IBM Storage Protect for Cloud

User Guide

Note:

Before you use this information and the product it supports, read the information in “Notices” on page 147.

Edition Notice (November 2023)

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

Contents

About this publication

This publication provides overview, planning, and user instructions for IBM Storage Protect for Cloud.

Who should read this publication

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

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

What's new

Learn about new features and updates in IBM Storage Protect for Cloud.

Release Date: November 17, 2023

New features and updates

- If your organization has a working subscription for IBM Storage Protect for Cloud Microsoft 365, and the IBM Storage Protect for Cloud Recovery Portal is available to your organization's end-users, in **IBM Storage Protect for Cloud** > **Administration** > **General settings**, you can now configure **Logo customization** and **Terminology mappings** to apply the custom logo and custom terminologies to the IBM Storage Protect for Cloud Recovery Portal.
- In **Auto discovery** > **Scan profiles**, if you turn on the **Enable daily scan** option for a scan profile, you can now customize the start time of the daily scan job.
- In **Auto discovery** > **Containers**, you can now rename custom containers.
- In **Auto discovery** > **Scan profiles**, when you configure an advanced mode scan profile for Power Apps or Power Automate objects, with the **Specified objects in one container** rule set for each object type, you can now customize the following criteria:

<table>
<tr><th>Object Type</th><th colspan="3">Criteria</th></tr>
<tr><td rowspan="7">Power App / Power Automate</td><td rowspan="7">Environment</td><td colspan="2">Name</td></tr>
<tr><td>Creator</td><td>City</td></tr>
<tr><td></td><td>Company</td></tr>
<tr><td></td><td>Country or region</td></tr>
<tr><td></td><td>Department</td></tr>
<tr><td></td><td>Email address</td></tr>
<tr><td></td><td>Office</td></tr>
</table>

IBM Storage Protect for CloudApp API Permission Updates

- If your organization has configured an app profile for the following service apps, goto IBM Storage Protect for Cloud> **Management** > **App management**and re-authorize the app profile to add the new API permissions.
  - IBM Storage Protect for Cloud Microsoft 365 service app has been updated to add the **BitLockerKey.Read.All** Microsoft Graph permission to support retrieving the BitLocker keys for all devices in your Microsoft tenant.

Chapter 1. About IBM Storage Protect for Cloud

IBM Storage Protect for Cloud 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 unified browser-based user interface and a fully distributed architecture, IBM Storage Protect for Cloud 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, Google Workspace, and others. No installation and minimal configuration make getting to the cloud a breeze.

IBM Storage Protect for Cloud serves as a central hub for the following services:

- IBM Storage Protect for Cloud Microsoft 365
- IBM Storage Protect for Cloud Salesforce
- IBM Storage Protect for Cloud Dynamics 365
- IBM Storage Protect for Cloud Azure VMs and Storage
- IBM Storage Protect for Cloud Google Workspace

Language Support

IBM Storage Protect for Cloud supports the following languages: English, Japanese German, and French.

IBM Storage Protect for Cloud Versions and Environments

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

Microsoft 365 Environment	IBM Storage Protect for Cloud Environment
Global Microsoft 365	https://sp4c.storage-defender.ibm.com

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

	Commercial Production Environment
Sign-in Address	https://sp4c.storage-defender.ibm.com
Sign-in Methods	Sign in with: Local account Microsoft 365 account Salesforce account
Supported Data Centers	Canada Central (Toronto) East US2 (Virginia) Germany West Central (Frankfurt) UK South (London) Australia East (New South Wales) Switzerland North (Zurich)

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

Use IBM Storage Protect for Cloud Public APIs

You can use the IBM Storage Protect for Cloud public APIs to communicate with IBM Storage Protect for Cloud for basic operations and information collection, such as obtaining audit records for activities in your IBM Storage Protect for Cloud tenant and adding containers to an advanced mode scan profile. For details, refer to IBM Storage Protect for Cloud Web API.

Chapter 2. FAQs

The following sections provide the answers to questions you may encounter when using the IBM Storage Protect for Cloud 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 Storage Protect for Cloud users cannot sign into IBM Storage Protect for Cloud with their Microsoft 365 login IDs. Microsoft will display the **Need admin approval** page to them.

Prior to adding Microsoft 365 users as IBM Storage Protect for Cloud users, IBM Storage Protect for Cloud recommends that you check the **Users can request admin consent to apps they are unable to consent to** option in **Microsoft Azure** > **Enterprise applications** > **User settings**. If the option is set to **No**, a Microsoft 365 Global Administrator must first consent to the IBM Storage Protect for Cloud app.

Microsoft 365 Global Administrator can consent to the **IBM Storage Protect for Cloud** app by completing the following steps:

1. Navigate to **Azure Active Directory admin center** > **Azure Active Directory** > **Enterprise applications**.
2. Select the **IBM Storage Protect for Cloud** 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 Storage Protect for Cloud** app are displayed. Review the permissions and click **Accept**.

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

Auto discovery requires an authentication method, either using a service account profile or an app profile. The app profile authentication method is recommended in most cases, and auto discovery scan profiles use the app profile authentication method as the preferred option. By using the app profile authentication method, the app token will be used to back up or manage data, and the credentials of the Microsoft 365 Global Administrator account will not be stored by Microsoft 365.

However, the service account authentication is required by some services. For more information, refer to “Will the App Profile Method Meet Your Data Management Requirements?” on page 7 If you configure a service account profile, the credentials of the account within the profile will be used to scan and manage Microsoft 365 objects. For details on configuring service account profiles, refer to Chapter 7, “Manage Service Account Profiles,” on page 31.

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 Storage Protect for Cloud 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 Storage Protect for Cloud 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 Storage Protect for Cloud 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, refer to the following information to configure the required settings based on your selection:

- **Microsoft 365 MFA service account profile** – If your organization has configured a Microsoft 365 MFA service account profile in the IBM Storage Protect for Cloud classic UI (before July 2023 release), you can refer to the instructions in the **Edit MFA Service Account Profiles** section below to edit the MFA service account profile.
- **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 Storage Protect for Cloud. 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 Chapter 8, "Manage Microsoft 365 Account Pool," on page 35.

Edit MFA Service Account Profiles

Navigate to IBM Storage Protect for Cloud > **Management** > **Service account**, and click the MFA service account profile. On the MFA service account profile detail page, click **Edit**. Then, refer to the following instructions to edit the MFA service account profile:

1. **Profile Name** – Enter a name for the service account profile.
2. **Description** – Enter an optional description.
3. **Enable MFA** – If you want to keep this MFA service account profile in the classic UI, select the **Our organization uses multi-factor authentication** checkbox, and refer to the following steps to edit this MFA service account profile.

   Note that MFA service account profiles have the following limitations:

   - The Microsoft 365 MFA service account profile cannot be used to invite Microsoft 365 users/groups as IBM Storage Protect for Cloud users.
4. **Username** – Specify an account with the permissions required by your tenant's cloud services. The permissions of the Microsoft 365 service account vary with the different cloud services your tenant is using. Refer to the "Required Permissions of Cloud Services" on page 32for more information.

   Note:

   - IBM Storage Protect for Cloud does not recommend that a personal active user account be used as the service account. We recommend you use a separate service account to handle all administration.

- With the **Enable MFA** option selected, you must enter the login ID of a Microsoft 365 Global Administrator account or SharePoint Administrator account.

5. **Password** – Enter the app password of the account above. For more information about app passwords, refer to the Microsoft technical article https://docs.microsoft.com/en-us/azure/multi-factor-authentication/end-user/multi-factor-authentication-end-user-app-passwords.
6. Click **Validation Test** to validate the information above.

   Note:

   - When the validation test is failed, and the error message indicates that your Microsoft 365 tenant has set access policies or enabled multi-factor authentication (MFA), refer to the **Validation Test Troubleshooting** section below.
   - As the Microsoft 365 user has multi-factor authentication (MFA) enabled, the user role information cannot be retrieved due to Microsoft API limitations, and the **User Role** field will be blank.
   - 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" on page 136.
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

Does IBM Storage Protect for Cloud Support Microsoft 365 Tenants with Multi-Geo Capabilities?

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 subscription for IBM Storage Protect for Cloud Microsoft 365.

Note: While you can use a standard IBM Storage Protect for Cloud Microsoft 365 subscription to support a multi-geo Microsoft 365 tenant with no changes, all data will be protected and stored centrally in a single IBM Storage Protect for Cloud tenant. To take advantage of our global network, you will need to purchase a subscription from IBM Storage Protect for Cloud to leverage our multi-geo infrastructure described below.

Because your tenant will be supported by IBM Storage Protect for Cloud 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** to configure mappings between the geo locations in your Microsoft 365 tenant and the data centers supported in IBM Storage Protect for Cloud. For more information, refer to Manage Data Center Mappings.

Note: The saved mappings cannot be changed and they will be used to create boundaries between different geo locations in your environment.

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" on page 20.

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 objects whose property values are equal to the entered value.
- **Contains** – Use this condition to scan objects whose property values contain the entered value.
- **Matches** – Use this condition to scan 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/***.

Which App Profiles Supoprt to Scan Microsoft 365 Objects?

The table below lists which app profiles support to scan Microsoft 365 objects via **Auto discovery**.

App Profile types	Supported object types	Notes
Microsoft 365 (All Permissions) IBM Storage Protect for Cloud Microsoft 365 (All Permissions) Custom app with required permissions (API Permissions Required by Custom Apps)	Exchange mailbox	**Exchange Administrator** role is required. For detailed instructions, see How to Assign the Exchange Administrator Role to an App?
	OneDrive for Business	
	SharePoint site	
	Microsoft 365 Group / Microsoft Team / Yammer community	
	Project site	
	Exchange public folder	
	Microsoft 365 user	
	Security and distribution group	**Exchange Administrator** role is required. For detailed instructions, see How to Assign the Exchange Administrator Role to an App?

App Profile types	Supported object types	Notes
IBM Storage Protect for Cloud Microsoft 365 (Exchange Permissions)	Exchange mailbox	**Exchange Administrator** role is required. For detailed instructions, see How to Assign the Exchange Administrator Role to an App?
	Exchange public folder	
	Microsoft 365 user	
IBM Storage Protect for Cloud Microsoft 365 (SharePoint Permissions)	OneDrive for Business	
	SharePoint site	
	Project site	

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 Storage Protect for Cloud **Auto discovery** to scan or add Microsoft 365 objects. Auto discovery can use the app profile and service account authentication methods to scan objects.

The app profile authentication method is the default option, as 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 Storage Protect for Cloud 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 Storage Protect for Cloud — only your Administrator's consent is recorded and this consent can be monitored in your Microsoft Entra and can be revoked at any time from your environment.

While we do suggest you use the app profile method, 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 Storage Protect for Cloud Microsoft 365

- It is recommended that you configure app profiles for managing backup data in IBM Storage Protect for Cloud Microsoft 365 for the best performance. When the app profile authentication method in a scan profile cannot meet your data management requirements, you can apply a service account profile to the scan profile as an additional method. For additional details, refer to the *IBM Storage Protect for Cloud Microsoft 365 User Guide* in IBM Documentation.
- 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 Storage Protect for Cloud 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 Microsoft Entra instance?

Note the following:

- The Global Admin account is not stored by IBM Storage Protect for Cloud. The consent process is managed by Microsoft, so your username and password are never shared with IBM Storage Protect for Cloud during the consent process.
- Admin consent does not grant admin privileges to the IBM Storage Protect for Cloud apps. For instructions on creating app profiles for installing the aSpps, refer to the Chapter 9, “Manage App Profiles,” on page 39 section.

Which Version Should I Use When I Need to Configure an App Profile for Managing Power Platform Objects?

If your organization enables the Power BI module in the IBM Storage Protect for Cloud Microsoft 365, to manage the Power Platform objects with the app profile authentication method, IBM Storage Protect for Cloud now supports configuring the following app profiles:

- Configure an app profile for the **Microsoft Delegated App** with the **Power BI** permissions that are required to protect the Power BI data via the IBM Storage Protect for Cloud Microsoft 365.

In **App Management**, when you create or re-authorize app profiles for the above apps, you must choose a version from **Commercial** and **GCC** based on the URLs of your Power Platform environment. For more information on Power Platform environment URLs, refer to the following Microsoft articles: Power BI environments, Power Automate environments, and Power Apps environments.

Chapter 3. Get Started

Refer to the following sections to get started in IBM Storage Protect for Cloud.

Sign Up for IBM Storage Protect for Cloud

IBM Storage Protect for Cloud provides new tenants with a 30-day trial license for each online service.

Procedure

1. Go to one of the following trial pages and select one of the following options to register for a 30-day free trial.
   - IBM Storage Protect for Cloud - M365 Free Trial
   - IBM Storage Protect for Cloud - Salesforce Free Trial
   - IBM Storage Protect for Cloud Dynamics Free Trial
   - IBM Storage Protect for Cloud Azure VMs and Storage Free Trial
   - IBM Storage Protect for Cloud- Free Trial for Business Partners
   - If you already have an IBM account, click **Log in** and provide your **IBMid**.
   - If you are a new user, complete the following steps to create an IBMid.

     Account Information - Enter the basic information in all required fields and then click **Next**.

     E-mail
     Enter your corporate e-mail address. This e-mail address will become your IBMid, and you can use this ID to log in to `IBM.com`.

     First name
     Enter your first name.

     Last name
     Enter your last name.

     Country or region of residence
     Select your country from the drop-down list.

     State or province
     Select your state from the drop-down list.
2. **Additional Information** – Complete the required fields and then click **Continue**.
   - Enter the additional information such as **Phone**, **Company**, and **Job title** in the respective fields.
   - Select the data center closest to your Microsoft 365 tenant from the drop-down list for the best performance. After the sign-up is finished, you cannot change the data center.
   - Confirm your communication preferences by choosing one of the following options:
     - by email
     - by telephone
3. You will be redirected to the **My IBM** home page where you can see the product and the activation status. A confirmation e-mail will be sent to your corporate email address.
4. Once you receive the e-mail, click the supplied link to activate your account. The link will be active for 30 days.

Sign into IBM Storage Protect for Cloud

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

- The production environment for commercial use https://sp4c.storage-defender.ibm.com

On the IBM Storage Protect for Cloud sign-in page, choose the following sign-in method:

- "Sign in with a Local Account" on page 10
- "Sign in with a Microsoft 365 Account" on page 10
- "Sign in with a Salesforce Account" on page 12

Sign in with a Local Account

Procedure

To sign in with an IBM Storage Protect for Cloud local account, complete the following steps:

1. On the sign-in page, enter your login information:
   - **Login ID**– Enter the email address used as your IBM Storage Protect for Cloud local account.
   - **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 to retrieve and reset your password.
2. Click **Sign In** to access IBM Storage Protect for Cloud homepage.

Reset Your Local Account Password

You can reset the password of your IBM Storage Protect for Cloud local account.

Procedure

Complete the following steps:

1. Navigate to the IBM Storage Protect for Cloud 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 Storage Protect for Cloud username.
   - **Verification Code** – Enter the verification code. Click **Refresh** to refresh the verification graphic if no image is displayed.
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 Storage Protect for Cloud 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

Procedure

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

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 Storage Protect for Cloud.
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 Storage Protect for Cloud, the required permissions are displayed. Review the permissions and click **Accept**. The IBM Storage Protect for Cloud app is generated in My apps on Microsoft 365. You can click the app to access IBM Storage Protect for Cloud within Microsoft 365. The app will remember your credentials when you sign in through it.

   Note: If the **Need admin approval** page appears, the Microsoft 365 Global Administrator can refer to the following instructions to complete the configurations based on your tenant's user consent settings:

   - If your tenant's user consent for applications setting is **Allow user consent for apps from verified publishers, for selected permissions (Recommended)**, the Microsoft 365 Global Administrator must complete the steps below:

     a. Sign in to Microsoft Entra admin center (or Microsoft Azure portal) as a Global Administrator.

     b. Navigate to **Microsoft Entra ID** > **Enterprise applications** > **Consent and permissions** > **User consent settings**.

     c. Click **Select permissions to classify as low impact**.

     d. On the **Permission classifications** page, select the **User.Read – sign in and read user profile** permission, and click **Yes, add selected permissions**.
   - If your tenant does not allow users to consent to apps, contact your Microsoft 365 Global Administrator to consent to the IBM Storage Protect for Cloud app first. For details of consenting to the IBM Storage Protect for Cloud app, 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 Storage Protect for Cloud, the Join IBM Storage Protect for Cloud 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 Storage Protect for Cloud.

API Permissions Required by the IBM Storage Protect for CloudApp (for Microsoft 365 Sign-in Method)

The table below lists the API permissions required by the IBM Storage Protect for Cloud app, which IBM has published to your Microsoft Entra ID.

API	Permission	Type	Why we need it?	Last update
Microsoft Graph	openid (Sign users in)	Delegated	Support signing into IBM Storage Protect for Cloud with Microsoft 365 accounts.	
	profile (View users' basic profile)	Delegated	Retrieve users' profile information.	
	offline_access (Maintain access to data you have given it access to)	Delegated	Retrieve users' information and support functions of other IBM Storage Protect for Cloud.	
	User.Read (Sign in and read user profile)	Delegated	Support signing into IBM Storage Protect for Cloud with Microsoft 365 accounts.	
	email (View users' email address)	Delegated	Retrieve users' email addresses.	Newly added in June 2023

Note: The **IBM Storage Protect for Cloud** app does not need to be re-consented for the newly added permissions.

Sign in with a Salesforce Account

Procedure

To sign in with a Salesforce Account, complete the following steps:

1. On the **sign-in** page, click **Sign in with Salesforce**.

   Note: If you are using the Salesforce account to sign into another app on the same browser, you will be automatically signed into IBM Storage Protect for Cloud.
2. On the Salesforce login page, enter an existing Salesforce login ID and password.
3. Click **Log In**.
4. If it is the first time that this Salesforce account is signing into IBM Storage Protect for Cloud, the required permissions are displayed. Review the permissions and click **Allow**. The IBM Storage Protect for Cloud app is generated in **Connected Apps** on Salesforce. The app will remember your credentials when you sign in through it.

   Note: If your Salesforce account does not exist but your tenant exists in IBM Storage Protect for Cloud, the **Join IBM Storage Protect for Cloud** 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 Storage Protect for Cloud.

Sign in with a Google Account

Procedure

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

1. On the sign-in page, click **Sign in with Google**.

   Note: If you are using the Google account to sign into another app on the same browser, you will be automatically signed into IBM Storage Protect for Cloud.
2. On the Google sign-in page, enter an existing Google username and password.
3. Click **Next**

   Note: If your Google account does not exist, but your tenant exists in IBM Storage Protect for Cloud, the **Join IBM Storage Protect for Cloud** 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 Storage Protect for Cloud.

Use the Quick Start Wizard

IBM Storage Protect for Cloud provides a **Quick start** wizard to help you get started. To open the wizard, click the **Quick start** button on the upper-right corner of the page. The **Quick start** wizard lists the following steps:

Procedure

1. **Tenant** – To get started with IBM Storage Protect for Cloud, you must connect your tenant to this platform first. For additional details, refer to "Connect your tenants to IBM Storage Protect for Cloud" on page 13.
2. **App profile** - An app profile is required for IBM Storage Protect for Cloud to connect your Microsoft or Salesforce environments. For additional details, refer to Chapter 9, "Manage App Profiles," on page 39 .
3. **Scan profile** – To discover objects in your environments and scan these objects into IBM Storage Protect for Cloudfor management, you must configure scan profiles. For additional details, refer to "Manage Scan Profiles" on page 65.
4. **Users and groups**- Add users/groups to IBM Storage Protect for Cloud as Service Administrators or Tenant Users. You can also assign permissions of different services to Tenant Users. For additional details, refer to "Manage Users" on page 20.

Connect your tenants to IBM Storage Protect for Cloud

To use IBM Storage Protect for Cloud services to manage a tenant in the Microsoft or Google or Salesforce or Amazon platform, the tenant owner or service administrators must connect the tenant to IBM Storage Protect for Cloud.

Before you begin

Before you connect a tenant, ensure that the following prerequisites are met:

- Connecting a Microsoft 365 tenant will create an app in the environment of the tenant, which requires a **Microsoft 365 global administrator** account within the same tenant to consent to the app.
- To connect a Google tenant, ensure that the IBM Storage Protect for Cloud Tenant Management app has been installed.

  Note: The IBM Storage Protect for Cloud Tenant Management app can only be accessed via the Google Workspace Marketplace link on the Connect tenant page in **IBM Storage Protect for Cloud** > **Tenant management**.

Connecting a Google tenant requires an account with the **Users** > **Read**, **Groups** > **Read**, and **License Management** > **License Read** privileges in the same tenant.

