the destination conflicting 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 destination conflicting app and AppData will be retained in the destination, and the backup data of the conflicting content will not be restored.

     Overwrite
     : The destination conflicting 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. Choose how you would like to restore the version history. 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 Spectrum Protect Plus Online Services for Microsoft 365 can restore up to **20** versions for one document. For the best performance and simplest experience, IBM Spectrum Protect Plus Online Services restore only the latest version.
   Note: 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.
8. Select if you would like to restore the sharing permissions. This feature only works for the sharing of items to specific people inside or outside your organization. The restore job will restore the permissions for the users who have accessed the sharing link. During the restore process, email notifications will be triggered and sent to each user who has accessed the sharing link.
   Note: The Sharing setting is a tenant-level setting, and IBM Spectrum Protect Plus Online Services for 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.
9. Select Yes or No for 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 license type. For IBM Spectrum Protect Plus Online Services default storage, the restore job will automatically rehydrate data.
   Note: IBM Spectrum Protect Plus Online Services recommends not storing 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. After the job has started, you can go to the Job Monitor to view more job details. For details, refer to Generate and Download a Job Report.

Restore Microsoft 365 Groups Data

You can use IBM Spectrum® Protect Plus Online Services for Microsoft 365 to restore Microsoft 365 Groups data, including soft-deleted groups. You can restore a soft-deleted group from the Microsoft 365 recycle bin to its last known good state.

About this task

IBM Spectrum Protect Plus Online Services 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 Spectrum Protect Plus Online Services backup data to roll back the entire group or granular contents.

Note: The check will only happen when you select the group as both the restore scope and the search level.
The IBM Spectrum Protect Plus Online Services for Microsoft 365 Groups service only supports restoring the group, group team site, group mailbox, and planner data to another location. 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. 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 Spectrum Protect Plus Online Services 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.
Note: If you use the app token to register objects, you must follow the steps in Restore Managed Metadata Service to ensure that the Term Store Administrator permission is in place so that the managed metadata can be successfully restored.

Procedure

Complete the steps below to restore the Microsoft 365 Groups data:

1. Click the Restore tab on the left pane, and then click the Microsoft 365 Groups button to restore the Microsoft 365 Groups data.
2. Select the items that you want to restore. You can choose one of the following methods to find the data to restore.
   - Select a restore object scope and search for the data to restore. Follow steps 3 to 4.
   - Select a recovery point (backup job) and select data from that backup to restore. Go to step 6.
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.
4. You can choose to use the Advanced Search feature on the same page to search for the contents within this group for granular data roll-back, or you can directly go 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 Spectrum Protect Plus Online Services for 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 go 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 Advanced Search feature 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 drop-down list under the Recovery Point column, select a backup job that backed up this item at the status that you want to restore. 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. Go to step 5 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. Click the Find the items in a specific backup job link or the Next button.
   b. 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.
   c. 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.
   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: 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.
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:

     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.

     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.

     Select a restore destination
     : Select a container as the restore destination. You can enter keywords to search the restore destination. The items that can be selected as the restore destination are listed under the Search a Restore Destination box.
     You can click the page number or enter the page number to go to a specific page to view the items on that page.

     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.

   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 destination conflicting container will be retained in the destination.

     Merge
     : The source container settings and the content will be merged to the destination conflicting container.

     Replace
     : The settings of the destination conflicting 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 destination conflicting content is earlier than that of the source content, the destination conflicting 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 destination conflicting content is the same, the restore will be skipped; if the last modified time is different, the destination conflicting 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 destination conflicting app and AppData will be retained in the destination, and the backup data of the conflicting content will not be restored.

     Overwrite
     : The destination conflicting 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.
10. Choose how you would like to restore the version history. 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 Spectrum Protect Plus Online Services for Microsoft 365 can restore up to **20** versions for one document. For the best performance and simplest experience, restore only the latest version.
    Note: 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.
11. Select if you would like to restore the sharing permissions. This feature only works for the sharing of items to specific people inside or outside your organization. The restore job will restore the permissions for the users who have accessed the sharing link. During the restore process, email notifications will be triggered and sent to each user who has accessed the sharing link.
    Note: The Sharing setting is a tenant-level setting, and IBM Spectrum Protect Plus Online Services for 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.

12. Select Yes or No for 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 license type. For IBM Spectrum Protect Plus Online Services 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 go to the Job Monitor to view more job details. For details, refer to Generate and Download a Job Report.

Restore Project Online Data

With IBM Spectrum® Protect Plus Online Services for 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.

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 Spectrum Protect Plus Online Services cannot be the destination of the restore.

Procedure

Complete the steps below to restore Project Online data:

1. Click the Restore tab on the left pane, and then click the Project Online button to restore the Project Online data.
2. Select the items that you want to restore. You can choose one of the following methods to find the data to restore.
   - Define a Project Online site collection as the search scope and then use the Advanced Search feature 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. 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 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.
   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 500 items. You can edit the search conditions and click Search to adjust the search results.
   f. Find and select the item you want to restore 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 restore. 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.
   g. Continue to step 3 to configure the Restore settings.
   - 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 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.
   c. 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.
   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. 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 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. 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. 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 (such as views and permissions) will be restored.
   - 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.

   When you select projects to restore, you can select No for only restoring the related settings for the selected projects. The associated Resources and Enterprise Project Type, and all the Enterprise Custom Fields and Lookup Tables under PWA will be restored.

   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.

6. 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 is backed up.

Restore the data to another location
: Restore the backup data to another destination. Configure the following settings:

  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.

  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.

  Domain mapping
  : Select a domain mapping profile from the drop-down list. For more details on creating a new domain mapping profile, refer to Configure Mapping Settings.

  Select a destination object type
  : Select a container as the restore destination. You can enter keywords to search the restore destination. The items that can be selected as the restore destination are listed under the **Search a Restore Destination** 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.
  You can click the page number or enter the page number to go to a specific page to view the items on that page.

  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.

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: The Project Online site collections, sites, projects, and apps do not support being restored to a custom storage location.

7. 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 destination conflicting container will be retained in the destination.

     Merge
     : The source container settings and the content will be merged to the destination conflicting container.

     Replace
     : The settings of the destination conflicting 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 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.

   - Apps conflict resolution – Select how to handle the apps conflict.

     Skip
     : The destination conflicting app and AppData will be retained in the destination, and the backup data of the conflicting content will not be restored.

     Overwrite
     : The destination conflicting 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.
8. Choose how you would like to restore the version history. 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 Spectrum Protect Plus Online Services for Microsoft 365 can restore up to **20** versions for one document. For the best performance and simplest experience, IBM Spectrum Protect Plus Online Services recommends restoring only the latest version.
   Note: 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.
9. Select if you would like to restore the sharing permissions. This feature only works for the sharing of items to specific people inside or outside your organization. The restore job will restore the permissions for the users who have accessed the sharing link. During the restore process, email notifications will be triggered and sent to each user who has accessed the sharing link.
   Note: The Sharing setting is a tenant-level setting, and IBM Spectrum Protect Plus Online Services for 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.
10. Select Yes or No for 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 license type. For IBM Spectrum Protect Plus Online Services default storage, the restore job will automatically rehydrate data.
    Note: IBM Spectrum Protect Plus Online Services recommends not storing the index database to the Azure archive storage tier.
11. Click Next to view the restore summary.
12. Click Restore to restore the selected items. After the job has started, you can go to the Job Monitor to view more job details. For details, refer to Generate and Download a Job Report.

Restore Public Folder Data

With IBM Spectrum® Protect Plus Online Services for Microsoft 365, you can restore Public Folder backup data to its original location.

Procedure

Complete the steps below to restore Public Folder data:

1. Click the Restore tab on the left pane, and then click the Public Folder button to restore the Project Folder data.
2. Select the items that you want to restore. You can choose one of the following methods to find the data to restore.
   - Define a Project Online site collection as the search scope and then use the Advanced Search feature to search for the items within the folder. Refer to the steps below:
   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. 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 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.
   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 500 items. You can edit the search conditions and click Search to adjust the search results.
   f. Find and select the item you want to restore 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 restore. 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.
   g. Go to step 3 to continue with the Restore settings.
   - 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. 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 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. Go 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. Select Yes or No for 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 license type. For IBM Spectrum Protect Plus Online Services default storage, the restore job will automatically rehydrate data.
   Note: IBM Spectrum Protect Plus Online Services 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

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.

Before you begin

Before you restore Teams data, note the following:

- To restore the Private Channel data, you can only use the time-based 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.
- 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.
- 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 in the name of the service account to the channel's Posts with the original message's sender information and sent date in the message body. To use this feature, you must be using service account authentication to scan Teams, and a Microsoft Delegated app must be ready for your tenant. For details on creating an app profile for Microsoft Delegated, refer to App Profile for a Microsoft Delegated App.
- 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.
- If a channel has ever been renamed in its backup lifecycle, note the following:
    - If the Team where this channel resides is deleted and you want to restore the backup data of this entire team, the restore job will create two channels for this renamed channel in the destination, one with the old name and one with the new name. The files will be restored to the channel with the old name, and the channel with a new name will not have any files restored to it.
    - If you select the channel's backup data to restore, note the following:
      If you select a pre-renaming recovery point to restore, the restore job will create a channel with the old name and restore the backup data at that recovery point.

      If you select a post-renaming recovery point to restore, the restore job cannot restore files to this channel.

    - Does not support backing up Teams chat (personal chat).
    - Does not support backing up and restoring folders added through the Add cloud storage method under the Files tab in channels.

About this task

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.

Note: If you use the app token to register objects, you must follow the steps in Restore Managed Metadata Service to ensure that the Term Store Administrator permission is in place so that the managed metadata can be successfully restored.
You can select to restore the Channel's conversations and files to your storage if you have a BYOS license.

IBM Spectrum Protect Plus Online Services for 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 Spectrum Protect Plus Online Services 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 Spectrum Protect Plus Online Services 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. Click the Restore tab on the left pane, and then click the Teams button to restore the Teams data.
2. Select the data that you want to restore. You can choose one of the following methods to find the data to restore.
    - Select a restore object scope and search for the data to restore. Follow steps 3 to 4.
    - Select a recovery point (backup job) and select data from that backup to restore. Go 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.
4. You can choose to use the Advanced Search feature on the same page to search for the contents within this team for granular data roll-back, or you can directly go 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 Spectrum Protect Plus Online Services for 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 go 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 Advanced Search feature 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 drop-down list under the Recovery Point column, select a backup job that backed up this item at the status that you want to restore. 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. Go 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. Click the Find the items in a specific backup job link or the Next button.
   b. 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.
   c. 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.
   d. 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.
   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.

   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.
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:

      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.

      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.

      Select a destination object type
      : Select a container as the restore destination. You can enter keywords to search the restore destination. The items that can be selected as the restore destination are listed under the Search a Restore Destination box.
      You can click the page number or enter the page number to go to a specific page to view the items on that page.

      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.

   Restore the data to your storage
   : If you have selected the Channels, Conversations, or Files, and you have the BYOS license, this option is available. You can restore the Channel's conversations and files to your storage.

8. 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 be using the service account authentication to scan Teams and have a Microsoft Delegated app registered in your tenant. For details on configuring the app, refer to App Profile for a Microsoft Delegated App. The product will post a new message in the name of the service account to the channel's Posts with the original message's sender information and sent date in the message body.
9. 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 destination conflicting container will be retained in the destination.

     Merge
     : The source container settings and the content will be merged to the destination conflicting 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 destination conflicting 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 the conflicts at the content level.

     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.

Overwrite by Last Modified Time
: If the last modified time of the destination conflicting content is earlier than that of the source content, the destination conflicting 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 destination conflicting content is the same, the restore will be skipped; if the last modified time is different, the destination conflicting 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 destination conflicting app and AppData will be retained in the destination, and the backup data of the conflicting content will not be restored.

Overwrite
: The destination conflicting app and AppData will be removed from the destination, and the backup data of the conflicting content will be restored.

10. Choose how you would like to restore the version history. 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 Spectrum Protect Plus Online Services for Microsoft 365 can restore up to **20** versions for one document. For the best performance and simplest experience, restore only the latest version.
    Note: 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.
11. Select if you would like to restore the sharing permissions. This feature only works for the sharing of items to specific people inside or outside your organization. The restore job will restore the permissions for the users who have accessed the sharing link. During the restore process, email notifications will be triggered and sent to each user who has accessed the sharing link.
    Note: The Sharing setting is a tenant-level setting, and the IBM Spectrum Protect Plus Online Services for 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.
12. Select Yes or No for 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 license type. For IBM Spectrum Protect Plus Online Services 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 go to the Job Monitor to view more job details. For details, refer to Generate and Download a Job Report.

Restore Yammer Data

Procedure

Complete the steps below to restore Yammer data:

1. Click the Restore tab on the left pane, and then click Search by Service Type.
2. Click the Yammer button to restore the Yammer data.
3. Select the data that you want to restore. You can choose one of the following methods to find the data to restore.
    - Select a restore object scope and search for the data to restore. Follow steps 4 to 5.
    - Select a recovery point (backup job) and select data from that backup to restore. Go to step 6.
4. Define a Yammer community as the search scope. You can enter the Yammer community address or display name to search, and then select the Yammer community from the Name list. The default search condition is to search the backup data for the selected community within the last backup cycle.
5. You can choose to use the Advanced Search feature on the same page to search for the contents within this community for granular data roll-back, or you can directly go to the next step to search and select the data to restore.
    For the details of using the Advanced Search feature 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 Yammer community 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 Yammer 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 Yammer 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 drop-down list under the Recovery Point column, select a backup job that backed up this item at the status that you want to restore. 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. Go to step 7 to continue with the Restore settings.
6. 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 Yammer 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 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.
    d. 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.

e. Continue to step 7 to configure the Restore settings.

7. If necessary, you can enter a description for this restore job in the Description text box.
8. 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 your storage** – If you have selected the Yammer conversations or files, and you have the BYOS license, this option is available. You can restore the Yammer conversations and files to your storage.
9. 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 Yammer community, and the owner and members of the source Yammer 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.
10. Choose how you would like to restore the version history. 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 Spectrum® Protect Plus Online Services for Microsoft 365 can restore up to **20** versions for one document. For the best performance and simplest experience, IBM Spectrum Protect Plus Online Servicesrecommends restoring only the latest version.
    Note: 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.
11. Select Yes or No for 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 license type. For IBM Spectrum Protect Plus Online Services default storage, the restore job will automatically rehydrate data.
12. Select Yes or No for 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 license type. For IBM Spectrum Protect Plus Online Services default storage, the restore job will automatically rehydrate data.
    Note: IBM Spectrum Protect Plus Online Services for 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.
13. Click Next to view the restore summary.
14. Click Restore to restore the selected items. After the job has started, you can go to the Job Monitor to view more job details. For details, refer to Generate and Download a Job Report.

