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 185.

Edition Notice (June 2024)

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

© Copyright International Business Machines Corporation 2022, 2024.
US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

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.

© Copyright IBM Corp. 2022, 2024

What's new

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

Release Date: November 2, 2025

New features and updates

General Updates

- The API permissions for the Microsoft tenant registration app have been updated. The **Organization.Read.All** permission has been removed, and the **LicenseAssignment.Read.All** permission has been added. Organizations that have previously granted consent to the tenant app will not be affected unless further action is taken. Upon reconnecting the tenant in IBM Storage Protect for Cloud, it will be necessary to approve the newly required API permissions.
- The **IBM Storage Protect for Cloud Azure VMs, Storage, and Entra ID** service app now includes the **DeviceManagementScripts.ReadWrite.All** Microsoft Graph application permission to allow the app to read and write Microsoft Intune device compliance scripts, device management scripts, device shell scripts, device custom attribute shell scripts and device health scripts, without a signed-in user.

  If your organization has configured an app profile for this service app, navigate to IBM Storage Protect for Cloud > **Management** > **App management** to re-authorize the app profile. This will apply the new API permissions and enable access to the related features.

  Note: Reauthorization is only required if you want to use the new features. Existing functionalities will remain unaffected if no action is taken.
- In **Auto discovery** > **Scan profiles**, when configuring an advanced mode scan profile with the **Specified objects in one container** rule selected for containers, you can now set conditions to filter **SharePoint** and **Microsoft 365 Group / Microsoft Team / Viva Engage community** objects based on the following criteria:
  - **SharePoint site**
  - **Creator** > **Custom property: Text**
  - **Last activity (UTC)**
- **Microsoft 365 Group / Microsoft Team / Viva Engage community**
  - **Group / Team / Viva Engage community property** > **Creator** > **Custom property: Text**
  - **Group team site property** > **Last activity (UTC)**

© Copyright IBM Corp. 2022, 2024

Chapter 1. About IBM Storage Protect for Cloud

IBM Storage Protect for Cloud is a multi-tenant Software-as-a-service (SaaS) platform. With a unified browser-based user interface and a fully distributed architecture, IBM Storage Protect for Cloud integrates IBM's powerful data organization and protection technologies into a scalable solution for Microsoft, Google, and Salesforce platforms. No installation and minimal configuration, moving to the cloud is simple.

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, Storage, and Entra ID
- IBM Storage Protect for Cloud Google Workspace

Language Support

IBM Storage Protect for Cloud supports the following languages: English, 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.

Sign-in Address	https://sp4c.storage-defender.ibm.com
Sign-in Methods	Sign in with: Local account Microsoft 365 account Salesforce account Google 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) Brazil South (Sao Paulo State)

Supported Browsers

The following table provides the required browser versions.

© Copyright IBM Corp. 2022, 2024

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 Graph APIs

You can use IBM Storage Protect for Cloud modern APIs to interact programmatically with IBM's solutions, such as facilitating automation, data integration, and enhanced operational capabilities. For details, refer to IBM Graph API Overview.

Note: The legacy APIs in IBM Storage Protect for Cloud Web API are scheduled for deprecation after the January 2025 release. Transitioning to the new APIs is highly recommended to ensure continued support and access to the latest features.

Which Cloud Services are Provided in Your Data Center?

The table below lists the IBM Storage Protect for Cloud services that are available in each data center.

Data Center	Cloud Service
Brazil South (Sao Paulo State)	IBM Storage Protect for Cloud Dynamics 365 IBM Storage Protect for Cloud Google Workspace IBM Storage Protect for Cloud Microsoft 365 IBM Storage Protect for Cloud Azure VMs, Storage, and Entra ID IBM Storage Protect for Cloud Salesforce
Canada Central (Toronto)	IBM Storage Protect for Cloud Dynamics 365 IBM Storage Protect for Cloud Google Workspace IBM Storage Protect for Cloud Microsoft 365 IBM Storage Protect for Cloud Azure VMs, Storage, and Entra ID IBM Storage Protect for Cloud Salesforce
East US (Virginia)	IBM Storage Protect for Cloud Dynamics 365 IBM Storage Protect for Cloud Google Workspace IBM Storage Protect for Cloud Microsoft 365 IBM Storage Protect for Cloud Azure VMs, Storage, and Entra ID IBM Storage Protect for Cloud Salesforce

Data Center	Cloud Service
Germany West Central (Frankfurt)	IBM Storage Protect for Cloud Dynamics 365 IBM Storage Protect for Cloud Google Workspace IBM Storage Protect for Cloud Microsoft 365 IBM Storage Protect for Cloud Azure VMs, Storage, and Entra ID IBM Storage Protect for Cloud Salesforce
UK South (London)	IBM Storage Protect for Cloud Dynamics 365 IBM Storage Protect for Cloud Google Workspace IBM Storage Protect for Cloud Microsoft 365 IBM Storage Protect for Cloud Azure VMs, Storage, and Entra ID IBM Storage Protect for Cloud Salesforce
Australia East (New South Wales)	IBM Storage Protect for Cloud Dynamics 365 IBM Storage Protect for Cloud Google Workspace IBM Storage Protect for Cloud Microsoft 365 IBM Storage Protect for Cloud Azure VMs, Storage, and Entra ID IBM Storage Protect for Cloud Salesforce
Switzerland North (Zurich)	IBM Storage Protect for Cloud Dynamics 365 IBM Storage Protect for Cloud Google Workspace IBM Storage Protect for Cloud Microsoft 365 IBM Storage Protect for Cloud Azure VMs, Storage, and Entra ID IBM Storage Protect for Cloud Salesforce

Chapter 2. Use Cases

Use Case - Want to Encrypt Your Data with a Custom Key Vault?

Event: Bob, an IT Administrator, wants to encrypt backup data and tenant sensitive information, such as the app profile token and/or the Microsoft 365 service account credentials, by using a custom key vault in Azure, instead of using the default key vault provided by IBM.

Resolution: Bob signs into IBM Storage Protect for Cloud and navigates to **Management** > **Encryption management**. Bob can create an encryption profile, provide information of the key vault he prepared, and then apply this encryption profile.

For more information on encryption profile management, refer to Manage Encryption Profiles.

Use Case - Want to Monitor the Subscription Usage of Your Services?

Event: Bob, an IT Administrator, wants to view the subscription expiration date of the IBM Storage Protect for Cloud they are using so that they can renew the services before they expire. He also wants to view the number of user seats they have purchased, to decide if he needs to purchase additional user seats for a group of incoming new hires.

Resolution: Bob signs into IBM Storage Protect for Cloud and navigates to **Administration** > **Subscription**. On the **Subscription** page, Bob can view the basic subscription information of services. He can also click a service name to view the detailed subscription information on a new page.

For more information on viewing subscription usage, refer to View Subscription Information.

Use Case - Want to Monitor the User Activity in Your Tenant?

Event: Bob, an IT Administrator, wants to view the user activity in his tenant during a defined time range within the IBM Storage Protect for Cloud platform.

Resolution: Bob signs into IBM Storage Protect for Cloud and navigates to **System** > **System auditor**. Bob can define the report scope by selecting the start time and the end time, and then he can export the report to an .xlsx file.

For more information on the user activity report, refer to Export the User Activity Report.

© Copyright IBM Corp. 2022, 2024

Chapter 3. 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 in to IBM Storage Protect for Cloud with their Microsoft 365 login IDs. Microsoft will display the **Need admin approval** page to them.

Follow the steps below to give consent to the app:

1. Click the corresponding consent link for your data center and then provide your Microsoft 365 global administrator credentials.
2. Select the **Consent on behalf of your organization** option and click **Accept**.
3. Once the consent finished, you will be redirected to IBM Storage Protect for Cloud Interface. Sign into IBM Storage Protect for Cloud if your global administrator has been invited into IBM Storage Protect for Cloud.

   Note: If your global administrator has not been invited, you may see the **Join IBM Storage Protect for Cloud** page. You can ignore this page since you have finished obtaining your consent.

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 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 12 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 8, “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 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 after you have run the first backup job, you must add at least 4 users to the account pool.

© Copyright IBM Corp. 2022, 2024

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, 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 Manage Account Pool (Obsolete).

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 IBM Storage Protect for Cloud" 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 C - Password Limitations and Requirements of Microsoft 365 Accounts" on page 175.

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 Chapter 11, "Manage Users," on page 85.

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**, **Equals any of**, **Contains**, and **Matches**:

- **Equals**- Use this condition to scan objects whose property values are equal to the entered value.
- **Equals any of** – Use this condition to scan objects whose property values are equal to any of the entered values.
- **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 multiple SharePoint sites, whose URLs are https://contoso.sharepoint.com/sites/site1 and **https://contoso.sharepoint.com/sites/site2**, into the specified container, choose the **Equalsany of** condition, and enter the desired SharePoint sites' URLs separated by semicolon (;).
- 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/***.

Note: The rules are executed sequentially from top to bottom, for example, ((1 And 2) Or 3).

What Should I Do If the Sites.FullControl.All Permission Cannot be Added to My Custom App?

If the **Sites.FullControl.All** SharePoint API permission is not allowed by your organization's security policy, you can add the **Sites.Selected** application permission as a replacement and refer to the steps below:

1. Configure your custom Azure app by referring to Create a Custom Azure App. When adding SharePoint API permissions, add the **Sites.Selected** permission instead of the **Sites.FullControl.All** permission. Ensure you click **Grant admin consent for [Tenant name]** to grant admin consent.
2. Specify which sites an app can access. For more information, refer to Specify Selected Sites via Graph Explorer.
3. Then, you can import these sites by referring to Import Objects in Batch.

Specify Selected Sites via Graph Explorer

Refer to the steps below to specify which sites the app can access.

1. Go to https://developer.microsoft.com/en-us/graph/graph-explorer, and click the profile icon to sign in.

   When the pop-up window appears, click **Accept**.
2. Refer to the steps below to search for sites that match your provided keywords.
   a. From the left navigation, click **search for a SharePoint site by keyword**.
   b. Under the **Modify permissions** tab, ensure that **Sites.Read.All** or **Sites.ReadWrite.All** permissions are granted. If not, click **Consent** to grant the permissions.
   c. Replace the text after `search=` with the desired site name.
   d. Click **Run query**. Then, check the response result and note down the site ID value. The site ID value will be used in the following steps.

3. Use the following API call to grant the FullControl permission for your app to access a specific site.
   a. Change the request method to POST.
   b. Enter the following URL in the address bar, replacing `{site-id}` with the site ID value obtained in the previous step.

      https://graph.microsoft.com/v1.0/sites/{site-id}/permissions

   c. In the **Request body** text box, enter the following JSON, replacing `{app-id}` and `{app-name}` with the custom app's client ID and display name.

```
{
"roles": [
"fullcontrol"
],
"grantedToIdentities": [
{
"application": {
"id": "{app-id}",
"displayName": "{app-name}"
}
}
]
}
```

   d. Under the **Modify permissions** tab, ensure that the **Sites.FullControl.All** permission has been granted. If not, click **Consent** to grant the permissions.
   e. Click **Run query** to execute the request. A successful execution indicates that the specified site operation is complete.

Which App Profiles Can 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
Custom app with required permissions (API Permissions Required by Custom Apps)	Exchange mailbox	**Exchange Administrator** role is required. For detailed instructions, refer to How to Assign the Exchange Administrator Role to an App?
	Security and distribution group	
	OneDrive	
	SharePoint site	
	Microsoft 365 Group / Microsoft Team / Viva Engage community	
	Project site	
	Exchange public folder	
	Microsoft 365 user	

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	
	Sharepoint site	
	Microsoft 365 Group / Microsoft Team / Viva Engage community	
	Project site	
	Exchange public folder	
	Microsoft 365 user	
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	
	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 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 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 is 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 Microsoft 365 Global Administrator or Priviledged Role Administrator since the Administrator must 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 Engage Administrator (Yammer Administrator) can also consent to the IBM Storage Protect for Cloud apps for Viva Engage.
- The Global Administrator, Privileged Role Administrator, or Engage Administrator (Yammer Administrator)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 more details on the permissions required by apps and the instructions for creating app profiles, refer to the Chapter 9, "Manage App Profiles," on page 35 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 4. Get Started

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

1. Access IBM Storage Protect for Cloud environment with a corresponding account. See the Sign in to IBM Storage Protect for Cloud section for details.
2. Register your tenants on the Microsoft/Google/Salesforce platform to IBM Storage Protect for Cloud. Navigate to **Management** > **Tenant Management** and see the Connect Your Tenants to IBM Storage Protect for Cloud section for details.
3. To configure app profiles for the apps that are required by your services, navigate to **Management** > **App Management**, and see the Manage App Profiles section for details.
4. To automatically scan objects from your platform into IBM Storage Protect for Cloud, refer to the Manage Auto Discovery section.
5. To invite users from your tenant into IBM Storage Protect for Cloud and assign permissions for services to users, navigate to **Management** > **User Management** and refer to the Manage Users section.
6. To configure security settings such as the reserved IP addresses that need to be added to your environment firewall, navigate to **Administration** > **Security** and see the Configure Security Settings section for details.
7. To enable data collection settings for generating reports in some services, to manage data center mappings for Microsoft 365 tenants with multi-geo capabilities, or to manage notification settings, see the Configure Other Administration Settings section for details.

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, Storage, and Entra ID 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.

© Copyright IBM Corp. 2022, 2024

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 in to 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 methods based on your environment:

- “Sign in with a Local Account” on page 16
- “Sign in with a Microsoft 365 Account” on page 17
- “Sign in with a Salesforce Account” on page 18
- Sign in with a Google Account

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 the IBM Storage Protect for Cloud homepage.

   If your organization has enabled the **MFA policy for local accounts**, continue with the following steps to sign in to IBM Storage Protect for Cloud:

   a. Download and install an authenticator app on your device. The Microsoft Authenticator app is the recommended choice, and most major authenticator apps are also supported. Click **Next**.

   b. Use the authenticator to scan the QR code. This step will connect your authenticator app with your account. Click **Next**.

   c. Enter the 6-digit code shown in the authenticator app. Click **OK**.

   Note: If you need to reconfigure the MFA settings, such as when switching to a new device, contact your administrator to reset MFA for your local account.

Reset Your Local Account Password

To 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** – The email address used as your IBM Storage Protect for Cloud username.
   - **Verification Code** – 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** – The new password.
   - **Confirm Password** – Retype new password again for confirmation.
   - **Verification Code** – 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 in to 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 the 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 or Privileged Role 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 is present in IBM Storage Protect for Cloud, the Join IBM Storage Protect for Cloud page will appear. To request to join the existing tenant, contact your Service Administrator for an invitation to IBM Storage Protect for Cloud.

API Permissions Required by the IBM Storage Protect for Cloud App (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	Purpose	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.	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** option on the left navigation pane. 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 20.
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 35 .
3. **Note:** This step is necessary for services that support **Auto discovery**. If your organization lacks a subscription for such service, this step will not appear in the wizard.

   Scan profile (optional) – To discover objects in your environments and scan these objects into IBM Storage Protect for Cloud for management, you must configure scan profiles. For additional details, refer to “Manage Scan Profiles” on page 75.
4. **Users and groups**- Add users/groups to IBM Storage Protect for Cloud as Service Administrators or Tenant Users. You can also assign permissions for different services to Tenant Users. For additional details, refer to Chapter 11, “Manage Users,” on page 85.

Connect your Tenants to IBM Storage Protect for Cloud

To use IBM Storage Protect for Cloud services to manage a tenant in the Microsoft , Google or Salesforce 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. For more information about the required admin consent, refer to Why Admin Consent is Required to Use the IBM Storage Protect for Cloud App?

  Note: If you want to connect a tenant which will be used to back up Azure AD B2C in IBM Storage Protect for Cloud Azure VMs, Storage, and Entra ID, the user consenting to this app must belong to the domain of this tenant, and cannot be an external user.

- 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** > **Management >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 for System Administrator profile in the same tenant.

  Note: Salesforce has published an announcement to restrict the use of uninstalled connected apps from early September 2025. This will not affect your organization if there are no apps to be created/ reconnected. However, for organizations who need to create a new tenant app or reconnect a tenant app, you must either install the tenant app in your Salesforce environment, or ensure that the user consenting to the tenant app has the following required permissions:

  – If API Access Control is enabled, only the "Use Any API Client permission" gives access to use uninstalled apps.

  – If API Access Control isn't enabled, trusted users can use uninstalled apps if they have the "Approve Uninstalled Connected Apps" permission.

For more information on the permissions required by the above tenant connections, see "Permissions Required by IBM Tenant Registrations" on page 22.

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** or **Salesforce** 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.

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.
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 to IBM 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 details** 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 21.
- 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 22.

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.

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/Google/Salesforce tenant, the Microsoft/Google/Saleforce 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**.

     Note: For organizations using IBM Storage Protect for Cloud Salesforce prior to the January 2025 release, upon reconnecting the Salesforce tenant, the new tenant app **IBM Storage Protect for CloudTenant Registration** will be created.

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.

API	Permission	Type	Purpose
Microsoft Graph	User.Read (Sign in and read user profile)	Delegated	Supports signing into IBM Storage Protect for Cloud with Microsoft 365 accounts.
	Domain.Read.All (Read doman information)	Application	Retrieve your Microsoft 365 domain information.
	LicenseAssignment.Read.All (Read all license assignments)	Application	Calculate user seats assigned in your Microsoft 365 tenant Microsoft 365 tenant
	Group.Read.All (Read all groups)	Application	Add Microsoft 365 Groups into IBM Storage Protect for Cloud, and support signing into IBM Storage Protect for Cloud with Microsoft 365 accounts.
	User.Read.All (Read all users' full profiles)	Application	Add Microsoft 365 users into IBM Storage Protect for Cloud, and support signing into IBM Storage Protect for Cloud with Microsoft 365 accounts.

Note: You do not need any permissions or Microsoft licenses other than those listed in this guide

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**.