- Connecting a Salesforce tenant will create an app in the tenant's Salesforce environment, which requires a Salesforce account with the **System Administrator** profile in the same tenant or another profile which includes the permissions of the system administrator profile in the same tenant. After connecting a Salesforce tenant successfully, the corresponding app profile will be created in **IBM Storage Protect for Cloud**> **Management**>**App management**.

Procedure

To connect a tenant, navigate to **Management**>**Tenant management**, and complete the following steps:

1. On the **Tenant management** page, click **Connect tenant**.
2. The **Connect tenant** pane appears on the right of the page. Based on the type of tenant that you want to connect, select the **Microsoft**, **Google Salesforce** or **Amazon**platform. In the following scenarios, you also need to select a version for the environment of the tenant:
   - **Azure environment version**
     In the IBM Storage Protect for Cloud production environment, refer to the following information to select a version when you connect a Microsoft 365 tenant:
     – Select the Commercial Microsoft 365 version if your Microsoft login URL ends with .com.
   - **Salesforce environment**
     Select the Salesforce or Salesforce Sandbox environment when you connect a Salesforce tenant.
   - **Amazon**
     Enter **Access key ID** and **Secret access key** to specify an IAM user, which will only be used to configure an IAM role and required policies in your AWS environment. For more details on managing your access key ID and secret access key, refer to AWS article.
3. Click **Connect**.
4. Refer to the instructions below based on your scenario:
   - When you connect a Microsoft/Google/Salesforce tenant, the sign in page appears in a new tab. Sign in with an account which meets the requirements mentioned above.
   - When you connect an Amazon tenant, IBM Storage Protect for Cloud will check whether your entered access key ID and secret access key are available.
5. Once your tenant is successfully connected to IBM Storage Protect for Cloud, a message prompt will be displayed.
6. Once a Microsoft 365 tenant has been successfully connected toIBM Storage Protect for Cloud, go to view details of the tenant and edit the **SharePoint Online admin center URL** value if it is incorrect.

What to do next

On the **Tenant management** page, the table lists all connected tenants and displays information in the following columns: **Name**, **Platform**, and **Modified time**. You can take the following additional actions:

- Use the search box to search for tenants by keywords of tenant names.
- To view details of a tenant, click the link in the tenant's **Name** column. The **Tenant detail** page appears on the right of the page. When you view details of a Microsoft 365 tenant, you can edit the **SharePoint Online admin center URL** value if it is incorrect.
- We recommend you reconnect to the tenants which are highlighted with the **New connection recommended** label. If you want to create new app profiles for a tenant, you must reconnect to the tenant. For additional details, refer to "Reconnect a Tenant" on page 15.
- If a tenant is no longer needed in IBM Storage Protect for Cloud, you can select the tenant and click **Remove** to remove the tenant. For additional details, refer to the "Remove a Tenant" on page 15.

Reconnect a Tenant

About this task

You can reconnect a tenant in the following scenarios:

- If your tenant management app has been deleted accidentally, you need to reconnect the tenant.
- When the permissions on the app for a tenant is updated, the tenant will be highlighted with the **New connection recommended** label, and then you must reconnect the tenant.

Note: You do not need to reconnect Salesforce tenants in **Tenant management**. If you want to re-authorize an app of a Salesforce tenant, navigate to **Management** > **App management** and re-authorize the related app profile.

Procedure

To reconnect a tenant, complete the following steps:

1. Select the tenant.
2. Click **Reconnect**.
3. Refer to the following instructions based on your scenario:
   - When you reconnect a Microsoft or Google tenant, the Microsoft or Google sign in page appears in a new tab. Sign in with an account which meets the requirements mentioned above.
   - When you reconnect an Amazon tenant, enter an access key ID and a secret access key to specify an IAM user with the required permissions for connecting an Amazon tenant. Then, click **Connect**.

Remove a Tenant

Procedure

If a tenant is no longer needed in IBM Storage Protect for Cloud, you must complete the following steps to remove the tenant:

1. Select the tenant that you want to remove.

   Note: Before you remove a tenant from IBM Storage Protect for Cloud, you must clean up the data related to the tenant, including app profiles, scan profiles, and more.
2. In the **Remove tenant** window, click **Confirm** to proceed.
3. If the tenant has some related data in IBM Storage Protect for Cloud, the **Alert** window appears. You must click **these related data** to view the data that you need to clean up.

Permissions Required by IBM Tenant Registrations

Refer to the following sections to see the permissions required by registering tenants of Microsoft, Google, Salesforce or Amazon:

Microsoft

Connecting a Microsoft 365 tenant will create the IBM Storage Protect for Cloud Tenant **Registration for Microsoft365** app in the tenant's Microsoft Entra ID. The table below lists the permissions required by the **IBM Storage Protect for Cloud Tenant Registration for Microsoft365** app.

Table 1.			
API	**Permission**	**Type**	**Why we need it?**
Microsoft Graph	User.Read (Sign in and read user profile)	Delegated	Supports signing into IBM Storage Protect for Cloud with Microsoft 365 accounts.
	Directory.Read.All (Read directory data)	Application	Retrieve your Microsoft 365 tenant information.

Google

You must accept the following permissions requested by IBM Storage Protect for Cloud when you install the IBM Storage Protect for Cloud Tenant Management app.

Note: The IBM Storage Protect for Cloud Tenant Management app can only be accessed via the Google Workspace Marketplace link on the Connect tenant page in **IBM Storage Protect for Cloud** > **Tenant management**.

Table 2.			
Scope	**Permission**	**Type**	**Why we need it?**
https://www.googleapis.com/auth/admin.directory.domain.readonly	Read domain information	sensitive	Retrieve customer's Google domain information.
https://www.googleapis.com/auth/apps.licensing	Read Google license information	sensitive	Collect user seats.
https://www.googleapis.com/auth/admin.directory.user.readonly	Read Google users	sensitive	Invite Google users for login.
https://www.googleapis.com/auth/admin.directory.group.readonly	Read Google groups	sensitive	Invite Google groups for login.

Salesforce

Connecting a Salesforce tenant will create the **IBM Storage Protect for Cloud Administration** app in the tenant's Salesforce environment. The following permissions are required by the **IBM Storage Protect for Cloud Administration** app:

- Access your basic information
- Access and manage your data
- Provide access to your data via the Web
- Access and manage your Chatter data
- Provide access to custom applications
- Allow access to your unique identifier

- Access custom permissions
- Access and manage your Wave data
- Access and manage your Eclair data
- Manage hub connections
- Access Pardot services
- Allow access to Lightning applications
- Allow access to content resources
- Perform requests on your behalf at any time

Amazon

Connecting an Amazon tenant will create an IAM role named **AWSTenantAdminRole** in the tenant's AWS environment. The following policies will be added to the IAM role:

- iam:ListAccountAliases
- iam:GetAccountSummary

Manage Your Services

The **Home** page provides the following views:

- **My Favorite services** – 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 services** – 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 services** view.
  - If the subscriptions of one or more services have expired, you can select the **Hide expired services from this view** check box, and you will not see the expired services under this view.
- **Store** – This view displays all services within the IBM Storage Protect for Cloud platform. You can start a trial for services that were not selected when your tenant signed up for IBM Storage Protect for Cloud. For details, refer to "Start Trial of Additional Services" on page 18.

IBM Storage Protect for Cloud 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's subscription agreement to activate the service.

Click the service in the **My favorite services** or **All services** view, and a pop-up window will appear displaying the subscription agreement. Read the terms of the agreement, and then click **Accept**.

Note: If the IBM Storage Protect for Cloud platform detects that your tenant needs to accept a subscription agreement of a service, a pop-up window will appear and display the new subscription agreement when you click the service.

Obtain a Full License

To obtain a full license for any of the IBM Storage Protect for Cloud, contact IBM Software Support.

IBM Storage Protect for Cloud charge licenses for certain Microsoft 365 subscriptions, Salesforce licenses. 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 Storage Protect for Cloud, the Tenant Owner and Service Administrators can start a trial on the **Home** page. Refer to the following section to obtain the trial licenses of services.

IBM Storage Protect for Cloud Dynamics 365 Trial

On the **Store** tab, navigate to **IBM Storage Protect for Cloud Dynamics 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 Storage Protect for Cloud Dynamics 365** in the **All Apps** view to access it. For detailed instructions on using IBM Storage Protect for Cloud Dynamics 365, refer to the IBM Storage Protect for Cloud Dynamics 365 User Guide.

IBM Storage Protect for Cloud for Google Workspace Trial

On the **Store** tab, navigate to **Cloud Backup for Google Workspace** 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.

You must click **Cloud Backup for Google Workspace** in the **All Apps** view to access it. For detailed instructions on using Cloud Backup for Google Workspace, refer to IBM Storage Protect for Cloud Google Worspace User Guide.

IBM Storage Protect for Cloud Microsoft 365 Trial

On the **Store** tab, navigate to IBM Storage Protect for Cloud Microsoft 365 and click **Start Microsoft 365 trial/Start Power Platform 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 Storage Protect for Cloud Microsoft 365 in the **All Apps** view to access it. For detailed instructions on using IBM Storage Protect for Cloud, refer to the IBM Storage Protect for Cloud Microsoft 365 User Guide .

IBM Storage Protect for Cloud Salesforce Trial

On the Store tab, navigate to IBM Storage Protect for Cloud Salesforce 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 Storage Protect for Cloud Salesforce in the All Apps view to access it. For detailed instructions on using IBM Storage Protect for Cloud Salesforce, refer to the IBM Storage Protect for Cloud Salesforce User Guide.

IBM Storage Protect for Cloud Azure VMs and Storage Trial

On the Store tab, navigate to IBM Storage Protect for Cloud Azure VMs and Storage 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 Storage Protect for Cloud Azure VMs and Storage in the All Apps view to access it. For detailed instructions on using IBM Storage Protect for Cloud Azure VMs and Storage , refer to the IBM Storage Protect for Cloud Azure VMs and Storage User Guide.

IBM Storage Protect for Cloud User Roles

In IBM Storage Protect for Cloud, 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 Storage Protect for Cloud. There is only one Tenant Owner per IBM Storage Protect for Cloud tenant. A Tenant Owner can perform the following actions:
  - Access online services (if there are available licenses)
  - View subscription 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 trusted IP address settings
  - Configure the security policy
  - Configure session timeout duration
  - Download a list of reserved IP addresses or ARM VNet IDs
  - Submit feedback
  - Edit personal profile information
- Service Administrator – The Tenant Owner or another Service Administrator can add Service Administrators to IBM Storage Protect for Cloud. 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 Storage Protect for Cloud. Tenant Users can be Standard Users or Application Administrators.
  - Standard Users can perform the following actions in IBM Storage Protect for Cloud:
    - 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” on page 20 for information that is specific to your service.

Manage Users

To manage IBM Storage Protect for Cloud 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:

- **Add** – Click **Add** and refer to the instructions in the "Add Users" on page 20 section.
- **Edit** – Select one user and click **Edit**. Then, refer to the instructions in "Edit User Permissions" on page 23.
- **Delete** – The Tenant Owner and Service Administrators can select one or multiple users, and then click **Delete**. In the confirmation window, click **Confirm**. All selected users and related data will be deleted.
- **Set as tenant owner** – The Tenant Owner and Service Administrators can select an activated Service Administrator and click **Set as tenant owner**. In the confirmation window, click **Confirm**. The email notification will be sent to the new Tenant Owner and the original Tenant Owner.
- **Deactivate** – The Tenant Owner and Service Administrators can select one or multiple users in the **Activated** status, and then click **Deactivate**. Deactivated users are not removed from IBM Storage Protect for Cloud but are restricted from accessing IBM Storage Protect for Cloud.
- **Activate** – The Tenant Owner and Service Administrators can select one or multiple users in the **Deactivated** / **Not Activated** status, and then click **Deactivate**.
- **Unlock** – If a user enters an incorrect password consecutively more than three times, the user account will be locked for an hour. Instead of waiting for the system to automatically unlock the account after an hour, the Tenant Owner and Service Administrators can manually unlock the account. To unlock an account, select the account and click **Unlock**.
- **Filter** – Set a filter to view users and groups by referring to the instructions below:

  1. Click **Filter** on the upper-right corner of the page. The **Filter** pane appears on the right of the page.
  2. In the **Filter** pane, configure conditions for the **Role**, **Service**, **Sign-in method**, or **Geo location** criteria.

     Note: The **Geo location** criterion is only available when your tenant has Multi-Geo Capabilities in IBM Storage Protect for Cloud Microsoft 365 service.
  3. Click **Apply**.

Note the following:

- Logged-in Tenant Owner and Service Administrators cannot edit, deactivate, or delete their own accounts.
- Application Administrators can only add/edit Tenant Users and manage available services for which they are Application Administrators.
- Logged-in Application Administrators cannot edit their own accounts.
- To manage the security settings for users in your IBM Storage Protect for Cloud tenant, refer to .Chapter 13, "Configure Advanced Settings," on page 87

Add Users

To add users and grant user permissions to IBM Storage Protect for Cloud 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 Storage Protect for Cloud users. They can use their Microsoft 365 login IDs to log into IBM Storage Protect for Cloud.

Note: To allow added users and group users to sign in to IBM Storage Protect for Cloud Microsoft 365 login IDs, IBM Storage Protect for Cloud recommends that the Microsoft 365 Global Administrator check the **Enterprise applications** configuration in **Microsoft Entra ID** > **Enterprise applications** > **Consent and permissions** > **User consent settings**. If the **Do not allow user** consent option is selected, the Microsoft 365 Global Administrator must consent to the **IBM Storage Protect for Cloud** 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?" on page 3

- **Salesforce User** – Salesforce users will become IBM Storage Protect for Cloud users. They can use their Salesforce login IDs to log into IBM Storage Protect for Cloud.

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.
   - **Salesforce tenant** – This option only appears if **Salesforce User** is selected as the sign-in method. Select the tenant of the users you want to add from the drop-down list.

   The tenants in the **Microsoft 365 tenant** and **Salesforce tenant** drop-down list are retrieved from **Tenant management**. For details on connecting tenants, refer to "Connect your tenants to IBM Storage Protect for Cloud" on page 13.
3. **Add Users** – Specify the users that you are about to add into IBM Storage Protect for Cloud.
   - For **Local User**, enter valid email addresses in the format of **someone@example.com**.
   - For **Microsoft 365 User/Group**, you can enter the following:
     - The username of Microsoft 365 usernames / email adddresses in the format of **someone@example.com**.
     - The aliases of Microsoft 365 users.
     - The names / email addresses 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 Storage Protect for Cloud.
   - For **Salesforce user**, enter usernames of Salesforce users in the format of **someone@example.com**.

   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 Entra ID. If you add **Everyone** as IBM Storage Protect for Cloud users, all available users can sign into IBM Storage Protect for Cloud 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 Storage Protect for Cloud, the following users cannot sign into IBM Storage Protect for Cloud:
     - The owner of the distribution group or mail-enabled security group.
     - If the security group has nested groups and the owner of a nested group is not a member of any other groups that have been added to IBM Storage Protect for Cloud, the nested group owner cannot sign into IBM Storage Protect for Cloud.
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 Storage Protect for Cloud User Roles" on page 19.
5. **Assign services and permissions to users** – Turn on the toggle of the service that the users should be able to access, and then select the permissions for the users. The services available for selection depend on your subscription. If your subscription for a specific service has expired, the service is unavailable for selection.

Service	Permission
IBM Storage Protect for Cloud Microsoft 365	**Standard User** In IBM Storage Protect for Cloud, Standard Users can configure restore settings, perform restores, and view activity reports. Additionally, Standard Users that are added to the Administrators group in IBM Storage Protect for Cloud 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 Storage Protect for Cloud 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 Storage Protect for Cloud Recovery Portal, run jobs to recover Microsoft 365 data, and view job reports.
	Application Administrator Application Administrators can use all the functionalities in IBM Storage Protect for Cloud Recovery Portal and manage access to IBM Storage Protect for Cloud Recovery Portal for Standard Users.
IBM Storage Protect for Cloud Azure VMs and Storage	**Application administrator** The application administrator can configure backup and restore settings, perform backup and restore, view activity reports, etc.
IBM Storage Protect for Cloud Salesforce	**Standard User** A standard user must be added into a user group in IBM Storage Protect for Cloud Salesforce by Administrators for using the specific features according to the permissions granted to the user group.
	Application Administrator The application administrator fulfills the role of an Administrator. The Administrator can perform backup/restore jobs, export backup data to CSV, download reports, and manage IBM Storage Protect for Cloud Salesforce settings.
IBM Storage Protect for Cloud Dynamics 365	**Application Administrator** The application administrator can configure backup and restore settings, perform backup and restore, view activity reports, etc.

Service	Permission
EnPower	**Standard user** In EnPower, Tenant Users map to the Standard user role.
	Application administrator In EnPower, Application administrators can use all the functions.

6. **Available geo location** If your tenant has Multi-Geo Capabilities in IBM Storage Protect for Cloud 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** or **Salesforce User**) – 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 into IBM Storage Protect for Cloud.

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:

   - **Assign services and permissions to users** – Turn on the toggle of the service that the users should be able to access, and then select the permissions for the users. For more information, refer to Assign services and permissions to users.
   - **Available geo location** – This field only appears when your tenant has Multi-Geo Capabilities in IBM Storage Protect for Cloud Microsoft 365service, 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.

Chapter 4. View Subscription Information

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

Your service may be in the **Out of policy** status if:

- The number of assigned licenses in Microsoft 365 has exceeded the purchased user seats for IBM Storage Protect for Cloud.
- The subscription you purchased for an IBM Storage Protect for Cloud does not provide enough capacity for all protected Microsoft 365 objects.

You can hover the mouse on the **Out of policy** label of a service to view the details. To ensure you can use the services without any interruption, you must contact IBM Software Support to purchase more user seats. For IBM Storage Protect for Cloud 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 Storage Protect for Cloud charge licenses for certain Microsoft 365 subscriptions and Salesforce licenses. For more information, refer to

To view the detailed information on the subscription for each available service, navigate to **Administration** > **Subscription** on the left pane. The **Subscription** page displays the subscription type, subscription status, and expiration date on the tile of each service. Click a service name to view more details about your subscription for this service. The details may include subscription agreement, purchased user seats, and specific services' additional information like purchased capacity, purchased modules, and so on.

Note: When you view subscription details of the IBM Storage Protect for Cloud Microsoft 365, you can click **Download usage details** or **Download capacity usage details** to download a report.

To obtain a full subscription for any of the IBM Storage Protect for Cloud, contact IBM Software Support.

Chapter 5. Manage Organization Profile Information

The Tenant Owner and Service Administrators can refer to the following steps to manage information for the organization profile in IBM Storage Protect for Cloud.

1. Click your account on the upper-right corner.
2. Click **Organization profile** from the drop-down list.
3. In the **Organization profile** pane, click **Edit**.
4. In the **Edit organization profile** pane, make your edits in any available fields.
5. Click **Save**.

Chapter 6. Manage Your Profile Information

To view/change your account information or to change your password, click your account 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/Salesforce Service Administrators.

The **My profile** pane appears on the right of the page, displaying your account information. You can take the following actions:

- **Edit** – Click **Edit** to change your first name and last name. Edit the information in any of the available fields. Click **Save** to save your changes, or click **Cancel**.
- **Change password** – Click **Change password** to reset a new password for your IBM Storage Protect for Cloud account when you're logged in. In the **Change password** pane, complete the following steps:
  - 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 **Change password** button 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.

Chapter 7. Manage Service Account Profiles

Configure a Microsoft 365 service account profile that contains a Microsoft 365 account with the permissions required by your tenant's cloud services. With the credentials of this account, you can invite Microsoft 365 users or groups as IBM Storage Protect for Cloud users. Auto Discovery also uses the credentials to scan Microsoft 365 objects. For an overview about when IBM Storage Protect for Cloud needs your Microsoft 365 account, see "Appendix E - When Service Account and App Profile are Used" on page 137.

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

- **Create** – Click **Create** on the ribbon. Then, refer to the instructions in "Create a Service Account Profile" on page 31.
- **Edit** – Select a service account profile and click **Edit**.

  To view details of a service account profile, click the link in the **Profile name** column. When you view the details of a service account profile, you can also click **Edit** to edit its details.

  Note: If your organization uses multi-factor authentication (MFA) in Microsoft 365 and has configured MFA service account profiles in the classic UI, you can edit MFA service account profiles by referring instructions in the appendix: "What Should I Do If My Organization Uses Multi-Factor Authentication (MFA) in Microsoft 365?" on page 4
- **Delete** – Select one or more service account profiles and click **Delete**. A pop-up window appears asking for your confirmation. Click **Confirm** to confirm your deletion.

Create a Service Account Profile

About this task

To create a service account profile, click **Create**. Then configure the following settings in the **Create Service Account Profile** pane.