Restore Managed Metadata Service

To restore the Managed Metadata Service, you must first ensure that the Term Store Administrator permission is in place. Refer to the instructions below for the different scenarios.

Procedure

- Your tenant only uses the service account to run jobs. This means you choose the service account authentication method to scan objects via IBM Spectrum® Protect Plus Online Services Auto Discovery. In this scenario, complete the following steps to grant the permission:
  1. Log into the Microsoft 365 admin center.
  2. Navigate to SharePoint admin center > term store > Term Store Administrators.
  3. Make sure the service account is one of the Term Store Administrators. If this account is not the administrator, enter its username in the text box.
  4. Click Save to save your changes.
- Your tenant only uses the app token to run jobs. This means you choose the app profile authentication method to scan objects via IBM Spectrum Protect Plus Online Services Auto Discovery, and your tenant does not use multi-factor authentication (MFA) in Microsoft 365. In this scenario, complete the following steps to grant the permissions:
  1. Log into the Microsoft 365 admin center.
  2. Navigate to SharePoint admin center > term store > Term Store Administrators.

3. Make sure the `app@sharepoint` account is one of the Term Store Administrators. If this account is not the administrator, enter `i:0i.t|00000003-0000-0ff1-ce00-000000000000|app@sharepoint` in the text box.
4. Click **Save** to save your changes.

- Your tenant uses the app token to scan objects and uses a multi-factor authentication (MFA) Microsoft 365 service account to run jobs. In the Auto Discovery profile of IBM Spectrum Protect Plus Online Services, you choose the app profile authentication method and select an MFA service account profile. In this scenario, complete the following steps to grant the permission.
  1. Log into Microsoft 365 admin center.
  2. Navigate to SharePoint admin center > term store > Term Store Administrators.
  3. Make sure the **app@sharepoint** account is one of the Term Store Administrators. If this account is not the administrator, enter **i:0i.t|00000003-0000-0ff1-ce00-000000000000|app@sharepoint** in the text box.
  4. Click Save to save your changes.

Monitor Your Restore

On the Home page, you can view the backup or restore details through the MORE DETAILS link for each object type. The Restore Details will display the number of items restored at each level in a specific time range and display the last restore record. You can click the View Details link under the Last Restore History to go to the Job Monitor page to generate and download the job report of the last restore job.

Procedure

To view restore job details and generate a restore job report, follow the steps below:

1. Go to the Home page, click the MORE DETAILS link in the Exchange Online, OneDrive for Business, SharePoint Online, Microsoft 365 Groups, Teams, Project Online, or Public Folders section. A pane that displays the backup and restore details appears.
2. Go to the Restore Details tab, which by default displays the total number of objects that are restored in the last 90 days and the number of objects at each level. To customize the time range, click the Calendar button in the Time Range field and then select the start time and end time to define your own time range.
3. On the right pane of the Restore Details tab, Last Restore History shows the information about the last restore job that has been completed, including the person who runs this job, the number of successful objects in this job, and the time when this job finished. Click View Details to navigate to the Job Monitor page for generating and downloading the job report. For detailed instructions on generating and downloading a job report, refer to Generate and Download a Job Report.

Data Management

Through Data Management, you can work with

- The Data Subject Access Requests wizard to discover the backup data of a given data subject and delete the backups.
- The Remove Unprotected Data report to check for the out-of-protection data and its expiration date for this backup data to be deleted. By default, the Remove Unprotected Data feature does not support BYOS customers or trial licenses.

The out-of-protection data means the data that you have moved from a protected selection to an unprotected scope, which indicates that you do not want this data protected. For your privacy, IBM Spectrum® Protect Plus Online Services for Microsoft 365 will remove such data. For details, refer to Remove Unprotected Data.

- **Data Subject Access Requests**
  To help your organization comply with the General Data Protection Regulation (GDPR), IBM Spectrum Protect Plus Online Services for Microsoft 365 provides a tool that discovers all copies of the Exchange Online Mailbox and OneDrive for Business backups of a given data subject that are stored by IBM Spectrum Protect Plus Online Services for Microsoft 365 solution and deletes the user-generated backups of Mailbox and OneDrive.
- **Remove Unprotected Data**
  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 Spectrum Protect Plus Online Services for Microsoft 365 will delete the corresponding backup data on the expiration Date.
- **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.

Data Subject Access Requests

To help your organization comply with the General Data Protection Regulation (GDPR), IBM Spectrum® Protect Plus Online Services for Microsoft 365 provides a tool that discovers all copies of the Exchange Online Mailbox and OneDrive for Business backups of a given data subject that are stored by IBM Spectrum Protect Plus Online Services for Microsoft 365 solution and deletes the user-generated backups of Mailbox and OneDrive.

About this task

The IBM Spectrum Protect Plus Online Services for 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: 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.

Procedure

Complete the steps below:

1. Click Data Subject Access Requests on the left page.
2. Click Discover & Delete to enter the Discover Data 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 for Business.
4. Click the box to load the data subject or enter the keyword to search for the data subject you are looking for. Select the data subject from the list and then click Next. You can select multiple items in the search result.
5. In the Delete Data step, you can at first export a list of recovery points to view the object backup history. Select the objects and click Export Recovery Point. A compressed file is 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 Spectrum Protect Plus Online Services for Microsoft 365.
   You can continue to discover and delete data, or click the Right to be Forgotten Requests to go to the Job Monitor page to view deletion jobs in response to right to be forgotten requests.

Remove Unprotected Data

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 Spectrum® Protect Plus Online Services for Microsoft 365 will delete the corresponding backup data on the expiration Date.

IBM Spectrum Protect Plus Online Services for Microsoft 365 will screen your backup scope once a week and update the report. Your administrator group or the partner's administrator group will receive the email notification "Legacy online services data for Microsoft 365 identified and scheduled for removal", including the data moved to the unprotected scope, the data moved back to the protected, or the data to be deleted in seven days. If you adjusted the backup scope accordingly to prevent certain backup data from being deleted, you will receive the email notification "Data protection scope updated -content no longer marked for deletion" as an update.

Note that this feature does not apply to the BYOS license or trial license, 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 looking to save storage space by removing unprotected data, contact the Support team to enable this feature for your environment.

Note: The backup data for the objects that have been protected by IBM Spectrum Protect Plus Online Services for Microsoft 365 but removed from your Microsoft 365 tenant is not within this scope. IBM Spectrum Protect Plus Online Services for Microsoft 365 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 Spectrum Protect Plus Online Services for Microsoft 365 may include the backup data of this object to the removed unprotected data report and send you email notifications. Your backup data will not be deleted since the IBM Spectrum Protect Plus Online Services 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.

The data on the Remove unprotected data page will be refreshed every seven days. You can check for the last updated time in the upper-right corner of this page. On the remove unprotected data page, you can also perform the following:

- Use the object type filter to have a custom view. You can select a service from the drop-down list.
- Click Export List button on the upper-right corner to export all the data on this page to your computer or expand an object type section and click the Export List button on the upper-right corner of the section to export the data of that object type.
- Click the Export All button on the upper-right corner of this page to expand all the nodes in the current view, or click the Collapse All button to collapse all the nodes.

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 Spectrum® Protect Plus Online Services for 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.

Note: If you want to avoid any accidental deletion of backup data, you can contact IBM Software Support to disable this feature.

Procedure

Follow the steps below:

1. In the Manually Delete Backup Data page, click the appropriate tab for the backup data that you are looking for.
2. Select the mailbox, site collection, group, or team where the object that you are looking for belongs from the Name list, and then select the granular level of the object from the Levels list.
3. Click Search. The Select and delete the backup data page appears. The items that meet the search conditions and have backups are displayed in the table.
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.

Configure Mapping Settings

If you want to out-of-place restore the 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, User Mapping, and Language Mapping.

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

- **Domain Mapping**
- **User Mapping**
- **Language Mapping**
  You can configure the language mappings in IBM Spectrum Protect Plus Online Services for Microsoft 365 for the languages that are available in the current release.

Domain Mapping

Procedure

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

- Click the Create a New Profile button to create a new domain mapping profile. For details, refer to Create a New Domain Mapping Profile.
- Click the View button in the Action column to view the details of a domain mapping profile.
- Click the Edit button in the Action column to edit a domain mapping profile.
- Click the Delete button in the Action column to delete a domain mapping profile.

- **Create a New Domain Mapping Profile**

Create a New Domain Mapping Profile

Procedure

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

1. Click Create a New Profile. The Create a 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 a Mapping Rule. 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.

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.
- Click the View button in the Action column to view the details of a user mapping profile.
- Click the Edit button in the Action column to edit a user mapping profile.
- Click the Delete button in the Action column to delete a user mapping profile.

- **Create a New 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 a New 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.

   Customize settings if the user does not exist in destination
   : This option is selected by default. With this option selected, enter the username of the **Target Default User**. Deselect this option if you do not want to customize the target default user.

   Mapping Rules
   : Configure user-mapping rules by clicking Add a Mapping Rule. 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.
3. Click Save to save the configurations for this user mapping profile and return to the Mappings-User Mapping page.

Language Mapping

You can configure the language mappings in IBM Spectrum® Protect Plus Online Services for Microsoft 365 for the languages that are available in the current release.

Procedure

In the Language 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.
- Click the View button in the Action column to view the details of a language mapping profile.
- Click the Edit button in the Action column to edit a language mapping profile.
- Click the Delete button in the Action column to delete a language mapping profile.

- **Create a New Language Mapping Profile**

Create a New Language Mapping Profile

Procedure

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

1. Click Create a New 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 a Mapping Rule. 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 Language 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.

Reporting

- **Generate and Download a Job Report**
  The Job Monitor page displays the backup and restore user activity. You can use the filters (Time Filter, Job Type filter, Object Type filter, and Job Status filter) or the Search box to search for the backup, restore, and export jobs.
- **View Subscription Consumption Report**
  The Subscription Consumption Report provides a licensing dashboard to show your license details, usage growth rate and trends, and utilizations, helping you understand how your license is consumed and predict when your license will reach the quota.
- **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. By default, this report is not available. If you want to enable this report, contact the IBM® Software Support team.
- **Use the Job Analytics Report**
  The Job Analytics report contains two tabs: Operation Overview and Backup Overview, respectively providing a chart overview for all backup jobs performed within 7 Days or This Month which can help you understand the job progress details of the SharePoint Online backups that are currently running slowly.
- **Audit User Activities in System Auditor**
  Navigate to the Reporting > System Auditor page to view the user activities in IBM Spectrum® Protect Plus Online Services for Microsoft 365, divided into the following categories: Backup, Restore, Report, Settings, Common, Export, and Delete.
- **Use Microsoft 365 Unusual Activities Analysis Report**
  IBM Spectrum Protect Plus Online Services for Microsoft 365 will learn from your OneDrive for Business backups and warn you for the OneDrive accounts with unusual activities or under a potential ransomware attack.

Generate and Download a Job Report

The Job Monitor page displays the backup and restore user activity. You can use the filters (Time Filter, Job Type filter, Object Type filter, and Job Status filter) or the Search box to search for the backup, restore, and export jobs.

About this task

To view the job summary information on this page, including Job ID, Start Time, Title (for restore jobs), the total number of items being backed up, restored, or exported, the number of the Successful, Failed, and Skipped items in the job, click Expand All next to the Search box to expand all activity records. Click **Collapse All** to fold up the information.

You can generate and download reports for the completed backup, restore, or export jobs to view the job summary, job settings, and the failed or skipped objects. In the reports for the restore jobs, the source and destination information can also be seen.

Procedure

To generate and download a job report, follow the steps below:

1. Click Job Monitor in the left pane. The Job Monitor page appears in the right pane.
2. You can use the Time Filter, Job Type, Object Type, Job Status to filter the user activities.
   - Click Time Filter: All, and then select Today, Last 7 Days, or This Month from the drop-down list to filter the activities whose start time matches the filter;
   - Click Job Type: All, and then select Backup, Restore, Export, Delete, or Retention from the drop-down list to filter the corresponding jobs;
   - Click Object Type: All, and then select a service from the drop-down list to search the jobs performed on the corresponding object type.
   - Click Job Status: All, and then select In Progress, Finished, Finished with Exception, Failed, or Partially Finished from the drop-down list to search the jobs of specified status.

   Additionally, you can use the **Search** box to search the activities by Username, Job ID, or Title (for restore jobs).
3. Click Generate Report button next to the job. The **Generate Report** window appears. You can select which type of reports to generate: A Simple Report which only includes the Failed and Skipped items, or a Detailed Report including the Successful top-level records (Exchange Online mailbox, OneDrive for Business, 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),Failed, or Skipped items.
4. After the report is generated, the Download Report button will appear. Click the Download Report link to download the report.
   Note: If you want to generate a report of the other type, you can click the Generate Report icon next to the Download Report button, and then select the other type to generate a new report.

View Subscription Consumption Report

The Subscription Consumption Report provides a licensing dashboard to show your license details, usage growth rate and trends, and utilizations, helping you understand how your license is consumed and predict when your license will reach the quota.

IBM Spectrum® Protect Plus Online Services provides a following option for IBM Spectrum Protect Plus Online Services for Microsoft 365 licensing:

- Protection for an unlimited amount of content in an organization for a set per-user license

You can get a glance at the subscription type and capacity of your purchased subscription in the subscription Details pane, view the number and percentage of the consumed licenses, the major consumers on your subscription, and the usage history respectively in the subscription Utilization pane, Top subscription Consumers, Largest Consumers, and Usage History.

- To view more usage statistics, such as the usage history and trend, average growth rate, spike, and the object type that consumed most, click on the upper right corner of the Usage History pane or click the Usage tab.
- To view overall subscription utilization of each object type or down to a single site collection, OneDrive for Business, mailbox, public folder, team, or a group, click the Expand button on the upper right corner of the Largest Consumer pane or click the Utilization tab.