Scope	Permission	Purpose
https://www.googleapis.com/auth/admin.directory.domain.readonly	Read domain information	Retrieve organization's Google domain information.
https://www.googleapis.com/auth/apps.licensing	Read Google license information	Collect user seats.
https://www.googleapis.com/auth/admin.directory.user.readonly	Read Google users	Invite Google users for login.
https://www.googleapis.com/auth/admin.directory.group.readonly	Read Google groups	Invite Google groups for login.

Salesforce

Connecting a Salesforce tenant will create the **IBM Storage Protect for Cloud Tenant Registration** app in the tenant's Salesforce environment. The table below lists the scope parameter values required by the app:

Value	Description
Access the identity URL service	Allows access to the identity URL service.
Manage user data via APIs	Allows access to the current, logged-in user's account using APIs.
Perform requests at any time	Allows a refresh token to be returned when the requesting client is eligible to receive one.

The purposes of using these scope parameter values are listed below:

- Support signing into IBM Storage Protect for Cloud with Salesforce accounts.
- Retrieve your Salesforce tenant information and calculate user seats.
- Add Salesforce users into IBM Storage Protect for Cloud, and support signing into IBM Storage Protect for Cloud with Salesforce accounts.

Manage Your Services

The **My Services** 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.

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). If the available license duration is less than 24 hours, it is calculated as one day.

Activate Your Services

Before 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 require licenses for certain Microsoft 365 subscriptions, Salesforce licenses. For more information, refer to Licensing Information.

Chapter 5. View Subscription and Licensing Information

On the **All Services** page, you 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 or Google Workspace 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, contact your IBM sales representative or business partner 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 agreements, purchased user seats, and specific services' additional information like purchased capacity, purchased modules, and so on.

Note: When you view subscription details, you can click **View usage details** or **Download capacity usage details** to check the usage report.

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

© Copyright IBM Corp. 2022, 2024

Chapter 6. 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**.

© Copyright IBM Corp. 2022, 2024

Chapter 7. 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/Google Workspace 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.

© Copyright IBM Corp. 2022, 2024

Chapter 8. Manage Service Account Profiles

The table below lists the services that support the service account authentication method.

Service account type	Service account
Cloud services	IBM Storage Protect for Cloud Dynamics 365
	IBM Storage Protect for Cloud Azure VMs, Storage, and Entra ID
	IBM Storage Protect for Cloud Microsoft 365

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 8
- **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 IBM Storage Protect for Cloud" 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 run a scan profile to scan SharePoint sites / Microsoft 365 Groups, the specified service account will be automatically added as one of the Term Store Administrators.

© Copyright IBM Corp. 2022, 2024

- 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 32 for 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 IBM Storage Protect for Cloud

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, Storage, and Entra ID

Note: You do not need any permissions or Microsoft licenses other than those listed in this guide

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.

Chapter 9. Manage App Profiles

IBM Storage Protect for Cloud can connect to your Microsoft, Google, or Salesforce platforms 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 tenant's custom apps, the API Permissions Required by IBM Apps and API Permissions Required by Custom Apps sections are for your reference. Note the following:

- For IBM Storage Protect for Cloud default apps, it is recommended that you configure an independent app for each of the services that you are using. For the apps that can be used by each service, refer to Apps for Individual Services. If you are using multiple services in the IBM Storage Protect for Cloud platform, you can also choose the method to configure an app for multiple services with all the required API permissions. For the apps that can be used for multiple services, refer to Apps for Multiple Services.
  - On the **App management**, **Consent to apps**, and **App profile details** pages, the related IBM default apps are marked with the icons as below:
    - Apps that utilize both application and delegated API permissions are marked with the hybrid ( ) icon.
    - Apps that have delegated API permissions only are marked with the purebred ( ) icon.
- If your organization has extremely limited required permissions and decides to use custom apps, refer to the “Create Custom Apps” on page 40section for additional details.

  Note: For Google tenants, using a default service app may encounter throttling issues caused by Google quota limits. If performance is a concern, consider configuring a custom Google app for your organization.
- IBM Storage Protect for Cloud will securely store the consent token of users for applications in Microsoft Entra ID that utilize delegated API permissions.

  Note: For the non-interactive user sign-in in Microsoft Entra, the IP address is always pointing to the original client IP when the application is using the delegated token. For more information, refer to this Microsoft article.
- If multi-factor authentication (MFA) is enabled on a Microsoft 365 account, this account can still be used to consent to app profiles. For apps with delegated permissions, the related app profiles need to be re-authorized if MFA is enabled on the consent users’ Microsoft 365 accounts after they have given consent to the app profiles. For additional details, refer to the Microsoft Tenant section.
- Salesforce has published an announcement to restrict the use of uninstalled connected apps from early September 2025. This will not affect your organization if there are no apps to be created/reauthorized. However, for organizations who need to create a new app or reauthorize an app, you must either install the app in your Salesforce environment, or ensure that the user consenting to the app has the following required permissions:
  - If API Access Control is enabled, only the “Use Any API Client permission” gives access to use uninstalled apps.
  - If API Access Control isn’t enabled, trusted users can use uninstalled apps if they have the “Approve Uninstalled Connected Apps” permission.

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 (modern mode, classic 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” on page 36.

© Copyright IBM Corp. 2022, 2024

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 20.

- 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 or Salesforce tenants. For detailed scenarios and instructions on reauthorizing app profiles, refer to Re-authorize an App Profile.

  Note: For Google tenants, the related app profiles are not supported to be re-authorized in IBM Storage Protect for Cloud. If you want to add new permissions to a Google app, to re-authorize the app, you must navigate to Google Admin console > **Apps** > **Google Workspace Marketplace apps** > **App list**, click the app, and click **Grant access** to add the required permissions to the app.
- 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.
- Before you delete an app profile, ensure it is no longer needed. To delete one or multiple app profiles, select the app profiles, click **Delete**, and click **Confirm** in the confirmation window.
- 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**.
- To find app profiles of specific tenants, services, or statuses, click **Filter** on the upper-right corner, select desired options in the **Tenant**, **Service**, and **Status** sections, and then click **Apply**.

Create an App Profile

Procedure

Before creating an app profile, refer to the Apps Required by Services section to see which apps are required by the services that your organization uses.

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 20 .
2. **Choose setup method** – Refer to the information below, and select a mode based on your scenario:
   - **Modern mode** is the recommended mode for all IBM Storage Protect for Cloud default apps. In this mode, the related apps are listed in a service-based view, and you can consent to apps separately for the selected services.

     Note the following:

     – For Google tenants, using a default service app may encounter throttling issues caused by Google quota limits. If performance is a concern, consider configuring a custom Google app for your organization. Then, choose the **Custom mode** to configure an app profile for the custom Google app.

     – 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 Entra ID**, and **Viva Engage**.

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.
Viva Engage	IBM Storage Protect for Cloud Microsoft 365	
Delegated App **Note:** If IBM Storage Protect for Cloud Azure VMs, Storage, and Entra ID is the only service that you select to use, the **Classic mode** is not available.	IBM Storage Protect for Cloud Microsoft 365 IBM Storage Protect for Cloud Azure VMs, Storage, and Entra ID	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 for organizations who have identified use cases with extremely limited required permissions.

  Before you create an app profile for a custom app, refer to "Create Custom Apps" on page 40 to create custom apps which meet the requirements of your services. When you create an app profile for a custom app, refer to Consent to Custom Apps to consent to the custom app.

  Note the following:

  – For Google tenants, it is recommended that you use custom Google apps to avoid the throttling issue caused by the quota limit. Refer to Create a Custom Google App for more information about custom Google apps.

  – If you want to make sure the custom apps in Azure can only be used by the IBM Storage Protect for Cloud production environments, you can Configure a Best Practice Conditional Access Policy for Custom Apps in Azure.

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:

   - For a Microsoft 365 tenant, creating app profiles for IBM apps in a Microsoft tenant's environment requires a **Microsoft 365 Global Administrator** or a **Privileged Role Administrator** account who is in the same tenant. For more details on this requirements, see the "Why is Admin Consent is Required to Use the IBM Storage Protect for Cloud App?" on page 13section.

     – The **Engage Administrator**, which is the **Yammer Administrator** in Microsoft Entra ID, can also consent to the IBM Storage Protect for Cloud apps for Viva Engage.

     – If multi-factor authentication (MFA) is enabled on a Microsoft 365 account, this account can still be used to consent to app profiles. For apps with delegated permissions, the related app profiles need to be re-authorized if MFA is enabled on the consent users' Microsoft 365 accounts after they have given consent to the app profiles.

     – When creating an app profile for a delegated app used by the **IBM Storage Protect for Cloud Microsoft 365** service, you also need to choose the functions that will use this app.

     – When creating an app profile for the IBM Storage Protect for Cloud Microsoft 365 service, note the following:

       - When consenting to the **Cloud Backup for Microsoft 365 delegated app**, you also need to choose the functions that will use this app. The user who consents to the app must have the **Microsoft 365 Global Administrator** role. For details, refer to the Required Permissions of Microsoft Delegated App section in the IBM Storage Protect for Cloud Microsoft 365 user guide.

- When consenting to a Viva Engage app profile used by IBM Storage Protect for Cloud Microsoft 365, the consent user must be a **Microsoft 365 Global Administrator** with the Viva Engage product license.

- To create an app profile for a custom app in a Microsoft/Google tenant, refer to the "Consent to Custom Apps" on page 44section for additional details.
- For a Google tenant, creating an app profile for the app used by the **IBM Storage Protect for Cloud Google Workspace** service requires the consent of a Super Admin account.

  Note: For the app used by **IBM Storage Protect for Cloud Google Workspace**, ensure that the Super Admin account has been assigned with the required licenses:

  – The Google Workspace module requires licenses for the Gmail, Calendar, Contacts, Drive, and Chat services. The following additional licenses are only needed for managing specific services: Shared drive for shared drives and Vault for Vault matters.

  – The Google Classroom module requires licenses for the Classroom service.
- For a Salesforce tenant, creating an app profile for the app used by **IBM Storage Protect for Cloud Salesforce** requires consent of a Salesforce account with the System Administrator profile or another profile with the same permissions.

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 **Invalid**. 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 an app will be used to manage Exchange mailboxes and settings / Security and distribution group objects / Microsoft Defender settings, you need to assign the **Exchange Administrator** role to the app. For additional details on assigning the role, refer to How to Assign the Exchange Administrator Role to an App?

   Note: You do not need any permissions or Microsoft licenses other than those listed in this guide.

Apps Required by Services

Refer to the table below for the apps that can be used by multiple services. For more details on the API permissions of these apps, refer to "Apps for Multiple Services" on page 52. You can also refer to "Apps for Individual Services" on page 58 for the service apps that you can use for each service in your tenant.

App type	App name	Service	Feature/Module	Concent from?
Microsoft 365 (All permissions)	IBM Storage Protect for Cloud Administrator for Office 365	IBM Storage Protect for Cloud Microsoft 365	SharePoint Online OneDrive Project Online (for auto discovery only) Exchange Online Public Folders (for auto discovery only) Microsoft 365 Groups Teams Yammer (for auto discovery only)	App management > Classic mode > Consented for all services
Microsoft 365 (SharePoint Online permissions)	IBM Storage Protect for Cloud Administrator for SharePoint	IBM Storage Protect for Cloud Microsoft 365	SharePoint Online OneDrive for Business Project Online (for auto discovery only)	Unsupported to create new.
Microsoft 365 (Exchange permissions)	IBM Storage Protect for Cloud Administrator for Exchange	IBM Storage Protect for Cloud Microsoft 365	Exchange Online Public Folders (for auto discovery only)	Unsupported to create new.
Delegated app	IBM Storage Protect for Cloud Delegated App	IBM Storage Protect for Cloud Azure VMs, Storage, and Entra ID	Azure Virtual Machines Azure Storage Azure SQL	App management > Classic mode or Modern mode > Consented separately for each service
		IBM Storage Protect for Cloud Microsoft 365	Restore Teams channel conversations as posts Protect Power Automate/Power Apps Protect Power BI Restore Planner task comments	
Viva Engage	IBM Storage Protect for Cloud Viva Engage	IBM Storage Protect for Cloud Microsoft 365	Viva Engage (backup and restore)	App management > Classic mode or Modern mode > Consented for all services

The list below links you to each online service user guide to get an overall instructions on how you can use the classic apps, service apps, or custom apps for each service:

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

Create Custom Apps

About this task

If your organization has extremely limited required permissions and decides to use custom apps, see "API Permissions Required by Custom Apps" on page 71 and follow the related sections in the table below to prepare custom apps.

Services	Supported app types	Create custom apps	Consent to apps
IBM Storage Protect for Cloud Microsoft 365 IBM Storage Protect for Cloud Azure VMs, Storage, and Entra ID IBM Storage Protect for Cloud Dynamics 365	Azure app with application permissions	First, create custom apps by referring to "Create a Custom Azure App" on page 40. If necessary, you can Configure a "Configure a Best Practice Conditional Access Policy for Custom Apps in Azure" on page 41.	Then, configure app profiles for custom apps by referring to "Consent to Custom Apps" on page 44.
IBM Storage Protect for Cloud Azure VMs, Storage, and Entra ID IBM Storage Protect for Cloud Microsoft 365	Azure app with delegated permissions		
IBM Storage Protect for Cloud Google Workspace	Google app	First, create custom apps by referring to Create a Custom Google App.	

Note: If you want to manage Exchange mailboxes and settings / Security and distribution group objects / Microsoft Defender settings, you need to assign the **Exchange Administrator** role to the app in Microsoft Entra ID. For additional details on assigning the role, refer to "How to Assign the Exchange Administrator Role to an App?" on page 46

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)
2. Navigate to **Identity** > **Applications** > **App registrations** > **New registration (or 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 have 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 or .crt file types are recommended):

   Note: If your organization does not have any certificates, you can refer to "Appendix F - Prepare a Certificate for the Custom Azure App" on page 179 to prepare a self-signed certificate.

   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 or .crt file and click **Add**.
   e. After the certificate file is successfully uploaded, it will be listed in the **Certificates** section.

   Then, refer to the Create an App Profile section to create an app profile in the **Custom mode**. If necessary, you can "Configure a Best Practice Conditional Access Policy for Custom Apps in Azure" on page 41.

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

To ensure that custom apps in Azure are only accessible by the IBM Storage Protect for Cloud production environment, follow the steps below to configure a conditional access policy.

1. Log in to Microsoft Entra admin center (or Microsoft Azure portal) and navigate to **Protection** (or **Microsoft Entra ID > 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.

      Note: The Workload identities license is required for the **Users or workload identities** option to appear.
   c. Click **Conditions**, click **Locations**, toggle **Configure** to **Yes**, choose the **Selected locations** option under the **Exclude** tab, and select the location created in step 3.
   d. Click **Grant** and select **Block access**.

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

f. Click **Create**.

Create a Custom Google App

Step 1: Create a New Project and Enable APIs

Refer to the instructions below to create a new project and enable APIs. Note the following:

- If you want to use an existing project, you can directly go to Enable APIs.
- Only the project owner can enable APIs for a project.

Create a New Project (Optional)

Follow the steps below to create a new project:

1. Go to Google Cloud IAM.
2. Click the current resource.
3. Click **New Project**.
4. Complete the **Project name**, **Organization**, and **Location** fields.
5. Click **Create**.
6. Search for and enable APIs that are required by your services (IBM Storage Protect for Cloud Google Workspace).
7. Click the API that you want to enable, and then click **ENABLE**.

Enable APIs

Follow the steps below to enable Google APIs:

1. Go to the Google Cloud Console.
2. Click the current resource to expand the projects list, and then select the project you want to use.

   Note: The user that can enable APIs for a project must be the project owner.
3. Click **Enable APIS and services**.
4. The API library page appears.
5. Search for and enable APIs that are required by your services (IBM Storage Protect for Cloud Google Workspace).
6. Click the API that you want to enable, and then click **Enable**.

Step 2: Turn off Policies and Create a Service Account

To create the service account, first make sure your organization has turned off the policies that disable service account creation. Note the following:

- If your organization has turned off the **Disable service account creation**, **Disable service account key creation**, and **Disable service account key upload** policies, you can proceed to Service Account Creation.
- If your organization is a newly created Google tenant or you are not sure about the policy's status, first see how to Turn off Policy for Disable Service Account Key Creation, then you can proceed with the Service Account Creation.

Turn off the Policies that Disable Service Account Creation

Before creating a service account, make sure the policy **Disable service account creation**, **Disable service account key creation**, and **Disable service account key upload** policies are turned off. You can refer to the steps below to turn off the policies:

1. If you are required to have the Organization Policy Administrator role to **Manage Policy**, refer to the instructions below to add the Organization Policy Administrator role:
   a. Go to Google Cloud IAM.
   b. In the resource list, select the organization of the project where you want to create the service account.
   c. Refer to the following instructions based on your scenario:
      - If you want to add a new principal, click **Grant access**. In the panel of granting access, enter your account in the **New principals** field, select the **Organization Policy Administrator** role from the **Role** drop-down list, and click **Save**.
      - If you want to edit an existing principal, click the **Edit principal** ( ) button next to the principal. In the panel of editing access, click **Add another role**, select the **Organization Policy Administrator** role from the **Role** drop-down list, and click **Save**.
2. Go to IAM-Organization Policies.
3. In the resource list, select the project where you create the service account.
4. From **Disable service account creation**, **Disable service account key creation**, and **Disable service account key upload** policies, click the policy that you want to turn off.
5. After you click a policy, the policy details page appears, and you can follow the steps below to turn off a policy:
   a. Click **Manage policy**.
   b. Select **Override parent's policy** to set a unique policy for this project.
   c. Click **Add a rule** to add a new rule.
   d. Select **Off** to disable the enforcement of the new rule, and click **Done**.
   e. Click **Set policy**.