Note: If you have configured service account profiles in the classic UI, these service account profiles still can be used to scan objects and invite users in the new UI.

Procedure

1. **Profile Name** – Enter a name for the service account profile.
2. **Description** – Enter an optional description.
3. **Select tenant** – Select a tenant from the drop-down list.
4. **Select service** – Select at least one service from the drop-down list.
5. **Username** – Specify an account with the permissions required by your tenant's cloud services. The permissions of the Microsoft 365 service account vary with the different cloud services your tenant is using. Refer to the "Required Permissions of Cloud Services" on page 32 for more information.

   Note the following:

   - IBM does not recommend that a personal active user account be used as the service account. We recommend you use a separate service account to handle all administration.
   - If you select the **IBM Storage Protect for Cloud Microsoft 365** service, to restore the Managed Metadata Service, the specified service account will be automatically added as one of the Term Store Administrators.

- The specified Microsoft 365 account cannot have multi-factor authentication (MFA) enabled. If your organization has MFA enabled, you can refer to the following link for additional details: "Helpful Notes for Passing the Validation Test of a Service Account" on page 32

6. **Password** – Enter the login password of the account above.

   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 Password Limitations and Requirements of Microsoft 365 Accounts.
7. Click **Save** to save your configurations, or click **Cancel** to go back to the **Service account** page without saving any configurations.
8. If you encounter the error **Your organization has set access policies that block the validation** and the service account profile cannot be saved, refer to "Helpful Notes for Passing the Validation Test of a Service Account" on page 32for troubleshooting.

Helpful Notes for Passing the Validation Test of a Service Account

About this task

If your organization uses multi-factor authentication (MFA), or if you encounter the error **Your organization has set access policies that block the validation**, causing that the service account profile cannot be saved, refer to the solutions below for troubleshooting:

- Delete or disable the access policies / multi-factor authentication.
- Edit the access policies to exclude the Microsoft 365 user set as the Service Account.
- Edit the access policies to exclude the reserved IP addresses of IBM Storage Protect for Cloud. The reserved IP addresses can be downloaded in **Administration** > **Security**.

Required Permissions of Cloud Services

The following services support 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. Refer to the information in the links below to prepare a Microsoft 365 account and assign the required roles to this account.

- IBM Storage Protect for Cloud Dynamics 365
- IBM Storage Protect for Cloud Microsoft 365
- IBM Storage Protect for Cloud Azure VMs and Storage

Validation Test Troubleshooting

When the validation test is failed and you encounter one of the following error messages, refer to the solutions below for troubleshooting:

Message 1: Your organization has set access policies which block the validation

Solution: Choose one of the following methods based on your scenario.

- Delete or disable the access policies.
- Edit the access policies to exclude the Microsoft 365 user set as the Service Account.
- Edit the access policies to exclude the reserved IP addresses of IBM Storage Protect for Cloud. The reserved IP addresses can be downloaded in **Administration** > **Security** > **Reserved IP addresses**.

Message 2: Check if this account has multi-factor authentication enabled or you have entered an app password

Solution: If the account has multi-factor authentication enabled, choose one of the following methods based on your scenario.

- In the field, select the **Our organization uses multi-factor authentication** checkbox. Enter the app password in the **PEnable MFAassword** field.
- If you do not want to select the **Our organization uses multi-factor authentication** checkbox, you need to disable multi-factor authentication for the Microsoft 365 user set as the Service Account.

If the account does not have multi-factor authentication enabled and you haven't entered an app password, check if the login password of the account is correct.

Message 3: This account has multi-factor authentication enabled

Solution: Choose one of the following methods based on your scenario.

- If this account has multi-factor authentication enabled on the **multi-factor authentication** interface, either select the **Our organization uses multi-factor authentication** checkbox in the **Enable MFA** field or disable multi-factor authentication for the Microsoft 365 user.
- If your Microsoft 365 tenant has enabled multi-factor authentication in Microsoft Entra ID conditional access policies, refer to the solution for Message 1 to either exclude the Service Account from the access policies or exclude IBM Storage Protect for Cloud reserved IP addresses from the access policies.

Create an On-premises Service Account Profile

To create an on-premises service account profile, navigate to **Management** > **Service account** > **On-premisesservice account**, click **Create** under the **On-premises service account** tab, and then configure the following settings:

1. **Profile name** – Enter a name for the service account profile.
2. **Description** – Enter an optional description.
3. **Exchange service provider** – Select an option from the drop-down list.
4. **Exchange version** – Select an option from the drop-down list.
5. **Exchange server host** – Enter the hostname of your Exchange server. If your Exchange server is hosted by any service provider, provide the Web access host of the Exchange server.
6. **Username** – Enter the username of an account that will be used to connect to the above Exchange server host. Note that the account must have a mailbox, and the format of the account must be **username@contoso.com**.
7. **Password** – Enter the password of the account above.
8. Click **Save** to save your configurations.

   Note: If the creation fails and the error message **Failed to validate this on-premises service account. Check the information you entered and try again.** appears, you can try the following methods for troubleshooting:

   - Ensure that the reserved IP addresses downloaded from IBM Storage Protect for Cloud have been added to your environment firewall. For details, refer to "Download a List of Reserved IP Addresses" on page 75 .
   - Use the Microsoft Remote Connectivity Analyzer tool to troubleshoot connectivity issues with your server deployments.

Chapter 8. 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 use an account pool that contains multiple Microsoft 365 accounts. When IBM Storage Protect for Cloud registers SharePoint Online site collections and OneDrive for Business, IBM Storage Protect for Cloud grants the site collection administrator permission to the group set in the account pool for **Sites, Mailboxes, Groups, Teams, Project Sites, Exchange Public Folders**, 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 Storage Protect for Cloud can work smoothly. For example, IBM Storage Protect for Cloud 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?" on page 4

To build an account pool in IBM Storage Protect for Cloud, 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.

Object Type	Need Account Pool?	Need Username?	Need Password?	Need SharePoint Administrator Role?	Need License?	
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 Microsoft Entra ID product licenses assigned in Microsoft 365: **Premium P1** or **Premium P2**.
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.

Note: For managing Microsoft 365 users, the EnPower service needs the Microsoft 365 Global Administrator role.

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 **Sites**, **Mailboxes**, **Groups**, **Teams**, and **Project Sites**, or **Exchange Public Folders** according to the objects you will back up or manage via services for Microsoft 365.

   Note: The **Sites, Mailboxes, Groups, and Teams** tab includes different object types for the following cloud services:

   - For the EnPower service, this tab includes SharePoint sites, OneDrive for Business, Microsoft 365 Group team sites, Exchange Online mailboxes, and Microsoft 365 mailboxes.
   - For other services, this tab includes SharePoint sites, OneDrive for Business, and Microsoft 365 Group team sites.

   Click a tab and configure the following settings:

   a. **Group Name** – 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?" on page 3.

      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 Storage Protect for Cloud 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 Micrsoft Entra ID, 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 Storage Protect for Cloud 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.

Chapter 9. Manage App Profiles

IBM Storage Protect for Cloud Microsoft 365 can connect to your Microsoft 365, Microsoft Azure Active Directory, Yammer, Dynamics 365, Salesforce or Salesforce Sandbox via app profiles for the related apps in your environments. To help you decide whether to use IBM Storage Protect for Cloud default apps or your organization's custom apps, the API Permissions Required by IBM Apps and API Permissions Required by Custom Apps sections are for your reference.

The Tenant Owner and Service Administrators can navigate to **Management** > **App management** to manage app profiles via the following actions:

- To create an app profile, click **Create**. On the **Create app profile** page, select a tenant, select services, select a setup method (classic mode, modern mode, or custom mode), and then consent to apps. After an app profile is created, the related app will be created in the environment. For details on creating an app profile, refer to Create an App Profile.

  Note: Before you create an app profile, you must ensure that the tenant has been connected to IBM Storage Protect for Cloud. For more details on connecting tenants, refer to "Connect your tenants to IBM Storage Protect for Cloud" on page 13.

  For the **Salesforce** platform, after the tenants in the **Salesforce** or **Salesforce Sandbox** environment are successfully connected in **Tenant management**, the related app profiles (Salesforce or Salesforce Sandbox) will be automatically created in **App management**.
- To edit the name and description of an app profile or change the services for which an app profile can be used, select the app profile and click **Edit**. On the **Edit app profile** page, edit the name or description, select services which will be supported by the app profile, and click **Save**.
- **Re-authorize** app profiles for Microsoft/Salesforce tenants in the following scenarios:
  - The app profiles which are in the **Expired** status must be re-authorized.

    Note: According to Microsoft's non-interactive user sign-ins, the sign-in logs show the original IP used for the original token issuance, as the IP address of non-interactive sign-ins performed by confidential clients (IBM Storage Protect for Cloud) doesn't match the actual original IP of the event when a Microsoft user signed in and consented to an app. If you create an app with delegated permissions, you must add the original IP address to your Microsoft tenant's conditional access policies (if any). Otherwise, the apps with delegated permissions will be **Expired**. After you add the original IP address to your conditional access policies, you can manually re-authorize the app profile to update its status or wait for IBM Storage Protect for Cloud to automatically update its status.
  - If you want to change the account used to consent to an app, you can re-authorize the related app profile.
  - If an app has been updated to add new API permissions required by new features, the related app profile must be re-authorized.
  - For a **Delegated app** used by the **IBM Storage Protect for Cloud Microsoft 365** service, you also need to re-authorize the app profile if you want to change the functions which will use the app. When you re-authorize the **Delegated app**, ensure that your organization's subscription for the IBM Storage Protect for Cloud Microsoft 365 service has included the modules you want to protect. Then, you can select desired functions from the following that are supported by the **Delegated app**:
  - **Restore Teams channel conversations as posts**
  - **Protect Planner data**
  - **Protect Power BI**
  - **Protect Power Automate / Power Apps**
  - For a custom **Yammer** app, you also need to re-authorize the app profile if you want to change the custom app.
  - For a **Custom azure app** / **Custom azure app with delegated permissions**, you also need to re-authorize the app profile if:

- you want to change the custom Azure app that connects IBM Storage Protect for Cloud to your tenant.
- the certificate file of the custom Azure app has been changed.

To re-authorize an app profile for a Microsoft/Salesforce tenant, refer to the following **Re-authorize an App Profile** section for more details.

- To view details of an app profile, click the link in the **Profile name** column. The **App profile detail** page appears on the right of the page. When you view the details of an app profile, you can edit or re-authorize the app profile.
- **Delete** – Before you delete an app profile, ensure it is no longer needed. To delete an app profile, select the app profile, click **Delete**, and click **Confirm** in the confirmation window.

  Note: For **Salesforce** and **Salesforce Sandbox** apps, if you delete an app profile, the related Salesforce tenant connection will be automatically removed from IBM Storage Protect for Cloud.
- To manage columns in the table on the **App management** page, click **Column** on the upper-right corner of the page, select desired options, and click **Apply**.

Create an App Profile

About this task

Procedure

In **Management** > **App management**, the Tenant Owner and Service Administrators can click **Create** and follow the steps below to create an app profile.

1. **Select services** – Select a tenant and select services for which you want to create app profiles. Click **Next**.

   Note: Before you create an app profile, you must ensure that the tenant has been connected to IBM Storage Protect for Cloud. For more details on connecting tenants, refer to "Connect your tenants to IBM Storage Protect for Cloud" on page 13 .

   For the **Salesforce** tenants, once the tenants are successfully connected in **Tenant management**, the related app profiles will be automatically created in **App management**.
2. **Choose setup method** – Refer to the information below, and select a mode based on your scenario:

   - **Modern mode** is supported by all IBM Storage Protect for Cloud, which is the recommended mode if you want to use the method of consenting to one app for one service. In this mode, the related apps are listed in a service-based view. You can consent to apps separately for the selected services.

     Note: In **Auto discovery**, scan profiles will run jobs and randomly use app profiles which have the required permissions to scan objects. For specific functionalities in services, only the related service apps have the required permissions to support. For additional details on the permissions of service apps, see Apps for Individual Service.
   - **Classic mode** includes the method of consenting to one app which can be used by multiple services. This mode will not be displayed if it is not supported by the selected services.

     If you select this mode, note the following:

     – In the **Application list**, you can consent to the following apps which can be used by multiple services: **Microsoft 365 (All permissions)**, **Microsoft Azure AD**, and **Yammer**.

     The table below lists the services supported by the apps in the classic mode **Application list**:

Apps	Supported services	Consent method
Microsoft 365 (All permissions)	IBM Storage Protect for Cloud Microsoft 365	Consent to one app to be used by multiple services.

Apps	Supported services	Consent method
Microsoft Azure AD	IBM Storage Protect for Cloud Microsoft 365	
Yammer	IBM Storage Protect for Cloud Microsoft 365	
Delegated App	IBM Storage Protect for Cloud Microsoft 365	Consent to the app separately for each service.

  - In the **Service app list**, you can also separately consent to the apps used by specific services.
- **Custom mode** is recommended only for users who have identified use cases with extremely limited required permissions. In this mode, you can manually create and maintain custom apps of the following types in your environment:

App Type	Supported Services
Azure app	IBM Storage Protect for Cloud Microsoft 365
Yammer	IBM Storage Protect for Cloud Microsoft 365

  Before you create an app profile for a custom app, refer to Create Custom Apps to create custom apps which meet the requirements of your services.

3. **Consent to apps** – To consent to an app, click **Consent** next to the app, and refer to the information below to continue with the consent:
   - Creating app profiles for IBM apps in a Microsoft tenant's environment requires a **Microsoft 365 Global Administrator** account who is in the same tenant. For more details on this requirements, see the "Why Admin Consent is Required to Use the IBM Storage Protect for Cloud App?" on page 7section.

     When creating an app profile for a delegated app used by the **Cloud Backup for Microsoft 365** service, you also need to choose the functions which will use this app.
   - For details on consenting to custom apps, refer to the following section: **Consent to Custom Apps**.

   When you finish creating app profiles, you can click **Finish** to exit the **Create app profile** wizard.

   Note: According to Microsoft's non-interactive user sign-ins, the sign-in logs show the original IP used for the original token issuance, as the IP address of non-interactive sign-ins performed by confidential clients (IBM Storage Protect for Cloud) doesn't match the actual original IP of the event when a Microsoft user signed in and consented to an app. If you create an app with delegated permissions, you must add the original IP address to your Microsoft tenant's conditional access policies (if any). Otherwise, the apps with delegated permissions will be **Expired**. After you add the original IP address to your conditional access policies, you can manually re-authorize the app profile to update its status or wait for IBM Storage Protect for Cloud to automatically update its status.
4. After you create app profiles for the following apps, you need to go to Microsoft Entra admin center (or Microsoft Azure portal) to assign roles to the apps:

   If the following apps will be used in scan profiles to scan **Exchange mailbox** / **Security and distribution group** objects, you need to assign the **Exchange Administrator** role to apps by referring to this section: How to Assign the Exchange Administrator Role to an App?
   - Microsoft 365 (All permissions)
   - IBM Storage Protect for Cloud Microsoft 365 (All permissions)
   - IBM Storage Protect for Cloud Microsoft 365 (Exchange permissions)
   - Custom app for IBM Storage Protect for Cloud Microsoft 365

Re-authorize an App Profile

Procedure

To re-authorize an app profile for a Microsoft/Salesforce tenant, follow the steps below:

1. Select the app profile and click **Re-authorize**.
2. In the **Re-authorize** window, refer to the information below to continue:
   - To grant consent to IBM apps in a Microsoft tenant's environment, sign in with a **Microsoft 365 Global Administrator** account that is in the same tenant. For more details on these requirements, see the "Why Admin Consent is Required to Use the IBM Storage Protect for Cloud App?" on page 7section.

     When granting consent to a delegated app used by the IBM Storage Protect for Cloud Microsoft 365 service, you also need to choose the functions which will use this app.
   - To grant consent to a **Custom azure app** / **Custom azure app with delegated permissions** app, complete the following settings:
     - **Application ID** – Enter the application ID of the application that has been created in Azure by referring to the Create Custom Apps section.
     - **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 prepare one by referring to Prepare a Certificate for the Custom Azure App.
     - **Certificate password** – Enter the password of the certificate.
     - **Impersonation name** – Enter the username of a user in your Microsoft 365 tenant. This user will be used to call the Microsoft APIs required by your services. This field is not needed when you consent to a custom Azure app with delegated permissions.
   - To grant consent to a custom **Yammer** app, sign in with an account that has the Verified Admin privileges and complete the following settings:
     - **Client ID** – Enter the client ID of your custom app.
     - **Client secret** – Enter the client secret of your custom app.
   - To grant consent to a **Salesforce** / **Salesforce Sandbox** app, sign in with a Salesforce account that has the System Administrator profile or another profile with the same permissions.
3. Click **Continue to consent** and sign in with an account that has the required permissions to grant consent to the app.

How to Assign the Exchange Administrator Role to an App?

About this task

If you create app profiles for the following apps and these apps will be used in scan profiles (see Manage Auto Discovery for more details on scan profiles) to scan **Exchange mailbox** or **Security and distribution group** objects, you need to go to Microsoft Entra admin center (or Microsoft Azure portal) to assign the **Exchange Administrator** role to the apps:

- IBM Storage Protect for Cloud Microsoft 365 (All permissions)
- IBM Storage Protect for Cloud Microsoft 365 (Exchange permissions)
- Microsoft 365 (All permissions)
- Custom apps of the following services: IBM Storage Protect for Cloud Microsoft 365

Procedure

To assign the **Exchange Administrator** role to the app, refer to the following steps:

1. Log in to Microsoft Entra admin center (or Microsoft Azure portal) and go to **Microsoft Entra ID**.
2. Click **Roles & admins (or Roles and administrators)** in the left pane, and click the **Exchange Administrator** role you want to assign.
3. On the **Assignments** page that opens, click **Add assignments**.
4. On the **Add assignments** page, enter the app name in the search box to search for the app to which you want to assign the role.
5. Select the app, and click **Add** to assign the role. Note that the assigned role will take effect in about 30 minutes.

Assign Custom Exchange Online Role Groups to the Application

Procedure

Follow the steps below to create custom Exchange Online role groups and assign custom Exchange Online role groups to an application:

Note: For more details on this method, refer to this Microsoft article.

1. Refer to the instructions in Create role groups to create custom Exchange Online role groups.
2. In Microsoft Graph PowerShell, run the *Get-MgServicePrincipal* command to store the details of the application.

```
Connect-MgGraph -Scopes 'Application.Read.All'
$AADApp = Get-MgServicePrincipal -Filter "DisplayName eq
```

   Replace <AppName>with the application name.
3. In the same PowerShell window, connect to Exchange Online PowerShell and run the following commands:
   - Run the *New-ServicePrincipal* command to create an Exchange Online service principal object for the application.
   - Run the *Get-ServicePrincipal* command to store the details of the service principal in a variable.

```
New-ServicePrincipal -AppId $AADApp.AppId -ObjectId $AADApp.Id -DisplayName "<Descriptive
Name>"
$SP = Get-ServicePrincipal -Identity "<Descriptive Name>"
```

   Replace <Descriptive Name> with the application name.
4. In Exchange Online PowerShell, run the following command to add the service principal as a member of the customer role group:

```
Add-RoleGroupMember -Identity "<CustomRoleGroupName>" -Member $SP.Identity
```

   Replace <CustomRoleGroupName> with the name of your custom Exchange Online role group.

Create Custom Apps

About this task

The table below lists which services are supported by custom apps.

App type	Supported services
Azure app	IBM Storage Protect for Cloud Microsoft 365
Yammer	IBM Storage Protect for Cloud Microsoft 365

To create custom apps, refer to the instructions in the sections below.

Create a Custom Azure App

Procedure

To create a custom app, follow the steps below:

1. Go to Microsoft Entra admin center (or Microsoft Azure portal). Azure Portal.
2. Navigate to **Microsoft Entra ID** > **App registrations** > **New registration**.
3. On the **Register an application** page, enter your application's registration information:
   - **Name** – Enter a name for the custom application.
   - **Supported account types** – Select which accounts you would like this application to support.
   - **Redirect URI** – This field is required when you create a custom Azure app with delegated permissions. Enter the following URL:
     – Commercial production environment: https://sp4c.storage-defender.ibm.com
4. Click **Register** to create the custom application.
5. Click the created custom application, and click **API permissions**.
6. Click **Add a permission** to add permissions to the app.