If you want to increase your subscription capacity, you can reach out to your IBM Spectrum Protect Plus Online Services sales representative.

You also need to note the following when using the Subscription Consumption Report:

- The Subscription Consumption Report is updated once a week and only available to the IBM Spectrum Protect Plus Online Services Administrator and the Application Administrators of IBM Spectrum Protect Plus Online Services for Microsoft 365. For the Multi-Geo license, only the IBM Spectrum Protect Plus Online Services Administrators can view this report.
- IBM Spectrum Protect Plus Online Services for Microsoft 365 counts the size of private channel sites to the Teams total size, which may cause a spike in your license consumption growth if your tenant has a lot of private channels. You can download the report to check for the details. We provide a Teams Private Channel Site sheet to show the private sites and their size in the report. If you do not want to back up private channels, go to General Settings > Backup Settings to deselect the Back up Private Channels option.
- The downloaded job report will provide a sheet "Summary per Container" to display the license consumptions per container in each service type. The service types and their containers will be displayed in descending order according to the Size.
- If you have ever included the Recordings folder in backup, the size of Recordings folders will be counted in license consumption thereafter.

- **Usage Tab**
  The Usage tab shows the average growth rate in the past 12 months, the largest spike, and the service that has the largest size of protected data. Also, a usage projection will be displayed in the upper-right corner for when your license capacity will be reached.
- **Utilization Tab**
  To view the detailed license consumption, click the Utilization tab. The license consumption of each object type will be listed in descending order. Click the tab of an object type on the left pane to view the usage information for the objects within this object type.

Usage Tab

The Usage tab shows the average growth rate in the past 12 months, the largest spike, and the service that has the largest size of protected data. Also, a usage projection will be displayed in the upper-right corner for when your license capacity will be reached.

You can click Download Report to download the Usage Statistics Report 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 license consumption, click the Utilization tab. The license consumption of each object type will be listed in descending order. Click the tab of an object type on the left pane to view the usage information for the objects within this object type.

You can click Download Report to download the license utilization data, including the overall license utilization information and the size of the protected objects within each object type, and the containers where the objects reside.

Note: For Exchange Online service, the mailboxes in the report will be distinguished by their mailbox types, such as User, Shared, In-Place Archive, and Resource.

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. By default, this report is not available. If you want to enable this report, contact the IBM® Software Support team.

The report is updated once a week and only available to the IBM Spectrum® Protect Plus Online Services Administrator and the Application Administrators of IBM Spectrum Protect Plus Online Services for Microsoft 365. For the Multi-Geo license, only the IBM Spectrum Protect Plus Online Services Administrators can view this report.

Note: This report does not support the trial license 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 the deletion jobs for the Data Subject Access Requests feature and the Manually Delete Backup Data feature, will still be included.

In the Dashboard tab 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.

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 two tabs: Operation Overview and Backup Overview, respectively providing a chart overview for all backup jobs performed within 7 Days or This Month which can help you understand the job progress details of the SharePoint Online backups that are currently running slowly.

Note that the Job Analytics Backup Overview report only supports SharePoint Online backups.

- **View the Charts for Job Operations**
  The Operation Overview tab in the Job Analytics report displays all backup jobs performed within the past 7 days or within the current month in the following charts: Status Base chart and the Object Base 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.

View the Charts for Job Operations

The Operation Overview tab in the Job Analytics report displays all backup jobs performed within the past 7 days or within the current month in the following charts: Status Base chart and the Object Base chart.

You can click 7 Days or This Month to switch the data to report 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 full backup jobs that have been running for 14 days and the incremental backups running for 2 days 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 backup jobs for SharePoint Online sites or Exchange Online mailboxes can still run in the background. The SharePoint Online backup jobs will be automatically paused if the jobs have been running for 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.

Audit User Activities in System Auditor

Navigate to the Reporting > System Auditor page to view the user activities in IBM Spectrum® Protect Plus Online Services for Microsoft 365, divided into the following categories: Backup, Restore, Report, Settings, Common, Export, and Delete.

Procedure

You can perform the following actions on the records of user activities:

- Use the Time Filter, Operation Component filter, and Object Type filter to filter the records.
- Use the Search box to search for the activities by username.
- Click the text of a record to expand or collapse the Details section, or you can click the Expand All or the Collapse All button next to the Search box for expanding or collapsing the details of all records.
- Scroll down to the bottom of the page. You can click the next or the previous button to turn the page to the next or to the previous page.
- Export the System Auditor records. Follow the steps below:
  1. Click the Export Audit Report button on the top bar. The Export window appears.
  2. You can select the Last 7 days option or the Last 30 Days option as the time range for the export.
  3. Click Export. The audit report will be exported to your browser's download location. Click Cancel to cancel the export.

Use Microsoft 365 Unusual Activities Analysis Report

IBM Spectrum® Protect Plus Online Services for Microsoft 365 will learn from your OneDrive for Business backups and warn you for the OneDrive accounts with unusual activities or under a potential ransomware attack.

To learn how you use your environment and build the pattern, the Microsoft 365 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 an email notification. To enable the alert, refer to Configure Alerts.

- **View the Report**
  The Dashboard tab displays the number of OneDrive accounts protected by IBM Spectrum Protect Plus Online Services for Microsoft 365 and the number of suspicious OneDrive accounts. The main chart in the Dashboard tab shows the data of OneDrive accounts tracked over the last 30 days for unusual activities and potential ransomware attacks.
- **Recover OneDrive to a Healthy State**

View the Report

The Dashboard tab displays the number of OneDrive accounts protected by IBM Spectrum® Protect Plus Online Services for Microsoft 365 and the number of suspicious OneDrive accounts. The main chart in the Dashboard tab shows the data of OneDrive accounts tracked over the last 30 days for unusual activities and potential ransomware attacks.

You can click the number to view all accounts 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 OneDrive. You can download the report in an Excel file.

You can also go 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 to view the report with its own details.

When you view the details of a specific OneDrive account, 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 download a list of the files for record or for further investigation.

Recover OneDrive to a Healthy State

Procedure

To recover the OneDrive to a safe state, you can choose the following ways:

- Click Restore on the row of that OneDrive or Click the Restore option next to the time range on the View details pane. In 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 OneDrive for Business Data.
- On the View Details pane, click a safe date and click the Go to Restore Page button. For details on the common restore settings, refer to Restore OneDrive for Business Data.

Licensing Information

- **Microsoft 365 Subscriptions**
  IBM Spectrum® Protect Plus Online Services supports Microsoft 365 solutions and count the total number of users with assigned licenses as described in the sections below. You can identify the number of Assigned Licenses in Microsoft 365 by navigating to the Microsoft 365 admin center > Billing > Licenses. The total quantity reported by IBM Spectrum Protect Plus Online Services will be the total of all the assigned licenses.

Microsoft 365 Subscriptions

IBM Spectrum® Protect Plus Online Services supports Microsoft 365 solutions and count the total number of users with assigned licenses as described in the sections below. You can identify the number of Assigned Licenses in Microsoft 365 by navigating to the Microsoft 365 admin center > Billing > Licenses. The total quantity reported by IBM Spectrum Protect Plus Online Services will be the total of all the assigned licenses.

An example: 100 E5 Licenses + 800 E3 Licenses + 100 F1 Licenses = 1000 Microsoft 365 Users reported by IBM Spectrum Protect Plus Online Services.

- **IBM Spectrum Protect Plus Online Services for Microsoft 365**
  IBM Spectrum Protect Plus Online Services for Microsoft 365 license will be added to your organization's, based on the Microsoft 365 subscription.

IBM Spectrum Protect Plus Online Services for Microsoft 365

IBM Spectrum Protect Plus Online Services for Microsoft 365 license will be added to your organization's, based on the Microsoft 365 subscription.

The table below lists the Microsoft 365 subscriptions for which IBM Spectrum Protect Plus Online Servicescount licenses:

Category	Subscription
For Business	Office 365 Small Business Premium
	Office 365 Midsize Business
	Office 365 Enterprise K2
	Office 365 Enterprise K1 without Yammer
	Office 365 Business Premium - DE
	Office 365 Small Business
	Office 365 Enterprise E4
	Office 365 E1
	Office 365 E2
	Office 365 E3
	Office 365 E3 Developer
	Office 365 E4
	Office 365 E5
	Office 365 E5 without Audio Conferencing
	Microsoft 365 E3
	Microsoft 365 E5
	Microsoft 365 E5 without Audio Conferencing
	Microsoft 365 Business Premium
	Microsoft 365 Business Basic
	Microsoft 365 Business Standard
For Education	Exchange Online (Plan 1) for Students
	Exchange Online (Plan 2) for Faculty
	Office 365 A1 Plus for Faculty
	Office 365 (Plan A3) for Faculty
	Office 365 (Plan A3) for Students
	Office 365 (Plan A4) for Faculty
	Office 365 (Plan A4) for Students
	Office 365 A3 for Faculty
	Office 365 A5 for Faculty
	Microsoft Office 365 (Plan A1) for Faculty
	Microsoft Office 365 (Plan A1) for Students
	Microsoft 365 A5 for Faculty
	Microsoft 365 A3 for Faculty
	Microsoft 365 A3 for Students Use Benefit
Others	Exchange Online (Plan 2)
	Exchange Online Protection
	OneDrive for Business (Plan 1)
	OneDrive for Business (Plan 2)
	SharePoint Online (Plan 1)
	SharePoint Online (Plan 2)
	SHAREPOINTSTANDAR_YAMMER

Note: IBM Spectrum Protect Plus Online Services will keep this list updated to the best of its ability based on current Microsoft SKUs for Microsoft 365. The content above is for information purposes only and is subject to change without notice.

Contact Support to Submit an Issue

If you encounter any trouble using IBM Spectrum® Protect Plus Online Services for Microsoft 365, you can contact IBM Software Support.

Submit Feedback

IBM® provides a platform to collect feedback where you can provide suggestions for product features from your IBM Spectrum® Protect Plus Online Services for 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 Spectrum Protect Plus Online Services for Microsoft 365 experience.

Module Name
: Select IBM Spectrum Protect Plus Online Services for 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 Spectrum Protect Plus Online Services for Microsoft 365 features.

3. Click Submit to submit your feedback to IBM , or click Cancel to leave this pane without submitting feedback.

Introduction to the Data Export Service

The Data Export Service is provided to IBM Spectrum® Protect Plus Online Services for 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 Spectrum Protect Plus Online Services for 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.

- For customers using IBM Spectrum Protect Plus Online Services-provided default storage
  IBM® will retain the backup data in IBM Spectrum Protect Plus Online Services storage for 15 days, subject to the terms of your service agreement, if the subscription to IBM Spectrum Protect Plus Online Services for Microsoft 365 ends. The backup data in IBM Spectrum Protect Plus Online Services 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 Spectrum Protect Plus Online Services 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 Spectrum Protect Plus Online Services for Microsoft 365 interface once your subscription has ended. For details on exporting encryption keys, refer to Export Encryption Key.

After the backup data is ready in your own device, you can use the following solutions to convert the backup data encrypted in IBM Spectrum Protect Plus Online Services format to readable content. for more details, Contact IBM Software Support for assistance.

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 guide.

Errors that occur in an IBM Spectrum® Protect Plus Online Services for 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 failed items 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 fail during the next three backup jobs, the backup status for these items will be marked as Failed, 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 Failed status, contact IBM Software Support for help.

- **SharePoint Online and Microsoft 365 Group Team Site**
- **Exchange Online, Teams, and Microsoft 365 Group Mailbox**
- **Common**

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 failed objects 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 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 failed objects will be automatically included in the next backup job. If this error persists, contact IBM Software Support for help.
An existing connection was forcibly closed by the remote host.	Warning	The connection with SharePoint Online Server is unstable. For backup, the failed objects will be automatically included in the next backup job. If this error persists, contact IBM Software Support for help.
The underlying connection was closed: The connection was closed unexpectedly.	Warning	The connection with SharePoint Online Server is unstable. For backup, the failed objects 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. For backup, the failed objects 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 request timed out. The failed objects 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.
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}.	Failed	{0} displays the URL of the site collection. You must update the service account credentials in IBM Spectrum Protect Plus Online Services and rerun the Auto Discovery scan job.
Access denied. You do not have permission to perform this action or access this resource.	Failed	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.	Failed	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.	Failed	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)	Failed	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.	Failed	This error occurs if you have disabled the ability for non-modern (legacy) authentication protocols within your SharePoint Online tenant.

Job Report Comment	Status	Causes and Solutions
Cannot contact site at the specified URL [SiteURL]. Access to this Web site has been blocked.	Failed	The site collection has been blocked. Contact your SharePoint administrator for help.
The remote server returned an error: (400) Bad Request.	Failed	Invalid request. Contact IBM Software Support for help.
The attempted operation is prohibited because it exceeds the list view threshold enforced by the administrator.	Failed	The number of requests has exceeded the list view threshold limit. Contact IBM Software Support for help.
Cannot complete this action. Please try again.	Failed	Invalid SharePoint Online data may exist in your environment. Contact IBM Software Support for help.
Invalid file name.	Failed	Invalid SharePoint Online data may exist in your environment. Contact IBM Software Support for help.
Stream was not readable.	Failed	An unknown error occurred. Contact IBM Software Support for help.
Microsoft.SharePoint.Client.ServerException: Exception of type 'System.ArgumentException' was thrown. Parameter name: value.	Failed	Unexpected exception of the Client API. Contact IBM Software Support for help.
Microsoft.SharePoint.Client.ServerObjectNullReferenceException: Object reference not set to an instance of an object on server. The object is associated with property CurrentUser.	Failed	Unexpected exception of the Client API. Contact IBM Software Support for help.
The request uses too many resources.	Failed	Resource limitation of client API. Contact IBM Software Support for help.
Save conflict.	Failed	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}.	Failed	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.	Failed	In a Microsoft 365 Group or Team, you can have a maximum of 200 plans.
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 Spectrum® Protect Plus Online Services to update the registration information.		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 Spectrum Protect Plus Online Services 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.	Failed	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 Spectrum Protect Plus Online Services 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.	Failed	{0} displays the name of the private group or team. IBM Spectrum Protect Plus Online Services for 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.	Failed	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.	Failed	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.