Service Account Creation

Follow the instructions below to create a service account and a client ID:

Create a Service Account

Refer to the steps below to create a service account and a client ID:

1. Navigate to **APIs & Services** > **Credentials**.
2. Click **Create credentials** and select **Service account**.
3. Enter a service account name and a service account ID. Then, click **Done**.
4. Click the service account, and then click the **Keys** tab.
5. Click **Add key**, and then click **Create new key**.
6. Select the **JSON** key type and click **Create**. The downloaded file contains important information for the configuration in the following steps, and you must store the file securely as it can't be recovered if lost.

Step 3: Configure OAuth Scopes

You can refer to the instructions below to configure scopes:

1. Go to Google Admin console, and then navigate to **Security** > **Access and data control** > **API controls**.
2. Click **MANAGE DOMAIN WIDE DELEGATION**.
3. Click **Add new**.
4. Add the client ID and OAuth scopes. After you finish the configuration, click **AUTHORIZE**.

Note the following:

- To get the client ID, you can open the private key file (downloaded when you Create a Service Account), or go to the **Credentials** page.
- The configured scopes should be the same as the scopes added to the app. You can add required permission scopes to a custom Google app by referring to IBM Storage Protect for Cloud Google Workspace.

  Note: You must add the permission scopes that are exactly required. For example, the **https://www.googleapis.com/auth/drive.readonly** scope cannot be replaced by the **https://www.googleapis.com/auth/drive** scope. It is recommended that one custom Google app is configured for one service only.

After you finish configuring scopes for the custom Google app, go to IBM Storage Protect for Cloud and navigate to **Management** > **App management** to create an app profile and consent to the custom Google app. For more details, refer to the Consent to Custom Apps section.

Consent to Custom Apps

Refer to the following instructions to configure app profiles for custom apps and consent to custom apps.

1. Navigate to **Management** > **App management**, and then click **Create**.
2. **Select services** – Select a tenant and select services for which you want to create app profiles. Click **Next**.
3. **Choose setup method** – Select the **Custom mode** option. Note that the **Custom mode** option only appears when the selected services support custom apps.
4. **Consent to apps** – Refer to the instructions in the following sections to consent to custom apps.

Note: If multi-factor authentication (MFA) is enabled on a Microsoft 365 account, this account can still be used to consent to app profiles. For apps with delegated permissions, the related app profiles need to be re-authorized if MFA is enabled on the consent users' Microsoft 365 accounts after they have given consent to the app profiles.

Consent to a Custom Azure App

When you consent to a custom Azure app with application permissions only, complete the following settings:

1. **App profile name** – Enter a name for the profile.
2. **Application ID** – Enter the application ID of the application that has been created in Azure by referring to the"Create a Custom Azure App" on page 40 .
3. **Certificate file (.pfx)** – Click **Browse** and select your app's private certificate (the .pfx file).

   Note: Ensure this .pfx file is paired with the .cer/.crt file uploaded to Microsoft Entra ID when your organization creates this custom app. If your organization does not have any certificates, you can create self-signed certificates by referring to "Appendix F - Prepare a Certificate for the Custom Azure App" on page 179.
4. **Certificate password** – Enter the password of the certificate.
5. Click **Finish**.
6. If you want to manage Exchange mailboxes and settings / Security and distribution group objects / Microsoft 365 Defender settings, you need to assign the **Exchange Administrator** role to the app. For additional details on assigning the role, refer to "How to Assign the Exchange Administrator Role to an App?" on page 46

Consent to a Custom Azure App with Delegated Permissions

When you consent to a custom Azure app with both application and delegated permissions, complete the following settings:

1. **App profile name** – Enter a name for the profile.
2. **Application ID** – Enter the application ID of the application that has been created in Azure by referring to the "Create a Custom Azure App" on page 40.
3. **Certificate file (.pfx)** – Click **Browse** and select your app's private certificate (the .pfx file).

   Note: Ensure this .pfx file is paired with the .cer/.crt file uploaded to Microsoft Entra ID when your organization creates this custom app. If your organization does not have any certificates, you can create self-signed certificates by referring to "Appendix F - Prepare a Certificate for the Custom Azure App" on page 179.
4. **Certificate password** – Enter the password of the certificate.
5. Click **Consent**.
6. **Consent method** – Choose a consent method between **Administrator consent** and **User consent**. If you want to consent to the app with a non-Administrator account in your Microsoft tenant, choose **User consent** and, note the following:

   a. Ensure that your organization has granted admin consent to the app in Microsoft Entra ID. You can refer to the steps below to grant admin consent to an app:

      i) Log in to Microsoft Entra admin center (or Microsoft Azure portal).

      ii) Navigate to **Identity** > **Applications** > **App registrations** (or **Microsoft Entra ID** > **App registrations**)

      iii) Click the app, and then click **API permissions** in the left menu.

      iv) Click **Grant admin consent for [Tenant name]**.

   b. Refer to the following information to prepare required users who consent to the apps:

      - To scan and manage **Power Platform** objects, the user who provides consent must have the following required license/role:
        - The **Power Platform Administrator** role must be assigned to the user who provides consent for the app profiles for scanning Environments, Connections, Power Apps, Solutions, Power Automate, or Copilot Studio objects.
        - The **Power BI license** and **Fabric Administrator** role must be assigned to the user who provides consent for the app profiles for scanning Power BI objects.
7. Click **Continue to consent**.
8. If you want to manage Exchange mailboxes and settings / Security and distribution group objects / Microsoft 365 Defender settings, you need to assign the **Exchange Administrator** role to the app. For additional details on assigning the role, refer to "How to Assign the Exchange Administrator Role to an App?" on page 46

Consent to a Custom Google App

When you consent to a custom Google app, complete the following settings:

1. **App profile name** – Enter a name for the profile.
2. **Admin account** – Enter the name of the Admin account that has the required privileges/roles. Refer to the table below for the required privileges/roles that vary with different features. For additional details, refer to the **Manage Admin Roles and Privileges** section below.

Service	Function/Module	Admin account permissions
IBM Storage Protect for Cloud Google Workspace	Users services protection (including Gmail, Drive, Calendar, Contacts, and Chat)	Admin API privileges: **Users > Read**
	Shared drives protection	Admin console privileges: **Drive and Docs > Settings**

Service	Function/Module	Admin account permissions
	Google Vault protection	Admin console privileges: • **Google Vault > View All Matters** • **Google Vault > Manage Exports** • **Google Vault > Manage Holds**
	Google Classroom protection	**Super Admin**

3. **Google service account** – Enter the service account email address.

   Note: You can get the email address from the **client_email** value in the downloaded private key file. For details, refer to Step 2: Create OAuth Credentials > Service Account Creation.

4. **Private key** – Enter the private key.

   Note: Make sure the private key starts with -----**BEGIN PRIVATE KEY**----- prefix and ends with the \n -----**END PRIVATE KEY**-----\n suffix.

Manage Admin Roles and Privileges

Refer to the instructions below to manage roles and privileges for an Admin account:

Note: The user must have the Super Admin role to manage roles and privileges.

1. Go to the Google Admin console.
2. Click **Manage** in the **Users** section.
3. Click the user you want to assign the roles. The user details page appears.
4. In the **Admin roles and privileges** section, click the Expand ( ) button.
5. If you want to assign a pre-built role such as **Super Admin** or **User Management Admin** to the account, toggle the switch to **Assigned** in the **Assigned state** column.
6. Click **SAVE**.
7. If you want to create a custom role with required privileges, click **Create custom role**.
8. Click **Create new role**.
9. The **Create role** page appears. Enter a role name and click **Continue**.
10. In the **Select Privileges** section, select required privileges by referring to the **Admin account** table above.
11. Click **Continue**.
12. Click **Create role**. The custom role is successfully created.
13. You can assign the custom role to the Admin account.

How to Assign the Exchange Administrator Role to an App?

About this task

If you create app profiles for the following apps and you want to manage Exchange mailboxes and settings / Security and distribution group objects / Microsoft 365 Defender settings, you need to go to Microsoft Entra admin center (or Microsoft Azure portal) to assign the **Exchange Administrator** role to the apps:

App profile type (in IBM Storage Protect for Cloud)		App name (in Microsoft Entra ID)
Classic mode	Microsoft 365 (All permissions)	IBM Storage Protect for Cloud Administrator for Microsoft 365
Modern mode	IBM Storage Protect for Cloud Microsoft 365(All permissions)	IBM Storage Protect for Cloud for Microsoft 365
	IBM Storage Protect for Cloud Microsoft 365(Exchange permissions)	IBM Storage Protect for Cloud Administrator for Exchange
Custom mode	Custom Azure apps of the following services: IBM Storage Protect for Cloud Microsoft 365	[custom app name] You can also get its application ID in the app profile detail page.

Note: To use IBM Storage Protect for Cloud Microsoft 365 , the **Exchange Administrator** role must be assigned to the related app.

Procedure

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

1. Log in to the 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.
3. On the **Roles and administrators page**, search the **Exchange Administrator** role, and then click **Exchange Administrator**.
4. On the **Assignments** page that opens, click **Add assignments**.
5. On the **Add assignments** page, click the button to select a member.
6. You can enter an app name (or application ID) in the search box to search for the app to which you want to assign the role.

   Note: The **Application ID** information is displayed on the **App profile details** page in IBM Storage Protect for Cloud > **Management** > **App management**.
7. Select the app and click **Select** 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.

Re-authorize an App Profile

About this task

Re-authorize app profiles for Microsoft/Salesforce tenants in the following scenarios:

- The app profiles which are in the **Invalid** status must be re-authorized.
- 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 Microsoft tenants, there are additional scenarios that require app profiles re-authorization. See more details in Microsoft Tenant.

Google tenants cannot re-authorize related app profiles in IBM Storage Protect for Cloud. To add new permissions to a Google app, navigate to the Google Admin console > **Apps** > **Google Workspace Marketplace apps** > **App list**, click the app, and click **Grant access** to add the required permissions to the app.

Microsoft Tenant

Refer to the instructions below to re-authorize app profiles for Microsoft tenants.

- If your tenant has an app with delegated permissions, note the following:
  - 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 **Invalid**. 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.
  - For an app with delegated permissions, the related app profile needs to be re-authorized when its consent user's Microsoft 365 account is in any of the following scenarios:
    - If multi-factor authentication (MFA) is enabled on the consent user's Microsoft 365 account after the user has given consent to the custom app profile, the app profile needs to be re-authorized.
    - If the consent user's Microsoft 365 account is unavailable (e.g. the password was changed or the user left the company), the app profile will be **Invalid** and need to be re-authorized.

      Note: To help you easily find the apps with delegated permissions, the related IBM default apps are marked with the icons as below:

    - Apps that utilize both application and delegated API permissions are marked with the hybrid ( ) icon.
    - Apps that have delegated API permissions only are marked with the purebred ( ) icon
- 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.
- 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 Power BI**
  - **Protect Power Automate / Power Apps**
  - **Restore Planner task comments**

    Note: If your tenant is using a scan profile configured in the IBM Storage Protect for Cloud classic UI for protecting Planner data via IBM Storage Protect for Cloud Microsoft 365, you can follow the steps below to update the method of Planner data protection.

    1. In IBM Storage Protect for Cloud, refer to the instructions below to prepare an app profile based on your scenario:
       - If you want to use a classic mode app, create/re-authorize an app profile of the **Microsoft 365 (All permissions)** app type, and ensure that the Microsoft Graph permission **Tasks.ReadWrite.All** has been added to the app.
       - If you want to use a modern mode app, create an app profile of the **IBM Storage Protect for Cloud Microsoft 365 (All permissions)** app type.
       - If you want to use a custom mode app, create an app profile of the **Custom Azure app** type and ensure that the Microsoft Graph permission **Tasks.ReadWrite.All** has been added to the custom app.
    2. Edit the scan profile and save it.

       Note: For a scan profile configured in the IBM Storage Protect for Cloud classic UI for protecting Planner data, the authentication method in the scan profile is a service account profile or app profile with an additional delegated app profile. In the IBM Storage Protect for Cloud new UI, once this kind of scan profile has been edited, the authentication method will be updated to the app profile. Thus, you can edit and save a scan profile even without any changes.
    3. Go to IBM Storage Protect for Cloud Microsoft 365 to check the backup setting and ensure that the option for Planner data backup has been enabled.
- The following apps support user consent, and you can re-authorize these apps with a non Administrator account in your Microsoft tenant. When you re-authorize one of the following apps, you can choose a consent method between **Administrator consent** and **User consent**.

  Note: When you re-authorize the other apps that are not in the table below, refer to Administrator Consent.

Service	App type (in IBM Storage Protect for Cloud
IBM Storage Protect for Cloud Azure VMs, Storage, and Entra ID	IBM Storage Protect for Cloud Azure
	Delegated App
	IBM Storage Protect for Cloud for Azure DevOps

Service	App type (in IBM Storage Protect for Cloud
IBM Storage Protect for Cloud Microsoft 365	Delegated App
IBM Storage Protect for Cloud Microsoft 365	Viva Engage
IBM Storage Protect for Cloud Azure VMs, Storage, and Entra ID IBM Storage Protect for Cloud Microsoft 365	Custom app with delegated permissions ("API Permissions Required by Custom Apps" on page 71)

Note: : You do not need any permissions or Microsoft licenses other than those listed in this guide.

Administrator Consent

Refer to the following instructions to re-authorize an app profile with a **Microsoft 365 Global** or a **Privileged Role Administrator** account.

1. Select an app profile and click **Re-authorize**.
2. Note the following when you re-authorize different app profiles:
   - When you re-authorize an IBM Storage Protect for Cloud default service app for Viva Engage, you can also consent to the app with an **Engage Administrator** (**Yammer Administrator** in Microsoft Entra ID) account.
   - When you re-authorize an app profile for the **IBM Storage Protect for Cloud Microsoft 365** service, note the following:
     – When consenting to the **IBM Storage Protect for Cloud Microsoft 365 delegated app**, you also need to choose the functions that will use this app. The user who consents to the app must have the **Microsoft 365 Global Administrator** role. For details, refer to the Required Permissions of Microsoft Delegated App section in the IBM Storage Protect for Cloud Microsoft 365 user guide.
     – When consenting to a Viva Engage app profile used by IBM Storage Protect for Cloud Microsoft 365, the consent user must have the **Verified Admin** role and the **Yammer Administrator** role with the Viva Engage product license.
   - When you re-authorize an app profile for a **Custom Azure app** / **Custom Azure app with delegated permissions** app, refer to the following instructions:
     a. **Application ID** – Enter the application ID of the custom app. To keep using the current app, you can get its application ID in the app profile detail page. If you want to change to another app, enter the application ID of the app that your organization has created. For additional details on creating an app, refer to "Create a Custom Azure App" on page 40.
     b. **Certificate file (.pfx)** – Click **Browse** and select your app's private certificate (the .pfx file).

        Note: Ensure this .pfx file is paired with the .cer/.crt file which is uploaded for this custom app in Microsoft Entra ID. If your organization does not have any certificates, you can create self-signed certificates by referring to "Appendix F - Prepare a Certificate for the Custom Azure App" on page 179.
     c. **Certificate password** – Enter the password of the certificate.
     d. Click **Consent**.

User Consent

The following apps support user consent, and you can re-authorize these apps with a non Administrator account in your Microsoft tenant.

Note: When you re-authorize the other apps that are not in the table below, refer to Administrator Consent.

Service	App type (in IBM Storage Protect for Cloud)	App name (in Microsoft Entra ID)
IBM Storage Protect for Cloud Azure VMs, Storage, and Entra ID	IBM Storage Protect for Cloud Azure	IBM Storage Protect for Cloud Azure
	Delegated App	IBM Storage Protect for Cloud - Delegated App
	IBM Storage Protect for Cloud Azure DevOps	IBM Storage Protect for Cloud Azure DevOps
IBM Storage Protect for Cloud Microsoft 365	Delegated App	IBM Storage Protect for Cloud Microsoft 365 - Delegated App
IBM Storage Protect for Cloud Microsoft 365	Viva Engage	IBM Storage Protect for Cloud Administration for Viva Engage
IBM Storage Protect for Cloud Microsoft 365 IBM Storage Protect for Cloud Azure VMs, Storage, and Entra ID	Custom app with delegated permissions (API Permissions Required by Custom Apps)	[custom app name] You can also get its application ID in the app profile detail page.

Before you choose the **User consent** method, complete the following preparations:

1. Ensure that your organization has granted admin consent to the app in Microsoft Entra ID. You can refer to the steps below to grant admin consent to an app:
   a. Log in to Microsoft Entra admin center (or Microsoft Azure portal).
   b. Follow the instructions below to grant admin consent to an IBM Storage Protect for Cloud app or a custom app:
      - To grant admin consent to an IBM Storage Protect for Cloud app, navigate to **Microsoft Entra ID** > **Enterprise applications**, click the app, click **Permissions** in the **Security** menu, and then click **Grant admin consent for [Tenant name]**.
      - To grant admin consent to a custom app, navigate to **Microsoft Entra ID** > **App registrations**, click the app, click **API permissions** in the **Manage** menu, and then click **Grant admin consent for [Tenant name]**.
2. Refer to the following information to prepare required users who consent to the apps:
   - To scan and manage **Power Platform** objects, the user who provides consent must have the following required license/role:
     – The **Power Platform Administrator** role must be assigned to the user who provides consent for the app profiles for scanning Environments, Connections, Power Apps, Solutions, Power Automate, or Copilot Studio objects.
     – The **Power BI license** and **Fabric Administrator** role must be assigned to the user who provides consent for the app profiles for scanning Power BI objects.

To re-authorize an app profile with the **User consent** method, refer to the steps below:

1. Select an app profile and click **Re-authorize**.
2. Note the following when you re-authorize different app profiles:
   - When you re-authorize an app profile for 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.
     a. **Application ID** – Enter the application ID of the custom app. To keep using the current app, you can get its application ID in the app profile detail page. If you want to change to another app, enter the application ID of the app that your organization has created. For additional details on creating an app, refer to “Create a Custom Azure App” on page 40.

b. **Certificate file (.pfx)** – Click **Browse** and select your app's private certificate (the .pfx file).