   The permissions that you need to grant to the custom app vary with the different cloud services your tenant is using. Refer to the API Permissions Required by Custom Apps section to view the required permissions for your services.
7. Click **Grant admin consent for [Tenant name]** to grant admin consent. After you successfully granted admin consent for the requested permissions, the **Status** will be **Granted for [Tenant name]**.
8. The application uses certificate authentication. Complete the following steps to upload your organization's public certificate (the .cer file):
   a. Locate your organization's certificate and export the certificate as a .cer file.
   b. Go to Microsoft Entra admin center (or Microsoft Azure portal), select the application, and click **Certificate & secrets**.
   c. In the **Certificates** section, click **Upload certificate**.
   d. Select the .cer file (the recommended file type) and click **Add**.
   e. 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 G - Prepare a Certificate for the Custom Azure App" on page 142 to prepare one.

   Then, refer to the Create an App Profile section to create an app profile in the **Custom mode**.

Create a Custom Yammer App

Procedure

To create a custom Yammer app, complete the following steps:

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 the following URL:
   - Commercial production environment: **https://sp4c.storage-defender.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 Storage Protect for Cloud.

   Then, refer to the Create an App Profile section to create an app profile in the **Custom mode**.

Additional Notes for Azure Apps with Delegated Permissions

To create a custom Azure app with delegated permissions, you can refer to the instructions in the **Create a Custom Azure App** section above. Note that **Redirect URI** and **ID tokens** are required by a custom Azure app with delegated permissions, and you can refer to the following instructions to configure the settings:

1. Go to Microsoft Entra admin center (or Microsoft Azure portal).
2. Navigate to Microsoft Entra ID > **App registrations**, and then click the app that you want to configure.
3. Click **Authentication** in the left pane.
4. On the **Authentication** page, follow the instructions below based on your scenario:
   - If the **Redirect URIs** setting is not displayed on the **Authentication** page, refer to the steps below:
     a. Click Add a platform.
     b. In the **Configure platforms** right pane, click **Web**.
     c. In the **Configure Web** right pane, enter a URL in the **Redirect URIs** field based on the version of your IBM Storage Protect for Cloud environment, select the **ID tokens** option, and click **Configure**.

        Note: If the **ID tokens** option has been selected on the **Authentication** page, it will not be displayed in the **Configure Web** pane.

        Below is the URL of the IBM Storage Protect for Cloud environment:

        https://sp4c.storage-defender.ibm.com
   - If the **Redirect URIs** setting is displayed on the **Authentication** page, refer to the steps below:
     a. Click **Add URI**, and then enter a URL in the field:
        – https://sp4c.storage-defender.ibm.com
     b. Select the **ID tokens** option.
     c. Click **Save**.

Configure a Conditional Access Policy on Custom Apps in Azure for Best Practice

If you want to make sure the custom apps in Azure can only be used by the IBM Storage Protect for Cloud production environment for best practice, you can refer to the instructions below to configure a conditional access policy.

1. Log in to Microsoft Entra admin center (or Microsoft Azure portal) and navigate to **Protection** (or **Security**) > **Conditional Access** > **Named locations**.
2. Click **IP ranges location**.
3. In the **New location (IP ranges)** right pane, complete the steps below:
   a. Name this location.
   b. Click **+** to add IP ranges based on the reserved IP addresses downloaded from IBM Storage Protect for Cloud. For details on the reserved IP addresses, see Download a List of Reserved IP Addresses.
   c. Click **Create**.
4. Go to the **Overview** page and click **Create new policy**.
5. Refer to the following instructions to configure a new policy:
   a. Enter a policy name.
   b. Click **Users or workload identities**, select **Workload identities**, choose **Select service principals**, and select your custom apps for IBM Storage Protect for Cloud.

c. Click **Conditions**, click **Locations**, toggle **Configure** to **Yes**, choose the **Selected locations** option under the **Exclude** tab, and select the location created in the step 3.

d. Click **Grant** and select **Block access**.

e. Toggle the **Enable policy** option to **On**.

f. Click **Create**.

API Permissions Required by IBM Apps

About this task

The following sections list the API permissions required by IBM apps.

- Apps for Multiple Services – This section lists the apps that can be used by multiple services.
- Apps for Individual Service – This section lists the apps that are only for individual services.

Apps for Multiple Services

About this task

The following sections list the apps which can be used by multiple services and the API permissions required by these apps.

Microsoft 365 (All Permissions)

The **Microsoft 365 (All permissions)** app profile can be used by the following services:

- IBM Storage Protect for Cloud Microsoft 365

Once you create a **Microsoft 365 (All permissions)** app profile, the **IBM Storage Protect for Cloud Microsoft 365** app will be generated accordingly in your Microsoft Entra ID. The table below lists the permissions that should be accepted when you authorize the **IBM Storage Protect for Cloud Microsoft 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	Backup 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.
Office 365 Management APIs	ActivityFeed.Read (Read activity data for your organization)	Application	Retrieve activity data in your organization to generate reports.

API	Permission	Type	Why we need it?
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)	Application	Support signing into IBM Storage Protect for Cloud with Microsoft 365 accounts.
	Group.ReadWrite.All (Read and write all groups)	Application	Scan Microsoft 365 Groups and Microsoft Teams via Auto Discovery.
			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)	Application	Backup and restore Microsoft Teams and Microsoft 365 Groups data.
	Sites.Read.All (Read items in all site collections [preview])	Application	Backup and restore Microsoft Teams and Microsoft 365 Groups data.
	Reports.Read.All (Read all usage reports)	Application	IBM Storage Protect for Cloud Microsoft 365 can retrieve data size directly, which improves the efficiency of the Subscription Consumption Report.
	ChannelMember.ReadWrite.All (Add and remove members from all channels)	Application	IBM Storage Protect for Cloud Microsoft 365uses it to back up and restore the members and messages of Teams private channels.
	ChannelMessage.Read.All (Read all channel messages)	Application	Backup 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.
	User.Read.All (Read all users' full profiles)	Application	Retrieves and displays user photos and user basic information.
	User.ReadWrite.All (Read and write all users' full profiles)	Application	It allows users to remove or block external users in Insights for Microsoft 365.
	AuditLog.Read.All (Read all audit log data)	Application	Insights for Microsoft 365 uses it to retrieve the last sign-in time of external users.
	TeamSettings.ReadWrite.All (Read and change all teams' settings)	Application	IBM Storage Protect for Cloud 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	Insights for Microsoft 365 can retrieve and manage members in your Teams.
	TeamsTab.ReadWrite.All (Read and write tabs in Microsoft Teams)	Application	IBM Storage Protect for Cloud Microsoft 365 uses it to back up and restore teams' tabs.
	Team.Create (Create teams)	Application	IBM Storage Protect for Cloud Microsoft 365 uses it to restore teams.
	TeamsAppInstallation.ReadWriteForTeam.All (Manage Teams apps for all teams)	Application	IBM Storage Protect for Cloud Microsoft 365 uses it to back up and restore teams' apps.
	Channel.Create (Create channels)	Application	IBM Storage Protect for Cloud Microsoft 365 uses it to restore teams' channels.
	InformationProtectionPolicy.Read.All (Read all published labels and label policies for an organization.)	Application	Insights for Microsoft 365 uses it to retrieve sensitivity labels from Microsoft 365.
	Chat.Read.All (Read all chat messages)	Application	IBM Storage Protect for Cloud Microsoft 365 uses it to back up Microsoft Teams Chat.
	Files.ReadWrite.All (Read and write files in all site collections)	Application	IBM Storage Protect for Cloud Microsoft 365 uses it to back up and restore the OneDrive for Business files.
	Sites.Manage.All (Create, edit, and delete items and lists in all site collections)	Application	IBM Storage Protect for Cloud Microsoft 365 uses it to back up and restore the OneDrive for Business files.
	Sites.FullControl.All (Have full control of all site collections)	Application	IBM Storage Protect for Cloud Microsoft 365 uses it to back up some files in specific conditions, such as DLP-sensitive files.
Microsoft Information Protection Sync Service	UnifiedPolicy.Tenant.Read (Read all unified policies of the tenant)	Application	Insights for Microsoft 365 can retrieve information of published sensitivity labels from Microsoft 365.

Microsoft 365 (SharePoint Online Permissions)

The **Microsoft 365 (SharePoint Online permissions)** app profile can be used by the following services:

- IBM Storage Protect for Cloud Microsoft 365

  The Microsoft 365 (SharePoint Online permissions) app profile is for the **IBM Storage Protect for Cloud** app in your Microsoft Entra ID. The table below lists the permissions that should be accepted when you authorize the **IBM Storage Protect for Cloud** 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	Backup and restore Managed Metadata Service of SharePoint Online site collections and Microsoft 365 Group team sites.
Office 365 Management APIs	ActivityFeed.Read (Read activity data for your organization)	Application	Retrieve activity data in your organization.
Microsoft Graph	User.Read (Sign in and read user profile)	Delegated	Support signing into IBM Storage Protect for Cloud accounts.
	Reports.Read.All (Read all usage reports)	Application	IBM Storage Protect for Cloud Microsoft 365 can retrieve data size directly, which improves the efficiency of the Subscription Consumption Report.
	Directory.Read.All (Read directory data)	Application	Retrieve your Microsoft 365 tenant information.
Microsoft Information Protection Sync Service	UnifiedPolicy.Tenant.Read (Read all unified policies of the tenant.)	Application	Insights for Microsoft 365 can retrieve information of published sensitivity labels from Microsoft 365.

Microsoft 365 (Exchange Permissions)

The **Microsoft 365 (Exchange permissions)** app profile can be used by the following services:

- IBM Storage Protect for Cloud Microsoft 365

The **Microsoft 365 (Exchange permissions)** app profile is for the **IBM Storage Protect for Cloud Microsoft 365** app in your Microsoft Entra ID. The table below lists the permissions that should be accepted when you authorize the **IBM Storage Protect for Cloud Microsoft 365** 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 Storage Protect for Cloud with Microsoft 365 accounts.
	Reports.Read.All (Read all usage reports)	Application	IBM Storage Protect for Cloud Microsoft 365 can retrieve data size directly, which improves the efficiency of the Subscription Consumption Report.
	Directory.Read.All (Read directory data)	Application	Retrieve your Microsoft 365 tenant information.

Yammer

When you create a **Yammer** app profile in IBM Storage Protect for Cloud, the **Yammer Delegate App** is automatically created in your Microsoft Entra ID. The account used to consent to the app must be **Microsoft 365 Global Administrator** account that is in the same tenant. The table below lists the permissions that should be accepted when you authorize the **Yammer Delegate App**.

API	Permission	Type	Why we need it?
Microsoft Graph	User.Read (Sign in and read user profile)	Delegated	Support signing into IBM Storage Protect for Cloud with Microsoft 365 accounts.
Yammer	user_impersonation (Read and write to the Yammer platform [preview])	Delegated	To access the Yammer platform on behalf of the signed-in user.

Delegated App

When you create an app profile for a **Delegated app**, refer to the following sections to see the delegated permissions that should be accepted when you authorize the **IBM Storage Protect for Cloud** app to be created in your Microsoft Entra ID.

IBM Storage Protect for Cloud Azure VMs and Storage

API	Permission	Why we need it?
Azure Service Management	user_impersonation (Access Azure Service Management as organization users [preview])	Allows the application to access Azure Service Management as you.

IBM Storage Protect for Cloud Microsoft 365

API	Permission	Why we need it?
Microsoft Graph	Group.ReadWrite.All (Read and write all groups)	Retrieves tabs information from Microsoft Teams. Protects planner data in Microsoft 365 Groups and 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.
	User.Read.All (Read all users' full profiles)	Retrieves information of user profiles in Planner data restore.
	Directory.Read.All (Read directory data)	Retrieves the profile and domain information of all users in your Microsoft 365 tenant.
Power BI Services	Tenant.ReadWrite.All (Read and write all content in tenant)	Retrieves the workspaces and backs up, or adds users to a workspace.
	Workspace.ReadWrite.All (Read and write all workspaces)	Gets and restores workspaces
	Capacity.Read.All (View all capacities)	Retrieves capacities (including multi-geo)
	Report.ReadWrite.All (Read and write all reports)	Performs backup for reports.
	Dataset.ReadWrite.All (Read and write all datasets)	Performs backup and restore for reports.
PowerApps Service	User (Access the PowerApps Service API)	Retreives information on Cloud Flows in Power Automate.

API	Permission	Why we need it?
Dynamics CRM	user_impersonation (Access Common Data Service as organization users)	Retreives information on Desktop Flows and Business Process Flows in Power Automate.

Apps for Individual Service

About this task

The following sections list the apps which can be used by individual services and the API permissions required by these apps.

IBM Storage Protect for Cloud Azure VMs and Storage

The following table lists the permissions that you must accept when you authorize the IBM Storage Protect for Cloud Azure VMs and Storage app.

API	Permission	Type	Why we need it?	Last update
Microsoft Graph	AdministrativeUnit.ReadWrite.All (Read and write administrative units)	Application	Allows the app to create, read, update, and delete administrative units and manage administrative unit membership on behalf of the signed-in user.	
	Application.ReadWrite.All (Read and write all apps)		Allows the app to create, read, update and delete applications and service principals on behalf of the signed-in user.	
	AppRoleAssignment.ReadWrite.All (Manage app permission grants and app role assignments)		Allows the app to manage permission grants for application permissions to any API (including Microsoft Graph) and application assignments for any app, on behalf of the signed-in user.	
	Directory.ReadWrite.All (Read and write directory data)		Allows the app to read and write data in your organization's directory, such as users, and groups. It does not allow the app to delete users or groups, or reset user passwords.	
	Group.ReadWrite.All (Read and write all groups)		Allows the app to create groups and read all group properties and memberships on behalf of the signed-in user. Also allows the app to read and write calendars, conversations, files, and other group content for all groups the signed-in user can access. Additionally allows group owners to manage their groups and allows group members to update group content.	
	RoleManagement.ReadWrite.Directory (Read and write all directory RBAC settings)		Allows the app to read and manage the role-based access control (RBAC) settings for your company's directory, on behalf of the signed-in user. This includes instantiating directory roles and managing directory role membership, and reading directory role templates, directory roles, and memberships.	
	User.ReadWrite.All (Read and write all users' full profiles)		Allows the app to read and write the full set of profile properties, reports, and managers of other users in your organization, on behalf of the signed-in user. Also allows the app to create and delete users as well as reset user passwords on behalf of the signed-in user.	
	User.Read (Sign in and read user profile)	Delegated	Allows users to sign into IBM Storage Protect for Cloud with Microsoft 365 accounts.	
	BitLockerKey.Read.All (Read BitLocker keys)	Delegated	Supports retrieving the BitLocker keys for all devices in your Microsoft tenant.	October 2023
	Policy.Read.All (Read your organization's policies)	Application	Retrieves all named locations.	Newly added in November 2022
	Organization.Read.All (Read organization information)		Retrieves all the organizational brandings.	Newly added in November 2022
	Policy.ReadWrite.AuthenticationMethod (Read and write all authentication method policies)		Retrieves all the authentication method policies and configurations.	Newly added in November 2022
	Policy.ReadWrite.ConditionalAccess (Read and write your organization's conditional access policies.)		Allows the app to read and write your organization's conditional access policies, without a signed-in user.	Newly added in March 2023
	Policy.ReadWrite.Authorization (Read and write your organization's authorization policy)		Allows the app to update the group general settings to enable or disable the capability for the users.	Newly added in June 2023
	UserAuthenticationMethod.ReadWrite.All (preview) (Read and write all users' authentication methods)		Allows the application to read and write authentication methods of all users in your organization without a signed-in user. Authentication methods include the information like a user's phone number and Authenticator app settings. This does not allow the app to see sensitive information, such as the password, or to sign in or use the authentication methods.	Newly added in November 2022
Office 365 Exchange Online	Exchange.ManageAsApp (Manage Exchange As Application)	Application	Allows the backup and restore of the distribution lists in MFA-enabled tenants.	Newly added in November 2022

IBM Storage Protect for Cloud Salesforce and Salesforce Sandbox

The following permissions requested by IBM Storage Protect for Cloud should be accepted to ensure the IBM Storage Protect for Cloud and IBM Storage Protect for Cloud Salesforce functionality works. Once you accept these permissions, the IBM Storage Protect for Cloud Administration app for authentication can be created accordingly in Salesforce or Salesforce Sandbox.

- Access your basic information

- Access and manage your data
- Provide access to your data via the Web
- Access and manage your Chatter data
- Provide access to custom applications
- Allow access to your unique identifier
- Access custom permissions
- Access and manage your Wave data
- Access and manage your Eclair data
- Manage hub connections
- Access Pardot services
- Allow access to Lightning applications
- Allow access to content resources
- Perform requests on your behalf at any time

IBM Storage Protect for Cloud Dynamics Customer Engagement

The **Dynamics Customer Engagement** app profile can be used by the IBM Storage Protect for Cloud Dynamics service. The table below lists the permissions that should be accepted when you authorize the **IBM Storage Protect for Cloud Dynamics Customer Engagement** app.

API	Permission	Type	Why we need it?
Microsoft Graph	User.Read (Sign in and read user profile)	Delegated	Retrieve your Microsoft 365 tenant information.
	Directory.Read.All (Read directory data)	Application	
Dynamics CRM	user_impersonation (Access Common Data Service as organization users)	Delegated	IBM Storage Protect for Cloud Dynamics 365 uses it to back up and restore records in Dynamics Customer Engagement.

IBM Storage Protect for Cloud Google Workspace

The following permissions requested by IBM Storage Protect for Cloud should be accepted when you install the IBM Storage Protect for Cloud Backup app from the Google Workspace Marketplace. These permissions will be used to ensure the IBM Storage Protect for Cloud and Cloud Backup for Google Workspace functionalities work.

Table 3.

Scope	Permission	Type	Why we need it?	Last update
https://mail.google.com/	Read, compose, send, and permanently delete all your emails from Gmail	restricted	Back up emails and labels in Gmail for future recovery.	

Table 3. (continued)

Scope	Permission	Type	Why we need it?	Last update
https://www.googleapis.com/auth/drive	See, edit, create, and delete all of your Google Drive files	sensitive	Back up folders and files under My Drive and Shared Drives for future recovery.	
https://www.googleapis.com/auth/calendar	See, edit, share, and permanently delete all the calendars you can access using Google Calendar	sensitive	Back up calendars and events from Google Calendar for future recovery.	
https://www.googleapis.com/auth/contacts.other.readonly	See and download contact info automatically saved in your "Other contacts"	sensitive	Back up **Other contacts** data.	
https://www.googleapis.com/auth/contacts	See, edit, download, and permanently delete your contacts	sensitive	Back up contact groups and contacts from Google Contacts for future recovery.	
https://www.googleapis.com/auth/admin.directory.group.readonly	View groups on your domain	sensitive	Retrieve groups in your domain.	
https://www.googleapis.com/auth/admin.directory.user.readonly	View users on your domain	sensitive	Retrieve users in your domain.	
https://www.googleapis.com/auth/admin.directory.customer.readonly	View customer-related information	sensitive	Retrieve customer information to segment operations and settings for different customers and isolate customer tenants.	
https://www.googleapis.com/auth/admin.reports.usage.readonly	View usage reports for your domain	sensitive	Retrieve customer subscription usage for backup admins to monitor their subscription in the app.	

Table 3. (continued)

Scope	Permission	Type	Why we need it?	Last update
https://www.googleapis.com/auth/admin.directory.orgunit.readonly	View organization units on your domain	sensitive	Retrieve groups to add users to the app through organization units.	
https://www.googleapis.com/auth/userinfo.email	View your email address	non-sensitive	Retrieve user email information when users log in to the app.	
https://www.googleapis.com/auth/userinfo.profile	See your personal info, including any personal info you've made publicly available	non-sensitive	Retrieve users' publicly available properties to identify users through our application.	
https://www.googleapis.com/auth/apps.licensing	View and manage Google Workspace licenses for your domain	sensitive	Retrieve users' license information, including product SKUs. This information would be used when backup admins set policies for which users to include or exclude in certain backup scopes. This enables admins to set different backup policies.	
https://www.googleapis.com/auth/drive.admin.labels	View, edit, create, and delete all Drive labels in your organization, and view your organization's label-related administration policies	sensitive	Retrieve all information of labels on files in Drives for backup and restore.	Newly added in January 2023
https://www.googleapis.com/auth/drive.labels	View, use, and manage Drive labels	sensitive	Back up and restore properties of labels on files in Drives.	Newly added in January 2023
https://www.googleapis.com/auth/classroom.courses	See, edit, create, and permanently delete your Google Classroom classes	sensitive	Back up and restore classes.	Newly added in August 2023

Table 3. (continued)

Scope	Permission	Type	Why we need it?	Last update
https://www.googleapis.com/auth/classroom.announcements	View and manage announcements in Google Classroom	sensitive	Back up and restore announcements in classes.	Newly added in August 2023
https://www.googleapis.com/auth/classroom.coursework.me	See, create and edit coursework items including assignments, questions, and grades	sensitive	Back up classwork in classes.	Newly added in August 2023
https://www.googleapis.com/auth/classroom.coursework.students	Manage course work and grades for students in the Google Classroom classes you teach and view the course work and grades for classes you administer	sensitive	Restore classwork in classes.	Newly added in August 2023
https://www.googleapis.com/auth/classroom.courseworkmaterials	See, edit, and create classwork materials in Google Classroom	sensitive	Back up and restore classwork materials.	Newly added in August 2023
https://www.googleapis.com/auth/classroom.rosters	Manage your Google Classroom class rosters	sensitive	Back up and restore students and teachers in classes.	Newly added in August 2023
https://www.googleapis.com/auth/classroom.profile.emails	View the email addresses of people in your classes	sensitive	Retrieve email addresses in classes.	Newly added in August 2023
https://www.googleapis.com/auth/classroom.topics	See, create, and edit topics in Google Classroom	sensitive	Back up and restore topics in classes.	Newly added in August 2023
https://www.googleapis.com/auth/classroom.topics.readonly	View topics in Google Classroom	sensitive	Retrieve information of topics.	Newly added in August 2023
https://www.googleapis.com/auth/classroom.guardianlinks.students	View and manage guardians for students in your Google Classroom classes	Retrieve guardians of students in classes.	Newly added in August 2023	

IBM Storage Protect for Cloud Microsoft 365

IBM Storage Protect for Cloud Microsoft 365 (Exchange Permissions)

The table below lists the permissions that should be accepted when you authorize the **IBM Storage Protect for Cloud Microsoft 365** app, which will be created in your Mictosoft Entra ID once you create an app profile of the **IBM Storage Protect for Cloud Microsoft 365 (Exchange permissions)** app type.

