IBM Storage Protect for Cloud Partners

User Guide

IBM

Contents

Note:

Before you use this information and the product it supports, read the information in "Notices" on page 86.

Edition Notice (June 2024)

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

About this publication

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

Who should read this publication

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

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

What's new

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

Release Date: November 2, 2025

New features and updates

- IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID pooled subscription for Azure Storage and Azure Virtual Machine modules is now available in IBM® Storage Protect for Cloud Partners.
- A new set of public APIs are now available, enhancing the common features for customer onboarding, service management, subscription tracking, tenant resource monitoring, and backup job reporting.

About IBM® Storage Protect for Cloud Partners

IBM® Storage Protect for Cloud Partners is a central hub for IBM® Storage Protect for Cloud partners to accelerate Microsoft 365 end-user adoption and usage. Partners can register, monitor, and manage their IBM® Storage Protect for Cloud customers, view reports about customers' jobs and requests for online services, view license usage, as well as resolve feedback all within a central platform.

Partners who are large account resellers that provide services for their own resellers can also invite and manage their resellers, view their pooled subscription details, and assign pooled subscriptions to resellers within IBM® Storage Protect for Cloud Partners. For the features that are supported for large account resellers, refer to the Reseller Management section.

When you sign in to IBM® Storage Protect for Cloud Partners with both the service provider and large account reseller permissions, you will see two tabs in the navigation pane: **Services** for customer and service management and **Licenses** for reseller and license management.

Supported Languages

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

Supported Browsers

The following table provides the supported browser versions.

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

> **Note:** The Safari browser is not recommended.

View Notifications

To view notifications in your IBM® Storage Protect for Cloud Partners environment, click the bell icon in the upper-right corner. The **Notifications** pane will appear, and you can view notifications under the following tabs:

- **Pending Tasks** – This tab will list pending tasks related to your customers, such as customer authentication and storage configuration. You can follow the corresponding guidance to complete pending tasks.
-
  - **Message** – This tab will list messages of the system and customers' expired subscriptions. You can click **Dismiss Announcements** to hide all announcements. If you want to view the message history, click the View history ( ) button button to open the **Notification center** page.

Manage Your Profile Information

To view and change your account information, click the user ( ) button in the upper-right corner, and then select **My profile** from the drop-down list.

On the **My profile** page, your account ID, tenant ID, and contact information are displayed. You can edit your first name, last name, and organization name. Click **Save** to save your changes, or click **Cancel** to go back to the **Home** page without saving any configurations.

Use Cases

Use Case - Want to Manage Multiple Tenants from a Single Platform?

Need:

Sophie, an Administrator at a Managed Service Provider that offers cloud management services, manages many customers with services within the IBM® Storage Protect for Cloud platform. Sophie wants the ability to manage her customers and monitor their activities from a central platform easily and efficiently. Sophie would like to perform tasks such as inviting customers, adding services, and managing her customers' IBM® Storage Protect for Cloud Subscriptions, all within one central portal.

Resolution:

Sophie logs into IBM® Storage Protect for Cloud Partners and navigates to the **Customers** page to perform management activities for her customers. She can invite new customers to IBM® Storage Protect for Cloud by clicking **Onboard new customer**, add services for an existing customer by selecting the customer and clicking **Add service**, and edit Subscription settings for customers.

The **Customers** page also displays the general account and service information for each customer of her tenants. Sophie can sort, filter, and search for various customers, view job details, support tickets, Job Reports, and Storage Consumption reports.

To get started with IBM® Storage Protect for Cloud Partners, complete the prerequisites in "Get Started" on page 13.

For more information on all actions that can be performed on the **Customers** page, refer to "Manage Customers" on page 21.

Use Case - Want to Manage Your Subscription Inventory and Understand Storage Consumption?

Need:

Sophie, an Administrator at a Managed Service Provider that offers cloud management services, wants to increase her operational efficiency by improving her Subscription inventory management and by monitoring and analyzing her customer storage consumption.

Resolution:

Sophie logs into IBM® Storage Protect for Cloud Partners and navigates to the **Reports** > **Report center** page. Sophie can access the **Customer operations report** page to view customers' operations, the **Subscription usage** page to view Subscriptions' current usage and modification history, the **Storage consumption report** page to view customers' storage consumption, and the **User activity report** page to view activities of users in IBM® Storage Protect for Cloud Partners. Sophie can create custom reports with the Pie Chart template. Sophie can analyze the data from the **Reports** page to better understand the needs of her customers based on their current activity and usage.

For more information on the reports, refer to "View and Create Reports" on page 46.

Use Case - Want the Ability to Co-Manage Your Customers from One Central Platform?

Need:

Sophie, an Administrator at a Managed Service Provider that offers cloud management services, wants the ability to co-manage her tenant with others. Sophie wants to be able to invite others to manage customers or users/groups in this portal.

Resolution:

Sophie logs into IBM® Storage Protect for Cloud Partners and navigates to the **Settings** page. Sophie can manage users on the **Users** page. She can also create custom roles on the **Roles** page. Custom roles are assigned specific system permissions and specific customer groups, so the users with different roles can only perform certain actions and manage certain customers in this portal.

For more information on managing users, roles, and customer groups, refer to the following sections:

- “Manage Users” on page 15
- “Manage Roles” on page 16
- “Manage Customer Groups” on page 17

Use Case - Want to Keep Yourself Informed of Any Troubleshooting Issues?

Need:

Sophie, an Administrator at a Managed Service Provider that offers cloud management services, wants the ability to monitor all IBM® Storage Protect for Cloud support tickets, as well as manage customer feedback from her tenant management platform.

Resolution:

Sophie logs into IBM® Storage Protect for Cloud Partners and navigates to the Settings page. Sophie can add her email address into the **Troubleshootin profile** page to add herself into the loop of any support emails her customers send. She can also navigate to the **Feedback management** page to view and monitor her customer feedback.

For more information on managing users and groups, refer to the following sections:

- “Manage Customer Feedback” on page 69

FAQs

You can find frequently asked questions and answers in the following categories: partner management, customer management, resources and feedback, and licensing.

Refer to the frequently asked questions and answers.

Partner Management

How can I add another administration account within my organization to IBM® Storage Protect for Cloud Partners?

Navigate to **Settings › Account manager › User management**, click **Add users** and add this user to the built-in **Administrator** group.

Customer Management

How can I invite new customers/tenants and assign subscriptions for them?

On the **Customers** page, click **Onboard new customer** and follow the instructions to provide customer information and assign subscriptions to the customer.

How can I learn about the job statuses of customers?

Go to the **Reports** > **Report center** page, and click **Customer operations report**. The **Customer operations report** page shows a summary of all customers sorted by online services. You can click a service card to view the details of the summary and filter the report by time range or job/request status.

How can I learn about the storage usage status of a customer?

Go to the **Reports** > **Report center** page and click **Storage consumption report**. The **Storage consumption report** page shows a summary of storage used by all customers. Under the summary, each customer has a card. You can click **View details** on a card to view this customer's storage usage.

How can I change a customer’s registered account (Tenant Owner)?

Ensure that the new Tenant Owner has the Service Administrator role in the customer's IBM® Storage Protect for Cloud environment. Log in to the customer's environment with the **Administrator** role, go to **User management**, select the new Tenant Owner, and then click **Set as tenant owner**. The selected user will become the customer's new Tenant Owner.

Resources and Feedback

How can I find the user guides?

IBM® Storage Protect for Cloud user guides.

How can I submit feedback about IBM® Storage Protect for Cloud Partners?

You can go to the **Submit feedback** page by accessing **Help** in the navigation pane and clicking **Submit feedback**on the IBM® Storage Protect for Cloud Partners interface.

Licensing

How does IBM® Storage Protect for Cloud Partners define licenses for Microsoft 365 tenants?

IBM® Storage Protect for Cloud licenses Microsoft 365 users that have assigned licenses in Microsoft 365. Each assigned Microsoft 365 user needs a corresponding license from IBM® Storage Protect for Cloud. The Microsoft 365 subscriptions that IBM® Storage Protect for Cloud subscriptions are included in Licensing Information.

Get Started

To begin using IBM® Storage Protect for Cloud Partners, follow the steps outlined in the sections below.

1. **Sign Up and Sign In**
   To create an IBM® Storage Protect for Cloud Partners account and sign in, refer to Sign Up for IBM® Storage Protect for Cloud Partners.

2. **Set Up Partner Access and App Profiles**
   As an administrator, you can add other partner users to IBM® Storage Protect for Cloud Partners and define their roles and the customers they can manage. Refer to Account Management for details.

   If you want to add Microsoft 365 users/groups to IBM® Storage Protect for Cloud Partners, an app profile for Microsoft 365 is required. For details, refer to Manage Partner App Profiles for more information.

3. **Onboard Customers**
   You can start onboarding your customers to IBM® Storage Protect for Cloud Partners. Refer to Invite a New Customer for details.