Note: Ensure this .pfx file is paired with the .cer/.crt file which is uploaded for this custom app in Microsoft Entra ID. If your organization does not have any certificates, you can create self-signed certificates by referring to"Appendix F - Prepare a Certificate for the Custom Azure App" on page 179 .

c. **Certificate password** – Enter the password of the certificate.

3. Select the **User consent** option.
4. Click **Continue to consent**.

Salesforce Tenant

To grant consent to a **Salesforce** / **Salesforce sandbox** app, follow the steps below:

1. Select the app profile and click **Re-authorize**.
2. In the **Re-authorize** window, click **Continue to consent**.
3. Sign in with a Salesforce account that has the System Administrator profile or another profile with the same permissions.

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 in IBM Storage Protect for Cloud, the **IBM Storage Protect for Cloud Microsoft 365 Administrator for Microsoft 365** app will be automatically set up in your Microsoft Entra ID. The table below lists the permissions that should be accepted when you authorize the IBM Storage Protect for Cloud Administrator for Microsoft 365 app.

API	Permission	Type	Purpose
SharePoint/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 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	Purpose
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.
	Tasks.ReadWrite.All (Read and write all users' tasks and task lists)	Application	Backup up and restore Planner data.
	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	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	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 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	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 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 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	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 Administraor for SharePoint** app in your Microsoft Entra ID.

  Note: The **Microsoft 365 (SharePoint Online permissions)** app profile is unsupported to create new, but you can re-authorize the existing app profile in your **IBM Storage Protect for Cloud** tenant when necessary.

  The table below lists the permissions that should be accepted when you authorize the **IBM Storage Protect for Cloud Administrator for SharePoint** app.

API	Permission	Type	Purpose
SharePoint/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 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.

API	Permission	Type	Purpose
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.

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 Administrator for Exchange** app in your Microsoft Entra ID.

  Note: The **Microsoft 365 (Exchange permissions)** app profile is unsupported to create new, but you can re-authorize the existing app profile in your IBM Storage Protect for Cloud Services tenant when necessary.

  The table below lists the permissions that should be accepted when you authorize the **IBM Storage Protect for Cloud Administrator for Exchange** app.

API	Permission	Type	Purpose
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.

Viva Engage

The **Viva Engage** app profile can be used by the following services:

- IBM Storage Protect for Cloud Microsoft 365

When you create a **Viva Engage** app profile in **IBM Storage Protect for Cloud Viva Engage** app will be automatically set up in your Microsoft Entra ID. The account used to consent to the app must be **Microsoft 365 Global Administrator**, **Privileged Role Administrator**, or **Engage Administrator** (refers to the **Yammer Administrator** in Microsoft Entra ID) account that is in the same tenant. account that is in

the same tenant. The table below lists the permissions that should be accepted when you authorize the **IBM Storage Protect for Cloud Viva Engage** app.

Note: When creating a Viva Engage app profile used by IBM Storage Protect for Cloud Microsoft 365, the consent user must be a **Microsoft 365 Global Administrator** with the Viva Engage product license. To re-authorize the Viva Engage app, the consent user must have the **Verified Admin** role and the **Yammer administrator** role with the Viva Engage product license.

The table below lists the permissions that should be accepted when you authorize the **IBM Storage Protect for Cloud Administration forViva Engage** app.

API	Permission	Type	Purpose
Microsoft Graph	User.Read (Sign in and read user profile)	Delegated	Support signing into IBM Storage Protect for Cloud with Microsoft 365 accounts.
Yammer	access_as_user (Read and write to the Yammer platform [preview])	Delegated	To access the Viva Engage platform on behalf of the signed-in user.
	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 the **Delegated app**, the **IBM Storage Protect for Cloud Delegated App** will be automatically setup up in your Microsoft Entra ID. Refer to the following sections to see the delegated permissions that should be accepted when you authorize the **IBM Storage Protect for Cloud Delegated App** .

IBM Storage Protect for Cloud Azure VMs and Storage

API	Permission	Purpose
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

When consenting to the IBM Storage Protect for Cloud Microsoft 365 delegated app profile, the consent user must have the Microsoft 365 Global Administrator role. For details, refer to the Required Permissions of Microsoft Delegated App section in the IBM Storage Protect for Cloud Microsoft 365 user guide.

API	Permission	Purpose
Microsoft Graph	openid (S ign users in)	Allows to authenticate users by retrieving their consent.
	profile (View users' basic profile)	Retrieves users' profile information.
	offline_access (Maintain access to data you have given it access to)	Maintains access over an extended period without requiring the user to re-authorize frequently
	Group.ReadWrite.All (Read and write all groups)	Retrieves the conversation thread.
	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.
	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.
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 Services

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 Dynamics

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

Dynamics Customer Engagement

The **Dynamics Customer Engagement** app profile can be used by the IBM Storage Protect for Cloud Dynamics service. The **Dynamics Customer Engagement** app profile is for the **IBM Storage Protect for Cloud Dynamics Customer Engagement** app. 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	Purpose
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.

Dynamics Unified Operations

The **Dynamics Unified Operations** app profile can be used by the IBM Storage Protect for Cloud Dynamics 365 service.

The **Dynamics Unified Operations** app profile is for the **IBM Storage Protect for Cloud Administration for Dynamics Unified Operations** app. The table below lists the permissions that should be accepted when you authorize the **IBM Storage Protect for Cloud Administration for Dynamics Unified Operations** app.

API	Permission	Type	Purpose
Microsoft Graph	User.Read (Sign in and read user profile)	Delegated	Retrieve your Microsoft 365 tenant information.
	Directory.Read.All (Read directory data)	Application	
	Group.Read.All (Read all groups)	Application	

API	Permission	Type	Purpose
Dynamics ERP	AX.FullAccess (Access Dynamics AX online as organization users)	Delegated	IBM Storage Protect for Cloud Dynamics 365 uses it to back up and restore records in Dynamics Unified Operations.
	Connector.FullAccess (Access Dynamics Connector Service APIs)	Application	
	CustomService.FullAccess (Access Dynamics AX Custom Service)	Delegated	
	Odata.FullAccess (Access Dynamics AX data)	Delegated	

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 IBM Storage Protect for Cloud Google Workspace functionalities work.

Scope	Purpose	Last update
https://mail.google.com/	Back up emails and labels in Gmail for future recovery.	
https://www.googleapis.com/auth/drive	Back up folders and files under My Drive and shared drives for future recovery.	
https://www.googleapis.com/auth/calendar	Back up calendars and events from Google Calendar for future recovery.	
https://www.googleapis.com/auth/contacts.other.readonly	Back up **Other contacts** data.	
https://www.googleapis.com/auth/contacts	Back up contact groups and contacts from Google Contacts for future recovery.	
https://www.googleapis.com/auth/admin.directory.group.readonly	Retrieve groups in your domain.	
https://www.googleapis.com/auth/admin.directory.user.readonly	Retrieve users in your domain.	
https://www.googleapis.com/auth/admin.directory.customer.readonly	Retrieve organization information to segment operations and settings for different organization and isolate customer tenants.	

Scope	Purpose	Last update
https://www.googleapis.com/auth/admin.reports.usage.readonly	Retrieve organization subscription usage for backup admins to monitor their subscription in the app.	
https://www.googleapis.com/auth/admin.directory.orgunit.readonly	Retrieve groups to add users to the app through organization units.	
https://www.googleapis.com/auth/userinfo.email	Retrieve user email information when users log in to the app.	
https://www.googleapis.com/auth/userinfo.profile	Retrieve users' publicly available properties to identify users through our application.	
https://www.googleapis.com/auth/apps.licensing	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	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	Back up and restore properties of labels on files in Drives.	Newly added in January 2023
https://www.googleapis.com/auth/classroom.courses	Back up and restore classes.	Newly added in August 2023
https://www.googleapis.com/auth/classroom.announcements	Back up and restore announcements in classes.	Newly added in August 2023
https://www.googleapis.com/auth/classroom.coursework.me	Back up classwork in classes.	Newly added in August 2023
https://www.googleapis.com/auth/classroom.coursework.students	Restore classwork in classes.	Newly added in August 2023
https://www.googleapis.com/auth/classroom.courseworkmaterials	Back up and restore classwork materials.	Newly added in August 2023
https://www.googleapis.com/auth/classroom.rosters	Back up and restore students and teachers in classes.	Newly added in August 2023
https://www.googleapis.com/auth/classroom.profile.emails	Retrieve email addresses in classes.	Newly added in August 2023
https://www.googleapis.com/auth/classroom.topics	Back up and restore topics in classes.	Newly added in August 2023
https://www.googleapis.com/auth/classroom.topics.readonly	Retrieve information of topics.	Newly added in August 2023

Scope	Purpose	Last update
https://www.googleapis.com/auth/classroom.guardianlinks.students	Retrieve guardians of students in classes.	

IBM Storage Protect for Cloud Azure VMs, Storage, and Entra ID

Refer to the following sections to see the permissions that should be accepted when you consent to the corresponding apps.

IBM Storage Protect for Cloud for Azure

When you create a **IBM Storage Protect for Cloud Azure** app profile in IBM Storage Protect for Cloud Azure VMs, Storage, and Entra ID , the IBM Storage Protect for Cloud Azure app will be automatically set up in your Microsoft Entra ID.

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

API	Permission	Type	Purpose	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.	
	AuditLog.Read.All (Read all audit log data)		Allows the app to read and query your audit log activities, without a signed-in user.	January 2024 release
	DeviceManagementScripts.ReadWrite.All (Read and write Microsoft Intune Scripts)		Allows the app to read and write Microsoft Intune device compliance scripts, device management scripts, device shell scripts, device custom attribute shell scripts and device health scripts, without a signed-in user.	October 2025
	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	Enables the app to access BitLocker keys for the signed-in user's devices, allowing it to read the recovery key	October 2023
	BitLockerKey.Read.All (Read BitLocker keys)	Application	Enables the app to access BitLocker keys for the signed-in user's devices, allowing it to read the recovery key	January 2024

API	Permission	Type	Purpose	Last update
	Policy.Read.All (Read your organization's policies)	Application	Allows the app to read all your organization's policies without a signed in user.	May 2025
	Organization.Read.All (Read organization information)		Retrieves all the organizational brandings.	November 2022
	Policy.ReadWrite.AuthenticationMethod (Read and write all authentication method policies)		Retrieves all the authentication method policies and configurations.	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.	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.	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.	November 2022
	DeviceManagementConfiguration.ReadWrite.All (Read and write Microsoft Intune device configuration and policies)		Allows the app to read and write properties of Microsoft Intune-managed device configuration and device compliance policies and their assignment to groups, without a signed-in user.	March 2024
	DeviceManagementApps.ReadWrite.All (Read and write Microsoft Intune apps)		Allows the app to read and write the properties, group assignments and status of apps, app configurations and app protection policies managed by Microsoft Intune, without a signed-in user.	March 2024
	DeviceManagementApps.ReadWrite.All (Read and write Microsoft Intune apps)	Delegated	Allows the app to read and write the properties, group assignments and status of apps, app configurations and app protection policies managed by Microsoft Intune, without a signed-in user.	April 2024
	DeviceManagementRBAC.Read.All (Read Microsoft Intune RBAC settings)	Application	Allows the app to read the properties relating to the Microsoft Intune Role-Based Access Control (RBAC) settings, without a signed-in user.	June 2024
	Domain.Read.All (Read domains)	Application	Allows the app to read all domain properties without a signed-in user.	May 2025
Office 365 Exchange Online	Exchange.ManageAsApp (Manage Exchange as Application)	Application	Allows the backup and restore of the distribution lists in MFA-enabled tenants.	November 2022

IBM Storage Protect for Cloud for Azure DevOps

When you create a **IBM Storage Protect for Cloud for Azure DevOps** app profile in IBM Storage Protect for Cloud, the **IBM Storage Protect for Cloud for Azure DevOps** app will be automatically set up in your Microsoft Entra ID.

The table below lists the permissions that should be accepted when you authorize the **IBM Storage Protect for Cloud for Azure DevOps** app.

API	Permission	Type	Purpose
Azure DevOps	user_impersonation (Have full access to Visual Studio Team Services REST APIs)	Delegated	Have full access to Visual Studio Team Services REST APIs.
Microsoft Graph	User.Read.All (Read all user's full profile)	Delegated	Allows the app to read the full set of profile properties, reports, and managers of other users in your organization, on behalf of the signed-in user.

IBM Storage Protect for Cloud Azure VMs, Storage, and Entra ID Azure AD B2C

When you create a **IBM Storage Protect for Cloud Azure VMs, Storage, and Entra ID Azure AD B2C**app profile in IBM Storage Protect for Cloud, the **IBM Storage Protect for Cloud Azure VMs, Storage, and Entra ID for Azure AD B2C** app will be automatically set up in your Microsoft Entra ID.

The table below lists the permissions that should be accepted when you authorize the **IBM Storage Protect for Cloud Azure VMs, Storage, and Entra ID for Azure AD B2C** app.

API	Permission	Type	Purpose
Microsoft Graph	IdentityUserFlow.ReadWrite.All (Read and write all identity user flows)	Application	Allows the app to read or write your organization's user flows, without a signed-in user.
	IdentityProvider.ReadWrite.All (Read and write identity providers)	Application	Allows the app to read and write your organization's identity (authentication) providers' properties without a signed-in user
	Application.ReadWrite.All (Read and write all applications)	Application	Allows the app to create, read, update and delete applications and service principals without a signed-in user. Does not allow management of consent grants.
	AuditLog.Read.All (Read all audit log data)	Application	Allows the app to read and query your audit log activities, without a signed-in user.
	Directory.Read.All (Read directory data)	Application	Allows the app to read data in your organization's directory, such as users, groups and apps, without a signed-in user.
	AppRoleAssignment.ReadWrite.All (Manage app permission grants and app role assignments)	Application	Allows the app to manage permission grants for application permissions to any API (including Microsoft Graph) and application assignments for any app, without a signed-in user.

API	Permission	Type	Purpose
	RoleManagement.ReadWrite.Directory (Read and write all directory RBAC settings)	Application	Allows the app to read and manage the role-based access control (RBAC) settings for your company's directory, without a 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)	Application	Allows the app to read and update user profiles without a signed in user.
	UserAuthenticationMethod.ReadWrite.All (Read and write all users' authentication methods)	Application	Allows the application to read and write authentication methods of all users in your organization, without a signed-in user. Authentication methods include things like a user's phone numbers and Authenticator app settings. This does not allow the app to see secret information like passwords, or to sign-in or otherwise use the authentication methods.
	GroupMember.ReadWrite.All (Read and write all group memberships)	Application	Allows the app to list groups, read basic properties, read and update the membership of the groups this app has access to without a signed-in user. Group properties and owners cannot be updated and groups cannot be deleted.
	User.ManageIdentities.All (Manage all users' identities)	Application	Allows the app to read, update and delete identities that are associated with a user's account, without a signed in user. This controls the identities users can sign-in with.

API	Permission	Type	Purpose
	User-Mail.ReadWrite.All (Read and write all secondary mail addresses for users)	Application	Allows the app to read and write secondary mail addresses for all users, without a signed-in user.
	User-Phone.ReadWrite.All (Read and write all user mobile phone and business phones)	Application	Allows the app to read and write the mobile phone and business phones for all users, without a signed-in user.
	User.EnableDisableAccount.All (Enable and disable user accounts)	Application	Allows the app to enable and disable users' accounts, without a signed-in user.

IBM Storage Protect for Cloud Microsoft 365

IBM Storage Protect for Cloud Microsoft 365 (All Permissions)

When you create a **IBM Storage Protect for Cloud Microsoft 365 (All permissions)** app profile in IBM Storage Protect for Cloud,**IBM Storage Protect for Cloud Microsoft 365 (All permissions)** app will be automatically set up in your Microsoft Entra ID.

About this task

The table below lists the permissions that should be accepted when you authorize the **IBM Storage Protect for Cloud Microsoft 365 (All permissions)** app.

API	Permission	Type	Purpose
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.
	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	Retrieve data size directly to improve the efficiency of Subscription 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.

API	Permission	Type	Purpose
	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	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	Back up and restore teams' members.
	TeamsTab.ReadWrite.All (Read and write tabs in Microsoft Teams)	Application	Back up and restore teams' tabs.
	Team.Create (Create teams)	Application	Restore teams.
	TeamsAppInstallation.ReadWriteForTeam.All (Manage Teams apps for all teams)	Application	Back up and restore teams' apps.
	Channel.Create (Create channels)	Application	Restore teams' channels.
	Chat.Read.All (Read all chat messages)	Application	Back up the Teams chat messages.
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.

API	Permission	Type	Purpose
SharePoint/ 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 sites.

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	Purpose
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.

API	Permission	Type	Purpose
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 (SharePoint Permissions)

When you create a **IBM Storage Protect for Cloud Microsoft 365 (SharePoint permissions)** app profile in IBM Storage Protect for Cloud, the **IBM Storage Protect for CloudAdministrator for SharePoint** app will be automatically set up 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 (SharePoint Permissions)** app.

API	Permission	Type	Purpose
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	Purpose
SharePoint/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.

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

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 IBM's default apps, you can configure your tenant’s custom app and create a custom app profile. Refer to the sections below for the permissions required by custom apps.

For the custom app created in your Microsoft 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.

Microsoft Tenant Custom Apps

For the custom app created in your Microsoft 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.

Note: If the **Sites.FullControl.All** SharePoint API permission is not allowed by your organization's security policy, you can add the **Sites.Selected** application permission as a replacement. For more information, see What Should I Do If the Sites.FullControl.All Permission Cannot be Added to My Custom App?