About this task

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	Scan, back up, and restore mailboxes
	Exchange.ManageAsApp (Manage Exchange As Application)	Application	Scan in-place archived mailboxes.
Windows Azure Active Directory	User.Read (Sign in and read user profile)	Delegated	Support signing into IBM Storage Protect for Cloud Microsoft 365 with Microsoft 365 accounts.
Microsoft Graph	MailboxSettings.Read (Read all user mailbox settings)	Application	
	Directory.Read.All (Read directory data)	Application	Retrieve your Microsoft 365 tenant information.
	User.Read.All (Read all users' full profiles)	Application	Verify the impersonation accounts for Public Folders.
	Reports.Read.All (Read all usage reports)	Application	Retrieve data size directly, which improves the efficiency of the subscription consumption report.

IBM Storage Protect for Cloud Microsoft 365 (All Permissions)

The table below lists the permissions that should be accepted when you authorize the **IBM Storage Protect for Cloud Microsoft 365** app, which IBM Storage Protect for Cloudhas published to your Microsoft Entra ID.

About this task

API	Permission	Type	Why we need it?
Office 365 SharePoint Online	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.
	Exchange.ManageAsApp (Manage Exchange as Application)	Application	Scan in-place archived mailboxes.
Microsoft Graph	Tasks.ReadWrite.All (Read the and write all users' tasks and tasklists)	Application	Backup and restore Planner data.
	User.Read.All (Read all users' full profiles)	Application	Retrieve the Microsoft 365 Users’ user profiles.
	Group. ReadWrite.All (Read and write all groups)	Application	Scan Microsoft 365 Groups and Microsoft Teams via Auto Discovery.
			Back up and restore Microsoft Teams and Microsoft 365 Groups data.

API	Permission	Type	Why we need it?
	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.FullControl.All (Have full control of all site collections	Application	Back up and restore site collections
	Sites.Manage.All (Create, edit, and delete items and lists in all site collections)	Application	Backup and restore the lists in OneDrive for Business, and it is required if the SharePoint list has content approval.
	Reports.Read.All (Read all usage reports)	Application	IBM Storage Protect for Cloud 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 Storage Protect for Cloud Microsoft 365 uses it to back up and restore teams’ settings.
	Files.ReadWrite.All (Read and write files in all site collections)	Application	Back up and restore the OneDrive for Business files.
	TeamMember.ReadWrite.All (Add and remove members from teams)	Application	IBM Storage Protect for Cloud Microsoft 365 uses it to back up and restore teams’ members.
	TeamsTab.ReadWrite.All (Read and write tabs in Microsoft Teams)	Application	IBM Storage Protect for Cloud Microsoft 365uses it to back up and restore teams’ tabs.

API	Permission	Type	Why we need it?
	Team.Create (Create teams)	Application	IBM Storage Protect for Cloud Microsoft 365 uses it to restore teams.
	TeamsAppInstallation.ReadWriteForTeam.All (Manage Teams apps for all teams)	Application	IBM Storage Protect for Cloud Microsoft 365 uses it to back up and restore teams' apps.
	Channel.Create (Create channels)	Application	IBM Storage Protect for Cloud Microsoft 365 uses it to restore teams' channels.
	Chat.Read.All (Read all chat messages)	Application	IBM Storage Protect for Cloud Microsoft 365 uses it to back up Microsoft Teams Chat.

IBM Storage Protect for Cloud Microsoft 365 (SharePoint Permissions)

The table below lists the permissions that should be accepted when you authorize the **IBM Storage Protect for Cloud Microsoft 365 SharePoint** app, which will be created in your Microsoft Entra ID once

you create an app profile of the **IBM Storage Protect for Cloud Microsoft 365 (SharePoint permissions)** app type.

API	Permission	Type	Why do we need it?
Microsoft Graph	Sites.ReadWrite.All (Read and write items in all site collections)	Application	Backup and restore the OneDrive for Business content.
	Sites.Manage.All (Create, edit, and delete items and lists in all site collections)	Application	Backup and restore the lists in OneDrive for Business, and it is required if the SharePoint list has content approval settings enabled.
	Files.ReadWrite.All (Read and write files in all site collections)	Application	Backup and restore the OneDrive for Business files.
	Directory.Read.All (Read directory data)	Application	Retrieve your Microsoft 365 tenant information.
	User.Read.All (Read all users' full profiles)	Application	Retrieve the UPN for the authors or editors.
	Sites.FullControl.All (Have full control of all site collections)	Application	Back up some files in specific conditions, such as DLP-sensitive files.
	Reports.Read.All (Read all usage reports)	Application	Retrieve data size directly, which improves the efficiency of the Subscription Consumption Report.
Microsoft Information Protection Sync Service	UnifiedPolicy.Tenant.Read (Read all unified policies of the tenant)	Application	Retrieve information of published sensitivity labels from Microsoft 365.
Office 365 Management APIs	ActivityFeed.Read (Read activity data for your organization)	Application	Retrieve activity data in your organization to generate reports.

API	Permission	Type	Why do we need it?
Office 365 SharePoint Online	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	Backup and restore Managed Metadata Service of SharePoint Online site collections and Microsoft 365 Group team sites.
Windows Azure Active Directory	User.Read (Sign in and read user profile)	Delegated	Support signing into IBM Storage Protect for Cloud Microsoft 365 with Microsoft 365 accounts.

API Permissions Required by Custom Apps

To use IBM Storage Protect for Cloud, an app is required for authentication. If you do not want to use the apps that IBM Storage Protect for Cloud will create in your Microsoft Entra ID, you can create a custom app in your Microsoft Entra ID and create a custom Azure app profile.

For the custom app created in your Micosoft Entra ID, to ensure it is available for common features in IBM Storage Protect for Cloud, 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**.

API	Permission	Type	Why we need it?
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).
	Exchange.ManageAsApp	Application	Only required by custom apps of the following services: IBM Storage Protect for Cloud Microsoft 365.

Chapter 10. Manage Auto Discovery

The **Auto discovery** feature can automatically discover objects in your Microsoft environment and scan objects into specific containers according to the configured scan profiles.

Note:

The **Auto discovery** feature is unsupported for Salesforce tenants. The Tenant Owner and Service Administrators can refer to instructions in the following sections to manage scan profiles, manage containers, and view details of scan jobs.

Manage Scan Profiles

In **Auto discovery** > **Scan profiles**, you can perform the following actions to manage scan profiles:

- **Create** - For each tenant, an object type can only be included in one scan profile. To create a scan profile for a tenant, click **Create** on the **Scan profiles** page, and refer to the instructions in the following sections based on the object types for which the scan profile is created.
  - “Auto Discovery for Microsoft 365” on page 66
  - “Auto Discovery for Google Workspace” on page 68
  - “Auto Discovery for Power Platform” on page 69
  - “Auto Discovery for Active Directory” on page 71

  Note:

  - The auto discovery for Microsoft 365 or Google Workspace or Power® Platform are supported by corresponding app profiles. Before you configure a scan profile for a tenant to scan objects, ensure that the required app profiles have been configured in **App management**. For details on app profiles, see Chapter 9, “Manage App Profiles,” on page 39.
  - The auto discovery for Active Directory objects is only supported by the EnPower service. Before you configure scan profiles, ensure you have installed agents. For additional details, see Manage Agents.
- **View details** - To view details of a scan profile, click the link in the **Profile name** column. The **View details** page appears. On the **View details** page, you can click **Edit** to edit the scan profile details and click **View scan job history** to view the scan profile’s job history. For details on monitoring scan jobs, refer to View Details in Job Monitor.

  Note: Scan profiles will run jobs and randomly use app profiles which have the required permissions to scan objects. When you view the details of a scan job, the app profile used in the scan job will be displayed in the **Authentication information** table.
- **Edit** - To edit a scan profile, select the profile on the **Scan profiles** page and click **Edit**, or click **Edit** on the **View details** page of the profile.

  Note: The tenant cannot be changed when you edit a scan profile.
- **Delete** - To delete one or multiple scan profiles, select the scan profiles and click **Delete**. A pop-up window appears asking for your confirmation. If you are about to delete an advanced mode scan profile, select a resolution from the following:
  - Delete the containers along with the profile.
  - Keep these containers in the system.

  Click **Confirm**.
- **Scan now** - To run a scan profile now, select the scan profile and click **Scan now**. Click **Confirm** in the confirmation window to confirm your action. You can check the job status or stop the job in **Job Monitor**. For details, refer to “View Details in Job Monitor” on page 73.

- **Download “what’s new report”** - This report only supports scan profiles for Microsoft 365 objects. To view the conclusion report of a scan profile’s scan results, select the scan profile, click **Download “what’s new report”**, and then click **Download weekly report** or **Download daily report**. If you want to enable email notification for the “What’s new” report, refer to“Auto Discovery Notification” on page 91 .

Auto Discovery for Microsoft 365

About this task

To manage scan profiles for scanning your Microsoft 365 objects into IBM Storage Protect for Cloud, navigate to **Auto discovery** > **Scan profiles**. On the **Scan profiles** page, you can create and edit scan profiles. For details on the other actions of managing scan profiles, see “Manage Scan Profiles” on page 65.

Procedure

To create or edit a scan profile, refer to the following steps to configure settings in the **Create scan profile** / **Edit scan profile** wizard:

1. **Choose object types** - In the **Tenant** drop-down list, select a tenant for which the scan profile is created. Then, select the object types to be included in a scan profile for Microsoft 365.

   Note:

   - The tenant cannot be changed when you edit a scan profile.
   - The Microsoft **365 Group** / Microsoft **Team** / **Yammer community** object type includes group team sites and group mailboxes.
   - For Yammer communities, only the ones with connected Groups turned on can be managed in Auto discovery.
   - Microsoft uses throttling to manage Microsoft 365 operations. The throttling limits can affect the scan of Exchange public folders and result in slow performance or failed scan jobs. If you select **Exchange public folder** to avoid slow performance and failed scan jobs, you can contact Microsoft Support to adjust the following Exchange parameter to significantly reduce throttling in Microsoft 365:

     EWSMaxConcurrency: highest limit
   - If your organization uses the IBM Storage Protect for Cloud Microsoft 365 service, note the following objects:
     - To back up Exchange Online public folders, contact your IBM sales representative to purchase the **Public Folders** module in a subscription of IBM Storage Protect for Cloud Microsoft 365. Then, the **Exchange public folder** object type will be available.
     - If your tenant only purchased several modules in the enterprise subscription of IBM Storage Protect for Cloud Microsoft 365, auto discovery scans objects according to the modules you purchased in the subscription. For example, only if the **Exchange Online module** is purchased in the subscription, then the mailboxes will be scanned.
     - **Project Online** module is not in the subscription you purchased for IBM Storage Protect for Cloud Microsoft 365, do not customize containers for Project sites.
2. Click **Next** to proceed.
3. **Profile settings** - Refer to the following information to configure the profile settings:
   - **Name:** Enter a name for the profile.
   - **Description :** Enter an optional description for the profile.
   - **Impersonation account :** Enter the username of a Microsoft 365 user to be used to invoke the Exchange Web Services API. This setting is required when the **Exchange public folder** object type is selected in the scan profile.

Note: To scan Exchange public folders, you must have an Exchange Online product license assigned in Microsoft 365 and have the **Read items** permission to public folders. If you want to scan and protect Exchange public folders in IBM Storage Protect for Cloud Microsoft 365, you also needs to be in the owner group of the public folders and have an admin role with the **ApplicationImpersonation** permission.

- **Scan in-place archived mailboxes:** This setting appears when the **Exchange mailbox** object type is included in the scan scope. If you want to scan in-place archived mailboxes, turn on this toggle.

  Note: Scanning in place archived mailboxes might affect the efficiency of the scan.

- **Ignore the locked objects when updating the job status:** This setting appears when the **OneDrive for Business**, **SharePoint site, Microsoft 365 Group / Microsoft Team / Yammer community**, or **Project site** object type is included in the scan scope. With this setting enabled, 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.
- **Enable daily scan:** If you want to run this scan profile every day, turn on this toggle. The default start time of the daily scan job is displayed, and you can customize the start time when necessary.
- **Send an email notification to the following recipients when objects are moved to other containers or removed from any containers:** Objects will be automatically moved to other containers when they match the containers' rules. If you want to enable this notification, turn on the toggle. Then, select an email recipient profile from the **Notification profile** drop-down list. Whenever objects are moved to other containers or removed from IBM Storage Protect for Cloud containers, the recipients in the selected profile will receive email notifications. If necessary, click **Create email recipient profile** to create one. For more instructions on configuring email recipient profiles, refer to Email Recipient Profile.

4. Click **Next** to proceed, or click **Previous** to go back to the previous page.
5. **Configure containers and rules** - Refer to the following information to select a scan mode:
   - **Express mode** will scan objects into default containers. This mode is the simplest way to get started.
   - **Advanced mode** will scan objects dynamically to containers defined by business rules you configure. If you select the advanced mode, complete the following instructions to configure containers and rules for each object type:
     a. To add a rule, click **Add**. The **Add rule** pane appears on the right of the page.
     b. **Select a container:** Select a container from the drop-down list. If necessary, click **New container** to create one. For details on configuring containers, refer to Manage Containers.
     c. **Rule:** Select **All objects in one container** or **Specified objects in one container** as the rule for this container.

        Note: It does not support to add more than one rule if you select **All objects in one container**.

     d. **Rule criteria and values:** If you select **Specified objects in one container**, complete the following instructions to configure **Rule criteria** and **values** to define specified objects.
        – To set a criterion, select an option from the drop-down list, and configure values in the text box. For more information on the supported criteria, refer to "Appendix A - Supported Criteria in Auto Discovery Rules" on page 109.
        – To add a criterion, click **add**. To delete a rule, click **delete**.
        – With multiple criteria, you must select **And** (objects that meet all criteria will be scanned into the container) or **Or** (objects that meet any of the criteria will be scanned into the container) as the logic for the criteria.
     e. Click **Add** to add the configured rule.
     f. If you add multiple containers, set a container's priority by selecting a number from the **Priority** drop-down list.
     g. To configure a rule for the condition when the scan profile discovers objects that don't meet the criteria configured in rules, click **Rule for excluded objects**. The default option is **Do not add**

them to any containers. If you change the rule to **Add them to one container**, select a container from the drop-down list. Then, click **Save**.

h. If you want to edit or remove a rule, hover the mouse on the rule, click the more options, and then click **Edit** or **Remove**.

6. Click **Next** to proceed, or click **Previous** to go back to the previous page.
7. Have an overview of the settings in the scan profile, and take one of the following actions:
   - If you want to save your configurations in the scan profile, click **Save**.
   - If you want to run the scan profile immediately, click **Save and run**.
   - If you want to go back to the previous page, click **Previous**.

Auto Discovery for Google Workspace

About this task

To manage scan profiles for scanning your Google Workspace objects into IBM Storage Protect for Cloud, navigate to **Auto discovery** > **Scan profiles**. On the **Scan profiles** page, you can create and edit scan profiles. For details on the other actions of managing scan profiles, see "Manage Scan Profiles" on page 65.

Procedure

To create or edit a scan profile, refer to the following steps to configure settings in the **Create scan profile** or / **Edit scan profile** wizard:

1. **Choose object types** – In the **Tenant** drop-down list, select a tenant for which the scan profile is created. Then, select the object types to be included in a scan profile for Google Workspace.

   Click **Next** to proceed.

   Note:

   For Google users, the **Suspended** users and **Archived** users are not included in the scan scope.
2. **Profile settings** – Refer to the following information to configure the profile settings:
   - **Name**: Enter a name for the profile.
   - **Description**: Enter an optional description for the profile.
   - **Enable daily scan**: If you want to run the scan profile every day, turn on this toggle. The default start time of the daily scan job is displayed, and you can customize the start time when necessary.
   - **Send an email notification to the following recipients when objects are moved to other containers or removed from any containers**: – Objects will be automatically moved to the other containers when they match the container's rules. If you want to enable this notification, turn on the toggle. Then, select an email recipient profile from the **Notification profile** drop-down list. Whenever objects are moved to other containers or removed from IBM Storage Protect for Cloud containers, the recipients in the selected profile will receive email notifications. If necessary, click **Create email recipient profile** to create one. For more instructions on configuring email recipient profiles, refer to "Email Recipient Profile" on page 92.

   Click **Next** to proceed, or click **Previous** to go back to the previous page.
3. **Configure containers and rules** – Refer to the following information to select a scan mode:
   - **Express mode** scans objects into default containers. This mode is the simplest way to get started.
   - **Advanced mode** scans objects dynamically to containers defined by business rules you configure. If you select the advanced mode, complete the following instructions to configure containers and rules for each object type:

     a. To add a rule, click **Add**. The **Add rule** pane appears on the right of the page.

b. Select a container from the drop-down list. If necessary, click **New container** to create a new container. For details on configuring containers, see "Manage Containers" on page 72.

c. Select All objects in one container or specified objects in one container as the rule for this container.

Note: If you have configured criteria for the **Specified objects in one container** rule, you can click **Rule for excluded objects** to configure an additional rule for the objects that do not meet the criteria. If you select the **All objects in one container** rule, you will not be allowed to add other rules.

d. If you select **Specified objects in one container**, complete the following instructions to configure **Rule criteria and values** to define specified objects.

- To set a criterion, select an option from the drop-down list, and then configure values in the textbox. For more information on the supported criteria, refer to "Appendix A - Supported Criteria in Auto Discovery Rules" on page 109.
- To add a criterion, click **add**, and to delete a rule, click **delete**.
- With multiple criteria, you must select **And** (objects that meet all criteria will be scanned into the container) or **Or** (objects that meet any of the criteria will be scanned into the container) as the logic for the criteria.

e. Click **Add** at bottom of the **Add rule** right pane to add the configured rule.

f. If you add multiple containers, set a container's priority by selecting a number from the **Priority** drop-down list.

g. If you select the **Specified objects in one container** option for the condition when the scan profile discovers objects that don't meet the criteria configured in rules, you can click **Rule for excluded objects** to configure an additional rule. The default option of the additional rule is **Do not add them to any containers**. If you change the rule to **Add them to one container**, select a container from the drop-down list. Then, click **Save**.

h. If you want to edit or remove a rule, hover the mouse on the rule, click the more options, and click **Edit** or **Remove**.

Click **Next** to proceed, or click **Previous** to go back to the previous page.

4. Have an overview of the settings in the scan profile, and take one of the following actions:

- If you want to save your configurations in the scan profile, click **Save**.
- If you want to run the scan profile immediately, click **Save and run**.
- If you want to go back to the previous page, click **Previous**.

Auto Discovery for Power Platform

About this task

To manage scan profiles for scanning your Power Platform objects into IBM Storage Protect for Cloud, navigate to **Auto discovery** > **Scan profiles**. On the **Scan profiles** page, you can create and edit scan profiles. For details on the other actions of managing scan profiles, see "Manage Scan Profiles" on page 65.