Job Report Comment	Status	Causes and Solutions
The account [{0}] does not have permission to impersonate the requested user. Please add Application Impersonation permission for this account in Exchange admin center (permission>admin roles>add) and try again.	Failed	{0} displays the username. The error message appears because the Auto Discovery job failed to assign the **ApplicationImpersonation** permission to this account. Add the permission as instructed and then rerun the Auto Discovery job.
Not all items in this folder are backed up successfully. Error: {0}	Failed	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.	Failed	Exchange Online Server is busy, or the network is unstable. The next backup job will automatically include failed objects. If these objects still fail to be backed up, contact IBM Software Support.
The server cannot service this request right now. Try again later.	Failed	
Too many concurrent connections opened. Cannot open mailbox.	Failed	

Common

Job Report Comment	Status	Causes and Solutions
Cannot find the service account "{0}" in IBM Spectrum® Protect Plus Online Services. To synchronize new service accounts, either run a one-time scan job in Auto Discovery or wait a scheduled scan job to complete.	Failed	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.	Failed	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.	Failed	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.	Failed	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.	Failed	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.	Failed	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.	Failed	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.	Failed	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.	Failed	Check if the user who is used to scan the mailbox has permission or not.
Cannot connect to the device due to network issues.	Failed	Check your device and the storage configurations, especially when your device is FTP/SFTP
There is no data in the backup scope to protect. You can go to the Auto Discovery interface in the IBM Spectrum Protect Plus Online Services portal to review your rules and include additional objects.	Failed	
Cannot find the service account for the destination node. Please configure a service account in IBM Spectrum Protect Plus Online Services and then try again.	Failed	The service account may have been deleted from IBM Spectrum Protect Plus Online Services. Go to the IBM Spectrum Protect Plus Online Services 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 Spectrum Protect Plus Online Services, and then try again.	Failed	The service account may have been deleted from IBM Spectrum Protect Plus Online Services. Go to the IBM Spectrum Protect Plus Online Services 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 Spectrum Protect Plus Online Services to configure an account or profile with access to this mailbox.	Failed	Go to the IBM Spectrum Protect Plus Online Services 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 Spectrum Protect Plus Online Services. Please configure a service account or an app profile with required permissions in IBM Spectrum Protect Plus Online Services, and then try again.	Failed	Go to the IBM Spectrum Protect Plus Online Services 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.	Failed	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.	Failed	The custom device's credentials may be incorrect, or you changed the device location.

Troubleshooting

CO-IncorrectUserNameOrPassword

Issue:
A site failed in backup with the following error code:

- **CO-IncorrectUserNameOrPassword**

Details:
The user credentials of the service account or account pool users may have been updated.
Solution:
You need to verify the user credentials provided to the service account profile or account pool users in the IBM Spectrum® Protect Plus Online Services interface. Then, you can wait for the subsequent backup job and monitor the status.

CO-NotFound

Issue:
The object failed in 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-Throttling

Issue:
Some items failed in 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 Spectrum® Protect Plus Online Services for 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.

Under the condition of service account authentication, you can also configure the account pool to distribute the requests in case of being throttled or blocked.

If you need additional assistance, contact IBM Software Support.

SP-FileBackupFailedDueToVirusScanner

Issue:
A file failed in backup with the following error code:

- **SP-FileBackupFailedDueToVirusScanner**

Details:
While downloading this file via API for backup, the SharePoint Virus Scanner scanned this file and blocked it from being downloaded. You can verify this issue by downloading this file on SharePoint GUI.

Solution:
The file is blocked from being downloaded is because it has the sensitive code (recorded as **Additional information** in this job report comment). For a successful backup of this file, you must remove the sensitive code from this file. If this is not possible and you still want to dismiss this error, you have to delete this file.

SP-PDFBackupFailedDueToIRM

Issue:
A PDF file failed in 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 and cannot be backed up.

Solution:
The locked site is inaccessible. Please check the status of your site. If you want to back up this site, you must unlock 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 Spectrum® Protect Plus Online Services > Microsoft > Auto Discovery > Containers page.

SP-SiteNotExist

Issue:
The site was skipped from 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 IBM Spectrum® Protect Plus Online Services interface to rescan and update the site status. For detailed instructions, refer to Manage Scan Profiles.

SP-WebPartNotExist

Issue:
An item failed in 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.

SP-IRMProtectedFileFailed

Issue:

An IRM protected file failed in the backup with the following error code:

- **SP-IRMProtectedFileFailed**

Details:

The super user's symmetric key configured for the tenant in **Backup Settings** is invalid. Therefore, the backup job failed to decrypt this IRM-protected file for backup.

Solution:

Check the super user configuration in **Backup Settings** and watch out for the status of the subsequent backup jobs. For details on configuring backup settings and super users, refer to Configure Additional Backup Settings, and Configuring Super Users.

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: Use OneDrive for Business and SharePoint or Stream for meeting recordings.

Enable Integration with SCOM

You can enable the integration between IBM Spectrum® Protect Plus Online Services for Microsoft 365 and System Center Operations Manager. With the integration enabled, you can monitor IBM Spectrum Protect Plus Online Services for Microsoft 365 jobs in System Center Operations Manager.
Note: The integration supports System Center Operations Manager 2012 R2 and System Center Operations Manager 2016.
To enable the integration, navigate to IBM Spectrum Protect Plus Online Services > Integration with SCOM, and then configure the settings. For details, refer to Enable Integration with SCOM.

Refer to the table below for the event ID and details that you can monitor in SCOM for IBM Spectrum Protect Plus Online Services for Microsoft 365.

Event ID	Action	Settings	Module
3101	Change Backup Scope	Backup	
3102	Change Backup Frequency		
3201	Start a Restore Job	Restore	
3202	Start an Export Job		
3401	Perform Deletion Job	Data Subject Access Requests	Date management
3402	Export Recovery Point		
3403	Export Report	Remove Unprotected Data	
3501	Generate Job Report	Job Monitor	
3502	Download Job Report		
3503	Download Content		
3602	Change Notification Setting	Notification Settings	Settings
3603	Create User Mapping	Mapping Settings	
3604	Edit User Mapping		
3605	Delete User Mapping		
3606	Create Language Mapping		
3607	Edit Language Mapping		
3608	Delete Language Mapping		
3609	Create Domain Mapping		
3610	Edit Domain Mapping		
3611	Delete Domain Mapping		
3612	Change Backup Setting	General Settings/Export key	
3613	Update Storage Location		
3614	Export Encryption Key		
3615	Create Security Group	Account Management	
3616	Grant User Permission		
3617	Edit Security Group		
3618	Delete Security Group		
3701	Download License Report	License Consumption Report	Reporting
3702	Export System Auditor Report	System Auditor	

Event ID	Action	Settings	Module
3001	Login	Others	
3002	Sign Out		
3003	Contact Support		
3004	Submit Feedback		
3005	Back to AOS		
3006	Start/Finish Job		
3007	Start/Finish Job		
3008	Start/Finish Job		
3010	Start/Finish Job		

Appendices

The following table details the appendices included in this document:

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 Spectrum® Protect Plus Online Services Team at the following website: www.ibm.com/support support team.

Appendix	Description
SharePoint Sites Data Types	Lists the supported and unsupported data types of SharePoint Online sites in IBM Spectrum Protect Plus Online Services for 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.
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.
Yammer Data Types	Lists the supported and unsupported data types of Yammer.
OneDrive for Business Data Types	Lists the supported and unsupported data types of OneDrive for Business.
Document-Related Data Types	Lists the supported and unsupported document-related data types.
Restore Options for Different Object Types	Lists the supported and unsupported restore options upon different object types.

- **SharePoint Sites Data Types**
- **Modern Team Site Data Types**
- **Project Online Data Types**
- **Exchange Online Data Types**
- **Public Folders Data Types**
- **Microsoft 365 Groups Data Types**
- **Teams Data Types**
- **Teams Chat Data Types**
- **Yammer Data Types**
- **OneDrive for Business Data Types**
- **Document-Related Data Types**
  Refer to the following tables for the supported/unsupported/partially supported data types related to document restore.
- **Restore Options for Different Object Types**
- **Restore Conflict Resolutions**

SharePoint Sites Data Types

The table below lists the supported and unsupported SharePoint Sites data types in IBM Spectrum® Protect Plus Online Services for Microsoft 365.

For the document-related data, refer to Document-Related Data Types.

- **Site Collection Settings**
- **Site Settings**
- **List/Library Settings**
- **Admin Center**
- **Features**
- **Templates**
- **Web Parts**
- **Others**

Site Collection Settings

Data Type		Default/Custom App Profile	Service Account
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
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	Supported	Supported
	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
Site collection upgrade		Unsupported	Unsupported

Site Settings

Data Types				Default/Custom App Profile	Service Account	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	
		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	

	Data Types			Default/Custom App Profile	Service Account	Comment
		Configure Search Navigation		Supported	Supported	
	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 go to **Community settings** and select the **Enable reporting of offensive content** option to enable this feature.			Unsupported	Unsupported	
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	

	Data Types		Default/Custom App Profile	Service Account	Comment
	Delete this site		Supported	Supported	
Hold	Hold Reports		Supported	Supported	
	Holds		Supported	Supported	
	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	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.
	Document Version History	No versioning	Supported	Supported	
		Create major versions	Supported	Supported	
		Create major and minor (draft) versions	Supported	Supported	
		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	
Metadata navigation settings	Configure Navigation Hierarchies		Supported	Supported	
	Configure Key Filters		Supported	Supported	
	Configure automatic column indexing for this list		Supported	Supported	

Data Types		Default/Custom App Profile	Service Account	Comment
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 more 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
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
			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
			Category Image	Supported	Supported
			Catalog Item Page Settings	Supported	Supported
		Faceted Navigation	Refiner	Unsupported	Unsupported

		Data Types		Default/Custom App Profile	Service Account
		Custom Properties	Shared Properties	Supported	Supported
			Local Properties	Supported	Supported
User profiles				Unsupported	Unsupported

Features

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
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
	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
	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

	Data Types	Default/Custom App Profile	Service Account
	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

Data Types			Default/Custom App Profile	Service Account
Site Collection Templates	Collaboration	Team Site	Supported	Supported
		Blog	Supported	Supported
		Developer Site	Supported	Supported
		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 Note: This data type does not exist in the GCC High environment.	Supported	Supported
		Business Intelligence Center	Unsupported	Supported
		Compliance Policy Center Note: This data type does not exist in the GCC High environment.	Supported	Supported
		Enterprise Search Center	Supported	Supported
		Enterprise Wiki	Supported	Supported
		My Site Host Note: This data type does not exist in the GCC High environment.	Supported	Supported
		Community Portal	Supported	Supported
		Basic Search Center	Supported	Supported
		Visio Process Repository	Supported	Supported
	Publishing	Publishing Portal	Supported	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 Note: This data type does not exist in the GCC High environment.	Supported	Supported
		Enterprise Search Center Note: This data type does not exist in the GCC High environment.	Supported	Supported
		Basic Search Center	Supported	Supported
		Visio Process Repository	Supported	Supported
	Publishing Note: This data type does not exist in the GCC High environment.	Publishing Site	Supported	Supported
		Publishing Site with Workflow	Unsupported	Supported
		Enterprise Wiki	Supported	Supported
	Duet Enterprise	SAP Workflow Site	Unsupported	Supported
Normal List Templates	Announcements		Supported	Supported
	Asset Library		Supported	Supported
	Calendar		Supported	Supported

	Data Types	Default/Custom App Profile	Service Account
	Contacts	Supported	Supported
	Custom List	Supported	Supported
	Custom List in Datasheet View	Supported	Supported
	Customized Template Note: This data type does not exist in the GCC High environment.	Supported	Supported
	Data Connection Library	Supported	Supported
	Discussion Board Note: This data type does not exist in the GCC High environment.	Supported	Supported
	Document Library	Supported	Supported
	External List	Unsupported	Unsupported
	Form Library	Supported	Supported
	Import Spreadsheet Note: This data type does not exist in the GCC High environment.	Supported	Supported
	Issue Tracking	Supported	Supported
	Links	Supported	Supported
	Picture Library	Supported	Supported
	Promoted Links	Supported	Supported
	Record Library	Supported	Supported
	Related Actions List Note: This data type does not exist in the GCC High environment.	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
	List Template Gallery	Supported	Supported
	Long-Running Operation Status	Supported	Supported
	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	Supported	Supported
	Theme Gallery	Supported	Supported
	Translation Package	Supported	Supported
	Translation Status	Supported	Supported
	User Information List	Supported	Supported
	Variation Labels	Supported	Supported
	Variation logs	Supported	Supported
Design List Templates	Web Part Gallery	Supported	Supported
	Workflow Tasks	Supported	Supported
	No Code Public Workflows	Unsupported	Unsupported

	Data Types	Default/Custom App Profile	Service Account
	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

Data Types		Default/Custom App Profile	Service Account
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
	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

Data Types		Default/Custom App Profile	Service Account
	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
	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
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		Unsupported	Supported
Solution	User Solution		Supported	Supported
Discussion Board	Folder version		Unsupported	Unsupported

Modern Team Site Data Types

The table below shows the specific data types of Modern Team Site that are supported or unsupported in IBM Spectrum® Protect Plus Online Services for Microsoft 365.

Table 1. Data Types

Data Types			Default/Custom App Profile	Service Account
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
	Microsoft 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
	Yammer		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
	Script		Supported	Supported

Project Online Data Types

The table below shows the Project Online data types that are supported or unsupported in IBM Spectrum® Protect Plus Online Services for Microsoft 365.
Note: Apart from the data types detailed below, the data types listed as unsupported in SharePoint Sites Data Types 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 cannot protect the **Project for the web** data due to the lack of APIs.
- 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, subproject, etc.