API	Permission	Type	Purpose
Microsoft Graph	Organization.Read.All (Read organization data)	Application	Check the status of app profiles.
	Group.Read.All (Read all groups)	Application	Scan mailboxes, Microsoft 365 Groups, Teams, and Viva Engage communities. Invite users and groups in **User management**
	User.Read.All (Read all users)	Application	Scan mailboxes, Microsoft 365 Groups, Teams, and Viva Engage communities. Invite users and groups in **User management**.
SharePoint/Office 365 SharePoint Online	Sites.FullControl.All (Have full control of all site collections)	Application	Scan SharePoint Online site collections, Project Online site collections, OneDrive, and Microsoft 365 Group team sites.
	User.Read.All (Read user profiles)	Application	Scan OneDrive to retrieve the OneDrive URL of each user from SharePoint user profiles.
Office 365 Exchange Online	full_access_as_app (Use Exchange Web Services with full access to all mailboxes)	Application	Scan Exchange Online Public Folders and in-place archived mailboxes (if necessary).
	Exchange.ManageAsApp (Manage Exchange As Application)	Application	Only required by custom apps of the following services: IBM Storage Protect for Cloud Microsoft 365.

The following services support using a custom Azure app for authentication. The permissions of the custom app vary with the different cloud services your tenant is using.

Click the links listed below to view the required permissions for your services.

- IBM Storage Protect for Cloud Azure VMs, Storage, and Entra ID

- IBM Storage Protect for Cloud Microsoft 365

Google Tenant Custom Apps

For Google tenants, using a default service app may encounter throttling issues caused by Google quota limits. If performance is a concern, consider configuring a custom Google app for your organization.

Click the links listed below to view the required permissions for your services.

- IBM Storage Protect for Cloud Google Workspace custom app.

Chapter 10. Manage Auto Discovery

The **Auto discovery** feature can automatically discover objects in your Microsoft or Google environments 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 76
  - “Auto Discovery for Google Workspace” on page 78
  - “Auto Discovery for Power Platform” on page 80

  Note:

  - The auto discovery for Microsoft 365 / Google Workspace / Power® Platform is 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 35.
  - 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. If you want to export the scan profile configuration, click the more actions (•••) button, and then click **Export configuration**. 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.
- To delete a scan profile, select the scan profile and click **Delete**. A pop-up window appears asking for your confirmation. To define how to deal with the scanned objects and configured custom containers, select a resolution from the following:
  - **Delete the objects and custom containers along with the profile**

    Note: The deletion only applies to scanned objects and configured custom containers. The default containers cannot be deleted.
  - **Keep the objects and custom containers in the system**

  Click **Confirm**.

© Copyright IBM Corp. 2022, 2024

- **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 83.
- **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 113 .
- **Export configuration** – To download a copy of a scan profile's configuration, select the scan profile and click **Export configuration**.

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 75.

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. For additional details on which app profiles can support to scan the Microsoft 365 objects, refer to "Which App Profiles Can Scan Microsoft 365 Objects?" on page 11

   Note:

   - The tenant cannot be changed when you edit a scan profile.
   - The Microsoft **365 Group** / Microsoft **Team** / **Viva Engage community** object type includes group team sites and group mailboxes.
   - The **Security and distribution group** object type includes security groups, mail-enabled security groups, distribution lists, and dynamic distribution lists.
   - For Viva Engage communities, only the ones with connected Groups turned on can be managed in Auto discovery.
   - For an orphaned user that no longer exists in your organization, this user's OneDrive is regarded as an orphaned OneDrive. If you want to include orphaned OneDrive in auto discovery scans, first contact IBM Software Support to turn on the switch in the backend.
   - 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 and request the **Public Folders** module be added to your enterprise IBM Storage Protect for Cloud Microsoft 365 tenant. 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.

– If your tenant purchased several modules in the enterprise subscription of IBM Storage Protect for Cloud Microsoft 365, and also has subscriptions to one or more other IBM Storage Protect for Cloud Microsoft 365, all object types will be available to you. However, if the **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. Except for IBM Storage Protect for Cloud Microsoft 365, all IBM Storage Protect for Cloud Microsoft 365 regard Project sites as normal SharePoint sites, and auto discovery will scan Project sites as normal SharePoint sites.

Click **Next** to proceed.

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.
   - **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.

     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.
   - **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 may affect the efficiency of the scan.
   - **Scan archived site collections** – This setting appears when the **SharePoint site** or **Project site** object type is included in the scan scope. This setting is disabled by default. If you want to scan archived sites, turn on this toggle.
   - **Scan Team sites (no Microsoft 365 Groups) into SharePoint sites containers** – This setting appears when the **SharePoint site** object type is included in the scan scope. With this setting enabled, the Team sites (including SharePoint classic and modern team sites) without a Group/Team connected will be scanned into **SharePoint site** containers. Note the following:

     – If this setting is not enabled, there is no effect on the modern team sites without a Group/Team connected as they can still be scanned into **SharePoint site** containers. However, without this setting enabled, the classic team sites cannot be scanned into any containers.

     – After you enable this setting, it will work on the Team sites that have been created without a Group/Team or may be orphaned Team sites that remain due to retention policies even after the Group/Team objects are no longer present. If there are a large amount of sites, the scan job may take a few more minutes.
   - **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.

   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** 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 **Create 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 137.

  – To add a criterion, click the add (+) button. To delete a rule, click the delete (×) button.

  – 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.

  Note: The rules are executed sequentially from top to bottom, for example, ((1 And 2) Or 3).

  e. Click **Add** at the 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 (···) button, and then click **Edit** or **Remove**.

4. Click **Next** to proceed, or click **Previous** to go back to the previous page.
5. 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 75.

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.

   The table below lists the services which can scan Google objects:

   Note: For Google tenants, using a modern mode service app may encounter throttling issues caused by Google quota limits. It is a recommended choice to configure a custom Google app for your organization.

Service	Required permissions	Scan object types
IBM Storage Protect for Cloud Google Workspace	Custom mode app: IBM Storage Protect for Cloud Google Workspace custom app	Google user Shared drive Google Classroom Vault matter
	Modern mode app: IBM Storage Protect for Cloud Google Workspace	Google user Shared drive Google Classroom

   Note: For Google users, the **Suspended** users and **Archived** users are not included in the scan scope.

   Click **Next** to proceed.
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 115.

   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** - Select a container from the drop-down list. If necessary, click **Create container** to create a new container. For details on configuring containers, see “Manage Containers” on page 82.
     c. **Rule** - 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. **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 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 137.

   – To add a criterion, click the add (+) button, and to delete a rule, click the delete (✕) button.

   – 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.

   Note: The rules are executed sequentially from top to bottom, for example, ((1 And 2) Or 3).

e. Click **Add** at the 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 (...) button, 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 75.

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.

   The table below lists the services and apps which can scan Power Platform objects:

Service	App type	Scan object types	Required license/role
IBM Storage Protect for Cloud Microsoft 365	delegated app	Power App, Power Automate, and Power BI	The **Power Platform Administrator** role must be assigned to the consent user of the app profiles for scanning Environments, Connections, Power Apps, Solutions, or Power Automate objects. The **Power BI license** and **Fabric Administrator** role must be assigned to the consent user of the app profiles for scanning Power BI objects.

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.
   - **Scan personal workspaces**(for Power BI only) – If you want to scan personal workspaces, turn on this toggle.
   - **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 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 **Create container** to create one. For details on configuring containers, refer to "Manage Containers" on page 82
     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 137.
- To add a criterion, click the add (+) button. To delete a rule, click the delete (×) button.
- 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.

  Note: The rules are executed sequentially from top to bottom, for example, ((1 And 2) Or 3).

e. Click **Add** at the 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. 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 (...) button, 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 (orphaned OneDrive cannot be imported)
  - SharePoint site
  - Microsoft 365 Group / Microsoft Team / Viva Engage 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 83.
- **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 remove only 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 SharePoint site or Microsoft 365 user objects, configure the following additional settings:
   - **How would you like to handle the imported object users in auto discovery scan jobs?**
     The default setting is **Ignore the scan rules and keep the objects in their original containers**. With this option selected, when the batch imported objects 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 objects to the new containers based on the scan rules**.
   - **How would you like to handle the imported objects in batch import jobs?**
     The default setting is **Move the objects to the new containers selected in the batch import job**. With this option selected, the objects 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 the objects in their original containers**.
6. If you want to include channels when importing Teams, select the **Include channels when importing** checkbox.
7. Click **Import** to import the objects into the selected container in batch, or click **Cancel** to close the pop-up window without importing any objects.

   Note: When Viva Engage communities are imported to containers, the Viva Engage community IDs are not retrieved. When you use IBM Storage Protect for Cloud Microsoft 365 to manage Viva Engage 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.
- **Filter** – Set a filter to view job results 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 **Scan profile** or **Status** criteria.

3. Click **Apply**

- **Stop** – If you want to stop a scan job at the **In progress** status, click the actions (•••) button of the job, and then click **Stop** from the drop-down menu. Note that **Batch import** in progress jobs cannot be stopped.
- **View details** – To view details of a job, you can click the job ID, or you can click the actions (•••) button of the job and click **View details** from the drop-down menu.

  For the scan jobs performed after the August 2024 release, when you view details of jobs at the **Finished** / **Finished with exception** status, you can have an overview of the objects' scan results from the **Number of objects** table. You can also click **Export job report** on the upper-right corner of the page to download the job report.
- **Export job report** – To download job report of a job with the **Finished** / **Finished with exception** status, click the actions () button of the job, and then click **Export job report** from the drop-down menu. In the **Export job report** window, select options from the following to define the scope of the objects' results that you want to cover in the exported job report:

  Note: Due to limitations in Excel: Excel specifications and limits - Microsoft Support, you may see an issue attempting to export job details in excess of 1 million objects. We strongly suggest limiting the scope of these reports to just failed objects.

  - **All** – Select/deselect this checkbox to include/exclude all statuses below.
  - **Exception** – The objects that were not scanned into containers due to minor errors.
  - **Keep** – The objects were kept in their original containers.
  - **Newly added** – The objects that were newly added to containers via this job.
  - **Out of policy** – The objects whose properties didn't match with the rules of their current containers.
  - **Removed** (for scan jobs only) – The objects that were deleted from the source or they were unsupported data types.
  - **Skipped** (for scan jobs only) – The objects that were filtered out by the scan rules configured on containers.
  - **Need to remove** – The objects need to be manually removed from their containers.
  - **Partially added** (for Microsoft 365 Groups only) – Not all data of the objects were scanned into the containers.

  Then, click **Export** to export the job report.

Chapter 11. Manage Users

The following user roles can manage users in IBM Storage Protect for Cloud: tenant owner, service administrators, and customized administrators assigned with the **Management** permission. For more details about the user roles, refer to IBM Storage Protect for Cloud User Roles.

To manage IBM Storage Protect for Cloud users, navigate to **Management** > **User management**. On the **User management** page, refer to the following instructions to manage users/groups:

- **Add** – Click **Add** and refer to the instructions in the “Add Users” on page 87 section.
- **Edit** – Select one user and click **Edit**. Then, refer to the instructions in “Edit User Permissions” on page 90.
- **Delete** – 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** – Select a service administrator in the **Activated** status, and then 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.
- **Reset MFA** – This is available for organizations which has enabled the **MFA policy for local accounts** setting in **Administration** > **Security**. If a user needs to reconfigure their MFA settings, such as when switching to a new device, select the user's local account, ensure it is in the **Activated** status, and then click **Reset MFA**.
- **Deactivate** – 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** – 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, tenant owner and service administrator 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 15, “Configure Advanced Settings,” on page 109

© Copyright IBM Corp. 2022, 2024

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:
  - Connect tenants from the Microsoft/Google/Salesforce platforms
  - 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
  - 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 – Service administrators can perform the same actions as the tenant owner. The following user roles can manage service administrators in IBM Storage Protect for Cloud: tenant owner, service administrators, and customized administrators assigned with the **Management** permission.
- Customized administrator – In IBM Storage Protect for Cloud, customized administrators can be assigned the following permissions: **Management**, **Auto discovery**, and **Administration**, and they can only access the functions for which they have been assigned permissions. When customized administrators go to each cloud service, their permissions are the same as the service administrators.
- Tenant User – 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 following user roles can also manage tenant users in IBM Storage Protect for Cloud: tenant owner, service administrators, and customized administrators assigned with the **Management** permission.

The role permissions for specific services vary by service, to learn more go to “Add Users” on page 87 for information that is specific to your service.

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 or Privileged Role Administrator must consent to the **IBM Storage Protect for Cloud** app first. For details on consenting to the app by the Administrator, refer to “What If Your Tenant Does Not Allow Users to Consent to Apps?” on page 7
   - **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.
   - **Google user/group** – Google users and groups will become IBM Storage Protect for Cloud users. They can use their Google login IDs to log into IBM Storage Protect for Cloud.

     Note: Due to Google API limitations, users in the nested Google groups cannot use their Google 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.
   - **Google tenant** – This option appears if **Google user/group** 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** / Google 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 20.
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**.
   - For **Google user/group**, you can enter the following:

- The usernames of Google users in the format of **someone@example.com**.
- The display names or email addresses of Google groups.

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 in to 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 in to 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 in to IBM Storage Protect for Cloud.
- Guest users cannot log in to IBM Storage Protect for Cloud

4. **Role** – Select the **Tenant User**, **Service Administrator**, or **Customized administrator** role.

   Note: For more details about the user roles, refer to "IBM Storage Protect for Cloud User Roles" on page 86.
5. **Assign permissions to users** (for **Customized administrator**) – If you select the **Customized administrator** role, turn on the toggle of the permission that you want to assign to the users. In IBM Storage Protect for Cloud, you can assign **Management**, **Auto discovery**, and **Administration** permissions to customized administrators, and they can only access the functions for which they have been assigned permissions. When customized administrators go to each cloud service, their permissions are the same as the service administrators.
6. **Assign services and permissions to users** for **Tenant user**) – If you select the **Tenant user** role, turn on the toggle of the service that the users can 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.

Service	Permission
IBM Storage Protect for Cloud Recovery Portal (for Microsoft 365) **Note:** This service is only supported for Microsoft 365 accounts. If you want to grant permissions to many 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, Storage, and Entra ID **Note:** This service is only supported for Microsoft 365 accounts and local accounts.	**Application administrator** In IBM Storage Protect for Cloud Azure VMs, Storage, and Entra ID, application administrators can manage backup and restore settings, perform backup/restore jobs, and view or download job reports.
	Standard user Standard users must be manually added to IBM Storage Protect for Cloud Azure VMs, Storage, and Entra ID account management. The standard users who are added to a security group will have the same permissions as this group has been granted. The standard user can also be added to the Administrators group to have the full control to the application.
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.
	Standard user In IBM Storage Protect for Cloud Dynamics 365, administrators must add standard users to specific security groups to access certain features.

Service	Permission
IBM Storage Protect for Cloud Google Workspace	**Standard User** Standard users must be manually added to IBM Storage Protect for Cloud Google Workspace account management. The standard users who are added to the security groups can access the IBM Storage Protect for Cloud Google Workspace portal to restore/export backup data and view job reports based on their permissions.
	Application administrator In IBM Storage Protect for Cloud Google Workspace, Application administrators can configure backup and restore settings, perform backup and restore, view activity reports, etc. Apart from these, in IBM Storage Protect for Cloud, Application administrators can add Tenant Users and assign IBM Storage Protect for Cloud Google Workspace to them.
IBM Storage Protect for Cloud Recovery Portal Google WorkSpace **Note:** This service is only supported for Google users.	**Standard User** Standard users can access the IBM Storage Protect for Cloud Recovery Portal portal, run jobs to recover Google Workspace 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 Tenant Users.

7. **Available geo location** If your tenant has Multi-Geo Capabilities in IBM Storage Protect for Cloud Microsoft 365, the **Available Geo Location** option 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.
8. **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.
9. 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 in to 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** – This option is only available if **Local user** is selected as the sign-in method when a Microsoft/Google/Salesforce account is added. After the changes have been saved, the user's sign-in method cannot be changed again.
2. **Role** – Select the **Tenant user**, **Service administrator**, or **Customized administrator** role.

Note: For more details about the user roles, refer to "IBM Storage Protect for Cloud User Roles" on page 86.

3. If you select the **Customized administrator** role, turn on the toggle of the permission that you want to assign to the users. In IBM Storage Protect for Cloud, you can assign **Management**, **Auto discovery**, and **Administration** permissions to customized administrators, and they can only access the functions for which they have been assigned permissions. When customized administrators go to each cloud service, their permissions are the same as the service administrators.
4. 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.
5. **Status** – Set the status of the selected user to **Activated** or **Deactivated**.
6. Click **Save** to save your changes, or click **Cancel** to cancel your changes.

Chapter 12. 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 120 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 **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.
- **MFA policy for local accounts** – Choose whether to enable the MFA (multi-factor authentication) policy for the local accounts to sign in to IBM Storage Protect for Cloud. Once enabled, the MFA policy will be applied to all local accounts within your tenant. For the steps of signing into IBM Storage Protect for Cloud with a local account after the MFA policy is enabled, refer to Sign in with a Local Account.

  Note: When you need to reset MFA for a local account, refer to Manage Users.
- **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 **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.
- **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.

  Note: This is not a real-time setting. If you disable this setting, it will take effect after a few minutes.
- **Service providers' access to IBM Storage Protect for Cloud** – This toggle is turned on by default and is only available to the customers of the managed service providers. As a customer, if you do not want to allow the managed service provider to access your IBM Storage Protect for Cloud environment, you can turn off this toggle.
- **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 121.
- **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 122.

© Copyright IBM Corp. 2022, 2024

Enable Trusted IP Address Settings

You can enable trusted IP address settings to only allow users/public APIs 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 **Trusted IP address settings** pane appears on the right of the page.
   - **Enable the settings for users** – Turn on this toggle and configure the following settings:
     - **Trusted IP address range for users for users** – Enter your trusted 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** – The default scope is **All user types**. If you want to apply the configured IP whitelisting to local users only, select the **Only local uses** option.
   - **Enable the settings for public APIs** – Turn on this toggle and enter your trusted IP address range in the **Trusted IP address range for public APIs** text box. If you want to enter multiple IP addresses, separate them with a comma (,).

     Note: The trusted IP address range limits the public APIs which have been added to app profiles registered in IBM Storage Protect for Cloud > **Administration** > **App registrations**. Due to the cache on the Microsoft identity server, it will take up to 15 minutes for the changes on the trusted IP settings to take effect.
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 are an organization with an enterprise subscription and 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 109.
3. Select a location to save the file.