Procedure

To create or edit a scan profile, refer to the following steps to configure settings in the **Create scan profile** / **Edit scan profile** wizard:

1. **Choose object types** - In the **Tenant** drop-down list, select a tenant for which the scan profile is created. Then, select the object types to be included in a scan profile for Power Platform.
2. Click **Next** to proceed.
3. **Profile settings** - Refer to the following information to configure the profile settings:

- **Name**- Enter a name for the profile.
- **Description** - Enter an optional description for the profile.
- **Enable daily scan** - If you want to run this scan profile every day, turn on this toggle.
- **Send an email notification to the following recipients when objects are moved to other containers or removed from any containers**- Objects will be automatically moved to other containers when they match the containers' rules. If you want to enable this notification, turn on the toggle. Then, select an email recipient profile from the **Notification profile** drop-down list. Whenever objects are moved to other containers or removed from IBM Storage Protect for Cloud containers, the recipients in the selected profile will receive email notifications. If necessary, click **Create email recipient profile** to create one. For more instructions on configuring email recipient profiles, refer to Email Recipient Profile.

4. Click **Next** to proceed, or click **Previous** to go back to the previous page.
5. **Configure containers and rules** - Refer to the information below to choose a scan mode:
   - **Express mode** will scan objects into default containers. This mode is the simplest way to get started.
   - **Advanced mode** will scan objects dynamically to containers defined by business rules you configure. If you select the advanced mode, complete the following instructions to configure containers and rules for each object type:
     a. To add a rule, click **Add**. The **Add rule** pane appears on the right of the page.
     b. **Select a container -** Select a container from the drop-down list. If necessary, click **New container** to create one. For details on configuring containers, refer to "Manage Containers" on page 72
     c. **Rule -** Select **All objects in one container** or **Specified objects in one container** as the rule for this container.

        Note: If you select **All objects in one container**, you cannot add more than one rule.
     d. **Rule criteria and values -** If you select **Specified objects in one container**, complete the following instructions to configure **Rule criteria and values** to define specified objects.
        – To set a criterion, select an option from the drop-down list, and configure values in the textbox. For more information on the supported criteria, refer to "Appendix A - Supported Criteria in Auto Discovery Rules" on page 109.
        – To add a criterion, click **add**. To delete a rule, click **delete**.
        – With multiple criteria, you must select **And** (objects that meet all criteria will be scanned into the container) or **Or** (objects that meet any of the criteria will be scanned into the container) as the logic for the criteria.
     e. Click **Add** to add the configured rule.
     f. If you add multiple containers, set a container's priority by selecting a number from the **Priority** drop-down list.
     g. To configure a rule for the condition when the scan profile discovers objects that don't meet the criteria configured in rules, click **Rule for excluded objects**. The default option is **Do not add them to any containers**. If you change the rule to **Add them to one container**, select a container from the drop-down list. Then, click **Save**.
     h. If you want to edit or remove a rule, hover the mouse on the rule, click the more options, and then click **Edit** or **Remove**.
6. Click **Next** to proceed, or click **Previous** to go back to the previous page.
7. Review the settings in the scan profile, and take one of the following actions:
   - If you want to save your configurations in the scan profile, click **Save**.
   - If you want to run the scan profile immediately, click **Save and run**.
   - If you want to go back to the previous page, click **Previous**.

Auto Discovery for Active Directory

About this task

To manage scan profiles for scanning your Active Directory objects into IBM Storage Protect for Cloud, navigate to **Auto discovery** > **Scan profiles**. On the **Scan profiles** page, you can create and edit scan profiles. For details on the other actions of managing scan profiles, see "Manage Scan Profiles" on page 65.

Procedure

To create or edit a scan profile, refer to the following steps to configure settings in the **Create scan profile** / **Edit scan profile** wizard:

1. **Choose object types** - In the **Tenant** drop-down list, select a tenant for which the scan profile is created. Then, select the object types to be included in a scan profile for Active Directory.
2. Click **Next** to proceed.
3. **Profile settings** - Refer to the following information to configure the profile settings:
   - **Name** – Enter a name for the profile.
   - **Description** – Enter an optional description for the profile.
   - **Enable daily scan** – If you want to run this scan profile every day, turn on this toggle.
   - **Send an email notification to the following recipients when objects are moved to other containers or removed from any containers** – Objects will be automatically moved to other containers when they match the containers' rules. If you want to enable this notification, turn on the toggle. Then, select an email recipient profile from the **Notification profile** drop-down list. Whenever objects are moved to other containers or removed from IBM Storage Protect for Cloud containers, the recipients in the selected profile will receive email notifications. If necessary, click **Create email recipient profile** to create one. For more instructions on configuring email recipient profiles, refer to Email Recipient Profile.
4. Click **Next** to proceed, or click **Previous** to go back to the previous page.
5. **Configure containers and rules** - Refer to the information below to choose a scan mode:
   - **Express mode** will scan objects into default containers. This mode is the simplest way to get started.
   - **Advanced mode** will scan objects dynamically to containers defined by business rules you configure. If you select the advanced mode, complete the following instructions to configure containers and rules for each object type:
     a. To add a rule, click **Add**. The **Add rule** pane appears on the right of the page.
     b. **Select a container -** Select a container from the drop-down list. If necessary, click **New container** to create one. For details on configuring containers, refer to "Manage Containers" on page 72
     c. **Rule -** Select **All objects in one container** or **Specified objects in one container** as the rule for this container.

        Note: If you select **All objects in one container**, you cannot add more than one rule.
     d. **Rule criteria and values -** If you select **Specified objects in one container**, complete the following instructions to configure **Rule criteria and values** to define specified objects.
        – To set a criterion, select an option from the drop-down list, and configure values in the textbox. For more information on the supported criteria, refer to "Appendix A - Supported Criteria in Auto Discovery Rules" on page 109.
        – To add a criterion, click **add**. To delete a rule, click **delete**.
        – With multiple criteria, you must select **And** (objects that meet all criteria will be scanned into the container) or **Or** (objects that meet any of the criteria will be scanned into the container) as the logic for the criteria.

e. Click **Add** to add the configured rule.

f. If you add multiple containers, set a container's priority by selecting a number from the **Priority** drop-down list.

g. To configure a rule for the condition when the scan profile discovers objects that don't meet the criteria configured in rules, click **Rule for excluded objects**. The default option is **Do not add them to any containers**. If you change the rule to **Add them to one container**, select a container from the drop-down list. Then, click **Save**.

h. If you want to edit or remove a rule, hover the mouse on the rule, click the more options, and then click **Edit** or **Remove**.

6. Click **Next** to proceed, or click **Previous** to go back to the previous page.
7. Review the settings in the scan profile, and take one of the following actions:
   - If you want to save your configurations in the scan profile, click **Save**.
   - If you want to run the scan profile immediately, click **Save and run**.
   - If you want to go back to the previous page, click **Previous**.

Manage Containers

Click **Containers** under **Auto discovery** in the left pane. The **Containers** page appears. You can select an object type from the list on the left of the **Containers** page, and refer to the following instructions to manage containers:

- **Create a container** - Click **Create**. In the **Create container** pane, enter a name for the container and click **Save**.
- **Rename a container** - To rename a custom container, select the container and click **Rename**. In the **Rename a container** window, change the value in the **Container name** field and click **Save**. The default containers in IBM Storage Protect for Cloud cannot be renamed.
- **Batch Import** - The Batch import method is supported by the following Microsoft 365 objects:
  - Exchange mailbox
  - OneDrive for Business
  - SharePoint site
  - Microsoft 365 Group / Microsoft Team / Yammer community (including group team sites and group mailboxes)
  - Project site
  - Microsoft 365 user
  - Security and distribution group (including security groups, mail-enabled security groups, distribution lists, and dynamic lists)

  To batch import objects into a container, select the container and click **Batch import**. For more details on batch import, refer to "Import Objects in Batch" on page 73.
- **View objects in a container** - Click the container name to open the page listing all objects in the container. If you want to delete some objects, select the objects and click **Delete**.
- **Remove objects only** - To only remove the objects from one or more containers, select the containers and click **Remove objects only**.
- **Delete Container** - Select one or more custom containers and click **Delete**. Click **Confirm** in the confirmation window. When the containers are deleted, the objects within the containers are removed from the groups.
- **Geo location view / Container view** - If your tenant has Multi-Geo Capabilities in IBM Storage Protect for Cloud Microsoft 365 service, you can switch to the **Geo location view** to view containers.

Import Objects in Batch

To batch import objects into a container, select the container and click **Batch import**. The **Batch import** pane appears on the right of the page.

Procedure

Complete the following steps to import objects in batch:

1. Select a tenant from the **Tenant** drop-down list.
2. Download an object list template by clicking the **Download template** link.
3. In the downloaded Excel file, enter the information about the objects you are about to import.
4. Click **Upload** 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.
5. If you batch import Microsoft 365 users, configure the following additional settings:
   - **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 users in their original containers**. With this option 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 change this setting, select **Move the users to the new containers based on the scan rules**.
   - **How would you like to handle the imported Microsoft 365 users in Batch Import jobs?** The default setting is **Move the users to the new containers selected in the batch import job**. With this option selected, the Microsoft 365 users existing in containers will be moved to the new container selected in this batch import job. If you want to change this setting, select **Keep users in their original containers**.
6. 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.

   When Yammer communities are imported to containers, the Yammer community IDs are not retrieved. When you use IBM Storage Protect for Cloud Microsoft 365 to manage Yammer communities, the community IDs are required. Therefore, after the batch import, you must create a scan profile. 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.

View Details in Job Monitor

In **Auto discovery > Job monitor**, you have the following options:

- **Refresh** – Click **Refresh** to refresh jobs displayed on the **Job monitor** page.
- **Stop** – You can select a scan job with the **In progress** status, and then click **Stop** to stop it if necessary.

  Note: Batch import in progress jobs cannot be stopped.
- **Export scan history:** You can select a scan job with the **Finished / Finished with exception** status, and then click **Export scan history** to export the results report of the scan job.
- **Download batch import report:** You can select an import job with the **Finished / Finished with exception status**, and then click **Download batch import report** to export the results report of the import job.
- **Filter:** Set a filter to view job results by referring to the following instructions:

  1. Click **Filter** on the upper-right corner of the page. The **Filter** pane appears on the right of the page.
  2. In the **Filter** pane, configure conditions for the **Scan profile** or **Status criteria**.

     Note: The **Geo location** criterion is only available when your tenant has Multi-Geo Capabilities in IBM Storage Protect for Cloud Microsoft 365 service.
  3. Click **Apply**.

Manage Agents

If your organization uses EnPower, to scan on-premises Active Directory objects into EnPower for management, navigate to **Management** > **Agent management** and follow the steps below to manage agents.

1. On the **Agent management** page, click **Download agent package**.
2. On the **Download agent package** page, click the **Download** button.
3. After you finish registering agents to IBM Storage Protect for Cloud, the basic information and status of agents will be displayed in the table on the **Agent management** page.

Configure Security Settings

The Tenant Owner and Service Administrators can navigate to **Administration** > **Security** to manage the following security settings:

- **Trusted IP address settings** – To only allow users to access IBM Storage Protect for Cloud from certain IP addresses or IP address ranges, configure this setting by referring to the "Enable Trusted IP Address Settings" on page 95 section.
- **Password rotation policy for local accounts** – This setting is for IBM Storage Protect for Cloud local accounts only (Users with the other sign-in methods follow the related systems' password policies). With the password rotation policy enabled for local accounts, the local accounts will be asked to change their account passwords regularly for the security of their accounts. Complete the following steps to enable the policy:

  1. Click **Password rotation policy for local accounts** on the **Security** page.
  2. In the **Edit password rotation policy for local accounts** pane, turn on the toggle, select **30**/**60**/**90**/**180** days as the lifespan of the passwords, and click **Save** to save the configuration.

  Once you enable the password rotation policy, email notifications will be sent to local users 15 days before their password expiration dates.
- **Session timeout setting** – By default, an IBM Storage Protect for Cloud account will be automatically signed out if there is no activity for 15 minutes, and the user can sign in again to start a new session. If you want to extend the session timeout duration to be longer than 15 minutes, complete the steps below:

  1. Click **Session timeout setting** on the **Security** page.
  2. In the **Edit session timeout settings** pane, set a value for the **Login will expire after** field by entering a proper number before **Hours**/**Minutes**, and click **Save** to save the configuration. Note that the duration cannot be less than 15 minutes.
- **Temporary account creation for IBM technical support** – Choose whether to allow temporary accounts to be created for IBM Technical Support.

  If your turn on the toggle to enable this setting, when the Tenant Owner, Service Administrators, or Application administrators invite support for assistance, the IBM Technical Support team members can use these accounts to access the IBM Storage Protect for Cloud to help resolve the issues.
- **Concurrent sign-ins from multiple locations for the same account** – If your organization does not allow concurrent sign-ins from multiple locations for the same account, turn off the toggle to disable this setting.

  The result will be like the following example: Bob has signed in to IBM Storage Protect for Cloud with an account, and John signed in to IBM Storage Protect for Cloud with the same account at a different location. Upon John's sign-in, Bob will be automatically signed out.
- **Reserved IP addresses**– If your organization has an access policy and only specific IP addresses are allowed, you must download the list of reserved IP addresses and add the IP addresses to the safe IP address list. For additional details, refer to "Download a List of Reserved IP Addresses" on page 97.

- **ARM VNet IDs** – If you are using the **Bring your own storage** model for IBM Storage Protect for Cloud, are storing your data in the same Microsoft Azure data center as your IBM Storage Protect for Cloud tenant (or in a paired region), and also have a firewall enabled on your storage, you will need to add our service to your virtual network. For additional details, refer to "Download ARM VNet IDs" on page 97.

Enable Trusted IP Address Settings

You can enable trusted IP address settings to only allow users to access IBM Storage Protect for Cloud from certain IP addresses or IP address ranges.

Before you begin

Note: Only IPv4 addresses are supported.

Procedure

Complete the following steps to enable trusted IP address settings:

1. Navigate to **Administration** > **Security** on the left pane.
2. On the **Security** page, click **Trusted IP address settings**.
3. The **Edit trusted IP address settings** pane appears on the right of the page. Turn on the toggle and configure the following settings:
   - **Trusted IP address range** – Enter the IP address in this text box. If you want to enter multiple IP addresses, separate them with a comma (,).
   - **User scope of the IP whitelisting** – If you want to apply the configured IP whitelisting to local users only, select the **Only local uses** option.
4. Click **Save** to save your configurations, or click **Cancel** to go back to the **Security** page without saving any configurations.

Download a List of Reserved IP Addresses

If your tenant has an enterprise subscription for IBM Storage Protect for Cloud, the Tenant Owner and Service Administrators can download a list of reserved IP addresses. The reserved IP addresses can be added to your Microsoft 365 firewall to ensure IBM Storage Protect for Cloud and other IBM Storage Protect for Cloud cloud services can operate in your environment. IBM Storage Protect for Cloud is a platform serving as the entry for all IBM Storage Protect for Cloud. Apart from adding the IP addresses of IBM Storage Protect for Cloud, you want to use, make sure the IP addresses of IBM Storage Protect for Cloud are also added to the trusted list in your environment.

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

1. Navigate to **Administration** > **Security** on the left pane.
2. On the **Security** page, click **Download** in the **Reserved IP addresses** section.

   Note: For Microsoft 365 multi-geo tenants, you must first configure mappings between your Microsoft 365 geo locations and IBM Storage Protect for Cloud data centers, and then you can download the reserved IP addresses. For additional details on the mappings, refer to Manage Data Center Mappings.
3. Select a location to save the file.

Note: The downloaded file contains the IP addresses of all data centers. When your organization's users need to access IBM Storage Protect for Cloud 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 **Microsoft Entra> 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 this Microsoft article.

Download ARM VNet IDs

If you are using or plan to use your own storage device for IBM Storage Protect for Cloud, you may find your storage account in the same Microsoft Azure data center as your IBM Storage Protect for Cloud tenant (or in a paired region). However, if you have enabled the firewall on your storage, you must download the Azure Resource Manager (ARM) VNet IDs and add the subnets to your virtual network.

Follow the steps below to get the ARM VNet IDs for your data center:

1. Navigate to **Administration > Security** on the left pane.
2. On the Security page, click **Download in the ARM VNet IDs** section.

   Note: For Microsoft 365 multi-geo tenants, you must first configure mappings between your Microsoft 365 geo locations and IBM Storage Protect for Cloud data centers, and then you can download the VNet IDs. For additional details on the mappings, refer to "Manage Data Center Mappings" on page 87.
3. Select a location to save the file.

For details on adding ARM VNet IDs, refer to Add ARM Virtual Networks.

Chapter 11. 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" on page 78.
- **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 **Confirm** to proceed. The **Applying** label is displayed next to the profile name. When the key vault in the profile is successfully applied, the **Applying** status is changed to **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?" on page 78 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 **Confirm** to proceed.

  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?" on page 78 to see when an encryption profile and the key specified in the profile can be deleted.

Note: IBM Storage Protect for Cloud provides a default encryption profile. You can also create a custom encryption profile and apply it.

Preparations

About this task

The encryption profile requires some properties of a key vault. Before creating an encryption profile, make sure you have a key vault in Azure. If you do not have any key vaults, refer to 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 MicrosoftAzure 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 Storage Protect for Cloud, 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 Storage Protect for Cloud encryption profile to encrypt data, and the key is deleted with no backup, the encrypted data will be damaged and IBM Storage Protect for Cloud 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" on page 77, 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. **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.
7. **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.
8. 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 Storage Protect for Cloud 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 Storage Protect for Cloud 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:

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 Storage Protect for Cloud encryption profile.

   Note: Skip this step if you already prepared a key.
2. Navigate to **IBM Storage Protect for Cloud** > **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 Storage Protect for Cloud starts applying the key, and the **Applying** label is displayed next to the new profile name. When IBM Storage Protect for Cloud 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 Storage Protect for Cloud 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 **Applying** to **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 Storage Protect for Cloud 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 Microsoft Entra admin center (or Microsoft 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 Storage Protect for Cloud** > **Encryption Management**, edit your custom encryption profile and update the client ID and client secret.

I Need to Use a New Key Vault

If you need to use a new key vault to replace the original key vault, follow the procedures below:

Procedure

1. In Microsoft Entra admin center (or Microsoft Azure Portal), create a new key vault. For details, see Appendix C - Create a Key Vault in Azure.
2. Navigate to **IBM Storage Protect for Cloud** > **Encryption Management**, and create a new encryption profile. For details, see"Create an Encryption Profile" on page 78 .
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 Storage Protect for Cloud starts applying the key vault, and the **Applying** label is displayed next to the new profile name. When IBM Storage Protect for Cloud 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 Storage Protect for Cloud 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 **Applying** to **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 Storage Protect for Cloud 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 Storage Protect for Cloud. IBM Storage Protect for Cloud recommends you first contact Microsoft Support to recover your key vault.

The table below shows the influence of the key vault deletion on IBM Storage Protect for Cloud and other cloud services.

Service	Influence
IBM Storage Protect for Cloud	You cannot use some of the IBM Storage Protect for Cloud features.
IBM Storage Protect for Cloud Microsoft 365	The data previously protected by IBM Storage Protect for Cloud Microsoft 365 cannot be restored.
IBM Storage Protect for Cloud Salesforce	The data previously protected by IBM Storage Protect for Cloud Salesforce cannot be restored.
IBM Storage Protect for Cloud Dynamics 365	The data previously protected by IBM Storage Protect for Cloud Dynamics 365 cannot be restored.
IBM Storage Protect for Cloud Azure VMs and Storage	The data previously protected by IBM Storage Protect for Cloud Azure VMs and Storage cannot be restored.

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

1. In Microsoft Entra admin center (or Microsoft Azure Portal), create a new key vault. For details, see Appendix C - Create a Key Vault in Azure.
2. Navigate to **IBM Storage Protect for Cloud** > **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 Storage Protect for Cloud 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 Storage Protect for Cloud tenant and IBM Storage Protect for Cloud environments until the new encryption profile is successfully applied.
4. IBM Storage Protect for Cloud 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

Chapter 12. 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 Storage Protect for Cloud 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 Storage Protect for Cloud 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** section, and then click **Get started** in the **Data in Microsoft 365** pane on the right of the page.

   Note: Only the Microsoft 365 data that is created after the report data collection is enabled can be collected and used by the related services.
3. In the **Edit settings to collect data in Microsoft 365** pane, turn on the toggle to enable the data collection.
4. Set the scope for the tenants whose data will be displayed on reports. Select **All tenants** or **Specific tenants**. If you choose **Specific tenants**, select desired tenants from the drop-down list and click **Apply**.
5. Refer to the table below to select your desired data source based on the reports you want to view or the functions you want to use.