4. **Add Services and Manage Subscriptions**
   After a customer is invited to IBM® Storage Protect for Cloud Partners, you can begin adding services and managing their subscriptions. Refer to Add Services for details.

   a. **Select Services**: Select the services you would like to add for the customer.

   b. **Assign Subscriptions**: Assign the corresponding service subscriptions to the customer and set the subscription expiration date.

   c. **Add Tenants**: If there are no tenants for the customer, you will be asked to Add a Microsoft 365 Tenant for this customer before you can continue.
   If you want to add Google tenants, you need to go to IBM® Storage Protect for Cloud and refer to Connect Your Tenants to IBM Online Services to complete the operations.

   d. **Authenticate Services**: Based on the services selected for the customer, the following methods may be available:

   - Consent to apps separately – You can click **Authenticate** to the right of a service component to consent to the app.
   - Create a custom app profile – Click **Create** to the right of **Custom app profile** to use a custom Azure app for authentication.
   - Create a service account profile – Click **Create** to the right of **Service account profile** to create a service account profile for authentication.
   - Create a Google Cloud service account profile – Click **Create** to the right of **Google Cloud service account profile** to create a Google Cloud service account profile for authentication.
   - > **Note:** A custom app profile and service account profile can only be created once per customer. Make sure all required services are added for a customer before you create the custom app profile or service account profile for this customer.

Sign Up for IBM® Storage Protect for Cloud Partners

To sign up for IBM® Storage Protect for Cloud Partners with a corporate email address, contact your sales representative.

Sign into IBM® Storage Protect for Cloud Partners

On the IBM Storage Protect for Cloud Partners sign-in page, choose one of the following sign-in methods:

- “Sign In as a Partner with a Local Account” on page 14
- “Sign In as a Partner with a Microsoft 365 Account” on page 14

Sign In as a Partner with a Local Account

Procedure

To sign in to this system with a local account, complete the following steps:

1. Launch the Partner Portal by clicking on this link: https://partner.sp4c.storage-defender.ibm.com
2. On the sign-in page, enter your user ID and password in the corresponding text boxes.
3. Click **Sign in**. The homepage appears.

Sign In as a Partner with a Microsoft™ 365 Account

Procedure

To sign in to IBM® Storage Protect for Cloud Partners as a partner 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 your Microsoft™ 365 account to sign in to another app on the same browser, you will be automatically signed into this system.

2. On the Microsoft 365 authentication page, enter an existing Microsoft 365 account and password.
3. Click **Sign in**. The homepage of this system appears.

   > **Note:** If it is the first time that this Microsoft™ 365 account is signing into IBM® Storage Protect for Cloud Partners, the permissions required for IBM® Storage Protect for Cloud Partners are displayed. Review the permissions and click **Accept**. The **IBM® Storage Protect for Cloud** app is generated in **My apps** on Microsoft™ 365. Click the app to access IBM® Storage Protect for Cloud Partners within Microsoft™ 365. The app will remember your credentials when you log in through it.

4. The homepage of this system appears.
   After you have signed in to IBM® Storage Protect for Cloud Partners with Microsoft 365, if you also have a local account, you can select the checkbox in the prompted window to choose Microsoft as the only sign-in method for your account.

Choose a Purchase Method

About this task

The first time that you sign in to the IBM® Storage Protect for Cloud Partners, a pop-up window appears asking you to choose a method from the following to purchase services for your customers:

Procedure

- **Contact a Distributor (recommended)** – In this system, this method is recommended. After selecting this option, a page opens in a new tab and lists available distributors. You can choose a distributor to purchase services.
- **Contact Sales Team** – If necessary, you can select this method. After selecting this option, the contact IBM® Storage Protect for Cloud Partners page appears in a new tab, and you can contact us to purchase services.

Account Management

Administrators can now manage users, roles, and customer groups in Account Management. Refer to the sections below for instructions.

Manage Users

Apart from the partner system account (tenant owner), which is the account used to sign up for IBM® Storage Protect for Cloud Partners, you can invite other users into this portal to manage customers, users, roles, and customer groups.

About this task

When a user is added to IBM® Storage Protect for Cloud Partners, an invitation email will be sent to the user automatically. IBM® Storage Protect for Cloud Partners provides a default email template. Prior to adding users, you can customize an invitation email template. For details, refer to "Manage Email Templates" on page 60.

Users with the built-in **Administrator** role to add users, delete users, and change the tenant owner. To manage users, go to the **Settings** page, and select **Users**in the **Account management** area. The **Users** page appears. Click **All users**, **Administrators**, and other role tabs in the left pane to view the corresponding users.

You can perform the following actions:

- **Search** –To search for a specific user, enter the keywords of the user's email address in the search box. Then, press **Enter** on the keyboard.
- **Add users** – Click **Add new user** in the upper-right corner. In the **Add user** panel, configure the following settings and click **Add** to add the user.
  - **Sign in type** – Select the sign in type from the drop-down list.
    - **Local user**– Enter valid email addresses in the format of **someone@example.com**.
    - **Microsoft 365 User/Group** – Microsoft 365 users and groups will become the system's users. Enter the email address of the user/group in the format of **someone@example.com**. The system will automatically check whether the users or groups are valid.
    - You can also click the browse () button to view the users or groups within the selected profile, and then select your desired users or groups.
  - **App profile**– This option only appears if **Microsoft 365 User/Group** is selected as the sign-in method. An app profile is required to add or verify Microsoft 365 users/groups users. Select a previously configured app profile or click **New app profile**. For more information, refer to "Create an App Profile for Microsoft 365" on page 19.
  - **Add as an administrator** – Select the checkbox to set the user/group as the Administrator.
  - **Assign roles to the user** – Select previously configured roles for the user. For more information about roles, refer to "Manage Roles" on page 16.

  After a user is added successfully, the user will receive an invitation email that contains the user ID. The user needs to activate the account and set the password.
- **Assign role**– To assign roles to a user, click the More actions (•••) button of the user, and select **Assign role** in the drop-down list. In the **Assign role** panel, you can select the **Add as an administrator** checkbox to set the user as an Administrator. Enable the roles you want to assign to the user, and click **Save** to save your edits. Note that you cannot assign roles to the Tenant Owner and Support accounts.
- **Remove role** – To remove the role of a user, in the **Administrator**or any other role tabs, click the More actions (•••) button of the user, and select **Remove role** in the drop-down list. Note that you cannot remove roles for Tenant Owner and Support accounts.
- **Add to role** – In the **Administrator** or any other role tabs, you can click **Add existing user** to add users to this role. In the panel, search for users by email address, select the users you want to add, and then click **Save** to add the users.
- **Change tenant owner** – In the **Administrator** tab, select the user you want to set as the Tenant Owner, and then click **Set as tenant owner**. A pop-up window appears asking for your confirmation. Click **Confirm** to confirm your action. The selected user will be set as the Tenant Owner. After the tenant owner is changed, all users with the **Administrator** role will receive a notification email about the tenant owner change.
- **Delete user** – In the **All users** tab, select one or more users and click **Delete**. A pop-up window appears asking for your confirmation. Click **Confirm** to confirm your deletion.

You can also click the More actions (•••) button of a user, and select **Delete** in the drop-down list. A pop-up window appears asking for your confirmation. Click **Confirm** to confirm your deletion.

Note that you cannot delete the Tenant Owner and Support accounts.

- **Unlock user** – If a user enters the wrong password three times, the user account will be locked for one hour. To manually unlock users, select the users with the lock () status and click **Unlock**.
- **Reset MFA settings** – If multi-factor authentication has been enabled for local accounts, you can reset MFA settings for them. Select the local users and click **Reset MFA settings**.

Manage Roles

A role determines the permissions of its members. This system provides a built-in role **Administrator**. Users with this role have full control permissions to this system and can manage all customers. You can create custom roles to allow the users with the roles to only perform certain actions in the system and to only manage certain customers.

About this task

Users with the built-in **Administrator** role can view role details and create/edit/delete custom roles. To manage roles, go to the **Settings** page, and select **Roles** in the **Account management** area. The **Roles** page appears.

Procedure

- **Search** – To search for a specific role, enter the keywords of the role name in the search box. Then, press **Enter** on the keyboard.
- **View and edit role details** – Click a role name. The **Role details** page appears displaying the role name, description, permissions, services, and customers managed by this role, and the users with this role. You can also click the Edit button in each section or tab to edit the role details. Refer to the instructions in “Create Roles” on page 16 for details.
- **Create role** – Click **Create role** in the upper-right corner, and then refer to the instructions in Create Roles.
- **Delete role** – Select one or more custom roles and click **Delete**. A pop-up window appears asking for your confirmation. Click **Confirm** to confirm your deletion.
  You can also click the More actions (•••) button of a role, and select **Delete** in the drop-down list. A pop-up window appears asking for your confirmation. Click **Confirm** to confirm your deletion.