For details on adding ARM VNet IDs, refer to .

Chapter 13. 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.).

AES-256 is used for encryption with keys unique to each tenant (either default keys or Bring-Your-Own-Key).

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 98.
- **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 98 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 98 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 Create a Key Vault in Azure.

Procedure

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

1. Log in to Microsoft Azure portal.
2. Navigate to **Key vaults**.
3. Click the key vault you prepared.
4. Refer to the instructions below based on your scenario:
   - To check Azure RBAC roles assigned on the key vault, follow the steps below:
     a. In the Key Vault's menu, click **Access control (IAM)**.
     b. Go to the **Role assignments** tab.
     c. Use the search bar or filter to find the **Key Vault Crypto User** role.
     d. Check the list of users, groups, or service principals assigned with this role.

© Copyright IBM Corp. 2022, 2024

- To check access policies added on the key vault, follow the steps below:
  a. In the Key Vault's menu, click **Access policies**.
  b. Locate the application that is used for your key vault.
  c. In the **Key permissions** drop-down list, make sure that at least the following operations are selected: **Get**, **Encrypt**, and **Decrypt**.
5. Navigate to the pane for key vault settings and click **Keys**.
6. Click a key and click a version of the key.
7. In the **Permitted operations** section, make sure that at least **Encrypt** and **Decrypt** are selected.
8. Copy the key identifier that resides in the **Properties** section. When you create an encryption profile in IBM Storage Protect for Cloud Services, you will need to provide this key identifier.

What to do next

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 will not 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 97, and then configure the following settings on the **Create Encryption Profile** page.

Note: Please properly manage and secure keys in your Azure Key Vault for custom encryption profiles. If the key is lost, the encrypted data will be non-recoverable.

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. Ensure that the valid version is included in the key identifier. For example, https://{vault-name}.vault.azure.net/keys/{key-name}/{key-version}.
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 icon needs to be added 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 (Google Workspace or 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 (Google Workspace or 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 applies 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 while 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 RBAC (role-based access control) or access policies, and then assign a new role or 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 the Microsoft Entra admin center (or Microsoft Azure Portal), create a new key vault. For details, see 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 98 .
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 (Google Workspace or 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.

Service	Influence
IBM Storage Protect for Cloud Google Workspace	The data previously protected by IBM Storage Protect for Cloud Google Workspace 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 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 14. Configure Other Administration Settings

Refer to the instructions in the following sections to configure related settings.

Enable Report Data Collection

You can enable report data collection for Microsoft 365.

Data in Microsoft 365

Note:

- To enable the data collection, you must first go to **App management** to create an app profile of the Microsoft 365 (All permissions), Reporting for Microsoft 365, or custom Azure app type. The app profile must include **IBM Storage Protect for Cloud common service** into the service scope.
- 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.
- IBM Storage Protect for Cloud will stop collecting audit data immediately after your tenant's subscription expires.

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** pagIe, 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.
3. In the **Data in Microsoft 365** pane on the right of the page, turn on the toggle to enable the data collection.

   Note: After you enable the data collection, IBM Storage Protect for Cloud can start jobs to collect data. The first job can collect data for six days before you 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 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.
   - 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:

© Copyright IBM Corp. 2022, 2024

- **Azure Storage** – If you select this custom storage type, configure the settings below:
  - **Account name** – Enter the 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.

6. 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.
   - **Exclude non site audit data in specific containers** (only for the **SharePoint Online** data source) – When this option is enabled, only the site audit data in the specific containers for SharePoint sites or OneDrive will be collected. If you want to enable this option, turn on the toggle, click **Choose containers** to specify containers, and then click **Save**.

     Note: The site audit data will be collected based on the **ObjectId** property (the full URL path name of the file or folder accessed by a user), and the containers are configured in **Auto discovery**. For additional information on the other audit data (e.g. **SearchQueryPerformed**) in SharePoint Online and OneDrive, refer to the Microsoft article: Audit log activities.
   - **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.
7. Click **Save** to save your edits, or click **Cancel** to go back to the **Report data collection** page without saving any changes.

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 121.
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

You can refer to Download ARM VNet IDs to get the VNet IDs for your data center. There are two ways to add ARM virtual networks:

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

```
## Use the Azure CLI tool

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

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

# Step 3: Get the IBM Storage Protect for
```

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

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

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

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

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

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

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

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

```
## Use the Azure Az PowerShell

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

# Step 2 (Optional): Confirm whether the subscription switch is correct
# This command retrieves the current subscription ID to verify the switch.
(Get-AzContext).Subscription.Id

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

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

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

# Step 6: Add the firewall virtual network rule to grant access to IBM Storage Protect for
Cloud
# This cmdlet adds a network rule to the specified
storage account, allowing access from the specified subnet.
Add-AzStorageAccountNetworkRule -ResourceGroupName $DESTRG -Name $DESTSTA
-VirtualNetworkResourceId $SUBNETID
```

```
# Step 7: List the current network rules for the storage account to verify the addition
# This cmdlet retrieves the network rule set for the specified storage account.
Get-AzStorageAccountNetworkRuleSet -ResourceGroupName $DESTRG -AccountName
```

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 15. 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 109and "Step 2: Define Central Locations in Microsoft 365 Tenants" on page 110 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 before 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.

© Copyright IBM Corp. 2022, 2024

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.

Step 2: Define Central Locations in Microsoft 365 Tenants

The central locations in your organization's 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 109. 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 110 section.
4. Click **Save**.

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 table below lists the services that can use the registered app.

IBM Cloud Service	Usage
IBM Storage Protect for Cloud Dynamics 365	Use public APIs to retrieve job information from IBM Storage Protect for Cloud Dynamics 365.
IBM Storage Protect for Cloud Azure VMs, Storage, and Entra ID	Use public APIs to retrieve job information from IBM Storage Protect for Cloud Azure VMs, Storage, and Entra ID.
IBM Storage Protect for Cloud	Use APIs of auto discovery to retrieve and scan job information
	Use public APIs to get the audit records of activities in your IBM Storage Protect for Cloud tenant.

IBM Cloud Service	Usage
IBM Storage Protect for Cloud Microsoft 365	Use public APIs to retrieve job information from IBM Storage Protect for Cloud Microsoft 365.
	Use public APIs to get the subscription consumption information of IBM Storage Protect for Cloud Microsoft 365.
IBM Storage Protect for Cloud Google Workspace	Use public APIs to retrieve data from IBM Storage Protect for Cloud Google Workspace.
IBM Storage Protect for Cloud Salesforce	Use public APIs to retrieve data from IBM Storage Protect for Cloud Salesforce.

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**.
   d. Credentials enable applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential. Follow the instructions below to configure credentials:
      - Select the **Certificate** tab, and then click **Upload new certificate** to upload a certificate (.cer or .crt file). The certificate serves as credentials that allow your application to authenticate itself, requiring no interaction from a user at runtime. If your organization does not have any certificate files, you can refer to "Appendix F - Prepare a Certificate for the Custom Azure App" on page 179 to prepare a self-signed certificate.
      - Select the **Client secret** tab, click **Add client secret**, set the **Effective duration** to **1 year**, **2 years**, or **3 years**, and then click **Add** to generate a client secret. Client secrets values cannot be entirely shown once they are saved. To get a client secret value for later use, click the **Copy** () button to copy and save it upon creation.

      If you want to delete a certificate or client secret, click the **Delete** () button.
   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 CloudIBM Storage Protect for Cloud.

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.

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 Settings

In **Administration** > **Notification**, the Tenant Owner and Service Administrators can configure notification settings by referring to the instructions in the sections below.

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

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 **Invalid** 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 notifications to service administrators and customized administrators (Management permission required)** – Select this checkbox if you want the email notifications to be sent to these administrators.

  Note: The customized administrators must have been assigned the **Management** permission to receive the notifications.

- **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 115.

  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. If the **Finished with exception** status is selected, you can additionally select the **Attach the job report to the email** option if you want to attach job reports to notification emails.

   Note: In a job report, one Excel sheet can display objects no more than the maximum limit of rows in a sheet.

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 115.

- **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 and Power Platform 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 115.

Click **Save** to save your configurations.

Subscription Notification

The tenant owner, service administrators, and customized 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 administrators and customized administrators im IBM Storage Protect for Cloud** - Select this check box if you want the email notifications to be sent to these 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 115.

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 115.

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, tenant owner, service administrators and customized 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 and customized 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 115.

  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 following sections 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, German, and French.

     The following table lists the default email language mappings.

Language	Country/Region
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 Configure Terminology Mapping for IBM Storage Protect for Cloud Recovery Portal. Note that some mappings may not take effect due to limitations, you can contact the IBM Software Support team 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**.

Logo Customization

If you want to apply a custom logo, refer to the instructions below:

Note: Currently, the custom logo can only be applied to IBM Storage Protect for Cloud Recovery Portal. For additional information on the places where the custom logo will be displayed, see the IBM Storage Protect for Cloud Recovery Portal.

1. Navigate to **Administration** > **General settings** > **Logo customization**.
2. In the **Logo customization** pane, turn on the **Customize logo** toggle, and then click **Upload** to upload a custom logo.

   Note: You can upload a logo in the file type of JPG, BMP, PNG, or SVG. The maximum limit of file size is 800 KB, and the recommended dimensions are: 180 pixels (width) * 48 pixels (height).
3. Click **Save**.

Email Settings

In **Administration** > **General settings** > **Email settings**, you can customize which email sender will be used to send IBM notification emails to a Microsoft 365 tenant.

Note: This function supports changing email sender for IBM Storage Protect for Cloud. Before you change the email sender for a Microsoft 365 tenant, ensure that the tenant has configured an app profile for one of the following apps:

- Custom app with the **Mail.Send** Microsoft Graph API permission

For additional information on configuring app profiles, refer to Chapter 9, “Manage App Profiles,” on page 35.

To change the email sender settings, refer to the instructions below:

1. Navigate to **Administration** > **General settings**, and then click **Email settings**.
2. **Email sender** – Select one of the following options:

- **The default email address** – The table below lists the default email address information.

Service	Email sender
IBM Storage Protect for Cloud	noreply@sp4c.storage-defender.ibm.com

- **Microsoft 365 account** – If you select this option, you can add multiple Microsoft 365 accounts or shared mailboxes as email senders.

  Follow the steps below to add Microsoft 365 accounts:

  a. Click **Add**. The **Add** pane appears on the right of the page.

  b. Select an option from the **Tenant** drop-down list.

  c. In the **Microsoft 365 account** field, enter the username of a Microsoft 365 account or shared mailbox, and then select the desired option from the suggestion list. The specified Microsoft 365 account must have an Exchange license.

  d. Click **Send a test email** to send a test email to validate the specified email sender.

  e. Click **Add** at bottom of the **Add** pane.

  f. If you want to add multiple accounts, repeat the steps above. To delete an account, click the **Delete** (🗑) button.

3. Click **Save** to update the email settings.

Integration with Microsoft Azure Event Hubs

If you want to build an integration between a hub in Microsoft Azure Event Hubs and the audit records from specific cloud services in IBM Storage Protect for Cloud, refer to the instructions below:

Note: With the integration, the audit records will be synced to the event hub once per day. Real-time sync is not yet supported.

1. Navigate to **Administration** > **General settings** > **Integration with Microsoft Azure Event Hubs**.
2. In the **Integration with Microsoft Azure Event Hubs** pane appearing on the right, turn on the toggle, and configure the following fields:
   - **Event hub name** – Enter the name of an event hub.
   - **Event hub connection string** – Enter the connection string of the event hub.
   - **Specific services** – Select one or more services from the drop-down list. The available options are listed below:
     - IBM Storage Protect for Cloud
     - IBM Storage Protect for Cloud Dynamics 365
     - IBM Storage Protect for Cloud Google Workspace
     - IBM Storage Protect for Cloud Microsoft 365
     - IBM Storage Protect for Cloud Salesforce
   - **Data format** – The default option is **CEF** (Common Event Format). You can change the data format to **JSON** if necessary.
3. Click **Save**.

For more information, you can refer to the Microsoft documents: Create an event hub and Get a connection string. Note that the connection string must have at least the **Send** permission.

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.

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 105.

   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 . 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 105.

Chapter 16. Export the User Activity Report

Tenant Owners 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 **System auditor** on the left navigation 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 Services 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 Change Password Edit My Profile
Tenant Management	Connect/Reconnect/Remove Tenant
App Management	Create/Updated/Delete/Re-authorize/Edit App Profile

© Copyright IBM Corp. 2022, 2024

Section	Information
User Management	Add/Edit/Delete/Activate/Deactivate/Unlock User Change Tenant Owner
Encryption Management	Create/Edit/Delete/Apply Encryption Profile Validate Key Vault Information for Encryption Profile
Auto Discovery	Create/Edit/Rename/Delete Container Remove Container from Scan Profile Add/Edit/Delete Scan Rule Add Container to Scan Profile 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/Run/Delete Scan Profile Export Scan Profile Configurations Stop Scan Job Export Job Report Batch Import Save Data Center Mappings
Service Account Service Account Pool	Create/Edit/Delete Service Account Profile Update SharePoint Online Admin Center URL Validate Administrator Account for Service Account Profile Create/Validate/Update/Delete On-premises Service Account Profile Save Service Account Pool Validate Group for Service Account Pool Validate User Account for Service Account Pool
User Activity Report	Configure Retention Setting for User Activity Report Export User Activity Report
Notification	Create/Edit/Delete Email Recipient List Save Email Notification Settings Save App Profile Notification Settings Save Service Account Notification Settings Save Auto Discovery Notification Settings

Section	Information
Security	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 Reserved IP Addresses Download Arm VNet IDs
General Settings	Configure Date Format Configure Email Language Save Logo Customization Save Terminology Mappings
App Registration	Create/Edit/Delete App Registration

Chapter 17. View Announcements

To view announcements in IBM Storage Protect for Cloud, click the **Notification center** ( ) button on the upper-right corner.

In the **Notification center** window, you can click **View all** to view the following announcements:

- **Current announcements** – To view current announcements, click the **Current announcements** tab.
- **Announcement history** – To view previous announcements, click the **Announcement history** tab. You can view all services' previous announcements here.

© Copyright IBM Corp. 2022, 2024

Chapter 18. 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.

© Copyright IBM Corp. 2022, 2024

Chapter 19. 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.

© Copyright IBM Corp. 2022, 2024

Chapter 20. IBM Licensing Information

IBM solutions support Microsoft 365 solutions and count the total number of users with assigned licenses as described in the sections below. You can identify the number of Assigned Licenses in Microsoft 365 by navigating to the Microsoft 365 admin center > **Billing** > **Licenses**. The total quantity reported by IBM will be the total of all the assigned licenses.

IBM Storage Protect for Cloud Microsoft 365

The following IBM Storage Protect for Cloud Microsoft 365 count licenses based on your organization's Microsoft 365 subscriptions:

- IBM Storage Protect for Cloud Microsoft 365
- IBM Storage Protect for Cloud Azure VMs, Storage, and Entra ID

The table below lists the Microsoft 365 subscriptions for which IBM services count licenses:

Category	Subscription
For Business	Office 365 Small Business Premium
	Office 365 Midsize Business
	Office 365 Enterprise K2
	Office 365 Enterprise K1 without Yammer
	Office 365 Business Premium - DE
	Office 365 Small Business
	Office 365 Enterprise E4
	Office 365 E1
	Office 365 E1 Plus
	Office 365 E2
	Office 365 E3
	Office 365 E3 Developer
	Office 365 E4
	Office 365 E5
	Office 365 E5 without Audio Conferencing
	Microsoft 365 E3
	Microsoft 365 E5
	Microsoft 365 E5 without Audio Conferencing
	Microsoft 365 Business Premium
	Microsoft 365 Business Basic
	Microsoft 365 Business Standard

© Copyright IBM Corp. 2022, 2024

Category	Subscription
For Education	Exchange Online (Plan 1) for Students
	Exchange Online (Plan 2) for Faculty
	Office 365 A1 Plus for Faculty
	Office 365 (Plan A3) for Faculty
	Office 365 (Plan A3) for Students
	Office 365 (Plan A4) for Faculty
	Office 365 (Plan A4) for Students
	Office 365 A3 for Faculty
	Office 365 A5 for Faculty
	Microsoft Office 365 (Plan A1) for Faculty
	Microsoft Office 365 (Plan A1) for Students
	Microsoft 365 A5 for Faculty
	Microsoft 365 A3 for Faculty
	Microsoft 365 A3 for Students Use Benefit
For Europe	Office 365 E1 EEA (no Teams)
	Office 365 E3 EEA (no Teams)
	Office 365 E5 EEA (no Teams)
	Office 365 E5 EEA (no Teams) without Audio Conferencing
	Microsoft 365 E3 EEA (no Teams)
	Microsoft 365 E3 EEA (no Teams) - Unattended License
	Microsoft 365 E3 EEA (no Teams) (500 seats min)_HUB
	Microsoft 365 E5 EEA (no Teams)
	Microsoft 365 E5 EEA (no Teams) (500 seats min)_HUB
	Microsoft 365 E5 EEA (no Teams) with Calling Minutes
	Microsoft 365 E5 EEA (no Teams) without Audio Conferencing
	Microsoft 365 E5 EEA (no Teams) without Audio Conferencing (500 seats min)_HUB
	Microsoft 365 Business Basic EEA (no Teams)
	Microsoft 365 Business Standard EEA (no Teams)
	Microsoft 365 Business Premium EEA (no Teams)

Category	Subscription
Others	ENTERPRISEPACKWITHOUTPROPLUS
	Exchange Online (Plan 1)
	Exchange Online Essentials
	Exchange Online (Plan 1) for Alumni
	Exchange Online (Plan 2)
	Exchange Online Protection
	OneDrive for Business (Plan 1)
	OneDrive for Business (Plan 2)
	SharePoint Online (Plan 1)
	SharePoint Online (Plan 2)
	SHAREPOINTSTANDARD_YAMMER

Note the following:

- IBM will keep this list updated to the best of its ability based on current Microsoft SKUs for Microsoft 365. The content above is for information purposes only and is subject to change without notice.
- Your licensing agreement may include SKUs that are not listed here.