Data source	Report/Function
SharePoint Online	User Reports
	The Site Analysis report
	Content Reports
	The Sharing Activity Analysis report
	Microsoft 365 Activity Reports (SharePoint Online sites)
	Auditor Reports
	Usage Reports
	The **Last Accessed Time** rule
	The **Auditor Mode** rules
Exchange Online	Microsoft 365 Activity Reports (Exchange Online activities)

Data source	Report/Function
Microsoft Entra ID	Microsoft 365 Activity Reports (Microsoft Entra activities)
	The **User Filter** and **Policy Enforcer** rules
	The **Auditor Mode** rules
General (other data sources such as Microsoft Teams)	Microsoft 365 Activity Reports

6. Refer to the instructions below to select a storage type and configure the storage for storing Microsoft 365 activity data.

   - **Default storage** – Select this if you want to use the default Azure storage provided by IBM. To set a retention policy on the default storage, turn on the toggle, and configure the **Retain data for _ Years/Months** setting.

   If you want to use a custom storage, note the following before the configuration:

   - Before adding the storage account to the IBM Storage Protect for Cloud interface, ensure that IBM agents have access to your storage. For details, refer to "Allow IBM Storage Protect for Cloud Agent Servers to Access Your Storage Account" on page 84.
   - If the default storage is used previously, 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, manually move the data from the old custom storage to the new one. IBM Storage Protect for Cloud does not have the permission to clear up data from the old custom storage.

   To use a custom storage, refer to the instructions below to complete the configuration:

   - **Azure Storage** – If you select this custom storage type, configure the settings below:
     - **Account name** – Enter an account name of Azure Blob Storage.
     - **Access key** – Enter the access key of the account above.
     - **Container name** – Enter the container name of the storage.
     - **Send an email notification of failed connection to all service administrators** – If you want to enable this notification, turn on the toggle.
   - **Amazon S3** – If you select this custom storage type, configure the settings below:
     - **Bucket name** – Enter the name of the bucket you want to access.
     - **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.
     - **Secret access key** – Enter the corresponding secret key ID to access the specified bucket. You can view the secret key ID from your AWS account.
     - **Storage region** – Select the storage region of this bucket from the drop-down list.
     - **Send an email notification of failed connection to all service administrators** – If you want to enable this notification, turn on the toggle.
7. Click **Advanced settings** and refer to the instructions below to complete the configuration:

   - **Exclude accounts** – Specify any user accounts you would like to exclude. This can be useful for filtering out service and test accounts to improve the quality and accuracy of reports. Enter one or more accounts in the format of **someone@example.com**, and separate each email address with a semicolon (;).
   - **Policy for the activities of Microsoft 365 service accounts** – If your tenant has configured a service account profile to scan Microsoft 365 objects, IBM recommends you select the **Exclude activities of Microsoft 365 service accounts** option to filter out activities of Microsoft 365 service accounts that

are used to register objects into IBM Storage Protect for Cloud, since the action records caused by scan jobs may affect the collected data and the analysis results.

- **Filter out data on the pages that contain the URL components below** – The default URL components is displayed in the textbox. If necessary, you can modify the URL components in the textbox. By default, only **View activities** on the pages will be filtered out. If you want to filter out all activities, select **All activities**.
- **Send an email notification when no data is collected** – IBM Storage Protect for Cloud collects data every day. If you want to enable this notification, turn on the toggle and set a period by selecting a number from the drop-down list. Then, select email recipients from the following:
  - **Service administrators in IBM Storage Protect for Cloud**
  - **Custom recipients (select an email profile)**

    If you select this option, select an email recipient profile or click **Create** from the drop-down list to create one. For details about managing email recipient profiles, refer to Email Recipient Profile.
- **Set container scope** – If you want to select containers created in **Auto discovery** for data collection of the **OneDrive for Business** / **SharePoint sites** object type, turn on the toggle and click **Choose containers**. Select containers and click **Save**.
- **Export Microsoft 365 tenant activity data to Azure SQL database** – With this setting enabled, the data will be exported to your Azure SQL database every hour. If you want to enable this setting, turn on the toggle and 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.

    Note: By default, this option is disabled and hidden. If necessary, you can contact IBM Support to enable this option.

8. Click **Save** to save your edits, or click **Cancel** to go back to the **Report data collection** page without saving any changes.

Activities in Microsoft 365

Turn on the toggle to enable this service, which monitors the Microsoft Activity API and provides auditing reports/alerts for the EnPower service.

Note the following:

- You can use this feature when your tenant in IBM Storage Protect for Cloud has a working subscription for the EnPower service. Once your subscription to the EnPower service expires, this collection will be stopped the next day. After your subscription to the EnPower service has been renewed, this collection will be reactivated the next day.
- Before you enable this feature, ensure that auditing is turned on for your organization. You can turn on auditing in the Microsoft 365 Purview compliance portal or by using Exchange Online PowerShell. For more instructions, refer to Turn on auditing.
- To enable this feature, ensure your organization has configured one of the following app profiles for the IBM Storage Protect for Cloud common service: **Microsoft 365 (All permissions)**, **Reporting for Microsoft 365**, or **Custom Azure app**.
- After you enable this feature, the first collection will collect activities for up to five days, and the following collections will collect activities hourly.
- The collections will have some delays of hours. For details about how long it will take to collect activities of different services or features in Microsoft 365, refer to the Microsoft article Before you search the audit log.

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

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

When you are using your own storage device, you may have set up the storage firewall to only allow the trusted clients for security concerns. To ensure that IBM Storage Protect for Cloud 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 Storage Protect for Cloud or your storage account is in its paired region, you must add the Azure Resource Manager (ARM) vNet subnets where the IBM Storage Protect for Cloud 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 Storage Protect for Cloud 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 Storage Protect for Cloud** interface and click **Advanced Settings** > **Reserved IP Addresses** to download the list of reserved IP addresses of IBM Storage Protect for Cloud. For details, refer to "Download a List of Reserved IP Addresses" on page 97.
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 Storage Protect for Cloud 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 Storage Protect for Cloud
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 the message.

Chapter 13. Configure Advanced Settings

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

Manage Data Center Mappings

If your IBM Storage Protect for Cloud Microsoft 365 enterprise subscription has multi-geo capabilities, you can navigate to **Administration** > **Data center mappings** to map your Microsoft 365 geo locations to IBM Storage Protect for Cloud data centers.

Note: Before you configure data center mappings for a Microsoft 365 tenant, ensure an app profile has been configured for the tenant.

Follow the instructions in "Step 1: Configure Mappings for Microsoft 365 Geo Locations" on page 87and "Step 2: Define Central Locations in Microsoft 365 Tenants" on page 88 to complete configurations.

The **Central location** is the data center where your primary IBM Storage Protect for Cloud tenant initially signed up. All data managed prior to your multi-geo capabilities 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.

Step 1: Configure Mappings for Microsoft 365 Geo Locations

Before you configure mappings, your organization's backup data is stored in the central location where your primary tenant initially signed up.

Follow the steps below to configure mappings between your Microsoft 365 geo locations and IBM Storage Protect for Cloud data centers:

1. Click **Add mapping**.
2. Select a geo location from the **Microsoft 365 geo location** drop-down list.

   Note: To check the geo locations in a Microsoft 365 tenant, refer to the following **Get Microsoft 365 Geo Locations** section.
3. For each geo location, choose one of the following methods to configure a mapping:
   - To keep the backup data of the geo location in the central location, select the **Keep in Central IBM-SP4C Location** check box. The central location will be displayed in the **IBM Storage Protect for Cloud data center** field and cannot be changed.
   - In the following scenarios, you can select a data center from the **IBM Storage Protect for Cloud data center** drop-down list:
     - IBM Storage Protect for Cloud 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 Storage Protect for Cloud yet.
4. In the following scenarios, you can configure storage locations for your organization's geo locations by selecting **IBM Azure Storage** or **Bring your own storage**.
   - New geo locations are added, and your organization uses **IBM Azure Storage.**
5. 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. IBM Storage Protect for Cloud will back up the data of these geo locations once again, and the backup data will be stored in different IBM Storage Protect for Cloud data centers according to the mappings, and the storage type for each region cannot be changed once saved.

Step 2: Define Central Locations in Microsoft 365 Tenants

The central locations in customers' Microsoft 365 tenants cannot be retrieved due to Microsoft API limitations. For each multi-geo Microsoft 365 tenant, follow the steps below to define the central location in the tenant:

1. Click **Add central location**.
2. The **Microsoft 365 tenant domain** field lists tenants based on app profiles configured in IBM Storage Protect for Cloud . Select a tenant from the drop-down list.
3. The **Microsoft Entra ID**, **SharePoint**, and **Exchange** fields list geo locations that you configured in "Step 1: Configure Mappings for Microsoft 365 Geo Locations" on page 87. Select the tenant's central location from the **Microsoft Entra ID**, **SharePoint**, and **Exchange** drop-down lists.

   Note: To check the central location in a Microsoft 365 tenant, refer to the following "Get Microsoft 365 Geo Locations" on page 88 section.
4. Click **Save**.

Get Microsoft 365 Geo Locations

Refer to the following instructions to get geo locations in a Microsoft 365 tenant:

- To get geo locations in SharePoint, go to the SharePoint admin center. The geo locations are listed in the left navigation.
- To get geo locations in Exchange, use the Exchange PowerShell Get-OrganizationConfigcmdlet. Open Windows PowerShell and run the script below with the **Exchange administrator** role.

```
Set-ExecutionPolicy RemoteSigned
$UserCredential = Get-Credential
$Session = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri https://
outlook.office365.com/powershell-liveid/ -Credential $UserCredential -Authentication Basic
-AllowRedirection
Import-PSSession $Session
Get-OrganizationConfig | Select -ExpandProperty AllowedMailboxRegions | Format-Table
```

  The geo locations will be listed in the result.
- To get geo locations in Microsoft Entra ID, use the Azure PowerShell *Get-MsolCompanyAllowedDataLocation* cmdlet. Open Windows PowerShell and run the script below.

```
Connect-MsolService
Get-msolcompanyalloweddatalocation | format-list
```

  The geo locations will be listed in the result.

Get Microsoft 365 Central Location

Refer to the following instructions to get the central location in a Microsoft 365 tenant:

- To get the central location in SharePoint, go to the SharePoint admin center. On the **Geo locations** page, there is an icon next to the central location.

Geo Locations	Country
APC	Asia-Pacific
ARE	United Arab Emirates
AUS	Australia
BRA	Brazil
CAN	Canada
CHE	Switzerland

Geo Locations	Country
DEU	Germany
EUR	EMEA
FRA	France
GBR	United Kingdom
IND	India
JPN	Japan
KOR	Korea
NAM	North America
ZAF	South Africa

- To get the central location in Exchange, use the Exchange PowerShell *Get-OrganizationConfigcmdlet*. Open Windows PowerShell and run the script below with the **Exchange administrator** role.

```
Set-ExecutionPolicy RemoteSigned
$UserCredential = Get-Credential
$Session = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri https://
outlook.office365.com/powershell-liveid/ -Credential $UserCredential -Authentication Basic
-AllowRedirection
Import-PSSession $Session
Get-OrganizationConfig | Select DefaultMailboxRegion
```

  The central location will be displayed in the result.

- To get the central location in Mictosoft Entra ID, use the Azure PowerShell *Get-MsolCompanyAllowedDataLocation* cmdlet. Open Windows PowerShell and run the script below.

```
Connect-MsolService
Get-msolcompanyalloweddatalocation | format-list
```

  The central location (**IsDefault** value is **True**) will be displayed in the result.

Configure App Registrations

If you need to leverage the resources of IBM Storage Protect for Cloud, you can register an app in IBM Storage Protect for Cloud and grant permissions to the app. With the registered app, you can use the generated application (client) ID for authentication.

The Tenant Owner and Service Administrators can navigate to **Administraton** > **App registrations**, and refer to the sections below for more instructions.

Edit an App

Follow the steps below to edit an app:

1. On the **App registrations** page, select the app you want to edit and click **Edit**.
2. On the **Edit app registration** page, you can update the app name, assign services and permissions, or add/delete certificates. You can refer to the instructions in the **Register an App** section above.
3. Click **Confirm** to delete the selected apps.

Register an App

Follow the steps below to register an app:

1. On the **App registrations** page, click **Create**.
2. On the **Create app registration** page, complete the following steps:

a. Enter a name for the app.

b. Click **Add service and permission**.

c. In the **Add service and permission** pane, select the services and corresponding permissions that you need to grant to this app, and then click **Add**.

Note: If your organization is using Cense and you want to batch-create scan profiles for Microsoft 365 users, select **autodiscovery.readwrite.all**.

d. Click **Add new certificate** to upload a certificate (.cer file). The certificate serves as credentials that allow your application to authenticate itself, requiring no interaction from a user at runtime. You can refer to "Appendix G - Prepare a Certificate for the Custom Azure App" on page 142.

e. Click **Save** to save your configurations.

When you finish the registration, click the app name to view the registration details, and you can copy the generated application (client) ID on the details page. You can use the client ID for authentication when leveraging the resources of IBM Storage Protect for Cloud.

Delete Apps

Follow the steps below to delete apps:

1. On the **App registrations** page, select the apps and click **Delete** on the ribbon.
2. A pop-up window appears asking for your confirmation.
3. Click **Confirm** to delete the selected apps.

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

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 **Service account authentication notification**.

- **App authorization notification** – With this notification configured, IBM Storage Protect for Cloud will send an email notification if any app profile is in the **Expired** status.
- **Service account authentication notification** – With this notification configured, IBM Storage Protect for Cloud will send an email notification if any account being used in a service account profile fails on the connection.

  The failed connection occurs when the configured account is deleted from Microsoft 365, or when the account's password is changed. An email notification will be sent every day if the connection continues to fail.

  After you turn on the toggle to enable notifications, refer to the following information to select the email notification recipients:

- **Send an email notification to service administrators** – Select this check box if you want the email notifications to be sent to Service Administrators.
- **Select an email recipient profile** – If you want to send email notifications to specific recipients, select this check box and select an email recipient profile from the drop-down list. If there is no

email recipient profile, click **Create** to create one. For more instructions on configuring email recipient profiles, refer to "Email Recipient Profile" on page 92.

Click **Save** to save your configurations.

Auto Discovery Notification

To monitor your Auto Discovery scan job, you can enable the following notifications:

- **Email notification for job completion status** – After you turn on the toggle to enable this notification, complete the following settings:
  1. **Send an email if any auto discovery scan job completes with the following status** – Select the check box of your desired status.
  2. **Select an Email Recipient List** – Select an email recipient profile from the drop-down list. Recipients in the selected profile will receive the email notifications. If there is no email recipient profile, click **Create** to create one. For more information on configuring email recipient profiles, refer to "Email Recipient Profile" on page 92.
- **Enable "What's New" digest that summarizes changes to your Auto Discovery** – With this notification configured, IBM Storage Protect for Cloud will automatically send scheduled conclusion reports of auto discovery updates to recipients. After you turn on the toggle to enable this notification, complete the following settings:

  Note: The **"What's new"** report feature is only supported in auto discovery for Microsoft 365 objects

  – **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 **Create** to create one. For more information on the email recipient list, refer to "Email Recipient Profile" on page 92.

Click **Save** to save your configurations.

Subscription Notification

The Tenant Owner and Services Administrators can refer to the following instructions to configure recipients who will receive subscription notifications (including subscription extension, subscription expiration, and out-of-policy notifications).

Note: If you are a customer managed by a service provider, **Subscription notification** setting in IBM Storage Protect for Cloud is not available to you.

- **Send an email notification to service administrators** - Select this check box if you want the email notifications to be sent to Service Administrators.
- **Select an email recipient profile** – If you want to send the email notifications to specific recipients, select this checkbox and select an email recipient profile from the drop-down list. If there is no email recipient profile, click **Create** to create one. For more instructions on configuring email recipient profiles, refer to "Email Recipient Profile" on page 92.

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 Storage Protect for Cloud.

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

- **Tenant Owner in IBM Storage Protect for Cloud**
- **All Service Administrators in IBM Storage Protect for Cloud**
- **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 Recipient Profile" on page 92.

Click **Save** to save your configurations.

Announcement Notification

To ensure important announcements can be received when they are published, IBM Storage Protect for Cloud enabled the announcement notification.

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

Note: If you are a customer managed by a service provider, **Announcement notification** setting in IBM Storage Protect for Cloud is not available to you.

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:**
  - **Service administrators in IBM Storage Protect for Cloud.**
  - **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 Recipient Profile" on page 92.

  Click **Save** to save your configurations.

Email Recipient Profile

You can configure email recipient profiles to customize recipients that will receive email notifications. Then, in other settings providing email notifications, you can select a recipient profile to receive specific notifications.

To manage email recipient profiles, click **Email recipient profile** on the **Notification** page. The **Email recipient profile** pane appears on the right of the page, and you can perform the following actions:

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

  Click **Save** to save the configuration.
- **Edit** – Select an email recipient profile, and click **Edit** to edit its settings. Click **Save** to save the configuration.
- **Delete** – Select one or multiple email recipient profiles, and click **Delete**. Click **Confirm** to confirm your deletion.

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.

Configure General Settings

In **Administration** > **General settings**, the Tenant Owner and Services Administrators can refer to the instructions below to configure settings.

Culture settings

Refer to the instructions below to select your preferred date format and email language.

1. Navigate to **Administration** > **General settings** > **Culture settings**.
2. The **Culture settings** pane appears on the right of the page. Refer to the information below to configure the date format and display language:
   - **Select a date format** – Select an option from the drop-down list. The selected date format will be displayed in the IBM Storage Protect for Cloud environment and notification emails.
   - **Select an email language** – By default, the display language is set according to the country or region you've selected while signing up for IBM Storage Protect for Cloud. You can select a language preference from English, Japanese, German, and French.

     The following table lists the default email language mappings.

Language	**Country/Region**
Japanese	Japan
French	Benin
	Burundi
	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

3. Click **Save**.

Terminology mappings

If you want to configure mappings to map default terms to custom terms, refer to the instructions below:

Note: Currently, the terminology mappings can only be applied to IBM Storage Protect for Cloud Recovery Portal. For additional information on the places where the default terms will be mapped to custom terms, see t_spp_olsrvcs_rc_config_term_mapping_for_recovery.dita. Note that some mappings may not take effect due to limitations, you can contact the IBM Software Supportteam when you encounter mapping issues.

1. Navigate to **Administration** > **General settings** > **Terminology mappings**.
2. In the **Terminology mappings** pane, click **Edit**, and then follow the instructions below to configure mappings:
   - To add a mapping, follow the steps below:
     a. Click **Add mapping**. The **Add mapping** sub pane appears.
     b. In the **Add mapping** sub pane, enter a default term in the **Default** textbox, enter a custom term in the **Custom** textbox, and then click **Add** to add a mapping.

        Note: The mapping is case sensitive. The value entered in the **Default** textbox must be the same as the default term in the service environment. Otherwise, the mapping will not take effect.
     c. If you want to add multiple mappings, repeat the above step **1** and step **2**.
   - To edit or remove a mapping, click the more options (…) button on the right of the mapping, and then click **Edit** or **Remove** from the drop-down menu.
3. Click **Save**.

Enable Trusted IP Address Settings

You can enable trusted IP address settings to only allow users to access IBM Storage Protect for Cloud 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 **Administration** > **Security** > **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.
   - If you want to apply the configured IP whitelisting to local users only, select the **IP whitelisting for local users only** checkbox.
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 Storage Protect for Cloud local users. Local users will be asked to change their account passwords regularly for the security of their accounts.

Note: Microsoft 365 and Salesforce users follow the related systems' password policies.

Complete the following steps to enable the password policy:

- Navigate to **Administration** > **Security** > **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 Storage Protect for Cloud.

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 Storage Protect for Cloud 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 Storage Protect for Cloud or other IBM Storage Protect for Cloud environments to help resolve issues, you must contact IBM Software Support to enable the option again.

Configure Session Settings

IBM Storage Protect for Cloud 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 Storage Protect for Cloud 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 Storage Protect for Cloud 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 **Administration** > **Security** > **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:
     a. Select the **Configure session timeout setting** checkbox.
     b. Enter a number in the text boxes before **hours** and/or **minutes**.

        Note: The duration cannot be less than 15 minutes.

     c. Click **Save** to save your configurations, or click **Cancel** to go back to the homepage without saving any configurations.
   - 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 Reserved IP Addresses or VNet IDs

If your tenant has the enterprise subscription for any IBM Storage Protect for Cloud, in **Firewalls and Virtual Networks**, you can download reserved IP addresses or Azure Resource Manager (ARM) VNet IDs according to your scenario. For details, refer to the sections below.