Create Roles

Procedure

To create roles, complete the following steps:

1. Click **Create role** in the upper-right corner. The **Create role** page appears.
2. In the **Basic information** step, enter a name and an optional description for the role. Then, click **Next**.
3. In the **Permissions** step, select the permissions you want to assign to this role. Then, click **Next**.
   - **Customers**
     - **View customers** – Allows users to view customers.
     - **Edit customers** – Allows users to edit customers.
     - **Manage subscriptions** – Allows users to manage customers’ subscriptions.
     - **Onboard new customer** – Allows users to onboard new customers.
   - **Report center**
     - **Customer operations report** – Allows users to manage the customer operations report.
     - **Subscription usage** – Allows users to manage the subscription usage report.
     - **Storage consumption report** – Allows users to manage the storage consumption report.

        - **Subscription expiration** – Allows users to manage the subscription expiration report.
    - **System settings**
        - **Feedback management** – Allows users to manage feedback.
        - **Receive email notifications** – Allows users to receive email notifications.
4. In the **Services** step, select the type of access for this role. Then, click **Next**.
    - **Tenant user** – The role will be the tenant user for customer services. You can also define the role in IBM® Storage Protect for Cloud Microsoft™ 365 after turning on the toggle.
    - For IBM® Storage Protect for Cloud Microsoft™ 365, you can select the **Custom security group** option to define delegated permissions for the role.
    - **Service administrator** – The role will be the administrator for customer services.
    - **No access to customer services** – The role cannot access customer services.
5. In the **Customers** step, choose the customer groups that can be managed by this role. To view the customers included in each customer group, click the number link to the right of the group. You can also select the checkbox to grant the access to all customers to this role. Then, click **Next**.
6. In the **Membership** step, manage the users with this role.
    - Click **Add users** to add users to this role. In the **Add** panel, search users by email addresses, select the users you want to add, and click **Save**.
    - Select one or more users and click **Delete** to delete the user from this role. A pop-up window appears asking for your confirmation. Click **Confirm** to confirm your deletion.
7. Click **Save** to save your configurations or click **Cancel** to go back to the **Roles** page without saving any configurations.

Manage Customer Groups

A customer group categorizes customers into different groups. Then, customers can be easily managed in bulk by roles.

About this task

There are two types of customer groups:

- Static group – You need to manually add users to this group.
- Dynamic group – You can configure specific conditions and users that meet the conditions can be automatically added to this group after sync. If you want to try this feature, contact IBM Software Support to help enable the feature for you.

Users with the built-in **Administrator** role can create/edit/delete customer groups. To manage customer groups, go to the **Settings** page, and select **Customer groups** in the **Account management** area. The **Customer groups** page appears.

Procedure

You can perform the following actions:

- **Search** –To search for a specific customer group, enter the keywords of the group name in the search box. Then, press **Enter** on the keyboard.
- **View and edit customer group details** – Click a group name. The **Customer group details** page appears displaying the group name, description, rules, and customer details in this group.
    - Click the **Edit** button to edit the group name, description, and rules. Refer to the instructions in “Create Customer Groups” on page 18s for details.
    - Click the **Refresh** button to refresh the customer group details.
    - Click the **Sync** button to synchronize the customers to this group.
- **Create customer group** – Click **Create customer group**, and then refer to the instructions in Create Customer Groups.

- **Sync customers** – For dynamic customer groups using custom conditions, you can select the groups and click **Sync** to sync the customers that meet the configured conditions to this group.
- **Delete customer group** – Select one or more customer groups and click **Delete**. A pop-up window appears asking for your confirmation. Click **Confirm** to confirm your deletion.

Create Customer Groups

To create a customer group, click **Create customer group**. The **Create customer group** window appears.

If you want to create a static group and add users manually, complete the following steps:

1. Enter a name and an optional description for the group.
2. Click **Create** to create the group. In the confirmation window, click **Confirm**. You will be directed to the **Edit customer group** page.
3. Click **Add customer**. In the **Add customer** panel, search and select the customers you want to add to this group, and click **Add**.
4. After adding customers, you can perform the following actions:
    - Enter the keywords of the customer's email address in the search box. Then, press **Enter** on the keyboard to search for customers.
    - Select the customers and click **Remove** to remove the customers from this group.

If you want to create a dynamic group using custom conditions and add users automatically after this feature is enabled, complete the following steps:

1. Enter a name and an optional description for the group.
2. Select the **Dynamically add customers using custom conditions** checkbox.
3. Select the **Tag**, **Data center**, or **Service** filters, and configure the conditions to define the users that will be automatically added to this group.
   Click **Add condition** to add more conditions and select the relationships among them.
4. Click **Create** to create the group. In the confirmation window, click **Confirm**.

Manage Partner App Profiles

An app profile for Microsoft 365 is required if you want to add Microsoft 365 users/groups as IBM® Storage Protect for Cloud Partners users and want to enable single sign-on. An app profile generates the **IBM® Storage Protect for Cloud Partners - User Management** app. This app connects IBM® Storage Protect for Cloud Partners to Microsoft 365.

About this task

Partner app profile allows users in the built-in **Administrator** group to create, reauthorize, and delete app profiles.

To access **Partner app profile**, go to the **Settings** page, and select **Partner app profile** in the **Additional settings** area. The **Partner app profile** page appears. You can perform the following actions:

Procedure

- **Create** – Click **Create**, and then refer to the instructions in "Create an App Profile for Microsoft 365" on page 19.
- **Edit a profile name** – Select an app profile and click **Edit a profile name**. A pop-up window appears. Modify the profile name and click **OK**.
- **Re-authorize app** – The app profile whose status is **App Authorization Expired** must be re-authorized. You can also re-authorize the app for an active app profile if you want to change the Microsoft 365 account used to authorize the app. Select an app profile, and click **Re-authorize App**. Then, refer to the instructions in "Reauthorize IBM Storage Protect for Cloud Partners - User Management App" on page 19.
- **Delete** – Select one or more app profiles and click **Delete**.

> **Note:** If an app profile is applied in the **User management** to add Microsoft 365 users/groups, and the Microsoft 365 users/groups exist in IBM® Storage Protect for Cloud Partners, the profile cannot be deleted.

Create an App Profile for Microsoft 365

Creating an app profile for Microsoft 365 requires a Microsoft 365 Global Administrator account.

Procedure

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

1. Click **Create** on the **Partner app profile** page.
2. In the **Create** window, enter a name for the app profile you want to create, and click **Next**.
3. A window appears to confirm if you want to jump to the Microsoft 365 login page and enter another account to create a new app profile.
   Click **OK** to proceed:
   a. On the Microsoft 365 **Sign in** page, enter the login ID and password of a Microsoft 365 Global Administrator account. Then, click **Sign in**.

      > **Note:** This account will be added into the built-in **Administrators** group, if the account does not already exist in this system.

   b. Review the permissions required for this app and click **Accept** to continue.
      The following permissions are required:
      - Read all groups
      - Read organization information
      - Read all users' full profiles
      - Read directory data
      - Read all group memberships
      - Read domains
      - Sign in and read user profile

Result

The **Partner app profile** page appears, and the app profile is created successfully.

Reauthorize IBM® Storage Protect for Cloud Partners - User Management App

The app profiles whose statuses are **App authorization expired** must be re-authorized. You can also re-authorize the app for an active app profile if you want to change the Microsoft 365 account used to authorize the app. The **Re-authorize app** action requires a Microsoft 365 Global Administrator account.

Procedure

Complete the following steps to re-authorize the **IBM® Storage Protect for Cloud User management** app for a Microsoft 365 app profile:

1. Select an app profile and click **Re-authorize app**.
2. Choose one of the following options in the pop-up window:
   - **Use the current account** – The currently signed-in account will be used to authorize the app.

a. Choose this option and click **OK**.

b. Review the permissions required for this system and click **Accept** to continue.

- **Sign out and use another account** – The currently signed-in account will be signed out, and you need to enter another account to authorize the app. The system will sign in IBM® Storage Protect for Cloud Partners with the signed-out account automatically.

  a. Choose this option and click **OK**.

  b. On the Microsoft 365 **Sign in** page, enter the login ID and password of a Microsoft 365 Global Administrator account. Then, click **Sign in**. The signed-out account is signed into IBM® Storage Protect for Cloud Partners again.

  > **Note:** This account will be added into the built-in **Administrator** group, if it does not exist in any existing IBM® Storage Protect for Cloud Partners tenant.

  c. Review the permissions required for this system and click **Accept** to continue.

Result

The **Partner app profile** page appears, and the **IBM® Storage Protect for Cloud - User management** app is successfully authorized for the selected profile.

Manage Customers

In IBM® Storage Protect for Cloud Partners, as a partner, you can manage your customers via **Customers**. Click **Customers** in the left navigation to go to the **Customers** page.

You can perform the following actions on the **Customers** page:

- **Onboard new customer** – To invite a new customer, click **Onboard new customer** in the upper-right corner, and then select an option below according to the account type of the customer you want to invite. The **Invite new customer** panel appears. For more information, refer to "Invite a New Customer" on page 25.
  - **Microsoft 365 global admin**
  - **Google super admin**
  - **Salesforce system admin**
  - **Local account**
  - **Authorization link**
- **Add services** – To add online services to a customer, click the More actions (•••) button of the customer, and select **Add services** in the drop-down list. You can also select the customer, click **Services**, and select **Add services** in the drop-down list.
  The **Add services** panel appears. For more information, refer to "Add Services" on page 27.
- **Start services** – You can set up Microsoft 365/Google Workspace objects backup for customers who have available subscriptions for the IBM® Storage Protect for Cloud Microsoft™ 365/ IBM® Storage Protect for Cloud Google Workspace.
  To start an online service to a customer, click the More actions (•••) button of the customer, and select **Start services** in the drop-down list. You can also select the customer, click **Services**, and select **Start services** in the drop-down list.