IBM Storage Protect for Cloud Dynamics 365

IBM Storage Protect for Cloud Dynamics 365 counts licenses that have the following subscriptions for Dynamics 365:

Category	Subscription
Dynamics 365 Sales	Dynamics 365 Sales Professional
	Dynamics 365 Sales Enterprise
	Dynamics 365 Sales Premium
	Microsoft Relationship Sales solution Plus
Dynamics 365 Customer Service	Dynamics 365 Customer Service Professional
	Dynamics 365 Customer Service Enterprise
Dynamics 365 Field Service	Dynamics 365 Field Service
Dynamics 365 Marketing	Dynamics 365 Marketing
Dynamics 365 Project Operations	Dynamics 365 Project Operations (Formerly, the Dynamics 365 Project Service Automation)
Dynamics 365 Team Members	Dynamics 365 Team Members
The following license types are no longer available but may still be used by existing customers	Dynamics 365 Plan
	Dynamics 365 Customer Engagement Plan Enterprise Edition
	Dynamics 365 for Team Members Enterprise Edition
	Microsoft Dynamics CRM Online Basic

Note: IBM will keep this list updated to the best of its ability based on current Microsoft SKUs for Dynamics 365. The content above is for information purposes only and is subject to change without notice.

IBM Storage Protect for Cloud Salesforce Licenses

IBM Storage Protect for Cloud Salesforce counts licenses from Salesforce users with specific license types. For more information on which license types will be charged, refer to the Subscription Information.

IBM Storage Protect for Cloud Google Workspace Subscriptions

IBM Storage Protect for Cloud Google Workspace count licenses from users (except for Suspended users and Archived users) with Google Workspace subscriptions assigned.

The following subscriptions are not charged by IBM Storage Protect for Cloud Google Workspace:

- Google Voice Starter (SKU ID: 1010330003)
- Google Voice Standard (SKU ID: 1010330004)
- Google Voice Premier (SKU ID: 1010330002)

Chapter 21. Appendices

The table details the appendices included in this document:

Appendix	Description
“Appendix A - Supported Criteria in Auto Discovery Rules” on page 137	Lists the criteria that are supported in Auto Discovery advanced mode rules.
Create a Key Vault in Azure	Details how to create an Azure Key Vault.
“Appendix C - Password Limitations and Requirements of Microsoft 365 Accounts” on page 175	Details the password limitations and requirements of Microsoft 365 accounts.
“Appendix D - When Service Account and App Profile are Used” on page 176	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 E - Helpful Notes When Auto Discovery Scan Results Return Error Codes” on page 177	Details solutions for some scan error messages in Auto Discovery.
“Appendix F - Prepare a Certificate for the Custom Azure App” on page 179	Details how to prepare a certificate for the custom Azure app.
IBM Storage Protect for Cloud App Registrations	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?

Microsoft 365

The table below lists the criteria that are supported in auto discovery advanced mode rules for Microsoft 365 objects.

Exchange Mailbox

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

© Copyright IBM Corp. 2022, 2024

Criteria	Condition
Company	Contains
	Does Not Contain
	Equals
	Does Not Equal
	Matches
	Does Not Match
Usage location	Equals
	Does Not Equal
Custom Attribute **Note:** After selecting this criterion, select an attribute number, which is retrieved from Exchange Online.	Contains
	Does Not Contain
	Equals
	Does Not Equal
	Matches
	Does Not Match
Department **Note:** If you want to configure multiple values for the **Equals any of** or **Does not equal any of** condition, separate the values with a semicolon (;).	Contains
	Does Not Contain
	Equals
	Does Not Equal
	Matches
	Does Not Match
	Equals any of
	Does not equal any of
Display Name **Note:** : If you want to configure multiple values for the **Equals any of** or **Does not equal any of** condition, separate the values with a semicolon (;).	Contains
	Does Not Contain
	Equals
	Does Not Equal
	Matches
	Does Not Match
	Equals any of
	Does not equal any of

Criteria	Condition
Email Address **Note:** : If you want to configure multiple values for the **Equals any of** or **Does not equal any of** condition, separate the values with a semicolon (;).	Contains
	Does Not Contain
	Equals
	Does Not Equal
	Matches
	Does Not Match
	Equals any of
	Does not equal any of
Group Membership Note the following: • This criterion allows you to scan the 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. • If you want to configure multiple values for the **Equals any of** or **Does not equal any of** condition, separate the values with a semicolon (;).	Contains
	Does Not Contain
	Equals
	Does Not Equal
	Equals any of
	Does not equal any of
Job Title	Contains
	Does Not Contain
	Equals
	Does Not Equal
	Matches
	Does Not Match
Exchange mailbox type **Note:** 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?	Equals
	Does Not Equal

Criteria	Condition
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* **Note:** This criterion corresponds to the **Preferred Data Location** property in a multi-geo Microsoft 365 tenant.	Equals
	Does Not Equal
State or Province	Contains
	Does Not Contain
	Equals
	Does Not Equal
	Matches
	Does Not Match
User ID	Contains
	Does Not Contain
	Equals
	Does Not Equal
	Matches
	Does Not Match
ZIP/Postal Code	Contains
	Does Not Contain
	Equals
	Does Not Equal
	Matches
	Does Not Match
Sign-in Status	Equals
	Does Not Equal

Criteria	Condition
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

OneDrive

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	
	Orphaned Drive* **Note:** For an orphaned user that no longer exists in your organization, this user's OneDrive is regarded as an orphaned OneDrive. To use this criterion, contact IBM Software Support to enable the scan for orphaned OneDrive first. For unified management, it is recommended that you configure one container for all orphaned OneDrive.	Equals	
		Does not equal	
	Site status	Equals	Active/Locked (Read-only)/Locked (No access)
		Does not equal	
	Primary administrator **Note:** If you want to configure multiple values for the **Equals any of** condition, separate the values with a semicolon (;).	Contains	
		Equals	
		Equals any of	
	Size	>=	
		<=	
	URL **Note:** : If you want to configure multiple values for the **Equals any of** or **Does not equal any of** condition, separate the values with a semicolon (;).	Contains	
		Does Not Contain	
		Equals	
		Does Not Equal	
		Matches	
		Does Not Match	
		Equals any of	
		Does not equal any of	

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
		Matches
		Does Not Match
	Department **Note:** If you want to configure multiple values for the **Equals any of** or **Does not equal any of** condition, separate the values with a semicolon (;).	Contains
		Does Not Contain
		Equals
		Does Not Equal
		Matches
		Does Not Match
		Equals any of
		Does not equal any of
	Group Membership **Note:** If you want to configure multiple values for the **Equals any of** or **Does not equal any of** condition, separate the values with a semicolon (;).	Contains
		Does Not Contain
		Equals
		Does Not Equal
		Equals any of
		Does not equal any of

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 **Note:** This criterion corresponds to the **Preferred Data Location** property in a multi-geo Microsoft 365 tenant	Equals
		Does Not Equal
	Username **Note:** If you want to configure multiple values for the **Equals any of** or **Does not equal any of** condition, separate the values with a semicolon (;).	Contains
		Does Not Contain
		Equals
		Does Not Equal
		Matches
		Does Not Match
		Equals any of
		Does not equal any of
	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 **Note:** If you want to configure multiple values for the **Equals any of** or **Does not equal any of** condition, separate the values with a semicolon (;).	Contains
		Does Not Contain
		Equals
		Does Not Equal
		Matches
		Does Not Match
		Equals any of
		Does not equal any of
	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 **Note:** If you want to configure multiple values for the **Equals any of** or **Does not equal any of** condition, separate the values with a semicolon (;).	Contains
		Does Not Contain
		Equals
		Does Not Equal
		Matches
		Does Not Match
		Equals any of
		Does not equal any of

SharePoint Site

Criteria	Condition
Created Time	Before
	After
	On
	Within
	Older Than
Creator > Department **Note:** : If you want to configure multiple values for the **Equals any of** or **Does not equal any of** condition, separate the values with a semicolon (;).	Contain
	Does not contain
	Equals
	Does not equal
	Matches
	Does not match
	Equals any of
	Does not equal any of
Creator > Microsoft Entra ID attribute	Contains
	Does Not Contain
	Equals
	Does Not Equal
	Matches
	Does Not Match
Creator > Group Membership **Note:** : If you want to configure multiple values for the **Equals any of** or **Does not equal any of** condition, separate the values with a semicolon (;).	Contains
	Does not contain
	Equals
	Does not equal
	Equals any of
	Does not equal any of
Creator > Custom property: Text	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	>=
	<=
	=

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	
Primary Administrator **Note:** If you want to configure multiple values for the **Equals any of** condition, separate the values with a semicolon (;).	Contains	
	Equals	
	Equals any of	
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* **Note:** This criterion corresponds to the **Preferred Data Location** property in a multi-geo Microsoft 365 tenant	Equals	
	Does Not Equal	
Site status	Equals	Active/Locked (Read-only)/Locked (No access)
	Does not equal	
Size	>=	
	<=	
Template Name **Note:** An example for **Template name** is **STS#0**.	Contains	
	Does Not Contain	
	Equals	
	Does Not Equal	
	Matches	
	Does Not Match	
Template Title **Note:** An example for **Template title** is **Team Site**.	Contains	
	Equals	

Criteria	Condition
Title **Note:** If you want to configure multiple values for the **Equals any of** or **Does not equal any of** condition, separate the values with a semicolon (;).	Contains
	Does Not Contain
	Equals
	Does Not Equal
	Matches
	Does Not Match
	Equals any of
	Does not equal any of
URL **Note:** : If you want to configure multiple values for the **Equals any of** or **Does not equal any of** condition, separate the values with a semicolon (;).	Contains
	Does Not Contain
	Equals
	Does Not Equal
	Matches
	Does Not Match
	Equals any of
	Does not equal any of
Hub site name **Note:** If you want to configure multiple values for the **Equals any of** or **Does not equal any of** condition, separate the values with a semicolon (;).	Contains
	Does not contain
	Equals
	Does not equal
	Matches
	Does not match
	Equals any of
	Does not equal any of
Last activity (UTC)	Before
	After
	On
	Within
	Older than
	Is no detected activity

Microsoft 365 Groups/Microsoft Teams/Viva Engage Community

Criteria		Condition
Group/Team/Viva Engage Community Property	Type	Equals
		Does Not Equal
	Team Status	Active
		Archived
	Display Name **Note:** Does not equal any of	Contains
		Does Not Contain
		Equals
		Does Not Equal
		Matches
		Does Not Match
		Equals any of
		Does not equal any of
	Creator: Department **Note:** If you want to configure multiple values for the **Equals any of** or **Does not equal any of** condition, separate the values with a semicolon (;).	Contains
		Does not contain
		Equals
		Does not equal
		Matches
		Does not match
		Equals any of
		Does not equal any of
	Creator: Microsoft Entra ID attribute Usage Location Custom property: Text **Note:** For more information about extended properties, refer to this Microsoft article: Add custom data to groups using schema extensions	Contains
		Does Not Contain
		Equals
		Does Not Equal
		Matches
		Does Not Match
	Custom attribute	Contains
		Does not contain
		Equals
		Does not equal
		Matches
		Does not match
	Custom Property: Number **Note:** For more information about extended properties, refer to this Microsoft article: Add custom data to groups using schema extensions.	>=
		<=
		=
	Custom Property: Text **Note:** : For more information about extended properties, refer to this Microsoft article: Add custom data to groups using schema extensions.	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 **Note:** If you want to configure multiple values for the **Equals any of** or **Does not equal any of** condition, separate the values with a semicolon (;).	Contains
		Does Not Contain
		Equals
		Does Not Equal
		Matches
		Does Not Match
		Equals any of

Criteria		Condition
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 **Note:** For more information about extended properties, refer to this Microsoft article: Add custom data to groups using schema extensions	>=
		<=
		=
	Custom Property: Text **Note:** For more information about extended properties, refer to this Microsoft article: Add custom data to groups using schema extensions.	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
	Hub site name If you want to configure multiple values for the **Equals any of** or **Does not equal any of** condition, separate the values with a semicolon (;).	Contains
		Does not contain
		Equals
		Does not equal
		Matches
		Does not match
		Equals any of
		Does not equal any of
	Last activity (UTC)	Before
		After
		On
		Within
		Older than
		Is no detected activity
	Sensitivity Label	Contains
		Does Not Contain
		Equals
		Does Not Equal
		Matches
		Does Not Match

Criteria		Condition	
	Site status	Equals	Active/Locked (Read-only)/Locked (No access)
		Does not equal	
	Size	>=	
		<=	
	Title **Note:** If you want to configure multiple values for the **Equals any of** or **Does not equal any of** condition, separate the values with a semicolon (;).	Contains	
		Does Not Contain	
		Equals	
		Does Not Equal	
		Matches	
		Does Not Match	
		Equals any of	
		Does not equal any of	
	URL **Note:** If you want to configure multiple values for the **Equals any of** or **Does not equal any of** condition, separate the values with a semicolon (;).	Contains	
		Does Not Contain	
		Equals	
		Does Not Equal	
		Matches	
		Does Not Match	
		Equals any of	
		Does not equal any of	

Project Site

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	
External sharing	Equals	Anyone New and existing guest Existing guests only Only people in your organization
	Does not equal	
Primary Administrator **Note:** If you want to configure multiple values for the **Equals any of** condition, separate the values with a semicolon (;).	Contains	
	Equals	
	Equals any of	
Sensitivity Label	Contains	
	Does Not Contain	
	Equals	
	Does Not Equal	
	Matches	
	Does Not Match	
Geo Location **Note:** This criterion corresponds to the **Preferred Data Location** property in a multi-geo Microsoft 365 tenant.	Equals	
	Does Not Equal	
Site status	Equals	Active/Locked (Read-only)/ Locked (No access)
	Does not equal	
Size	>=	
	<=	
Template Name	Contains	
	Does Not Contain	
	Equals	
	Does Not Equal	
	Matches	
	Does Not Match	
Template Title	Contains	
	Equals	

Criteria	Condition
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

Exchange Public Folder

Criteria	Condition
Display Name **Note:** If you want to configure multiple values for the **Equals any of** or **Does not equal any of** condition, separate the values with a semicolon (;).	Contains
	Does Not Contain
	Equals
	Does Not Equal
	Matches
	Does Not Match
	Equals any of
	Does not equal any of
Path	Is Under
	Is Not Under

Microsoft 365 Users

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
Department **Note:** If you want to configure multiple values for the **Equals any of** or **Does not equal any of** condition, separate the values with a semicolon (;).	Contains
	Does Not Contain
	Equals
	Does Not Equal
	Matches
	Does Not Match
	Equals any of
	Does not equal any of
Display Name **Note:** If you want to configure multiple values for the **Equals any of** or **Does not equal any of** condition, separate the values with a semicolon (;).	Contains
	Does Not Contain
	Equals
	Does Not Equal
	Matches
	Does Not Match
	Equals any of
	Does not equal any of
Domain	Equals
	Does Not Equal
Email Address **Note:** If you want to configure multiple values for the **Equals any of** or **Does not equal any of** condition, separate the values with a semicolon (;).	Contains
	Does Not Contain
	Equals
	Does Not Equal
	Matches
	Does Not Match
	Equals any of
	Does not equal any of

Criteria	Condition
Geo location **Note:** This criterion corresponds to the **Preferred Data Location** property in a multi-geo Microsoft 365 tenant.	Equals
	Does not equal
Group Membership **Note:** If you want to configure multiple values for the **Equals any of** or **Does not equal any of** condition, separate the values with a semicolon (;).	Contains
	Does Not Contain
	Equals
	Does Not Equal
	Equals any of
	Does not equal any of
Job Title	Contains
	Does Not Contain
	Equals
	Does Not Equal
	Matches
	Does Not Match
Microsoft 365 Subscription Name	Contains
	Does Not Contain
	Equals
	Does Not Equal
Office	Contains
	Does Not Contain
	Equals
	Does Not Equal
	Matches
	Does Not Match
Primary Email Domain **Note:** If you want to configure multiple values for the **Equals any of** condition, separate the values with a semicolon (;).	Equals
	Does Not Equal
	Equals any of
Sign-in Status	Equals
	Does Not Equal

Criteria	Condition	
State or Province	Contains	
	Does Not Contain	
	Equals	
	Does Not Equal	
	Matches	
	Does Not Match	
User ID **Note:** If you want to configure multiple values for the **Equals any of** or **Does not equal any of** condition, separate the values with a semicolon (;).	Contains	
	Does Not Contain	
	Equals	
	Does Not Equal	
	Matches	
	Does Not Match	
	Equals any of	
	Does not equal any of	
ZIP/Postal Code	Contains	
	Does Not Contain	
	Equals	
	Does Not Equal	
	Matches	
	Does Not Match	
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	
Sync Status	Equals	
	Does Not Equal	
User type	Equals	Member
	Does Not Equal	Guest
B2B invitation status	Equals	Accepted
	Does Not Equal	Pending acceptance

Security and Distribution Group

The **Security and distribution group** object type includes security groups, mail-enabled security groups, distribution lists, and dynamic distribution lists.