The following table is provided 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
			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	Supported
			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

Top Level	Second Level		Third Level	Support Status
			%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**
- **PWA Settings**

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
		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

Top Level	Second Level	Third Level		Support Status
	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
	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
			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

Top Level	Second Level	Third Level	Support Status
		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
		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 Spectrum® Protect Plus Online Services for Microsoft 365:

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
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

Top Level	Second Level	Third Level			Support Status
	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	
		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	
		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		Type	Supported

Top Level	Second Level	Third Level		Support Status
		Note: If there are conflicts, the **Budget,** and **Generic** fields will not be updated.	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
			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
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

Top Level	Second Level	Third Level		Support Status
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
		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 Spectrum® Protect Plus Online Services for Microsoft 365:

Data Types		Check Points	Default/Custom App Profile	Service Account
Different types of Mailboxes	User's mailbox		Supported	Supported
	In-Place Archived Mailboxes		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 Note: Unsupported in GCC High environment		Supported	Supported
	Conversation History		Supported	Supported
	Deleted Items		Supported	Supported
	Drafts		Supported	Supported
	Inbox		Supported	Supported

	Data Types	Check Points	Default/Custom App Profile	Service Account
	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
		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

	Data Types	Check Points	Default/Custom App Profile	Service Account
		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
	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
		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

	Data Types	Check Points	Default/Custom App Profile	Service Account
		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
	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 Spectrum® Protect Plus Online Services for Microsoft 365.
Note: If the URL or the name of an object in Public Folder contains "\", "\" will be replaced by "/" on Restore overview page.

Object Level		Check Points	Default/Custom App Profile	Service Account
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
		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

Object Level		Check Points	Default/Custom App Profile	Service Account
		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
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

Object Level		Check Points	Default/Custom App Profile	Service Account
		Font, art word, special character, and display languages	Supported	Supported
Metadata	Enable	Enable	Unsupported	Supported
		Disable	Unsupported	Supported
	Folder Permission	User	Unsupported	Supported
		Group	Unsupported	Supported
	General	Name	Unsupported	Supported
		Path	Unsupported	Supported
		Total items	Unsupported	Supported
		Size	Unsupported	Supported
		Public folder mailbox	Unsupported	Supported
		Modified	Unsupported	Supported
		Maintain per-user read and unread information for this public folder	Unsupported	Supported
	Statistics	Associated items	Unsupported	Supported
		Deleted items	Unsupported	Supported
		Total size of associated items (MB)	Unsupported	Supported
		Total size of deleted items (MB)	Unsupported	Supported
		Owner count	Unsupported	Supported
		Contact count	Unsupported	Supported
		Last modified time	Unsupported	Supported
	Limits	Use organization quota defaults	Unsupported	Supported
		Issue warning at (MB)	Unsupported	Supported
		Prohibit post at (MB)	Unsupported	Supported
		Maximum item size: (MB)	Unsupported	Supported
		Use organization retention defaults	Unsupported	Supported
		Retain deleted items for (days)	Unsupported	Supported
		Use organization age limit defaults	Unsupported	Supported
		Age limit for folder content (days)	Unsupported	Supported

Microsoft 365 Groups Data Types

Refer to the table below for the supported and unsupported data types of Microsoft 365 Groups in IBM Spectrum® Protect Plus Online Services for Microsoft 365.
Note: IBM Spectrum Protect Plus Online Services for 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 Spectrum Protect Plus Online Services interface to configure a Microsoft delegated app for IBM Spectrum Protect Plus Online Services for 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 Spectrum Protect Plus Online Services for 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.

Object Level			Details	Default/Custom App Profile	Service Account	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	

	Object Level		Details	Default/Custom App Profile	Service Account	Note
			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	
		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	
Planner	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	Unsupported	Unsupported	
	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	
		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				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 Spectrum® Protect Plus Online Services, 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.
- Private Channels in Teams can now be protected with limitations. For details, refer to Components in Private Channels.
- IBM Spectrum Protect Plus Online Services for 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.
- 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 six tabs: Planner, Word, Excel, PowerPoint, PDF, and document library tab.

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**
- **Components in Private Channels**
- **Settings and Permissions**
- **Planner Data**
- **Archived Teams**

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.
  - Currently, the restore as posts feature only works under the circumstance where you are using service account authentication to scan Teams and have a Microsoft Delegated app configured in your tenant.
- If you are using custom app authentication, ensure your app has access to the protected APIs of Microsoft Teams. To request access to the protected APIs, refer to the Microsoft article: Protected APIs in Microsoft Teams. Otherwise, the public and private channels' conversations cannot be protected.
- 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		Comment
			Restore to HTML file	Restore as Posts	
Format	Add subject	Supported	Supported	Supported	
	Mention/Tag (@)	Supported	Supported	Supported	The link cannot be kept after being restored to the HTML file.
	Bold	Supported	Supported	Supported	
	Italic	Supported	Supported	Supported	
	Underline	Supported	Supported	Supported	
	Strikethrough	Supported	Supported	Supported	
	Text highlight color	Supported	Supported	Supported	
	Font color	Supported	Supported	Supported	
	Font size	Supported	Supported	Supported	
	Monospaced	Supported	Supported	Supported	
	Heading	Supported	Supported	Supported	
	Paragraph	Supported	Supported	Supported	
	Decrease indent	Supported	Supported	Supported	

Components/Properties		Default/Custom App Profile	Service Account		Comment
			Restore to HTML file	Restore as Posts	
	Increase indent	Supported	Supported	Supported	
	Bulleted list	Supported	Supported	Supported	
	Numbered list	Supported	Supported	Supported	
	Quote	Supported	Supported	Supported	
	Insert link	Supported	Supported	Partially Supported	
	Code Snippet	Unsupported	Unsupported	Supported	API limitation
	Inset horizontal rule	Supported	Supported	Supported	
	Insert table	Supported	Supported	Supported	
	Mark as important	Supported	Supported	Supported	
	Show for me	Unsupported	Unsupported	Unsupported	API limitation
	Show for members	Unsupported	Unsupported	Unsupported	API limitation
Post in multiple channels		Unsupported	Unsupported	Unsupported	
Announcement type post's specific elements	Background	Unsupported	Unsupported	Supported	
	Icon	Unsupported	Unsupported	Supported	
	Color scheme	Unsupported	Unsupported	Supported	
	Subheader	Supported	Supported	Supported	
	Headline	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	
	Browse Teams and Channels	Supported	Supported	Supported	
	OneDrive	Supported	Supported	Supported	
	Upload from my computer	Supported	Supported	Supported	
Emoji		Supported	Supported	Supported	
Giphy		Supported	Supported	Supported	
Praise		Unsupported	Unsupported	Partially Supported	
Sticker		Supported	Supported	Supported	
Stream		Unsupported	Unsupported	Supported	
Form		Unsupported	Unsupported	Partially Supported	
News		Unsupported	Unsupported	Partially Supported	
Places		Supported	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	Partially Supported	
Weather		Supported	Supported	Partially Supported	
Wikipedia Search		Unsupported	Unsupported	Partially Supported	
YouTube		Unsupported	Unsupported	Partially Supported	
Post		Supported	Supported	Supported	
Voice Message		Unsupported	Unsupported	Unsupported	
Reply		Supported	Supported	Supported	
Edit Post/Reply		Partially Supported	Partially Supported	Unsupported	The Edited status of a post or reply cannot be kept.
Delete post/Reply		Unsupported	Unsupported	Unsupported	The message for a post or a reply being deleted cannot be kept.
Notification		Unsupported	Unsupported	Unsupported	
Mark as unread		Unsupported	Unsupported	Unsupported	
Like/Unlike		Unsupported	Unsupported	Unsupported	
Copy Link		Supported	Supported	Supported	
The "Save this message" mark		Unsupported	Unsupported	Unsupported	
Get email address	Send email to channel	Partially supported	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	
		ShareFile		Unsupported	Unsupported	
		Google Drive		Unsupported	Unsupported	
Tab	Add a tab			Supported	Supported	Restore job supports adding your tabs back.
	Word			Supported	Supported	Supports adding the tabs back and update the tabs to the previous settings and configurations.
	Excel					
	PowerPoint					
	PDF					
	Document library					
	Planner					
	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 Channels

Refer to the following table for the supported and unsupported status of the components in Private Channels, and the supported and unsupported status for the data that is added or attached to the Private Channels through the corresponding methods.

Note the following for the Private 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 Channels can only be restored through the time-based restore wizard, and Private Channels do not support out-of-place restore.

Conversations

Components/Properties		App Profile	Service Account		Comment
			Restore to HTML file	Restore as Posts	
Format	Add subject	Supported	Supported	Supported	
	Mention (@)	Supported	Supported	Supported	
	Bold	Supported	Supported	Supported	
	Italic	Supported	Supported	Supported	
	Underline	Supported	Supported	Supported	
	Strikethrough	Supported	Supported	Supported	
	Text highlight color	Supported	Supported	Supported	

Components/Properties		App Profile	Service Account		Comment
			Restore to HTML file	Restore as Posts	
	Font color	Supported	Supported	Supported	
	Font size	Supported	Supported	Supported	
	Monospaced	Supported	Supported	Supported	
	Heading	Supported	Supported	Supported	
	Paragraph	Supported	Supported	Supported	
	Decrease indent	Supported	Supported	Supported	
	Increase indent	Supported	Supported	Supported	
	Bulleted list	Supported	Supported	Supported	
	Numbered list	Supported	Supported	Supported	
	Quote	Supported	Supported	Supported	
	Insert link	Supported	Supported	Unsupported	
	Code Snippet	Unsupported	Unsupported	Supported	API limitation
	Inset horizontal rule	Supported	Supported	Supported	
	Insert table	Supported	Supported	Supported	
	Mark as important	Supported	Supported	Supported	
Post in multiple channels		Unsupported	Unsupported	Unsupported	
Announcement type post's specific elements	Background	Unsupported	Unsupported	Supported	
	Color scheme	Unsupported	Unsupported	Supported	
	Subheader	Supported	Supported	Supported	
	Headline	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	
	Browse Teams and Channels	Supported	Supported	Supported	
	OneDrive	Supported	Supported	Supported	
	Upload from my computer	Supported	Supported	Supported	
Emoji		Supported	Supported	Supported	
Giphy		Supported	Supported	Supported	
Sticker		Supported	Supported	Supported	
Post		Supported	Supported	Supported	
Voice Message		Unsupported	Unsupported	Unsupported	
Reply		Supported	Supported	Supported	
Edit Post/Reply		Partially Supported	Partially Supported	Unsupported	The Edited status of a post or reply cannot be kept.
Delete post/Reply		Unsupported	Unsupported	Supported	The message for a post or a reply being deleted cannot be kept.
Mark as unread		Unsupported	Unsupported	Unsupported	
Like/Unlike		Unsupported	Unsupported	Unsupported	
The "Save this message" mark		Unsupported	Unsupported	Unsupported	
Get email address	Send email to channel	Partially Supported	Partially Supported	Unsupported	The To information and the Download original email link are not kept in the restored HTML file.

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	

Objects	Components/Properties		App Profile	Service Account	Comment
		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	
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

Refer to the table below for the supported and unsupported settings and permissions.

Components	Settings/Permissions			Default/Custom App Profile	Service Account	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 Note: 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 Note: 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	

Components		Settings	Permissions		Default/Custom App Profile	Service Account	Comment
			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
	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	

Components	Settings/Permissions	Default/Custom App Profile	Service Account	Comment
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 authen-tication, 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	

Planner Data

Refer to the table below for the supported Planner data and note the following issues for Planner backup and restore:

Authentication Method

- To protect Planner data, you can choose to configure a service account profile to scan Teams in Auto Discovery or configure a Delegated app to protect Planner data when using app profile authentication for Auto Discovery.
  Note: If you use a service account for Auto Discovery, IBM Spectrum® Protect Plus Online Services for Microsoft 365 will use the service account to protect the Planner data regardless of whether that Delegated app is in place.
  If your organization uses multi-factor authentication (MFA) in Microsoft 365, by default, Planner data cannot be protected using service account authentication. For more details, refer to the information in the table of Authentications in Auto Discovery and Hybrid Approach.

- If you are using a service account profile for Auto Discovery, the service account must be both the owner and a member of the teams/groups.
- If you are using the Delegated app, the authentication user of this app must have an Exchange license. This authentication user is also required to be the owner and member of the teams/groups, and you can choose to allow the scan job to automatically add the authentication user as the owner and member of the scanned teams/groups.

General

- 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 Support team for assistance.

Data Type			Default/Custom App Profile	Service Account
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

	Data Type		Default/Custom App Profile	Service Account
		Comments	Supported	Supported
		Label	Supported	Supported
		Priority	Unsupported	Unsupported
Chart		Status	Supported	Supported
		Members	Supported	Supported

Archived Teams

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.

Object Type	Backup Status	Restore Status	Note
Teams mailbox	Supported	Supported	
Teams team site	Supported	Supported	
Public channels	Supported	Supported	
Private channels	Partially Supported	Partially Supported	If the team has been archived before being registered to Auto Discovery, the private channels' sites cannot be registered to IBM Spectrum Protect Plus Online Services or protected. If the team is archived after being registered, the private channels' sites can be protected. The Teams backup service does not protect the content of private channels other than the private channels' sites. The backup and restore the status of private channels in an archived team does not affect the job status and will not be reported in the job report.
Planner	Supported	Supported	
Tabs	Unsupported	Unsupported	The backup and restore the status of tabs and apps does not affect the job status and will not be reported in the job report.
Apps	Unsupported	Unsupported	

Teams Chat Data Types

Note the following about the Microsoft Teams Chat service and refer to the table below for the supported and unsupported data types of Teams chats.

- Microsoft Teams Chat service in IBM Spectrum® Protect Plus Online Services for Microsoft 365 currently uses the Microsoft Graph Teams Export API to export Teams chat messages to an HTML file. Currently, we are using the Export API model A to protect the chats of Microsoft 365 users with any of the following licenses:
  - Microsoft 365 A5 for Faculty
  - Microsoft 365 E5
  - Microsoft 365 E5 Compliance
  - Microsoft 365 E5 Security
  - Microsoft 365 E5 without Audio Conferencing
- The Microsoft Teams Chat backup service does not support GCC tenants.