  The **Start services** panel appears displaying the customer's service status. For more information, refer to "Start Services" on page 34.
- **Edit services** – If you have the pooled subscription for IBM® Storage Protect for Cloud Microsoft™ 365, you can select up to 20 customers with this service, click **Services**, and select **Edit services** in the drop-down list to batch edit their subscription of IBM® Storage Protect for Cloud Microsoft™ 365. In the **Edit services** panel, complete the following steps:
  a. Select the **IBM® Storage Protect for Cloud Microsoft™ 365** card and click **Next**.
  b. On the **Subscription information** page, edit the subscription information for the customers. You can refer to Add Services and Manage Customer Subscriptions sections to view how to edit the settings.
  c. Click **Save**. IBM® Storage Protect for Cloud Partners will edit subscriptions for the customers, and you will be directed to the result page that shows the progress and result of edits. Note that some edits will fail if you close this page before all of them are completed. After it is completed, you can click **Export** to export the result report for the edit.
- **Hide/Show expired services** – You can hide all expired services of a customer. Then, the expired services will not be displayed in IBM® Storage Protect for Cloud Dynamics 365 as well as the IBM® Storage Protect for Cloud home page. You can also show the hidden services.
  To hide/show expired services of a customer, click the More actions (•••) button of the customer, and select **Hide expired services/Show expired services** in the drop-down list. You can also select the customer, click **Services**, and select **Hide expired services/Show expired services** in the drop-down list.
- **View customer information** – To view detailed information about a customer, click the More actions (•••) button in the upper-right corner, and select **View customer information** in the drop-down list.
  You can also click the customer's organization name. The customer detailed dashboard appears. For more information, refer to "View the Customer Detailed Dashboard" on page 23.

  There is also a sample customer detailed dashboard for you to view what information is included on the dashboard. You can expand the navigation pane and click **View now** to access it.

- **Edit customer information** – To edit the information of a customer, click the More actions (•••) button of the customer, and select **Edit customer information** in the drop-down list.
  You can edit the customer information, upload an image as the symbol of the customer, and choose whether to send billing reports, apply a job notification profile, and send service reports to the customer. Then, click **Save** to save your changes or click **Cancel** to go back to the **subscriptions** page without saving any changes.

  Note the following:

  - If you want to send billing reports to the customer, select the **Send billing reports to the customer** checkbox, enter email addresses in the **Email recipients** text box, and select an option from the **Billing profile** drop-down list. For more information on billing profiles, refer to "Manage Billing Profiles" on page 65.
  - If you want to apply a job notification profile to the customer, in the **Select job notification profile** drop-down list, select a job notification profile. For more information on job notification profiles, refer to "Manage Job Notification Profiles" on page 62.
  - If you want to send service reports to the customer, select the **Send service reports to the customer** checkbox, and then enter email addresses in the **Email recipients** text box. For more information on service reports, refer to Manage Report Templates and Generate Reports.

- **Generate reports** – To generate a report for the customer, click the More actions (•••) button of the customer, and select **Generate report** in the drop-down list. In the **Generate report** window, complete the following settings, and then click **Generate report**.
  - **Template** – All report templates where no customers have been defined will be loaded. Select a report template.
  - **Who should receive this report?** – Select users who will receive this report.

    > **Note:** To send a report to a customer, make sure the setting for sending service reports is enabled for the customer, otherwise, the customer cannot receive the generated report. If you choose to send a report to a customer, after clicking **Generate report**, an email notification will be sent to the customer. The customer needs to verify the email address used to receive the generated report before they can finally view the report.

- **View reports** – To view the customer's storage consumption report and job status report, click the More actions (•••) button of the customer, and select **View reports** in the drop-down list.
  The **View reports** panel appears. Click the **Storage consumption** or **Job status** tab to view each report.

  You can export the storage consumption report by clicking **Export** at the bottom. A window appears. You can choose the report format, choose whether to include details in the report, and modify the file name in this window. Then, click **Export** to export the report.

- **Pin/Unpin customers** – To pin a customer to the dashboard, click the More actions (•••) button of the customer, and select **Pin customer** in the drop-down list. The customer will be pinned and displayed in the **Pinned customers** section on the dashboard. If the customer has been pinned, you can also select **Unpin customer** in the drop-down list.

- **Disconnect customers** – To disconnect a customer, click the More actions (•••) button of the customer, and select **Disconnect customer from IBM® Storage Protect for Cloud Partners** in the drop-down list.
  If you disconnect a customer, only the data related to this customer in the partner portal will be permanently deleted. The data in other product environments will not be deleted (for example: backup data). A pop-up window appears asking for your confirmation. Enter **Yes** in the text box, and click **Delete** to confirm your operation.

- **Search for a customer** – To search for a specific customer, enter the keywords of the customer's organization name in the search box in the upper-left corner. Then, press **Enter** on the keyboard.

- **Filter customers** – You can filter customers by **Product subscriptions**, **Status**, **Country or Region**, **Tags**, and **Services**. Click **Filter** in the upper-right corner and customize the filter criteria.
  Click **Filter** to apply the criteria to filter customers. All your filter criteria will be displayed at the top of the table, and you can also click the remove ( ) button next to each filter criterion to remove it.

- **Manage columns** – Click **Manage columns** in the upper-right corner to choose the columns you want to display on the page.
- **Export reports** – Click **Reports**, and select the report you want to export: **Export customer information report** or **Export IBM® Storage Protect for Cloud Microsoft™ 365 Job status report**.
  A panel appears. You can choose one of the following methods to export the report:
  - If you want to export the report right away, click **Export now**.
  - If you want to set a schedule to export the report, select **Specify a schedule**. For details about schedule settings, refer to "Configure Export Schedule" on page 42.
- **Access customer's service environment** – To access a customer's IBM® Storage Protect for Cloud environment, click the customer's registered account ID under the **Registered account** column. You can also click the (☰) button of the customer and select a service in the drop-down list to access the specific service environment.

  > **Note:** When you access a customer's IBM® Storage Protect for Cloud environment, any other open customer environment will time out.

- **Sort** – Sort customers by the customer's organization name by clicking the **Customer** column.

View the Customer Detailed Dashboard

The customer detailed dashboard displays the information of customer's subscriptions, report activities, backup status, storage reports, unusual activities analysis, policy monitor, and risk insights.

> **Note:** If your access to a customer's IBM® Storage Protect for Cloud tenant and services has been disabled, you can only view the **Products & subscriptions** information on the customer detailed dashboard.

There is also a sample customer detailed dashboard for you to view what information is included on the dashboard. You can expand the left navigation and click **View Now** to access it.

- **Products & subscriptions** – View the products/services and their status. You can click the ( ) arrow button next to **All** to filter products/services by their subscription status. To edit a customer's subscription for a service, hover your mouse over the service, click the More actions (•••) button, and click **Edit subscription**. For more information, refer to "Manage Customer Subscriptions" on page 34.
  If the customer's IBM® Storage Protect for Cloud Microsoft™ 365 or IBM® Storage Protect for Cloud Google Workspace is not started or partially completed, you can also click the link to start the service. For more information, refer to "Start Services" on page 34.

  > **Note:** If you cannot access the customer's IBM® Storage Protect for Cloud tenant and services, the **Products & subscriptions** information of each product/service will be displayed in a card view. To edit a customer's subscription for a service, click the edit () button on the card.

- **Report activity** – View the activities taken on the risk insights report and storage consumption report.
- **Backup status** – View the backup status of jobs in IBM® Storage Protect for Cloud Microsoft™ 365, IBM® Storage Protect for Cloud Google Workspace, IBM® Storage Protect for Cloud Dynamics 365, and IBM® Storage Protect for Cloud Salesforce. You can click the **Storage report** link to view the customer's storage report of IBM® Storage Protect for Cloud Microsoft™ 365.
- **Unusual activities analysis** – When the customer enables OneDrive and SharePoint Online in IBM® Storage Protect for Cloud Microsoft™ 365, IBM® Storage Protect for Cloud will learn from customer backups and report the OneDrive and SharePoint Online sites with unusual activities or under a potential ransomware attack. You can select a time range to view the corresponding report of the customer tenant in this section.

The main chart shows the data of OneDrive accounts or SharePoint Online sites tracked within the selected time range for unusual activities and potential ransomware attacks.

In the upper-right corner, the number of OneDrives or SharePoint Online sites protected by IBM® Storage Protect for Cloud and the number of suspicious OneDrives are displayed. You can click the number of suspicious items to view more information on the unusual activities and suspicious files for the reported OneDrives or SharePoint Online sites in the **Suspicious items** panel. In the panel, you can also click **Restore in Cloud Backup** to navigate to IBM® Storage Protect for Cloud Microsoft™ 365 to restore the OneDrives or SharePoint Online sites.