Download a List of Reserved IP Addresses

If your tenant has the enterprise license for any service offered by IBM Storage Protect for Cloud 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 Storage Protect for Cloud and IBM Storage Protect for Cloud Microsoft 365 can operate on your environment. IBM Storage Protect for Cloud is the entry for all IBM Storage Protect for Cloud. Apart from adding the IP addresses of the IBM Storage Protect for Cloud you want to use, make sure the IP addresses of IBM Storage Protect for Cloud 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 **Administration** > **Security** > **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 Storage Protect for Cloud 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" on page 84.

   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 Continuous access evaluation in the Microsoft article.

Download ARM VNet IDs

If you are using or plan to use your own storage device for any of IBM Storage Protect for Cloud, you may find your storage account in the same Microsoft Azure data center as your IBM Storage Protect for Cloud tenant (or in a paired region). However, if you have enabled the firewall on your storage, you must download the Azure Resource Manager (ARM) VNet IDs and add the subnets to your virtual network.

Procedure

Complete the following steps to get the ARM VNet IDs for your data center:

1. Navigate to **Administration** > **Security** on the left pane.
2. On the **Security** page, click **Download** in the **ARM VNet IDs** section.

   Note: For Microsoft 365 multi-geo tenants, you must first configure mappings between your Microsoft 365 geo locations and IBM Storage Protect for Cloud data centers, and then you can download the VNet IDs. For additional details on the mappings, refer to Manage Data Center Mappings.
3. Select a location to save the file.

   For details on adding ARM VNet IDs, refer to "Add ARM Virtual Networks" on page 84.

Chapter 14. Export the User Activity Report

The Tenant Owner and Service Administrators can export reports of their tenant's user activities in IBM Storage Protect for Cloud 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 **Administration** > **User Activity Report** on the left pane.
2. Complete the following based on your scenario:
   - **Retain user activity policy** - Complete the steps below to change the retention time of the activity logs:
     a. In the **Retain user activity logs for** field, select **Years** or **Months** from the drop-down list, and then enter a proper number in the nearby text box.
     b. Click **Save** to save your changes.
   - **Export user activity report** – Complete the steps below to export user activity reports:
     a. Click the calendar button to select a time range.
     b. Click **Export**. 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

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 Storage Protect for Cloud Microsoft 365 Download License Report Access IBM Storage Protect for Cloud Microsoft 365 Submit Invite Support Request Reset Password

Section	Information
App Management Service Account Service Account Pool	Create/Updated/Delete/Re-authorize/Edit App Profile SharePoint Online Admin Center URL 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

Section	Information
Advanced Settings	Create/Edit/Delete Email Recipient List Configure Date Format in Notification & Email Settings Configure Email Language Saved Email Notification Settings 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

Chapter 15. 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.

Chapter 16. Contact Support to Submit an Issue

If you encounter any trouble using IBM Storage Protect for Cloud, choose either of the following actions based on your subscription to resolve the issue:

- If you have a trial subscription, send an email to sp4csupport@ibm.com.
- If you have a full subscription, you can contact IBM Software Support.

Chapter 17. Submit Feedback

IBM Storage Protect for Cloud provides a platform to collect feedback where you can provide suggestions for service features from your IBM Storage Protect for Cloud 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 Storage Protect for Cloud Experience
   Click the stars to evaluate your IBM Storage Protect for Cloud experience.

   Your Suggestion
   Enter your suggestions about IBM Storage Protect for Cloud features.
3. Click **Submit** to submit your feedback, or click **Cancel** to return to the IBM Storage Protect for Cloud homepage without submitting your feedback.

Appendices

The table details the appendices included in this document:

Appendix	Description
"Appendix A - Supported Criteria in Auto Discovery Rules" on page 109	Lists the criteria that are supported in Auto Discovery advanced mode rules.
"Appendix B - Objects Supported by Batch Import" on page 134	Lists the objects that can be and cannot be registered via Batch Import.
"Appendix C - Create a Key Vault in Azure" on page 134	Details how to create an Azure Key Vault.
"Appendix D - Password Limitations and Requirements of Microsoft 365 Accounts" on page 136	Details the password limitations and requirements of Microsoft 365 accounts.
"Appendix E - When Service Account and App Profile are Used" on page 137	Details when Service Account, Microsoft 365 MFA Service Account, and App Profile for Microsoft 365, App Profile for Dynamics 365, and App Profile for a Microsoft Delegated App are used.
"Appendix F - Helpful Notes When Auto Discovery Scan Results Return Error Codes" on page 138	Details solutions for some scan error messages in Auto Discovery.
"Appendix G - Prepare a Certificate for the Custom Azure App" on page 142	Details how to prepare a certificate for the custom Azure app.
"Appendix H - IBM Storage Protect for Cloud App Registrations" on page 143	Details how to register, update, and delete IBM Storage Protect for Cloud apps that can be used to leverage resources of IBM Storage Protect for Cloud Microsoft 365.

Appendix A - Supported Criteria in Auto Discovery Rules

The table 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 Mailbox

Criteria	Condition
City	Contains
	Does Not Contain
	Equals
	Does Not Equal
	Matches
	Does Not Match

Criteria	Condition
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

Criteria	Condition
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
	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

Criteria	Condition
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
	Does Not Equal
Property Synced from On-premises: Distinguished Name Domain Name Immutable ID SAM Account Name Security Identifier User Principal Name	Contains
	Does Not Contain
	Equals
	Does Not Equal
	Matches
	Does Not Match

Note the following:

- **Exchange mailbox type** – This criterion only supports app profiles with the **Exchange.ManageAsApp** API permission. You also must ensure that the app has been assigned with the Exchange Administrator role. For additional details, see How to Assign the Exchange Administrator Role to an App?
- **Custom attribute** – After selecting this criterion, 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.
- **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 Storage Protect for Cloud 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
	Primary Administrator	Contains
		Equals
	Size	>=
		<=
	URL	Contains
		Does Not Contain
		Equals
		Does Not Equal
		Matches
		Does Not Match

Criteria		Condition
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

Criteria		Condition
	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
		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

Criteria		Condition
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 Storage Protect for Cloud 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
	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 Existing Guests Only Only People in Your Organization	Equals
	Does Not Equal

Criteria	Condition
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

Criteria	Condition
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 Storage Protect for Cloud 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 Microsoft Entra ID 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

Criteria		Condition
		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
	Custom Property: Number	>=
		<=
		=

Criteria		Condition
	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 Storage Protect for Cloud 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 Storage Protect for Cloud 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
	After
	On
	Within
	Older Than
Custom Property: Number	>=
	<=
	=
Custom Property: Text	Contains
	Does Not Contain
	Equals
	Does Not Equal
	Matches
	Does Not Match

Criteria	Condition
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 Storage Protect for Cloud 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

Criteria	Condition
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

Criteria	Condition
Primary Email Domain	Equals
	Does Not Equal
Sign-in Status	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
Sync Status	Equals
	Does Not Equal

Security and Distribution Group

Criteria	Condition
Group Type: Security Group Mail-enabled Security Group Distribution List Dynamic Distribution List	Equals
	Does Not Equal

Criteria	Condition
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	>=
	<=
	=

Criteria	Condition
Custom Property: Text	Contains
	Does Not Contain
	Equals
	Does Not Equal
	Matches
	Does Not Match
Sync Status	Equals
	Does Not Equal

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 Storage Protect for Cloud 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.

Environment

Criteria	Condition
Created Time	Before
	After
	On
	Within
	Older Than
Creator: City Company Country Department Office	Contains
	Does Not Contain
	Equals
	Does Not Equal
	Matches
	Does Not Match

Criteria	Condition
Region	Contains
	Does Not Contain
	Equals
	Does Not Equal
	Matches
	Does Not Match

Connections

Criteria	Condition
Creator / Custom Connector Creator: City Company Country Department Office	Contains
	Does Not Contain
	Equals
	Does Not Equal
	Matches
	Does Not Match
Custom Connector	Equals
	Does Not Equal
Environment	Contains
	Does Not Contain
	Equals
	Does Not Equal
	Matches
	Does Not Match
Status	Equals
	Does Not Equal

Power App

Criteria		Condition
Created time		Before
		After
		On
		Within
		Old than

Criteria		Condition
Environment	Name	Contains
		Does not contain
		Equals
		Does not equal
		Matches
		Does not match
	Creator: City Company Country or region Department Email address Office	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
Owner: City Company Country or region Department Email address Office		Contains
		Does not contain
		Equals
		Does not equal
		Matches
		Does not match
License designation		Equals
		Does not equal

Power Automate

Criteria		Condition
Created time		Before
		After
		On
		Within
		Old than
Environment	Name	Contains
		Does not contain
		Equals
		Does not equal
		Matches
		Does not match
	Creator: City Company Country or region Department Email address Office	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
Owner: City Company Country or region Department Email address Office		Contains
		Does not contain
		Equals
		Does not equal
		Matches
		Does not match
License designation		Equals
		Does not equal

Power BI

Criteria	Condition
Display Name	Contains
	Does Not Contain
	Equals
	Does Not Equal
	Matches
	Does Not Match
Geo Location	Equals
	Does Not Equal
Workspace Admin	Contains
	Does Not Contain
	Matches
	Does Not Match

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 lists the objects that can be and cannot be registered by using 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 Storage Protect for Cloudencryption profile will access the key vault via the application.
   a) Go to Microsoft Entra admin center (or Microsoft Azure portal), navigate to **Microsoft Entra ID** > **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 Storage Protect for Cloud 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 the Microsoft 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 a key vault** page appears.

c. In the **Basics** tab, provide the basic information for the key vault, and then click the **Access configuration** tab.

d. In the**Access Policies**section, click **Create**.

e. The **Create an Access policy** pane appears. In the **Permissions** tab , select the following **Key permissions** :

- In the **Key Management Operations** field, select **Get**.
- In the **Cryptographic Operations** field, select **Decrypt** and **Encrypt**.

f. Click **Next** to go to the **Principal** tab.

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 **Enable public access** which allows all networks to connect to this key vault.

Note: If you only allow the IBM Storage Protect for Cloud and the IBM Storage Protect for Cloud 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. Follow the steps below to 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. Edit the key vault's firewall

If you only allow the IBM Storage Protect for Cloud and the IBM Storage Protect for Cloud 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 **Allow public access from specific virtual networks and IP addresses.**.

c) In the **Firewall** field, enter the IP addresses of the IBM Storage Protect for Cloud and the IBM Storage Protect for Cloud Microsoft 365 you are using in the text boxes.

Note: To get the IP addresses, sign in to IBM Storage Protect for Cloud and navigate to **Administration** > **Administration** > **Security** > **Reserved IP address**.

d) Click **Save** to save your configurations.

Appendix D - Password Limitations and Requirements of Microsoft 365 Accounts

The table 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.
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 table details when Service Account, Microsoft 365 MFA Service Account, App Profile for Microsoft 365, App Profile for a Microsoft Delegated App, and App Profile for Dynamics 365 are used.

Service	App Profile	Service Account	App Profile + 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 Storage Protect for Cloud 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
Power Platform Management	Supported	Supported	Supported	Microsoft Delegated App
Dynamics Customer Engagement Management	Supported	Supported	N/A	Unsupported

Service	App Profile	Service Account	App Profile + Service Account	App Profile Type
Dynamics Unified Operations Management	Supported	Unsupported	N/A	Unsupported

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 Storage Protect for Cloud Microsoft 365 your tenant is using.

Note: Refer to "Will the App Profile Method Meet Your Data Management Requirements?" on page 7 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 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
The account in the authentication method profile of this scan profile does not have the license to access the Environments listed below.	ps0000001
The account in the authentication method profile of this scan profile does not have sufficient permissions to access the Environments listed below.	ps0000002

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 App Profile and Service Account Profile?" on page 3
- 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:
  - If your organization has configured service account pools in the IBM Storage Protect for Cloudclassic UI (before July 2023) 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 Chapter 8, “Manage Microsoft 365 Account Pool,” on page 35 and “How Many Accounts Should be Added into an Account Pool?” on page 3

– Check the scan profile’s settings to ensure that scan jobs will not run when there are other services sending a lot of requests to SharePoint Online.

  Note: If your organization has configured scan profiles with the service account authentication method before July 2023 release, to continue using service account authentication method for Auto discovery scan jobs, you must not update your Auto discovery scan profiles. Otherwise, the service account authentication methods will be absent from scan profiles.

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:

- Configure app profiles to rerun the scan job with the app profile authentication method. For more information about app profile, refer to Manage App Profiles.
- If the error still exists, you can refer to the steps below to check the audit log details.

  1. Search for jobs in Microsoft Purview, in the **Audit**tab under **Solutions**. Fill in the appropriate date and time range.
  2. The jobs which meet your search conditions will be added to the queue. You can select a job in the **Completed** status to export audit logs.
  3. Click **Export** to export audit logs.

  Note: 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 or have enabled conditional access policies in Microsoft Azure, it is recommended to configure the app profiles to be used by the scan profiles in **Auto discovery**. For additional details on app profiles and auto discovery, refer to Manage App Profiles and Manage Auto Discovery

If your organization still wants to use scan profiles with the service account authentication method (these scan profiles were transferred from the IBM Storage Protect for Cloud classic UI in July 2023 release),

you must not update the scan profiles. To troubleshoot this error, you can edit the service account profile to update the Microsoft 365 account used in the profile by referring to instructions in Helpful Notes for Passing the Validation Test of a Service Account

ps0000001

Go to Microsoft 365 admin center and navigate to **Users** > **Active users**, find the account (applied in the service account profile or used to authorize the delegated app), and then click **Manage product licenses** from the **More actions** drop-down list.

In the account details panel, click the **Licenses and apps** tab, and ensure that the licenses and apps related to Power Automate or Power Apps have been selected. Click **Save changes**.

After the changes are saved and this account can successfully sign into Power Automate or Power Apps, wait for at least 15 minutes, and then go to IBM Storage Protect for Cloud to run the scan profile again.

For more information about the Power Platform licenses, refer to the following Microsoft articles: Sign up for Power Apps and Signing up for Power Automate.

ps0000002

Go to the Power Platform admin center, click **Environments**, and click an environment which is reported in the scan history. Click **Settings** on the ribbon of the environment details page.

On the **Settings** page, navigate to **Users + permissions** > **Users**.

On the **Users** page, find the account (applied in the service account profile or used to authorize the delegated app) and take the following actions based on your scenarios:

- If the account is not in the users list, click **Add user** to add the account.
- If the account is in the users list, check whether this account has the **System Administrator** role.

If the **System Administrator** role is not displayed, either click **Manage roles** and assign the role to the account, or click **Refresh user** to synchronize the role from Microsoft Entra.

After the changes are saved and this account can successfully sign into Power Automate or Power Apps, wait for at least 15 minutes, and then go to IBM Storage Protect for Cloud to run the scan profile again.

For more information, refer to Microsoft Article.

Appendix G - Events Monitored by SCOM

Refer to the table below for IBM Storage Protect for Cloud 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.	
1004	A user updated an app profile for Salesforce.	
1005	A user updated an app profile for Yammer.	

Event ID	Event	Function
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.	

Event ID	Event	Function
1200	One or more users were added to the IBM Storage Protect for Cloud 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.	
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 G - Prepare a Certificate for the Custom Azure App

This section details how to prepare certificate files (.cer file and .pfx file). The .cer file can be used to "Create Custom Apps" on page 43 in Microsoft Entra ID, and the .pfx file can be used to "Create an App Profile" on page 40 for apps in the custom mode.

To prepare self-signed certificate files based on your scenario, choose one of the following methods:

- "Use a Key Vault in Azure to Prepare Certificates" on page 142
- "Use IIS Manager to Prepare Certificates" on page 143

Use a Key Vault in Azure to Prepare Certificates

Before you begin

Before preparing a certificate with this method, make sure you have a key vault in Azure. If you have an Azure subscription but do not have any key vaults, refer to the instructions in "Appendix C - Create a Key Vault in Azure" on page 134. Then follow the instructions below to prepare the certificate.

Procedure

1. In the Microsoft 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.

   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.

- 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
```

- Press **Enter** to execute the script.

What to do next

After completing the steps above, you will get two certificate files. The .cer file can be used to "Create Custom Apps" on page 43 in Microsoft Entra ID, and the .pfx file can be used to "Create an App Profile" on page 40 for apps in the custom mode.

Use IIS Manager to Prepare Certificates

Procedure

To create the certificates via Internet Information Services (IIS) Manager, complete the following steps:

1. Go to **Administrative Tools** > **Internet Information Services (IIS) Manager**.
2. Click the server name in the **Connections** pane and double-click **Server Certificates** in the right pane.
3. Click **Create Self-Signed Certificate** in the **Actions** pane.
4. Enter a name for the certificate, and click **OK**. The certificate will be listed in the **Server Certificates** pane.
5. Double-click the created certificate and click the **Details** tab. Click **Copy to File** to export the certificate.
6. In the **Certificate Export Wizard** window, click **Next**.
7. Select the certificate type.
   - To export a PFX certificate with private key, select the **Yes, export the private key** option.
   - To export a CER certificate, select the **No, do not export the private key** option.
8. Click **Next**. Keep the default option on the page, and click **Next**.

   If you select to export the private key, you need to enter the password for the certificate and confirm the password. Remember this password, and it will be used when creating the app profile.
9. Enter a name for the certificate file. You can also click **Browse** to specify the location where you want to save the certificate.
10. Click **Next**. The certificate information will be displayed.
11. Click **Finish**. The certificate file will be exported.

Appendix H - IBM Storage Protect for Cloud App Registrations

If you need to leverage the resources of IBM Storage Protect for Cloud Services, you can register an app in IBM Storage Protect for Cloud 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 Storage Protect for Cloud	Usage
IBM Storage Protect for Cloud	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 Storage Protect for Cloud 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 Storage Protect for Cloud, and then use the link to open the **IBM Storage Protect for Cloud 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 G - Prepare a Certificate for the Custom Azure App" on page 142 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 Storage Protect for Cloud Microsoft 365.

Edit an App

You can edit an app in IBM Storage Protect for Cloud.

Procedure

1. On the IBM Storage Protect for Cloud 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 Storage Protect for Cloud.

Procedure

1. On the IBM Storage Protect for Cloud 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.

Appendix J - Accessibility features for the IBM Storage Protect for Cloud

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

Overview

The IBM Storage Protect for Cloud includes the following major accessibility features:

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

The IBM Storage Protect for Cloud product ensures compliance with US Section 508, Web Content Accessibility Guidelines (WCAG) 2.0, and EN 301 549. To take advantage of accessibility features, use the latest release of your screen reader and the latest web browser that is supported by the product.

The product documentation in IBM Documentation is enabled for accessibility.

Keyboard navigation

This product uses standard navigation keys.

Interface information

User interfaces do not have content that flashes 2 - 55 times per second.

Web user interfaces rely on cascading style sheets to render content properly and to provide a usable experience. The application provides an equivalent way for low-vision users to use system display settings, including high-contrast mode. You can control font size by using the device or web browser settings.

Related accessibility information

In addition to standard IBM help desk and support websites, IBM has a TTY telephone service for use by deaf or hard of hearing customers to access sales and support services:

TTY service
800-IBM-3383 (800-426-3383)
(within North America)

For more information about the commitment that IBM has to accessibility, see IBM Accessibility.

Notices

This information was developed for products and services offered in the US. This material might be available from IBM in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

The performance data discussed herein is presented as derived under specific operating conditions. Actual results may vary.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work must include a copyright notice as follows: © (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. _enter the year or years_.

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

Adobe is a registered trademark of Adobe Systems Incorporated in the United States, and/or other countries.

Linear Tape-Open, LTO, and Ultrium are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

Intel and Itanium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

The registered trademark Linux® is used pursuant to a sublicense from the Linux Foundation, the exclusive licensee of Linus Torvalds, owner of the mark on a worldwide basis.

Microsoft, Windows, and Windows NT are trademarks of Microsoft Corporation in the United States, other countries, or both.

Java™ and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Red Hat®, OpenShift®, Ansible®, and Ceph® are trademarks or registered trademarks of Red Hat, Inc. or its subsidiaries in the United States and other countries.

UNIX is a registered trademark of The Open Group in the United States and other countries.

VMware, VMware vCenter Server, and VMware vSphere are registered trademarks or trademarks of VMware, Inc. or its subsidiaries in the United States and/or other jurisdictions.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the IBM website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

Privacy policy considerations

IBM Software products, including software as a service solutions, (“Software Offerings”) may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user, or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering’s use of cookies is set forth below.

This Software Offering does not use cookies or other technologies to collect personally identifiable information.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, see IBM’s Privacy Policy at http://www.ibm.com/privacy and IBM’s Online Privacy Statement at http://www.ibm.com/privacy/details in the section entitled “Cookies, Web Beacons and Other Technologies,” and the “IBM Software Products and Software-as-a-Service Privacy Statement” at http://www.ibm.com/software/info/product-privacy.

Product Number: 5900-AP6