Components/Properties		Restore to HTML file	Comment
Format	Mention/Tag (@)	Unsupported	The link cannot be kept after being restored to the HTML file.
	Bold	Supported	
	Italic	Supported	
	Underline	Supported	
	Strikethrough	Supported	
	Text highlight color	Supported	
	Font color	Supported	
	Font size	Supported	
	Monospaced	Supported	
	Heading	Supported	
	Paragraph	Supported	
	Decrease indent	Supported	
	Increase indent	Supported	
	Bulleted list	Supported	
	Numbered list	Supported	
	Quote	Supported	
	Insert link	Supported	
	Code Snippet	Supported	
	Inset horizontal rule	Supported	
	Insert table	Unsupported	

Components	Properties	Restore to HTML file	Comment
	Mark as important	Supported	
	Mark as urgent	Unsupported	
Attach File	OneDrive	Unsupported	
	Upload from my computer	Unsupported	
Loop components	Bulleted list	Unsupported	
	Numbered list	Unsupported	
	Checklist	Unsupported	
	Paragraph	Unsupported	
	Table	Unsupported	
	Task list	Unsupported	
Emoji		Supported	
Giphy		Supported	
Praise		Unsupported	
Sticker		Supported	
Stream		Unsupported	
Form		Unsupported	
News		Supported	
Places		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		Supported	
Weather		Supported	
Wikipedia Search		Supported	
Post		Supported	
Voice Message		Unsupported	
Reply		Supported	
Edit Post/Reply		Supported	
Delete post/Reply		Supported	
Mark as unread		Unsupported	
Like/Unlike		Unsupported	
The “Save this message” mark		Unsupported	
Translate		Unsupported	
Image (screenshot)		Supported	
Image (attachment)		Unsupported	
Recordings/Video		Unsupported	

Yammer Data Types

The table below lists the data types supported or unsupported for Yammer in IBM Spectrum® Protect Plus Online Services for Microsoft 365:

Note:

- Yammer services currently support in place recovery only (restoring to the original location), meaning the Yammer community needs to be there already, as well as the ability to export files and conversations.
- The External Network, Private Message, and Classic Yammer are not supported.
- Only the message content and comment are supported for the Discussions, Questions, Praise, and Poll messages. In the current release, Yammer messages are only available in the time-based recovery wizard and will be restored to HTML files.

Data Type			Default Yammer App
Internal Network	Yammer Group		Supported
	Yammer community Members		Supported
	Yammer community favorites status (Only in new Yammer view)		Unsupported
	Yammer Group settings	Name	Unsupported
		Description	Unsupported
		Image	Unsupported
		Who can view conversations and post messages?	Unsupported
		Default publisher type	Unsupported
		Pattern (Only in classic Yammer view)	Unsupported
	Mute/Unmute Yammer community status (Only in new Yammer view)		Unsupported
	Yammer community mute for Network status (Only in new Yammer view)		Unsupported
	Yammer community cover photo (Only in new Yammer view)		Unsupported
	Info		Unsupported
	Pinned		Unsupported
	Related Groups (Only in classic Yammer 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 Yammer group site		Supported
	Content in Yammer 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

OneDrive for Business Data Types

IBM Spectrum® Protect Plus Online Services for Microsoft 365 for OneDrive for Business 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 for Business since OneDrive for Business is the cloud service used to securely store, share, and access your files.

Refer to the table below for the supported and unsupported data types in OneDrive for Business.

Data Types			Default/Custom App Profile	Service Account
Lists/libraries	Permission	Users Note: Restore the users before the content.	Supported	Supported
		Role Assignments	Supported	Supported
	Versioning settings	Content Approval	Supported	Supported
	Document Version History	No versioning	Supported	Supported
		Create major versions	Supported	Supported
		Create major and minor (default) versions	Supported	Supported
	Content Types		Unsupported	Unsupported
	Columns		Unsupported	Unsupported
	List Views		Unsupported	Unsupported
Documents	Permission	Users Note: Restore the users before the content.	Supported	Supported
		Role Assignments	Supported	Supported
	Column values	Author	Supported	Supported
		Editor	Supported	Supported
		Modified	Supported	Supported
		Created	Supported	Supported
		Column values on the edit and view form	Supported	Supported
		Column values for the required fields	Supported	Supported
		Other	Unsupported	Unsupported
	Content		Supported	Supported
History Version	Column values	Author	Supported	Supported
		Editor	Supported	Supported
		Modified	Supported	Supported
		Created	Supported	Supported
		Column values on the Version History	Supported	Supported
		Other	Supported	Supported
	Content		Unsupported	Unsupported
List view			Supported	Supported
Workflow			Unsupported	Unsupported
Term set			Unsupported	Unsupported
Site settings			Unsupported	Unsupported
Library settings			Unsupported	Unsupported
Subsites			Unsupported	Unsupported
IRM			Supported	Supported
Asset library			Supported	Supported
Other lists/libraries			Unsupported	Unsupported
Web part			Unsupported	Unsupported
Site features			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
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 Folders	_catalogs	Supported	Supported
		_cts	Partially Supported	Supported
		_vti_pvt	Supported	Supported
		images	Supported	Supported
		Lists	Supported	Supported
		m	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
	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 suspported for restore as Microsoft no longer supports SharePoint 2010 workflows in Microsoft 365.

Data Types		Default/Custom App Profile	Service Account
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

Data Types		Default/Custom App Profile	Service Account
	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
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

Column

Data Types			Default/Custom App Profile	Service Account
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
	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

	Data Types		Default/Custom App Profile	Service Account
		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
		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
		Category	Supported	Supported
		Comments	Supported	Supported
		Contributor	Supported	Supported
		Copyright	Supported	Supported
		Coverage	Supported	Supported
		Date Created	Supported	Supported

	Data Types		Default/Custom App Profile	Service Account
		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
	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

	Data Types		Default/Custom App Profile	Service Account
		Locale ID	Supported	Supported
		Product	Supported	Supported
		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
		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

	Data Types		Default/Custom App Profile	Service Account
		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
		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
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

	Data Types		Default/Custom App Profile	Service Account
		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
		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
		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

	Data Types		Default/Custom App Profile	Service Account
	Special Content Types	Unknown Document Type	Supported	Supported

Restore Options for Different Object Types

The table below shows the supported/unsupported restore options for different object types.

Note:

- The Project Online data, the Apps, and the Planner data (plans and tasks) are not supported when using the app profile only.
- Data exporting in IBM Spectrum® Protect Plus Online Services for Microsoft 365 does not support exporting metadata.

Object Type	Level	Restore to Original Location	Restore to Another Location	Restore to Storage	Export
SharePoint Online	Site Collection	Supported	Supported (SharePoint Site Collection or OneDrive)	Unsupported	Unsupported
	Site	Supported	Supported (SharePoint Site Collection or OneDrive)	Unsupported	Unsupported
	List/Library	Supported	Supported (Share Point Site Collection, OneDrive, or the List/Library in Share Point Site Collection or OneDrive.)	Supported	Supported
	Folder	Supported	Supported (Library or Folder in SharePoint or OneDrive)	Supported	Supported
	Item/Document	Supported	Supported (Library or Folder in SharePoint or OneDrive)	Supported	Supported
	Apps	Supported	Supported (Share Point Site Collection or OneDrive)	Unsupported	Unsupported
Exchange Online	Mailbox	Supported	Supported (Mailbox)	Supported	Supported
	Folder	Supported	Supported (Mailbox/Folder)	Supported	Supported
	Mailbox Item	Supported	Supported (Folder)	Supported	Supported
OneDrive for Business	OneDrive for Business User	Supported	Supported (OneDrive/SharePoint Online site collection)	Unsupported	Supported
	Library	Supported	Supported (OneDrive, SharePoint, or the Library in OneDrive/SharePoint)	Supported	Supported
	Folder	Supported	Supported (Library or folder in OneDrive/SharePoint)	Supported	Supported
	Document	Supported	Supported (Library or folder in OneDrive/SharePoint)	Supported	Supported
Microsoft 365 Groups	Group	Supported	Supported (Group)	Unsupported	Unsupported
	Group Team Site	Supported	Supported (Group)	Unsupported	Unsupported
	Site	Supported	Unsupported	Unsupported	Unsupported
	List/Library	Supported	Unsupported	Supported	Supported
	Folder in SharePoint	Supported	Unsupported	Supported	Supported
	Item/Document	Supported	Unsupported	Supported	Supported
	Apps	Supported	Unsupported	Unsupported	Unsupported
	Plan	Supported	Supported	Unsupported	Unsupported
	Task	Supported	Unsupported	Unsupported	Unsupported
	Group Mailbox	Supported	Supported (Group)	Supported	Supported
	Folder in Mailbox	Supported	Unsupported	Supported	Supported
	Mailbox Item	Supported	Unsupported	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

Object Type	Level		Restore to Original Location	Restore to Another Location	Restore to Storage	Export
	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
Teams	Teams		Supported	Unsupported	Unsupported	Unsupported
	Group Mailbox		Supported	Supported (Team)	Unsupported	Unsupported
	Folder in Mailbox		Supported	Unsupported	Unsupported	Unsupported
	Mailbox Item		Supported	Unsupported	Unsupported	Unsupported
	Team Site		Supported	Supported (Team)	Unsupported	Unsupported
	Sites		Supported	Unsupported	Unsupported	Unsupported
	List/Library		Supported	Unsupported	Unsupported	Unsupported
	App		Supported	Unsupported	Unsupported	Unsupported
	Folder in SharePoint		Supported	Supported (Channel)	Supported	Supported
	Document		Supported	Supported (Channel)	Supported	Supported
	Items		Supported	Unsupported	Supported	Supported
	Plan		Supported	Supported (Team)	Unsupported	Unsupported
	Task		Supported	Unsupported	Unsupported	Unsupported
	Public Channel	Channel	Supported	Supported (Team)	Supported	Supported
		Conversations	Supported	Unsupported	Supported	Supported
		Files	Supported	Supported (Teams)	Supported	Supported
	Private Channel	Private Channel	Supported	Unsupported	Supported	Supported
		Conversations	Supported	Unsupported	Supported	Supported
		Files	Supported (Channel)	Supported	Supported	Supported
	Meeting		Supported	Unsupported	Unsupported	Unsupported
	Group conversation		Supported	Unsupported	Unsupported	Unsupported
Microsoft Teams Chat	User		Unsupported	Unsupported	Unsupported	Supported
	Chat		Unsupported	Unsupported	Unsupported	Supported
	Chat Message		Unsupported	Unsupported	Unsupported	Supported
Yammer Note: In the current release, Yammer messages are only available in the timebased recovery wizard and will be restored to HTML files.	Yammer Community		Supported	Unsupported	Unsupported	Unsupported
	Site Collection		Supported	Unsupported	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
	Yammer Messages		Supported	Unsupported	Supported	Supported

- **Teams Data Supported for Out-of-Place Restore**

Teams Data Supported for Out-of-Place Restore

How to Find Data	Source Object	Destination Object	Action	Comment
Object-Based Restore	Group Mailbox	Teams	Attach	Only restore Inbox and Calendar.
	Group Team Site	Teams	Attach	Permissions are not supported yet.
	Plan	Teams	Attach	Plan configurations and the tasks that belong to the selected plans can be restored.
	Folder in a team site	Channel	Attach	
	Documents	Channel	Attach	

How to Find Data	Source Object	Destination Object	Action	Comment
Time-Based Restore Note: The Private Channels can only be restored through the time-based restore wizard, but Private Channels do not support the out-of-place restore.	Channel	Teams	Attach	Channel settings, conversations, and files can be restored.
	Group Team Site	Teams	Attach	
	Plan	Teams	Attach	Plan configurations and the tasks belong to the selected plans can be restored.
	Channels' Files folder	Channel	Attach	
	Folder and files in the Channel's Files folder	Channel	Attach	
	Folder in a team site	Channel	Attach	
	Documents	Channel	Attach	

Restore Conflict Resolutions

Refer to the table below for the available conflict resolutions against each object type in Exchange Online, OneDrive for Business, 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 for Business	OneDrive for Business 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	/
	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

Service Type	Object Type	Container Level Conflict Resolution	Content Level Conflict Resolution	App Conflict Resolution
	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
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
	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

Service Type	Object Type	Container Level Conflict Resolution	Content Level Conflict Resolution	App Conflict Resolution
	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
	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	/
	Private Channel	Skip Merge Replace	Skip Overwrite Overwrite by Last Modified Time Append an “_1” to the Item/Document	/
	Private Channel > Conversations	/	/	/

Service Type	Object Type	Container Level Conflict Resolution	Content Level Conflict Resolution	App Conflict Resolution
	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	/
Yammer	Yammer Community	Skip Merge	Skip Overwrite Overwrite by Last Modified Time Append an “_1” to the Item/Document	Skip Overwrite
	Yammer Messages	Skip Merge Replace	Skip Overwrite Overwrite by Last Modified Time Append an “_1” to the Item/Document	/
	Yammer Files	Skip Merge Replace	Skip Overwrite Overwrite by Last Modified Time Append an “_1” to the Item/Document	/
	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	/

Service Type	Object Type	Container Level Conflict Resolution	Content Level Conflict Resolution	App Conflict Resolution
	Plan	/	Skip Overwrite	/
	Task	/	Skip Overwrite	/
Microsoft Teams Chat	User	/	/	/
	Chat	/	/	/
	Chat Message	/	/	/

IBM Spectrum Protect Plus Online Services Web API

- **IBM Spectrum Protect Plus Online Services Web API Updates**
- **Download SDK**
  Downloads the client-side library that is used to communicate with IBM Spectrum Protect Plus Online Services.
- **Account Logon**
  Sets the information of the account for logging into IBM Spectrum Protect Plus Online Services.
- **Get Audit Records**
  Gets the audit records for activities in your IBM Spectrum Protect Plus Online Services tenant within a time range.
- **Get Segmented Audit Records**
  Gets the segmented audit records for activities in your IBM Spectrum Protect Plus Online Services tenant for IBM Spectrum Protect Plus Online Services and IBM Spectrum Protect Plus Online Services for Microsoft 365.
- **Get Data Centers**
  All available data centers in IBM Spectrum Protect Plus Online Services.
- **Get Credential Profiles**
  Gets your tenant's app profiles or Microsoft 365 service account profiles.
- **Batch Import Objects**
  Imports a batch of Microsoft 365 objects into a container.
- **Add Container**
  Adds a container to an advanced mode scan profile.
- **Register a Partner's Customer**
  Register a Partner's Customer for IBM Spectrum Protect Plus Online Services.
- **Get IBM Spectrum Protect Plus Online Services for Microsoft 365 Job Information**
  Gets the job information of IBM Spectrum Protect Plus Online Services for Microsoft 365.
- **Get IBM Spectrum Protect Plus Online Services for Microsoft 365 License Consumptions**
  Gets the License Consumption Report for IBM Spectrum Protect Plus Online Services for Microsoft 365.

IBM Spectrum Protect Plus Online Services Web API Updates

Release Date: July 31, 2022

Improved the **Response Information** of APIs that can be used to get audit records for user activities in your IBM Spectrum Protect Plus Online Services tenant. For details, refer to Get Audit Records and Get Segmented Audit Records.