You can download the report in an Excel file by clicking **Export**.

- **Policy monitor** – View the number of compliant rules/non-compliant rules/fixed violations/unfixed violations in the customer tenant. Click the non-compliance rules icon to view the non-compliant rules of the customer tenant in the panel. Click other icons to quickly navigate to Policies for Microsoft 365 to view details and take action.
- **Risk insights** – View the last 7 day trends of high risk items/medium risk items/sensitive items/external users/external links in the customer tenant. Click **Show risk insights summary** in the upper-right corner to view the detailed number of items/users with risk. To download a PDF report which contains more information on risks in a customer's workspaces, click **Run detailed report**.

  > **Note:** To export the report of Exchange Online, make sure a service account without multi-factor authentication enabled has been created for the customer. If not, the authentication alert window appears. You can click **Create service account** to create one for the customer, or you can click **Continue to export** to export the risk report without the Exchange Online report.

- **SharePoint storage** – View the last 90-day trends of customer's SharePoint storage usage as well as the estimated trends in the next 90 days.
  In the **Monthly storage budget** section, the estimated budget on the SharePoint storage monthly is displayed.

  To view the SharePoint storage trends of the customer, make sure the customer has an app profile with the Microsoft Graph API > **Reports.Read.All** permission in IBM® Storage Protect for Cloud. To know more about app profiles and permissions, refer to the IBM® Storage Protect for Cloud User Guide.

You can perform the following additional actions:

- **View customer information** – To view the detailed information about a customer, click theMore actions (•••) button in the upper-right corner, and select **View customer information** in the drop-down list.
- **Edit customer information** – To edit the information of a customer, click the More actions (•••) button in the upper-right corner, and select **Edit customer Information** in the drop-down list.
  You can edit the customer information, upload an image as the symbol of the customer, and choose whether to send billing reports to the customer. Then, click **Save** to save your changes or click **Cancel** to go back to the customer detailed dashboard without saving any changes.

  > **Note:** If you select the **Send billing reports to the customer** checkbox, enter email addresses in the **Email recipients** text box, and select an option from the **Billing profile** drop-down list. For more information on billing profiles, refer to "Manage Billing Profiles" on page 65.

- **Generate report** – To generate a report for the customer, click the More actions (•••) button of the customer, and select **Generate report** in the drop-down list. In the **Generate report** window, complete the following settings, and then click **Generate report**.
  - **Template** – All report templates where no customers have been defined will be loaded. Select a report template.
  - **Who should receive this report?** – Select users who will receive this report.

> **Note:** To send a report to a customer, make sure the setting for sending service reports is enabled for the customer, otherwise, the customer cannot receive the generated report. If you choose to send a report to a customer, after clicking **Generate report**, an email notification will be sent to the customer. The customer needs to verify the email address used to receive the generated report before they can finally view the report.

- **Add services** – To add online services to a customer, click the More actions (•••) button in the upper-right corner, and select **Add services** in the drop-down list.
  The **Add services** panel appears. For more information, refer to "Add Services" on page 27.
- **Hide/Show expired services** – You can hide all expired services of a customer. Then, the expired services will not be displayed in IBM® Storage Protect for Cloud Partners as well as the IBM® Storage Protect for Cloud home page. You can also show the hidden services.

  To hide/show expired services of a customer, click the More actions (•••) button of the customer, and select **Hide expired services**/**Show expired services** in the drop-down list.
- **Pin/Unpin customer** – To pin a customer to the dashboard, click the More actions (•••) button in the upper-right corner, and select **Pin customer** in the drop-down list. The customer will be pinned and displayed in the **Pinned customers** section on the dashboard. If the customer has been pinned, you can also select **Unpin customer** in the drop-down list.
- **Disconnect customers from IBM® Storage Protect for Cloud Partners** – To delete a customer, click the More actions (•••) button in the upper-right corner, and select **Delete customer** in the drop-down list.
  If you disconnect a customer from IBM® Storage Protect for Cloud Partners, only the data related to this customer in the partner portal will be permanently deleted. The data in other product environments will not be deleted (for example: backup data). A pop-up window appears asking for your confirmation. Enter **Yes** in the text box, and click **Delete** to confirm your operation.
- **Access customer's service environment** – To access a customer's IBM® Storage Protect for Cloud environment, click the customer's organization name. This action will not be displayed if you cannot access the customer's IBM® Storage Protect for Cloud tenant and services.

  > **Note:** When you access a customer's IBM® Storage Protect for Cloud environment, any other open customer environment will time out.

Invite a New Customer

Procedure

Click **Onboard new customer** in the upper-right corner, and then complete the following steps to invite a new customer:

1. Select the type of new customer account that will be used to sign up to IBM® Storage Protect for Cloud.
   - Local account
   - Microsoft 365 account
     a. Click **Microsoft 365 global admin**.

     > **Note:** If the Microsoft 365 account already exists in IBM® Storage Protect for Cloud, the account information will be automatically populated, and you can go to step "3" on page 27 directly.

     b. Enter the login ID and password of the new customer's Microsoft 365 Global Administrator account. This account will become the customer's registered account.

> **Note:** The Global Administrator account must have the license for SharePoint Online assigned.

c. Click **Sign in**.

d. Click **OK** to confirm that you want to invite this new customer.

- Google account
  a. Click **Google super admin**, and a confirmation window appears.
  b. Select **The customer has installed the IBM® Storage Protect for Cloud app** checkbox.
  c. Click **Continue**.
  d. The Google sign-in page appears. Sign in with the new customer's Google Super Admin account.
  e. Click **OK** to confirm that you want to invite this new customer.
- Salesforce account
  a. Click **Salesforce system Aamin**, and the Salesforce login page appears.
  b. Enter the login ID and password of the new customer's Salesforce account. This account will become the customer's registered account.

  > **Note:** The Salesforce account must be associated with the System Administrator profile or another profile that has the same permissions as those of the System Administrator profile.

  c. Click **Log In**.
- Authorization link
  When you do not have the Global Admin credentials for a customer, the system provides a way for you to send an authorization link to the customer, which allows the customer to authorize the partner to manage the customer tenant. Note that this is only supported when you invite the customer from the Next Gen Directory page.
  - Click **Authorization link**, and the Authorization Link panel appears.
  - Enter the email address of the customer's Tenant Owner account.
  - Click **Generate authorization link**. The generated link will be displayed in the textbox. The link is only valid within 72 hours.
  - Click **Copy** to copy the link. Then, you can send the link to the customer you want to invite. After the customer clicks the link and completes the authorization, you can manage the customer in IBM® Storage Protect for Cloud Partners. You can ignore the following steps.

2. Provide the following account information.
   - If the account type you chose above is **Microsoft 365 global admin** or **Google super admin**, the following information is automatically filled in: **Customer Account** and **Name**. You need to enter the customer's **Organization name** and **Telephone number**, select an option from the **Country** drop-down list, and select the closest **Data center** to the customer's location.
   - If the account type you chose above is **Salesforce system admin**, the following information is automatically filled in: **Customer account**, **First name**, and **Last name**. You need to provide the customer's **Organization name**, **Country code**, **Telephone number** and select the closest **Data center** to the customer's location.
   - If the account type you chose above is **Local Account**, you need to enter the **Customer Account**, **Password**, **Confirm password**, **Name**, **Organization name**, and **Telephone number**, select an option from the **Country** drop-down list, and select the closest **Data center** to the customer's location.

You can select tags for the customer and upload an image as the symbol of the customer, as well as configure the following settings on behalf of the customer: **Job notification profile**, **Terms and Conditions and Privacy Policy**, and **Communication preferences**.

3. Click **Invite and next** to invite the customer and proceed with adding services and managing subscriptions for the customer. For more information on how to add services and manage subscriptions for a customer, refer to Add Services.
   Alternatively, you can click **Invite and close**, which allows you to invite the customer now, add services and manage subscriptions for the customer at a later time.

Add Services

Procedure

You can add new services for a customer and configure the subscription settings by referring to the instructions below:

1. Select online services by clicking their cards.
   - 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
2. Click **Continue** to proceed.
3. On the **Licensing** page, configure subscription information for each service by selecting that service on the left and editing its subscription information on the right.
   There is a **Skip for now** button for each service, allowing you to cancel adding the service. After clicking it, **Skipped** will appear.
   - **Subscription type** – Select the subscription type: **Trial** or **Subscription**
   - **Subscription model** - Select the subscription model for the customer.

     > **Note:** This field only appears while assigning the subscription for IBM® Storage Protect for Cloud Microsoft™ 365, IBM® Storage Protect for Cloud Dynamics 365, IBM® Storage Protect for Cloud Google Workspace, or IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID

   - **Service Type** – Select the service type for the customer.

     > **Note:** This field only appears while assigning the **Subscription** IBM® Storage Protect for Cloud Salesforce

   - **Source** – Select a value to indicate the source of your subscription.