Criteria	Condition
Group Type: Security Group Mail-enabled Security Group Distribution List Dynamic Distribution List **Note:** This criterion cannot be used to filter room list type distribution lists.	Equals
	Does Not Equal
Display Name **Note:** If you want to configure multiple values for the **Equals any of** or **Does not equal any of** condition, separate the values with a semicolon (;).	Contains
	Does Not Contain
	Equals
	Does Not Equal
	Matches
	Does Not Match
	Equals any of
	Does not equal any of

Criteria	Condition
Owner Note the following: • This criterion only scans users with the Exchange license assigned. • **Equals** – If you use this condition to scan a Microsoft 365 Group which has more than one owner, you 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 '@'. • **Equals any of** / **Does not equal any of** – Enter the full user ID before domain '@', and separate the values with semicolon (;). • **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. This criterion cannot be used to filter dynamic distribution lists.	Contains
	Does Not Contain
	Equals
	Does Not Equal
	Matches
	Does Not Match
	Is a member of the group*
	Domain is
	Equals any of
	Does not equal any of

Criteria	Condition
Member Note the following: • This criterion only scans users with the Exchange license assigned. • If you use the **Contains** / **Does not contain** / **Equals any of** / **Does not equal any of** condition to scan groups, enter the full user ID before domain '@'. • If you want to configure multiple values for the **Equals any of** or **Does not equal any of** condition, separate the values with a semicolon (;). • This criterion cannot be used to filter dynamic distribution lists and room lists..	Contains
	Does Not Contain
	Matches
	Does not match
	Equals any of
	Does not equal any of
	Is Not Empty
Primary Email Address Note the following: • This criterion cannot be used to filter security groups, but it works for mail-enabled security groups. • If you want to configure multiple values for the **Equals any of** or **Does not equal any of** condition, separate the values with a semicolon (;).	Contains
	Does Not Contain
	Equals
	Does Not Equal
	Matches
	Does Not Match
	Equals any of
	Does not equal any of
Created Time	Before
	After
	On
	Within
	Older Than
Custom Attribute **Note:** This criterion cannot be used to filter security groups, but it works for mail-enabled security groups.	Contains
	Does Not Contain
	Equals
	Does Not Equal
	Matches
	Does Not Match

Criteria	Condition	
Custom Property **Note the following**: • For more information about extended properties, refer to this Microsoft article: Add custom data to groups using schema extensions. • This criterion cannot be used to filter dynamic distribution lists and room lists.	Number	>=
		<=
		=
	Text	Contains
		Does not contain
		Equals
		Does not equal
		Matches
		Does not match
Custom Property: Text **Note the following**: • For more information about extended properties, refer to this Microsoft article: Add custom data to groups using schema extensions • This criterion cannot be used to filter dynamic distribution lists.		Contains
		Does Not Contain
		Equals
		Does Not Equal
		Matches
		Does Not Match
Sync Status	Equals	
	Does Not Equal	

Power Platform

The table below lists the criteria that are supported in auto discovery advanced mode rules for Power Platform objects.

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

Connection

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	
	Type	Equals	
		Does not equal	
Owner	Company Department Office	Contains	
		Does not contain	
		Equals	
		Does not equal	
		Matches	
		Does not match	
		Is empty	
	Group membership	Contains	
		Does not contain	
		Equals	
		Does not equal	
	City Country or region Email address Display name	Contains	
		Does not contain	
		Equals	
		Does not equal	
		Matches	
		Does not match	
	Type	Equals	System/User
License designation		Equals	
		Does not equal	

Solution

Criteria		Condition
Creator: City Company Country or region Department Email address Office		Contains
		Does not contain
		Equals
		Does not equal
		Matches
		Does not match
Environment	Name	Contains
		Does not contain
		Equals
		Does note equal
		Matches
		Does not match
	Creator: City Company Country or region Department Email address Office Display name	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
Name		Contains
		Does not contain
		Equals
		Does not equal
		Matches
		Does not match

Criteria	Condition	
Publisher	Contains	
	Does not contain	
	Equals	
	Does not equal	
	Matches	
	Does not match	
Package type	Equals	Managed
	Does not equal	Unmanaged

Power Automate

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

Criteria		Condition	
Owner	Company Department Office	Contains	
		Does not contain	
		Equals	
		Does not equal	
		Matches	
		Does not match	
		Is empty	
	Type	Equals	System/User
	Group membership	Contains	
		Does not contain	
		Equals	
		Does not equal	
	City Country or region Email address Display name	Contains	
		Does not contain	
		Equals	
		Does not equal	
		Matches	
		Does not match	
State		Equals	
		Does not equal	

Power BI

Criteria	Condition
Capacity	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

Criteria	Condition
Geo Location	Equals
	Does Not Equal
Workspace Admin	Contains
	Does Not Contain
	Matches
	Does Not Match
	Is empty
Workspace admin email address	Contains
	Does Not Contain
	Matches
	Does Not Match
	Is empty

Google Workspace

The table below lists the criteria that are supported in auto discovery advanced mode rules for Google objects.

Google User

Criteria	Condition
Address: Home Work Other	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
Google subscription name	Contains Does not contain Equals Does not equal

Group membership	Contains Does not contain Equals Does not equal
Job title	Contains Does not contain Equals Does not equal Matches Does not match
Name	Contains Does not contain Equals Does not equal Matches Does not match
Organizational units	Contains
	Does not contain
	Equals
	Does not equal
	Matches
	Does not match
Primary email	Contains Does not contain Equals Does not equal Matches Does not match

Shared Drive

Criteria	**Condition**
Created Date	After
	Before
	Older Than
Member	Contains
	Does Not Contain

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

Vault Matter

Note: Currently, only the IBM Storage Protect for Cloud Google Workspace service with the Vault protection enabled supports configuring app profiles and scan profiles to scan **Vault matter** objects.

Criteria	Condition
Collaborator: Name Primary email	Contains
	Does not contain
	Matches
	Does not match
Name	Contains
	Does Not Contain
	Equals
	Does not equal
	Matches
	Does not match
Owner: Name Primary email	Contains
	Does Not Contain
	Equals
	Does Not Equal
	Matches
	Does Not Match

Google Classroom

Note: Currently, only the IBM Storage Protect for Cloud Google Workspace service supports configuring app profiles and scan profiles to scan **Google Classroom** objects.

Criteria	Condition

Name	Contains Does not contain Equals Does not equal Matches Does not match
Created date	After Before Other than

Active Directory

The table below lists the criteria that are supported in auto discovery advanced mode rules for Active Directory objects.

Active Directory User

Criteria	Condition
City	Contains Does not contain Equals Does not equal Matches Does not match
Company	Contains Does not contain Equals Does not equal Matches Does not match
Country or region	Equals Does not equal
Department	Contains Does not contain Equals Does not equal Matches Does not match

Display name	Contains Does not contain Equals Does not equal Matches Does not match
Distinguished name (A sample value: OU=Sp4c,OU=Storage-defender,DC=Ibm,DC=Com)	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
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

State or province	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

Active Directory Group

Criteria	Condition
Created time	Before After On Within Older than
Display name	Contains Does not contain Equals Does not equal Matches Does not match
Distinguished name (A sample value: OU=Sp4c,OU=Storage-defender,DC=Ibm,DC=Com)	Contains Does not contain Equals Does not equal Matches Does not match
Group type	Equals Does not equal

Owner	Contains Does not contain Equals Does not equal Matches Does not match
Primary email address	Contains Does not contain Equals Does not equal Matches Does not match
Scope	Equals Does not equal

Appendix B - Create a Key Vault in Azure

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

Step 1: Create an application.

This application is only used for Azure Key Vault. IBM Storage Protect for Cloud encryption profile will access the key vault via the application.

1. Go to Microsoft Entra admin center (or Microsoft Azure portal), navigate to **Identity** > **Applications** > **App registrations** (or **Microsoft Entra ID** > **App registrations**).
2. Click **New registration** on the ribbon.
3. On the **Register an application** page, configure the application settings.
4. Click **Register** to create your application.
5. 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.

Step 2: Add a client secret for the application

The client secret will be used in the IBM Storage Protect for Cloud encryption profile.

1. After creating the application, click **Certificates & secrets** in the left menu.
2. In the **Client secrets** field, click **New client secret**.
3. In the **Add a client secret** pane, enter a description for the client secret and select a duration.
4. Click **Add**. The value of the client secret is automatically generated and displayed.
5. 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.

Step 3: Create a Key Vault

According to your permission model (Azure RBAC or Key Vault access policy), refer to instructions in the related sections below.

- Azure RBAC (Role-based Access Control)
- Vault access policy

Step 4: Create a Key

Follow the steps below to create a key:

1. On the **Key vaults** page, click the newly created key vault.
2. Click **Keys** in **Objects**. In the **Keys** pane, click **Generate/Import** on the ribbon and create a key.
3. In the **Keys** pane, click the key name, and then click the current version. The key properties are displayed.
4. Copy the key identifier. You will need to provide the key identifier when configuring the encryption profile.

Step 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:

1. On the **Key vaults** page, click the name of the key vault you created, and then click **Networking** in **Settings**.
2. In the **Firewalls and virtual networks** tab, select **Allow public access from specific virtual networks and IP addresses**.
3. 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**.
4. Click **Save** to save your configurations.

Azure RBAC (Role-based Access Control)

Follow the steps below to create a key vault:

1. Open the Microsoft Azure portal.
2. Search for **Key vaults**, and then click the result to access the **Key vaults** page.
3. Click **Create**. The **Create a key vault** page appears.
4. In the **Basics** tab, provide the basic information for the key vault, and then click the **Access configuration** tab.
5. In the **Permission model** section, select **Azure role-based access control (recommended)**.
6. Click the **Networking** tab.
7. Select **Enable public access** which allows all networks to connect to this key vault.

   Note: If you only allow IBM Storage Protect for Cloud and the IBM cloud services you are using to connect to this key vault, you can edit the key vault's firewall settings after the key vault provisioning.
8. Click the **Tags** tab, and you can add tags to categorize your key vault.
9. 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.

After the key vault is created, follow the steps below to assign the role:

10. Open the Microsoft Azure portal, and navigate to the Key Vaults resource.
11. Click **Access control (IAM)** in the Key Vault's menu.
12. Click **Add** and select **Add role assignment**.
13. In the **Role** list, select **Key Vault Crypto User**.
14. Go to the **Members** tab.
15. In the **Assign access to** section, select **User, group, or service principal**.
16. Click **Select members**.
17. Search for and select your application.
18. Click **Review+assign** to complete the role assignment.

Vault Access Policy

Follow the steps below to create a key vault:

1. 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.
2. Click **Create**. The **Create a key vault** page appears.
3. In the **Basics** tab, provide the basic information for the key vault, and then click the **Access configuration** tab.
4. In the **Permission model** section, select **Vault access policy**.
5. In the **Access Policies** section, click **Create**.
6. 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**.
7. Click **Next** to go to the **Principal** tab.
8. In the **Principal** pane, complete the following steps:
   a. Enter the application name or application ID in the search box.
   b. Select the application and click **Select** at the bottom.
   c. Click **Next** at the bottom.
9. Click **Create** to add the access policy.
10. Click the **Networking** tab.
11. 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.
12. Click the **Tags** tab and you can add tags to categorize your key vault.
13. Click **Review + create** to review all of your configurations first, and then click **Create** at the bottom to create the key vault.
14. If you need to change some settings before creating the key vault, you can click the **Previous** button to change previous settings.

Appendix C - 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 D - 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 12 to help you determine if using the app profile method will satisfy your data management requirements.

Appendix E - 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, Microsoft Teams, and Viva Engage communities 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 7
- 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 Manage Account Pool (Obsolete) and "How Many Accounts Should be Added into an Account Pool?" on page 7
- 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 there are no existing Group team sites, the property needs to be initialized in Microsoft 365 Outlook.

The scan result of this issue is **Partially Scanned**. To initialize the Group team sites, sign in to Outlook with a Global Admin account, find Microsoft 365 Groups / Microsoft Teams / Viva Engage communities under the **Group** tab, and then click **Files**. Then, the initialization will be completed.

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 F - Prepare a Certificate for the Custom Azure App

This section details how to prepare self-signed certificate files (.cer/.crt file and .pfx file). The .cer/.crt file must be used to “Create Custom Apps” on page 40 in Microsoft Entra ID, and the .pfx file must be uploaded to IBM Storage Protect for Cloud to consent to the app. For security, we recommend you use the new certificate to re-authorize apps so you do not need to keep certificate files once they have been successfully uploaded.

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 179
- “Use Windows PowerShell to Prepare Certificates” on page 180

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 Create a Key Vault in Azure. 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 to your PFX]` with the full path of the certificate (.pfx file) in your local machine. Note that quotes are required when you enter the commands.

     ```
     $pfxPath="[Full path to your PFX]"
     Export-PfxCertificate --Password $(Read-Host -AsSecureString -Prompt "Enter a password to
     protect the certificate") -PFXData $(Get-PfxData -FilePath $pfxPath) -FilePath $pfxPath
     ```
   - Press **Enter** to execute the script.

     Note: The .pfx file contains your private key.

What to do next

After completing the steps above, you will get two certificate files.

- The .cer file must be uploaded for the custom app in Microsoft Entra ID. For additional details on uploading the certificate, refer to"Create a Custom Azure App" on page 40 .
- The .pfx file must be uploaded to IBM Storage Protect for Cloud to consent to the app. For additional details, refer to"Consent to Custom Apps" on page 44 or "Re-authorize an App Profile" on page 48.

Use Windows PowerShell to Prepare Certificates

About this task

To create a self-signed certificate using Windows PowerShell, refer to the following steps:

Note: The steps below are based on running the Windows PowerShell on a machine with the Windows 10 or Windows 11 operating system.

Procedure

1. Right-click **Windows PowerShell** on the machine, and select **Run as administrator** from the drop-down list.
2. Refer to the following example to use the New-SelfSignedCertificate cmdlet to generate certificate files.

   ```
   $cert = New-SelfSignedCertificate -Subject CN=IBMCustomApp -CertStoreLocation
   'Cert:\CurrentUser\My'
   ```

   Press **Enter** on the keyboard.

   Note: If you want to customize the parameters in the command, refer to the information below.

   - **Subject** – This parameter specifies the subject of the certificate. It typically includes the Common Name (CN) which identifies the entity the certificate is issued to.

- **CertStoreLocation** – This parameter specifies the certificate store in which to store the new certificate. You can choose between user-specific or machine-wide stores. For example, `-CertStoreLocation 'Cert:\CurrentUser\My'` for the current user or `-CertStoreLocation 'Cert:\LocalMachine\My'` for the local machine.
- **NotAfter** – This parameter sets the expiration date of the certificate. The `Get-Date` cmdlet retrieves the current date and time, and `AddMonths(24)` adds 24 months to it, meaning the certificate will be valid for two years from the date of creation. If necessary, you can change the number of `AddMonths`.

3. Export the .crt (or .cer) file by entering the following command:

```
Export-Certificate -Cert $cert -FilePath IBMCustomApp.crt
```

Note the following:

- If you want to export a .cer file, replace the **.crt** with **.cer** in the cmdlet example above.
- In this command, the file will be saved to the current working directory of the PowerShell session. If you want to specify a different directory, provide the full path by referring to the cmdlet example below:

```
Export-Certificate -Cert $cert -FilePath "C:\Temp\IBMCustomApp.crt"
```

4. Export the .pfx file with a password by entering the following command

```
Export-PfxCertificate -Password $(Read-Host -AsSecureString -Prompt "Enter a password to
protect the certificate") -Cert $cert -FilePath IBMCustomApp.pfx
```

Press **Enter** on the keyboard.

After completing the steps above, you will get two certificate files:

- The .cer file must be uploaded for the custom app in Microsoft Entra ID. For additional details on uploading the certificate, refer to “Create a Custom Azure App” on page 40.
- The .pfx file must be uploaded to IBM Storage Protect for Cloud to consent to the app. For additional details, refer to “Consent to Custom Apps” on page 44 or “Re-authorize an App Profile” on page 48.

If you want to remove the certificate files, enter the following command and press **Enter** on the keyboard:

```
Remove-Item "Cert:\CurrentUser\My\$($cert.Thumbprint)”
```

About Throttling

In Microsoft 365 environments, throttling may be automatically applied to ensure service stability and prevent excessive requests from negatively impacting the system.

- Throttling thresholds are determined and enforced by Microsoft. IBM has no control over when or how throttling is triggered.
- When throttling occurs, certain operations (e.g., backup or migration) may experience temporary slowdowns. However, there is no impact on user-facing environments or data integrity. This mechanism is part of Microsoft’s commitment to maintaining a reliable cloud service. IBM products are designed to operate in compliance with these controls.

Appendix G - Suggestions after Service Termination (for Microsoft 365 Tenants)

Once your subscription has expired, all information related to the expired subscription will be preserved for about 15 days before they are permanently deleted from IBM Storage Protect for Cloud. If you want to terminate an Enterprise subscription, no further action is required in IBM Storage Protect for Cloud and

following the instructions below will ensure you a clean and orphan-free environment in your Microsoft 365 tenant.

Remove IBM Applications from Your Microsoft Entra Applications

If you have configured app profiles in **App management**, you can refer to the instructions below to remove the consented applications from your Microsoft Entra environment:

1. Go to Microsoft Entra admin center (or Microsoft Azure portal).
2. Navigate to **Identity** > **Applications** > **Enterprise applications** (or **Microsoft Entra ID** > **Enterprise applications**).
3. Enter the keyword **IBM** to search for applications by application name.
4. Click the application that you want to remove.
5. Click **Properties** in the **Manage** section on the left menu.
6. Click **Delete** on the top menu.
7. In the confirmation window, click **Yes** to confirm your action.

Remove Reserved IP Addresses from Your Microsoft Entra Access Policies

If you have configured Conditional Access policies to add the reserved IP addresses downloaded from IBM Storage Protect for Cloud, you can refer to the instructions below to remove reserved IP addresses from your policies:

1. Log in to Microsoft Entra admin center (or Microsoft Azure portal).
2. Navigate to**Protection** (or **Microsoft Entra ID** > **Security**) > **Conditional Access**.
3. Click **Policies**.
4. Find the policy related to IBM.
5. Edit the policy to remove the reserved IP addresses related to the cloud services that you want to terminate.

Remove the Key Used in IBM Storage Protect for Cloud

If you have configured a custom encryption profile in **Encryption management**, you can refer to the instructions below to remove the key:

1. 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.
2. On the **Key vaults** page, click **Keys** in **Settings**.
3. Find the key used in IBM Storage Protect for Cloud and click the key.
4. Click **Delete** on the top menu.

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

© Copyright IBM Corp. 2022, 2024

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