Download SDK

Downloads the client-side library that is used to communicate with IBM Spectrum® Protect Plus Online Services.

SDK link: https://www.nuget.org/packages/IBMSPPOS.Public.Sdk

Account Logon

Sets the information of the account for logging into IBM Spectrum® Protect Plus Online Services.

Note: Only supports local accounts and Microsoft 365 accounts, and the accounts must have the Service Administrator role in IBM Spectrum Protect Plus Online Services.

Examples

```
var context = PublicApi.GetContext("https://api.spponlineservices.ibm.com", "username", "password");
```

Request Information

Represents the information of an IBM Spectrum Protect Plus Online Services account with the Service Administrator role.

Element	Description	Type
Username	Sets the username of the account used to log into IBM Spectrum Protect Plus Online Services.	String
Password	Sets the password of the account used to log intoIBM Spectrum Protect Plus Online Services.	String

Get Audit Records

Gets the audit records for activities in your IBM Spectrum® Protect Plus Online Services tenant within a time range.

You can get the audit records for IBM Spectrum Protect Plus Online Services and IBM Spectrum Protect Plus Online Services for Microsoft 365.

Note: These command lines support getting a maximum of 200 audit records. If you would like to get all the audit records for specific products in a certain data center within a long time range, use Get Segmented Audit Records.

Examples

```
var context = PublicApi.GetContext("https://api.spponlineservices.ibm.com", "username", "password");

var records = context.AuditService.GetAuditRecords(DateTime.UtcNow.AddDays(-30).Ticks, DateTime.UtcNow.Ticks);
```

Note: For the start time and end time of the time range, use the **Date Time** struct to represent an instant in time.

Response Information

The response when getting audit records of activities in your IBM Spectrum Protect Plus Online Services tenant.

Element	Description	Type
ActionName	Operation name	String
ActionUser	Operation user	String
ActionParameters	Operation parameters	String
ActionTime	Operation time	String
ControllerName	Operation controller name	String
Product	Product name	String
PreviousValue	Previous value	String
CurrentValue	Current value	String
PartnerTenantOwner	Partner tenant owner	String
Status	Operation status	String
Comment	Operation comment	String
ObjectType	Operation object type	String
OperationType	Operation type	String
Module	Operation module	String
Functionality	Operation functionality	String
ObjectName	Operation object name	String

Get Segmented Audit Records

Gets the segmented audit records for activities in your IBM Spectrum® Protect Plus Online Services tenant for IBM Spectrum Protect Plus Online Services and IBM Spectrum Protect Plus Online Services for Microsoft 365.

You can specify the products and data centers for the audit records that you want to obtain.

Examples

```
var context = PublicApi.GetContext("https://api.spponlineservices.ibm.com","username", "password");

var records = context3.AuditService.SegmentedQueryAudit(10, 0, $"actiontime ge {"2020-
10-01T01:02:03Z"} and actiontime le { "2020-10-05T01:02:03Z"} and product eq
'Office365Backup' and geolocation in ('CAN','EUR','NAM')");
```

Request Information

Element	Description	Type	Required
Top	Specifies the count of the audit records that you want to get. Set the property to 0, if you do not want to set up the limit for the number of audit records to get. If you do not set up the property, the command lines will get the first 200 audit records by default.	int	No

Element	Description	Type	Required
Skip	Specifies the count of the audit records that you want to skip. The command lines will get the audit records starting from the number after the specified.	int	No
Actiontime	Specifies the time range to get the audit records. The time range between the start action time and end action time cannot be more than 7 days.	string	No
Product	Specifies the products that you want to get the audit records for.	String Valid values are: **Portal** for IBM Spectrum Protect Plus Online Services **Office365 Backup** for IBM Spectrum Protect Plus Online Services for Microsoft 365	No
Geolocation	Specifies the data center where to get the audit records.	string Valid values are: **CAN** for Canada **EUR** for Europe / Middle East / Africa **NAM** for North America For more details on the code values, refer to this Microsoft article	No

Response Information

The response when getting segmented audit records of activities in your IBM Spectrum Protect Plus Online Services tenant.

Element	Description	Type
ActionName	Operation name	String
ActionUser	Operation user	String
ActionParameters	Operation parameters	String
ActionTime	Operation time	String
ControllerName	Operation controller name	String
Product	Product name	String
PreviousValue	Previous value	String
CurrentValue	Current value	String
PartnerTenantOwner	Partner tenant owner	String
Status	Operation status	String
Comment	Operation comment	String
ObjectType	Operation object type	String
OperationType	Operation type	String
Module	Operation module	String
Functionality	Operation functionality	String
ObjectName	Operation object name	String

Get Data Centers

All available data centers in IBM Spectrum® Protect Plus Online Services.

To get all available data centers in IBM Spectrum Protect Plus Online Services, use the following method:

```
var partnerContext = PublicApi.GetParnterContext("https://api.spponlineservices.ibm.com",
"partnername","partnerpassword");

var dataCenters = partnerContext.PartnerService.GetDataCenters();
```

Response Information

The response of getting available data centers in IBM Spectrum Protect Plus Online Services.

Element	Description	Type
Id	Displays the ID of a data center.	String
Name	Displays the name of a data center.	String

Get Credential Profiles

Gets your tenant's app profiles or Microsoft 365 service account profiles.

Examples

```
var context = PublicApi.GetContext("https://api.spponlineservices.ibm.com",
"username", "password");

var profiles = context.TenantService.GetCredentialProfiles();
```

Response Information

The response of getting credential profiles.

Element	Description	Type
Id	Displays a profile's ID.	String
Name	Displays a profile's name.	String
Type	Displays a credential profile's type.	Enum The returned value can be: ServiceAccount (a Microsoft 365 service account profile) AppToken (an app profile)
AppProfileType	Displays an app profile's type.	The returned value can be:SharePointOnline (for Microsoft 365 all permissions) AzureAD (for Microsoft Azure AD) SharePoint (for Microsoft 365 SharePoint Online permission) Exchange (for Microsoft 365 Exchange Online permission)

Batch Import Objects

Imports a batch of Microsoft 365 objects into a container.

Examples

```
var context = PublicApi.GetContext("https://api.spponlineservices.ibm.com", "username", "password");
var profiles = context.TenantService.GetCredentialProfiles();
var biResult = context.TenantService.BatchImportObjects(new ImportObjectsModel()
{
 Container = "Default Site Collection Container",
 ImportMode = BatchImportMode.ServiceAccountProfile,
 ProfileId = profiles.First().Id
 IsUserEnableMFA = false,
 O365UserName = "testuser@userdomain.onmicrosoft.com",
 O365UserPassword = "******",
 Objects = new List<string>() {"https://userdomain.sharepoint.com/sites/testteam"},
 SharePointAdminUrl = "https://userdomain-admin.sharepoint.com",
 ObjectType = RemoteNodeType.SiteCollection,
});
```

Request Information

Represents the request to import a batch of objects into a container.

Element	Description	Type	Required
ContainerName	Sets the container's name.	String	Yes
ImportMode	Sets the method used to retrieve a Microsoft 365 account's information from your Microsoft 365 environment.	Enum Valid values: Unserviceable (use an existing service account profile) AppProfile (use an existing app profile) Manually Account (manually designate a Microsoft 365 account)	Yes
ProfileId	Sets the ID of a Microsoft 365 service account profile or app profile.	String	
IsUserEnableMFA	True, if the account has enabled MFA. Otherwise, false.	Bool	Yes, if the ImportMode is set to ManuallyAccount. Otherwise, no.
O365UserName	Sets the username of a Microsoft 365 account that meets the requirements of objects batch import.	String	
O365UserPassword	Sets the password of the account.	String	

Element	Description	Type	Required
SharePointAdminUrl	Sets the Share Point Online admin center URL.	String	
ObjectType	Sets the type for the objects you want to import.	Enum Valid values: SiteCollection (for SharePoint Sites) Mailbox (for Mailboxes) OneDrive (for OneDrive for Business) Office365Group (for Microsoft 365 Groups)	Yes
Objects	Sets the objects you want to import.	List<String>	Yes

Add Container

Adds a container to an advanced mode scan profile.

Example

```
var context = PublicApi.GetContext("https://api.spponlineservices.ibm.com", "username", "password");

      var cResult = context.TenantService.AddContainer(new RemoteGroupNode()
                {
                     ContainerName = "APITestContainer",
                     NodeType = RemoteNodeType.SiteCollection,
                     ScanProfileName = "Test",
                     Rule = new FilterPolicyContent()
                     {
                        Name = "APITestRule",
                        NodeType = RemoteNodeType.SiteCollection,
                        Filters= new List<FilterRule>()
                         {
                            new FilterRule()
                             {
                               Condition = PolicyCondition.Contains,
                               Type= PolicyFilterType.Url,
                               Value = new PolicyValue()
                                {
                                  Value1 = "test",
                                }
                             },
                             new FilterRule()
                               {
                                 Condition = PolicyCondition.Contains,
                                 Type= PolicyFilterType.Url,
                                 ExpressionType = ExpressionType.Or,
                                 Value = new PolicyValue()
                                  {
                                    Value1 = "test2",
                                  }
                               }
                         }
                     }
                 });
```

Request Information

Represents the request to add a container to an advanced mode scan profile.

Element	Description	Type
ContainerName	Sets a name for the container.	String
NodeType	Sets the type for objects that will be scanned into the container.	Enum Valid values: SiteCollection (for SharePoint Sites) Mailbox (for Mailboxes) OneDrive (for OneDrive for Business) Office365Group (for Microsoft 365 Groups)
ScanProfileName	Sets the name of the scan profile where the container will be added.	String
Rule	Sets the container's rule that will be used to filter objects.	For details, refer to FilterPolicyContent Class Parameters.

- **FilterPolicyContent Class Parameters**
  Represents the FilterPolicyContent class information.

- **FilterRule Class Parameters**
  Represents the FilterRule class information.
- **PolicyValue Class Parameters**
  Represents the PolicyValue class information.

FilterPolicyContent Class Parameters

Represents the FilterPolicyContent class information.

Element	Description	Type
Name	Sets a name for the rule.	String
NodeType	Sets the object type to the value same as the container's object type.	Enum Valid values: SiteCollection (for SharePoint Sites) Mailbox (for Mailboxes) OneDrive (for OneDrive for Business) Office365Group (for Microsoft 365 Groups)
Filter	Sets filters for the rule.	List<Filter Rule> For details, refer to FilterRule Class Parameters.

FilterRule Class Parameters

Represents the FilterRule class information.

Element	Description	Type
Type	Sets a criterion for the filter.	Enum Valid values: Url (for "URL") Title Template (for "Template Title") CreatedTime Owner (for "Primary Administrator") TemplateName Size CustomPropertyText CustomPropertyBoolean (for "Custom Property: Yes/No") CustomPropertyNumber CustomPropertyDateTime (for "Custom Property: Date and Time") MailType (for "Mailbox Type") Department City StateOrProvince PostalCode (for "ZIP/Postal Code") Office UserID DisplayName GroupId Privacy GroupOwner Classification (for "Group Classification")

Element	Description	Type
		Company Country (for “Country or Region”) UserPropertyBoolean (for “User Profile Property” > “Boolean”) UserPropertyDate (for “User Profile Property” > “Date”) UserPropertyDateTime (for “User Profile Property” > “Date Time”) UserPropertyTextEmail (for “User Profile Property” > “Email”) UserPropertyTextPerson (for “User Profile Property” > “Person”) Region (for “Geo Location”) UserPropertyTextString (for “User Profile Property” > “String (Single Value)”) UserPropertyTextURL (for “User Profile Property” > “URL”) LicenseName (for “Microsoft 365 Subscription Name”) GroupMembership (for “Basic User Information” > “Group Membership”) CustomAttribute GroupEnableWay (for “Group Property” > “Group Type”) JobTitle UsernameEmail (for “Basic User Information” > “Username”) EmailAddress GroupMember (for “Group Property” > “Group Member”) Region (for "Geo Location")
Condition	Sets a condition for the filter’s criterion.	Enum Valid values: Contains LessOrEqualThan (for “<=”) GreaterOrEqualThan (for “>=”) Before After On WithIn OlderThan Equals DoesNotContains Match DoesNotMatch DoesNotEquals IsNotEmpty
Value	Sets a value for the filter’s condition.	Class For details, refer to PolicyValue Class Parameters.
ExpressionType	Sets a expression for the filter.	Enum Valid values: And Or

PolicyValue Class Parameters

Represents the PolicyValue class information.

Element	Description	Type	Required
Value1	Sets a value for the filter condition.	String	Yes, if the filter condition needs a value. Otherwise, No.
Value1Unit	Sets a unit for the value.	Enum Valid values: KB MB GB Days Weeks Months Years	Yes, if the filter criterion is about data size or date time. Otherwise, no.

Register a Partner's Customer

Register a Partner's Customer for IBM Spectrum® Protect Plus Online Services.

To register a partner's customer to IBM Spectrum Protect Plus Online Services, follow the instructions below:

1. Get the available data centers. For details, refer to Get Data Centers.
2. Provide information of a partner's customer account that signs up for IBM Spectrum Protect Plus Online Services. For details, refer to Provide Information of a Sign-up Account.

Provide Information of a Sign-up Account

Provides information of a partner's customer account that signs up for IBM Spectrum Protect Plus Online Services.

Examples

```
var partnerContext = PublicApi.GetParnterContext("https://api.spponlineservices.ibm.com", "partnername",
"partnerpassword");

var dataCenters = partnerContext.PartnerService.GetDataCenters();

var customerResgisterResult = partnerContext.PartnerService.AddCustomer(new CustomerRegistrationInfoModel()
                {
                  UserName = "testuser@testdomain.com",
                  Password = "******",
                  DataCenter = dataCenters[0].Id,
                  DataCenterName = dataCenters[0].Name,
                  CountryCode = Country.US.ToString(),
                  CountryOrRegion = Country.US.ToString(),
                  FirstName = "FirstName",
                  LastName = "LastName",
                  Industry = ((int)IndustryInfo.InformationTechnology).ToString(),
                  Title = ((int)CustomerTitle.Developer).ToString(),
                  Organization = "testcompany",
                  Telephone = "123456789",
                  State = "",
                });
```

Request Information

Represents the request to register a partner's customer.