     > **Note:** This field only appears while assigning the **Subscription** type.

   - **Module** – Select the module.

     > **Note:** This field only appears while assigning the **Subscription** type.

   - **Storage** - Choose to use the customer's own storage or IBM storage (Microsoft Azure Blob).

> **Note:** This field only appears while assigning the subscription for IBM® Storage Protect for Cloud Microsoft™ 365, IBM® Storage Protect for Cloud Google Workspace, IBM® Storage Protect for Cloud Dynamics 365 and IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID) – Choose to use the customer's own storage or IBM® Storage Protect for Cloud.

> **Note:** If customers use their own storage for IBM® Storage Protect for Cloud Dynamics 365, they must go to the IBM® Storage Protect for Cloud Dynamics 365 service to configure custom storage locations. If a customer uses IBM storage first and then wants to use a custom storage location for IBM® Storage Protect for Cloud Microsoft™ 365 and IBM® Storage Protect for Cloud Dynamics 365, the customer can contact the IBM Software Support to migrate the previous backup data from the IBM storage location to the custom storage location.

- **Storage Profile** - Select a storage profile from the drop-down list. If there is no storage profile, click **Create a profile** to create one. For more information about storage profiles, refer to "Manage Storage Profiles" on page 51.

  > **Note:** This field only appears while choosing to use the customer's own storage for IBM® Storage Protect for Cloud Microsoft™ 365and IBM® Storage Protect for Cloud Google Workspace

- **Retention** - If the customer uses IBM storage, configure the data retention by choosing one of the following options:

  > **Note:** This field only appears while assigning the subscription for IBM® Storage Protect for Cloud Microsoft™ 365, IBM® Storage Protect for Cloud Dynamics 365, or IBM® Storage Protect for Cloud Google Workspace

  - **Retain data for _ years** – The data generated within the specific years will be kept.

    > **Note:** The time to keep data is determined by the subscriptions you purchased from IBM® Storage Protect for Cloud.

  - **Unlimited retention** – All data will be kept without any pruning.

    > **Note:** This option is available when you assign the trial subscription. For **Subscription** type, it is determined by the subscription you purchased from IBM® Storage Protect for Cloud.

- **Add subscription for Microsoft 365 services** – While assigning the **Subscription** IBM® Storage Protect for Cloud Microsoft™ 365, if you have a pooled subscription for Microsoft 365 services, you can click this button to add the Microsoft 365 services subscription for the customer while assigning the. The following information can be configured additionally:
  - **Source** – Select a value to indicate the source of your subscriptions.
  - **Package** – Select the package of the subscription.
- **Add Subscription for Power platform** – While assigning the **Subscription** IBM® Storage Protect for Cloud Microsoft™ 365, if you have a pooled subscription for Power Platform, you can click this button to add the Power Platform subscription for the customer. The following information can be configured additionally:
  - **Type** – Select the type for the subscription.

- **Limit** – Enter a number to define the limit of the subscription.

- **Add capacity** – While assigning the **Subscription** IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID, if you have a pooled subscription of the Capacity mode (including Azure Virtual Machine or Azure Storage), you can click this button to add the Capacity subscription for the customer. The following information can be configured additionally:
  - **Capacity model** – Select the capacity model of the subscription.
  - **Purchased capacity for CAP Gateway mode** – Enter the purchased capacity for the CAP Gateway mode.
  - **Retention** – If the customer uses IBM storage, configure the data retention by choosing one of the following options:
    - **Retain data for _ years/months** – The data generated within the specific years/months will be kept.

      > **Note:** The time to keep data is determined by the subscriptions you purchased from IBM.

    - **Unlimited retention** – All data will be kept without any pruning.

      > **Note:** If this option is available is determined by the subscriptions you purchased from IBM.

      In the **Azure Virtual Machine** module,you can configure the subscription settings, and the configurations will also apply to other modules.
- **Add Microsoft Entra ID** – While assigning the **Subscription** IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID, if you have a pooled subscription of the user seat mode (including Microsoft Entra ID, Azure AD B2C, and Azure portal settings modules), you can click this button to add the Microsoft Entra ID subscription for the customer. The following information can be configured additionally:
  - **Purchased user seats** – Enter the purchased user seats of the customer.
  - **Retention** – If the customer uses IBM storage, configure the data retention by choosing one of the following options:
    - **Retain data for _ years/months** – The data generated within the specific years/months will be kept.

      > **Note:** The time to keep data is determined by the subscriptions you purchased from IBM.

    - **Unlimited retention** – All data will be kept without any pruning.

      > **Note:** If this option is available is determined by the subscriptions you purchased from IBM.

      In the **Microsoft Entra ID** module,you can configure the subscription settings, and the configurations will also apply to other modules.
- **Available Microsoft 365/Google Workspace licenses** – View the number of all Microsoft 365/Google Workspace licenses that the customer's tenant purchased in Microsoft 365/Google Workspace.
- **Assigned Microsoft 365/Google Workspace licenses** – View the number of Microsoft 365/Google Workspace licenses that have been assigned to users in the customer's tenant. IBM® Storage Protect for Cloud for Microsoft 365/Google Workspace charge the tenant according to this number.

When adding the IBM® Storage Protect for Cloud Microsoft™ 365 service, you can click the **Download Subscription Details** link to download the customer subscription information.

- **User Seats/Licenses/Objects/Capacity/Tenants** – Refer to the table below.

Service	Subscription Type	User Seats/Licenses/ Objects/Capacity/Tenant
IBM® Storage Protect for Cloud Microsoft™ 365 IBM® Storage Protect for Cloud Dynamics 365 IBM® Storage Protect for Cloud Google Workspace	Subscription	**User seats** – If the customer has assigned product licenses in Microsoft 365, the number of user seats will be the same as the number of assigned Microsoft 365 licenses. Otherwise, the newly added license will have one user seat, and the existing license will keep the current number of user seats. **User licenses** – If the customer has assigned Google Workspace licenses to users, the number of user licenses will be the same as the number of the assigned Google Workspace licenses. Otherwise, the newly added service will have one user license, and the existing service will keep the current number of user licenses.
IBM® Storage Protect for Cloud Salesforce	Trial	N/A
	Subscription – Basic	Enter the number of user seats that you want to assign to the customer.
	Subscription – Standard	
	Subscription – Premier	
IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID	Trial	N/A
	Subscription	Enter the number of user seats that you want to assign to the customer.

- **Subscription expiration date** (for **Subscription** only) – Click the calendar button and select the expiration date for the customer's subscription. You can also select **Same as Pooled Subscription** to keep the same expiration date as the pool subscription.
- **Contract end date** – Click the calendar button and select the contract end date.

4. Click **Save and continue**.
5. If there are no tenants for the customer, a message will appear, asking you to add tenants for this customer. For detailed instructions on how to add a tenant, refer to Add a Microsoft 365 Tenant.

> **Note:** Currently, IBM® Storage Protect for Cloud Partners only supports adding Microsoft tenants. If you want to add Google tenants and Salesforce tenants, you need to go to IBM® Storage Protect for Cloud to complete the operations. For detailed instructions, refer to Connect your Tenants to IBM® Storage Protect for Cloud.

6. On the **Permissions** page, tenants (tenant name and type) and services you have added for the customer are displayed. Based on the service you selected for the customer, the following methods may be available for authentication:

- Consent to app – In each service section, the required apps are displayed, and your consent to the apps are required. For detailed instructions, refer to Consent to an App.
- Create custom app profile – For the Microsoft tenant, you can create a custom app profile IBM® Storage Protect for Cloud Microsoft™ 365 ; for the Google tenant, you can create custom app profiles for IBM® Storage Protect for Cloud Google Workspace.
  For detailed instructions, refer to Create a Custom App Profile.
- Create service account profile – For IBM® Storage Protect for Cloud Microsoft™ 365 and IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID services, you can create a service account profile. For detailed instructions, refer to Create a Service Account Profile.
  If you want to add a new Microsoft 365 tenant, click **Add new tenant**. For detailed instructions, refer to Add a Microsoft 365 Tenant.

Note the following:

- The custom app profile and service account profile can only be created once for each customer. Make sure all required services have been added for a customer before you create the custom app profile or service account profile for the customer.
- Multiple app profiles for IBM® Storage Protect for Cloud Microsoft™ 365 can be created for a customer. After adding services, you can create additional app profiles for the customer by following the instructions in the Manage Customer App Profiles section.
- For some services, a message will appear below the app type, indicating that you need to assign the **Exchange Administrator** role to the app in the Microsoft Entra admin center. For detailed instructions, refer to How to Assign the Exchange Administrator Role to an App.

7. Click **Continue**.
8. On the **Overview** page, view the customer's services and their subscription information.
9. Click **Finish**. If the services you have added for the customer include IBM® Storage Protect for Cloud Microsoft™ 365 or IBM® Storage Protect for Cloud Google Workspace, the **Finish and Start Service** button will be available, allowing you to start service. For detailed instructions on starting services, refer to Start Services.

Add Microsoft 365 Tenants

Complete the following steps to add a Microsoft 365 tenant:

1. Click **Add tenants** or **Add new tenant** to open the **Add new tenant** window.
2. Enter a display name and an optional description for the new tenant.
3. Click **Continue**.
4. Enter the login ID and password of the customer's Microsoft 365 Global Administrator account, and click **Sign in**.
5. The permissions required for IBM® Storage Protect for Cloud Partners are displayed. Review the permissions and click **Accept**.
6. A page appears indicating that your tenant was connected to IBM® Storage Protect for Cloud.
7. Close this page, and you will be redirected back to the **Permissions** page.

Consent to an App

Complete the following steps to consent to the app for a service:

1. Select a service and click **Authenticate**.
2. For Microsoft tenant, enter the login ID and password of the customer's Microsoft 365 Global Admin account, and click **Sign in**.
   For Google tenant, enter the login ID and password of the customer's Google Super Admin account, and click **Sign in**.

   For Salesforce tenant, enter the login ID and password of the customer's Salesforce Super Admin account, and click **Sign in**

3. The permissions required by the service are displayed. Review the permissions and click **Accept**.
4. A page appears indicating that the app was authorized for the service.
5. Close this page, and you will be redirected back to the **Permissions** page.

Create a Custom App Profile

Complete the following steps to create a custom app profile for the Microsoft 365 tenant:

> **Note:** Before you create an app profile for a custom app, make sure you've created a custom app and added the required permissions to the app. For detailed instructions, refer to Create Custom Apps.

1. Complete the following steps to create a custom app profile for the Microsoft 365 tenant:
2. Click **Create** next to **Custom app profile**.
3. Complete the following information on the **Create app profile** window:
   - **Custom app type** – **Azure app** is automatically selected.
   - **App profile name** – Enter a name for the app profile.
   - **Application ID** – Enter the application ID of the application that has been created in Microsoft Entra ID.
   - **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 Prepare a Certificate for the Custom Azure App.

   - **Certificate password** – Enter the password of the certificate.
4. Click **Save** to save the configurations.

1. Complete the following steps to create a custom app profile for the Google tenant:

   > **Note:** Before you create an app profile for a custom app, make sure you've created a custom app. For detailed instructions, refer to Create a Custom Google App.

2. Click **Create** next to **Custom app profile**.
3. Complete the following information on the **Create app profile** window:
   - **App profile name** – Enter a name for the app profile.
   - **Admin account** – Enter the name of the Admin account that has the **User ManagementAdmin** and **Services Admin** roles.
   - **Google service account** – Enter the service account email address.

     > **Note:** You can copy the email address when creating the service account. For details, refer to Create a Service Account.

   - **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.

4. Click **Save** to save the configurations.

Create a Service Account Profile

About this task

The service account profile you create must contain a Microsoft 365 account with the permissions required by your customer's cloud services. The service account's permissions vary with the cloud services your customer is using. For detailed instructions, refer to Required Permissions of Cloud Services.

Procedure

Complete the following steps to create a service account profile:

1. Click **Create** next to **Service account profile**.
2. Complete the following information on the **Create service account profile** window:
   - **Service account profile name** – Enter a name for the service account profile.
   - **Description** – Enter an optional description.
   - **Service** – Select at least one service from the drop-down list.
   - **Username** – Specify an account with the permissions required by the cloud services.
     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 manage 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.
     - The specified Microsoft 365 account cannot have multi-factor authentication (MFA) enabled. If the organization has MFA enabled, you can refer to additional details in the following section: Helpful Notes for Passing the Validation Test of a Service Account.
   - **Password** – Enter the login password of the account above.

     > **Note:** The password is validated via the Microsoft 365 API. Due to a limitation of the Microsoft 365 API, you may encounter an issue where the password is deemed invalid here, but can still be used to log into Microsoft 365 successfully. To resolve this issue, please change your password in Microsoft 365 and then enter the new password here. For more information about password limitations and requirements, refer to Password Limitations and Requirements of Microsoft 365 Accounts.
3. Click **Save** to save the configurations.

Create a Google Cloud Service Account Profile

Procedure

Complete the following steps to create a Google Cloud service account profile:

1. Click **Create** next to **Google Cloud service account profile**.
2. Complete the following information on the **Create Google Cloud service account profile** window:
   - **Profile name** – Enter a name for the service account profile.
   - **Service** – Only IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID is available.

- **Service account email** – Enter the client email that is included in the JSON file downloaded from the Google Cloud Platform when you create keys for the service account.
- **Private key** – Enter the private key that is included in the JSON file downloaded from the Google Cloud Platform when you create keys for the service account.
- **Project ID** – Enter the project ID that is included in the JSON file downloaded from the Google Cloud Platform when you create keys for the service account.

3. Click **Save** to save the configurations.

> **Note:** For the **Service account email**, **Private key**, and **Project ID** values, refer to the instructions below to create the service account key and download the JSON file.

4. Go to Google Cloud IAM.
5. Click **Service Accounts** and select the project where your service account has been created.
6. Click your service account, and then click the **Keys** tab.
7. Click **Add key**, and then click **Create new key** from the drop-down list.
8. Select the **JSON** key type and click **Create**.
9. Open the downloaded file and find the **Project ID**, **Project key**, and **Client email** values.

Start Services

To scan a customer's Microsoft 365/Google Workspace objects and start backup for the scanned objects, click **Start** to consecutively start **Step 1. Auto Discovery** and **Step 2. General information**.

You can select whether to scan archive mailboxes in the auto discovery.

In the **Backup Status** section of IBM® Storage Protect for Cloud Microsoft™ 365, you can click the arrow button next to an object type to view the summary of the backup scope.

When you select one customer to start the backup service, note the following:

- For IBM® Storage Protect for Cloud Microsoft™ 365, the IBM® Storage Protect for Cloud Partners system will check whether the customer has a Microsoft 365 app profile/custom Azure app profile/service account profile, a Microsoft Delegated app profile, and a Viva Engage app profile.
  - If the customer wants to back up Viva Engage data, a Viva Engage app profile is required.
  - If the customer wants to back up Teams chat data, a custom Azure app profile with the **All permissions** type is required.
  - If the customer wants to back up Power Platform data, a Microsoft Delegated app profile for IBM® Storage Protect for Cloud Microsoft™ 365 is required, and a Power Platform Objects scan profile is required.

If the required profile is not configured, a pop-up window will appear. If the customer does not have a Microsoft 365 app profile/custom Azure app profile/Microsoft Delegated app profile/service account profile, click **Create an app profile** or **Create a service account** in the window to go to IBM® Storage Protect for Cloud to create one.

If the customer wants to back up Viva Engage data but does not have a Viva Engage app profile, you can click **Create an app profile** in the Viva Engage section to go to IBM® Storage Protect for Cloud to create one.

- For IBM® Storage Protect for Cloud Google Workspace, the IBM® Storage Protect for Cloud Partners system will check whether the customer has a Google Workspace app profile in IBM® Storage Protect for Cloud. If not, a pop-up window will appear, and you can click the **Create Google Workspace app profile** link to go to IBM® Storage Protect for Cloud and create a Google Workspace app profile.

Manage Customer Subscriptions

If you are managing a trial subscription, you can only change the subscription type from **Trial** to **Subscription**. When the subscription type is changed to **Subscription**, you must configure settings for services.

If you are managing a **Subscription** service, you can change the settings for subscription service.

Settings for Services

The subscription settings vary with services. The table below displays the details.

Service	Subscription Settings
IBM® Storage Protect for Cloud Microsoft™ 365	• **Subscription model** – Select the subscription model for the customer. **Note:** The options available to you are determined by the subscriptions you purchased from IBM® Storage Protect for Cloud. • **Storage** – Choose to use the customer's own storage or IBM® Storage Protect for Cloud storage. **Note:** If a customer uses IBM® Storage Protect for Cloud storage first and then wants to use a custom storage location, the customer can contact IBM Software Support team to migrate the previous backup data from the IBM® Storage Protect for Cloud storage location to the custom storage location. • **Storage profile** (for **Bring your own storage** only) – Select a storage profile from the drop-down list.

Service	Subscription Settings
	• **Retention** - If the customer uses IBM® Storage Protect for Cloud storage, configure the data retention by choosing one of the following options: ◦ **Retain data for _ years** – The data generated within the specific years will be kept. **Note:** The time to keep data is determined by the subscriptions you purchased from IBM® Storage Protect for Cloud. ◦ **Unlimited retention** – All data will be kept without any pruning. **Note:** If this option is available is determined by the subscriptions you purchased from IBM® Storage Protect for Cloud. • **Available Microsoft 365 licenses** – This is the number of all Microsoft 365 licenses that the customer's tenant purchased in Microsoft 365. • **Assigned Microsoft 365 licenses** – This is the number of Microsoft 365 licenses that have been assigned to users in the customer's tenant. IBM® Storage Protect for Cloud Microsoft™ 365 charge the tenant according to this number. You can click the **Download subscription details** link to download the customer subscription information. • **Source** - Select a value to indicate the source of your subscription. • **Package** - Select the package of the subscription. This field only appears when you configure the Microsoft 365 Services subscription. • **User seats** – If the customer has assigned product subscriptions in Microsoft 365, the number of user seats will be the same as the number of assigned Microsoft 365 subscriptions. Otherwise, the newly added subscription will have one user seat, and the existing subscription will keep the current number of user seats. This field only appears when you configure the Microsoft 365 subscriptions services. To view the user seats you own, click **View details of available user seats**. • **Purchased capacity (GB)** (For **Unlimited users** subscription model of Microsoft 365 only) – This value is the same as the value of the customer's protected capacity.