Element	Description	Type	Required
DataCenter	Sets the data center ID.	Globally unique identifier	Yes
DataCenterName	Sets the data center name.	String	Yes
FirstName	Sets the user's first name.	String	Yes
LastName	Sets the user's last name.	String	Yes
UserName	Sets the user's corporate email address.	String	Yes
Password	Sets the user's password.	String	No
Organization	Sets the customer's organization name.	String	Yes

Element	Description	Type	Required
Title	Sets the user's title in their organization.	Valid values: 1 (for "C-Level") 2 (for "General Manager/VP") 3 (for "Director") 4 (for "Manager") 5 (for "Team Lead") 6 (for "Specialist/Analyst/Consultant") 7 (for "Architect") 8 (for "Engineer") 9 (for "Developer") 10 (for "Administrator") 11 (for "Other")	Yes
Industry	Sets the industry for the customer's organization.	Int Valid values: 1 (for "Consumer") 2 (for "Education") 3 (for "Energy") 4 (for "Financial") 5 (for "Government") 6 (for "Health Care") 7 (for "Industrial") 8 (for "Information Technology") 9 (for "Not for Profit") 10 (for "Services") 11 (for "Other")	Yes
CountryCode	Sets the two letters country code for the user, such as "US" for the United States and "JP" for Japan.	String	Yes
State	Sets the state for the user from the United States.	String	No
Telephone	Sets the user's telephone number.	String	Yes

Get IBM Spectrum Protect Plus Online Services for Microsoft 365 Job Information

Gets the job information of IBM Spectrum Protect Plus Online Services for Microsoft 365.

Examples

```
var context = PublicApi.GetContext("https://api.spponlineservices.ibm.com",
"username", "password");

var records = context.CloudBackupService.GetJobs(filter);
```

Note: For the start time and end time of the time range, use the **DateTime** struct to represent an instant in time.

Request Information

Represents the filter that you can use to get IBM Spectrum Protect Plus Online Services for Microsoft 365 jobs.

Element	Description	Type	Required
StartTime	Sets a start time (UTC time) for the time range.	long	Yes
FinishTime	Sets an end time (UTC time) for the time range.	long	Yes

Element	Description	Type	Required
JobType	Sets the job types that you want to get.	Enum Valid values: 0 (for All) 1 (for Backup) 2 (for Restore) 3 (for Export) 4 (for Delete) 5 (for Retention)	Yes
ObjectType	Sets the service type of the jobs to get.	Enum Valid values: 0 (for All) 1 (for Exchange Online) 2 (for Share Point Online) 3 (for OneDrive for Business) 4 (for Microsoft 365 Groups) 5 (for Project Online) 6 (for Public Folder) 7 (for Teams)	Yes
JobState	Sets the job status	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)	Yes
PageIndex	Sets the starting number of the page to get the jobs. The default value is 0.	int	Yes
PageSize	Sets the number of jobs to display on one page. The default value is 10.	int	Yes

Response Information

Table 1. Retrieved result:

Element	Description	Type
TotalCount	The total count of the retrieved jobs	int
Jobs	A list of jobs	List

Table 2. IBMSPP-OSM job summary:

Element	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

Table 3. Backup details:

Element	Description	Type
TotalCount	Total count	long
FailedCount	Number of failed objects	long
SuccessfulCount	Number of successful objects	long
SkippedCount	Number of skipped objects	long

Get IBM Spectrum Protect Plus Online Services for Microsoft 365 License Consumptions

Gets the License Consumption Report for IBM Spectrum Protect Plus Online Services for Microsoft 365.

Examples

```
var context = PublicApi.GetContext("https://api.spponlineservices.ibm.com", "username", "password");

var records = context.CloudBackupService.GetLicenseConsumption();
```

Response Information

Element	Description	Type
OutOfPolicyTime	The UTC time 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

IBM Spectrum Protect Plus Online Services Recovery Portal

- **About IBM Spectrum Protect Plus Online Services Recovery Portal**
  IBM Spectrum Protect Plus Online Services Recovery Portal is a portal where users can run jobs to recover their lost data. IBM Spectrum Protect Plus Online Services Recovery Portal is available and free for customers who use IBM Spectrum Protect Plus Online Services for Microsoft 365 to protect their data in Microsoft 365.
- **Get Started**
  Refer to the following section to get started with IBM Spectrum Protect Plus Online Services Recovery Portal.
- **Use IBM Spectrum Protect Plus Online Services Recovery Portal for Microsoft 365**

About IBM Spectrum Protect Plus Online Services Recovery Portal

IBM Spectrum Protect Plus Online Services Recovery Portal is a portal where users can run jobs to recover their lost data. IBM Spectrum Protect Plus Online Services Recovery Portal is available and free for customers who use IBM Spectrum Protect Plus Online Services for Microsoft 365 to protect their data in Microsoft 365.

In IBM Spectrum Protect Plus Online Services Recovery Portal, invited Microsoft 365 users can run jobs to recover their data that is protected by IBM Spectrum Protect Plus Online Services for Microsoft 365, as well as view job reports.

Note: The IBM Spectrum Protect Plus Online Services Recovery Portal has been deployed to the data centers where IBM Spectrum Protect Plus Online Services for Microsoft 365 is available. For details on data centers, refer to the **Supported Data Centers** section in IBM Spectrum Protect Plus Online Services User Guide. IBM Spectrum Protect Plus Online Services Recovery Portal supports the following language: English.

In IBM Spectrum Protect Plus Online Services Recovery Portal, you can click the question mark button on the top bar to access the user guide.

Supported Browsers

The following table provides the required browser versions.

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

Get Started

Refer to the following section to get started with IBM Spectrum® Protect Plus Online Services Recovery Portal.

- **Configure Microsoft 365 Data**

Configure Microsoft 365 Data

About this task

If your organization is using IBM Spectrum® Protect Plus Online Services for Microsoft 365, before users can access the IBM Spectrum Protect Plus Online Services Recovery Portal with their Microsoft 365 accounts, the following configurations need to be completed by the organization's administrators:

Procedure

1. If this is the first time that you are signing in to IBM Spectrum Protect Plus Online Services or IBM Spectrum Protect Plus Online Services Recovery Portal with your Microsoft 365 account and the permissions requested by the IBM Spectrum Protect Plus Online Services app are displayed, to consent to this app for all users in your organization, select the Consent on behalf of your organization checkbox and click Accept.
   After you consent to this app on behalf of your organization, the requested permissions will no longer be displayed when your organization's users sign in to IBM Spectrum Protect Plus Online Services or IBM Spectrum Protect Plus Online Services Recovery Portal.

   Note: If your Microsoft 365 tenant does not allow users to consent to apps on their behalf and the Microsoft 365 Global Administrator hasn't consented the **IBM Spectrum Protect Plus Online Services** app on behalf of your organization, the Microsoft 365 Global Administrator can consent to the app by following the steps in the What If Your Tenant Does Not Allow Users to Consent to Apps? section in the IBM Spectrum Protect Plus Online Services user guide.
2. If you want to set trusted IP addresses to only allow users to access IBM Spectrum Protect Plus Online Services Recovery Portal from certain IP addresses or IP address ranges, go to IBM Spectrum Protect Plus Online Services and navigate to Advanced Settings > Trusted IP Address Settings to configure the settings. For details about configuring trusted IP addresses, refer to Enable Trusted IP Address Settings in the IBM Spectrum Protect Plus Online Services user guide.
3. To manage users' access to IBM Spectrum Protect Plus Online Services Recovery Portal, in IBM Spectrum Protect Plus Online Services > User Management, add Microsoft 365 users or Microsoft 365 Groups, assign them at least the Standard User permission to the IBM Spectrum Protect Plus Online Services Recovery Portal, and ensure they are in the Activated status. For details about managing users, refer to Manage Users in the IBM Spectrum Protect Plus Online Services user guide.
   Note the following:
   - Ensure your organization has accepted the license agreement of the IBM Spectrum Protect Plus Online Services for Microsoft 365.
   - If you want to grant permissions to a large number of users, it is recommended to grant permissions to Microsoft 365 Groups instead of Microsoft 365 users.
4. Ensure your organization's Microsoft 365 data has been protected in IBM Spectrum Protect Plus Online Services for Microsoft 365.
   Note: The administrator of IBM Spectrum Protect Plus Online Services for Microsoft 365 can configure whether to allow end users to restore data from the archive tier. If the option is disabled, the end users will not be able to restore data from the archive tier.
5. The IBM Spectrum Protect Plus Online Services Recovery Portal is an application that can be added as a custom tile in the Microsoft 365 app launcher. For details, refer to Add a Custom Tile of the IBM Spectrum Protect Plus Online Services Recovery Portal to the App Launcher.

- **Add a Custom Tile of the IBM Spectrum Protect Plus Online Services Recovery Portal to the App Launcher**

Add a Custom Tile of the IBM Spectrum Protect Plus Online Services Recovery Portal to the App Launcher

Procedure

To add a custom tile of the IBM Spectrum Protect Plus Online Services Recovery Portal to the app launcher, refer to the instructions below:

1. Sign in to the Microsoft 365 admin center as a Global Administrator.
2. In the left navigation menu, go to Settings > Org settings, and click the Organization profile tab.
3. Under the Organization profile tab, click Custom app launcher tiles.
4. Click Add a custom tile.
5. In the URL of website field, enter the following URL:
   https://recovery.spponlineservices.ibm.com
   For more details, refer to the Microsoft article Add custom tiles to the app launcher.

6. Click Save to add the custom tile.

Use IBM Spectrum Protect Plus Online Services Recovery Portal for Microsoft 365

You can access the IBM Spectrum Protect Plus Online Services Recovery Portal via the following methods:

- After your administrator added a custom tile of the IBM Spectrum Protect Plus Online Services Recovery Portal to the app launcher, you can follow the steps below to access the IBM Spectrum Protect Plus Online Services Recovery Portal:
  1. Sign in to Microsoft 365, click the App launcher button on the upper-left corner of the page, and click All apps.
  2. Find the app in the apps list. Since your administrator can define the app name, you can contact the administrator if you are unsure of the app name.
  3. Click the app to access the portal.
- Sign in to the IBM Spectrum Protect Plus Online Services commercial production environment (https://spponlineservices.ibm.com) with your Microsoft 365 account, select the All Apps view, and then click IBM Spectrum Protect Plus Online Services Recovery Portal to access the portal. If you have added IBM

Spectrum Protect Plus Online Services Recovery Portal to your favourite apps, you can also select the My Favorite Apps view to access the IBM Spectrum Protect Plus Online Services Recovery Portal.
Note: If the information of your Microsoft 365 account has been updated after you sign in to IBM Spectrum Protect Plus Online Services Recovery Portal, to synchronize with the updated information, IBM Spectrum Protect Plus Online Services Recovery Portal can display a page for you to sign out and clear your previous information. Then, the updated information will be synchronized to IBM Spectrum Protect Plus Online Services Recovery Portal when you sign in with the Microsoft 365 account.

- **Recover Your Microsoft 365 Data**
- **View Request History**

Recover Your Microsoft 365 Data

In Data recovery, you can search for backup data from Exchange Online or OneDrive for Business, and restore the selected backup data to its original location.

For more details on recovering your data, refer to the following sections:

- Exchange Online
- OneDrive for Business

- **Exchange Online**
- **OneDrive for Business**

Exchange Online

Procedure

Follow the steps below to recover backup data of Exchange Online:

1. Click Start now in the Exchange Online tile.
2. To search for backup data of Exchange Online items, choose one of the following methods:
   - If you want to search for backup data by their subjects, enter keywords in the search box.
   - If you want to narrow your search by additional conditions, click Advanced to expand the search panel and configure the following conditions:

     Subject
     : Enter keywords of a subject.

     Folder name or location
     : Enter keywords of a folder name, or enter a folder location (example: folder name\subfolder name).

     Sent from
     : Enter keywords of the sender's display name or email address.

     Sent to
     : Enter keywords of the receiver's display name or email address.

     Date sent
     : Specify a time range.

   Click Search to search for the backup data. If you want to reset the search conditions, click Reset.
3. The search results are listed in the table.
   You can do the following:
   - For the items with the Email icon, you can click their subjects to open the Preview Email pane and have a preview of the email content. In the Preview Email pane, you can click Restore to restore this item.
     Note: The Preview Email feature only supports backup data that is stored in the cool tier on the IBM Spectrum® Protect Plus Online Services default storage or your own Microsoft Azure Blob Storage.
   - By default, the items listed in the search results table are the latest backup data. If your desired items are not in the table and there is a message indicating that you can search for more backup data, click here in the message at the bottom of the table.
   - If you want to modify the search conditions, click the Advanced search button to expand the advanced search panel and configure the search conditions. You can click the Cancel button to clear the current search conditions.
4. To restore one or multiple items, select the checkboxes next to the items, and click Restore.
5. After the restore job starts, you can go to Request history to view details of the job. For more details, refer to View Request History.

OneDrive for Business

Procedure

Follow the steps below to recover backup data of OneDrive for Business:

1. Click Start now in the OneDrive for Business tile.
2. To search for backup data of OneDrive for Business items, choose one of the following methods:
   - If you want to search for backup data by their document names, enter keywords in the search box.
   - If you want to narrow your search by additional conditions, click Advanced to expand the search panel and configure the following conditions:
     - Document name – Enter keywords of a document name.

- Folder name or location – Enter keywords of a folder name, or enter a folder location (example: folder name\subfolder name).

Click Search to search for the backup data. If you want to reset the search conditions, click **Reset**.

3. The search results are listed in the table.
   You can do the following:
   - By default, the items listed in the search results table are the latest backup data. If your desired items are not in the table and there is a message indicating that you can search for more backup data, click here in the message at the bottom of the table.
   - If you want to modify the search conditions, click the Advanced search button to expand the advanced search panel and configure the search conditions. You can click the Cancel button to clear the current search conditions.
4. To restore one or multiple items, select the checkboxes next to the items, and click Restore.
   Note: 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 file name.
5. After the restore job starts, you can go to **Request history** to view details of the job. For more details, refer to View Request History.

View Request History

Procedure

Click Request history on the left pane. The Request history page appears.

Follow the instructions below to view job details:

1. Select an option in the Time filter, Object type, and Job status drop-down lists to filter jobs.
2. Clicking the arrow button next to a job summary will expand the job's details pane.