Service	Subscription Settings
	• **Protected capacity (GB)** (For **Unlimited users** subscription model of Microsoft 365 only) – View the size of the customer's protected data in Microsoft 365. • **Type** - Select the type for the subscription. This field only appears when you configure the Power Platform subscription. • **Limit** - Enter a number to define the limit of the subscription. This field only appears when you configure the Power Platform subscription. • **Subscription expiration Date** – Click the calendar button and select the subscription expiration date. To make the subscription expire immediately, select **Expire now**.
IBM® Storage Protect for Cloud Salesforce	• **Service Type** – Select the service type, **Basic**, **Standard**, or **Premier**. • **Salesforce user seats** – This field displays the number of active users in the customer's Salesforce platform. • **User seats** – Enter the total number of user seats this customer has purchased for this service. The previously purchased user seat amount plus the newly purchased user seat amount is the total number. To view the user seats you own, click **View details of available user seats**. • **Subscription expiration date** – Click the calendar button and select the subscription expiration date. To make the subscription expire immediately, select **Expire now**.

Service	Subscription Settings
IBM® Storage Protect for Cloud Dynamics 365	• **Storage** – Choose to use the customer’s own storage or IBM® Storage Protect for Cloud storage. • **Dynamics 365 user seats** – This is the number of all Dynamics 365 licenses that the customer’s tenant purchased in Dynamics 365 that could potentially be assigned to users. • **Assigned Dynamics 365 user seats** – This is the number of Dynamics 365 licenses that have been assigned to users in the customer's tenant. IBM® Storage Protect for Cloud licenses are based on the number of assigned licenses in a Dynamics 365 tenant. • **User Seats** – If the customer has assigned product licenses in Dynamics 365, the number of user seats will be the same as the number of assigned Dynamics 365 licenses. Otherwise, the newly added license will have one user seat, and the existing license will keep the current number of user seats. To view the user seats you own, click **View details of available user seats**. • **Subscription expiration date** – Click the calendar button and select the subscription expiration date. To make the subscription expire immediately, select **Expire now**.

Service	Subscription Settings
IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID	**Storage** – Choose to use the customer's own storage or IBM® Storage Protect for Cloud storage. **Note:** If a customer uses IBM® Storage Protect for Cloud storage first and then wants to use a custom storage location, the customer can contact the support team to migrate the previous backup data from the IBM® Storage Protect for Cloud storage location to the custom storage location. **User seat** – View and edit the User seat subscription of the customer's Microsoft Entra ID, Azure AD B2C, and Azure portal settings modules: • **Purchased user seats** – Enter the purchased user seats of the customer. • In the **Microsoft Entra ID** module,you can configure the subscription settings, and the configurations will also apply to other modules. **Retention** – If the customer uses IBM® Storage Protect for Cloud storage, configure the data retention by choosing one of the following options: • **Retain data for _ years/months** – The data generated within the specific years/months will be kept. **Note:** The time to keep data is determined by the subscriptions you purchased from IBM® Storage Protect for Cloud. • **Unlimited retention** – All data will be kept without any pruning. **Note:** If this option is available is determined by the subscriptions you purchased from IBM® Storage Protect for Cloud.

Service	Subscription Settings
IBM® Storage Protect for Cloud Google Workspace	• **Storage** - Choose to use the customer's own storage or IBM® Storage Protect for Cloud storage. • **Storage profile** (for **Bring Your Own Storage** only) – Select a storage profile from the drop-down list. • **Retention** – Configure the data retention by choosing one of the following options: ◦ **Retain Data for _ Years** – The data generated within the specific years will be kept. **Note:** The time to keep data is determined by the subscriptions you purchased from IBM® Storage Protect for Cloud. ◦ **Unlimited retention** – All data will be kept without any pruning. **Note:** If this option is available is determined by the subscriptions you purchased from IBM® Storage Protect for Cloud. • **User seats** – If the customer has assigned Google Workspace licenses to users, this number will be the same as the number of the assigned Google Workspace licenses. Otherwise, the newly added service will have one user license, and the existing service will keep the current number of user licenses. • **Subscription expiration date** – Click the calendar button and select the subscription expiration date. To make the subscription expire immediately, select **Expire now**.

Dashboard

The Dashboard page provides the following information:

- **Backup status** – In this section, you can view the total number of failed and finished with exception backups and auto discoveries in IBM® Storage Protect for Cloud Microsoft™ 365, IBM® Storage Protect for Cloud Google Workspace, IBM® Storage Protect for Cloud Dynamics 365, and IBM® Storage Protect for Cloud Salesforce, the number of customers with failed backups, finished with exception backups, auto discoveries, issues that occur, and the number of customers with no backup updates. You can also click the customer's organization name to view the backup details of the customer. Note that the products or modules that have expired will not be calculated here.
- **SharePoint storage** – In this section, you can view the customers whose SharePoint storage has exceeded the limit or are trending towards exceeding the limit in 90 days. By default, 5 customers are displayed in each section, and you can click **View nore** to view more records if any.
  - In the **Storage quota exceeded** section, you can view the following information about each customer:
    - 1 - The SharePoint storage limit of the customer.
    - 2 – The exceeded storage quota of the customer.
  - In the **Approaching storage limit** section, you can view the following information about each customer:
    - 1 – The SharePoint storage limit of the customer.
    - 2 – The exceeded storage quota of the customer. The value=consumed storage quota-storage limit.
    - 3 – The number of days when the customer will exceed the storage limit.

  > **Note:** To make sure a customer's SharePoint storage information can be retrieved and displayed in this section, the customer must have an app profile with the Microsoft Graph API > **Reports.Read.All** permission in IBM® Storage Protect for Cloud.

- **Storage** – In this section, you can view the storage type and usage of IBM® Storage Protect for Cloud Microsoft™ 365. To export the storage consumption report, click the **Export** button. A panel appears. You can choose one of the following methods to export the report:
  - If you want to export the report right away, click **Export now**.
  - If you want to set a schedule to export the report, select **Specify a schedule**. For details about schedule settings, refer to "Configure Export Schedule" on page 42.
- **Unusual activities analysis** – In this section, you can view the top five customers with the most OneDrives and SharePoint Online sites detected with unusual activities. Click the customer row to view the unusual activity details of the customer. To download a report which contains more information on unusual activities in a customer tenant, click **Export** in the row.
- **Policy monitor** – In this section, you can view the number of compliant customers without policy violations and non-compliant customers with policy violations as well as the percentage of the compliant/non-compliant customers. Click the number to view the customer list and you can click the customer to quickly access the customer detailed dashboard.
- **High risks** – In this section, you can view the top five customers with the most high risk items in the last 7 days together with a sample. Click the customer row to view the risk details of the customer. To download a PDF report which contains more information on risks in a customer's workspaces, click **Export** in the row.
- > **Note:** To export the report of Exchange Online, make sure a service account without multi-factor authentication enabled has been created for the customer. If not, the authentication alert window appears. You can click **Create service account** to create one for the customer, or you can click **Continue to export** to export the risk report without the Exchange Online report.

- **Total customers** – In this section, you can view the number of customers under your management.
- **New in last 7 days** – In this section, you can view the number of customers that were newly invited in the last 7 days.
- **Pinned customers** – In this section, you can view the customers you have pinned from the customer detailed dashboard or the **Customer subscriptions** page. You can also click the Unpin button to unpin the customer from this list.
- **YOUR CUSTOM WIDGET HERE** – In this section, you can enter your suggestions about what content, data, or tools you would like to see here to improve your Partner experience. Click **Submit** to submit your suggestions.

Configure Export Schedule

Procedure

Follow the steps below to configure the export schedule:

1. Select **Specify a schedule**.
2. Configure the following settings:
   - **Frequency** – Select a frequency from the drop-down list.
   - **File type** – Now, only **Excel workbook** is supported.
   - **Start date** – Click the calendar button and set a date to start sending the report.
   - **End date** – Choose **No end date** or **End by**. If you select **End by**, click the calendar button to set an end date.
   - **Recipients** – Enter one or multiple recipients' email addresses and use semicolons (;) to separate them.

   > **Note:** The scheduled reports will be exported at UTC 12:00 on the day you configured.

3. Click **Save** to save the export schedule settings. You can also click **Save and export** to export the report directly.

Manage Report Templates and Generate Reports

You can create a report template for IBM® Storage Protect for Cloud Microsoft™ 365 and then periodically generate reports using the template.

You can perform the following operations to manage templates on the **Reports** > **Template management** page:

- Search – You can search for templates by template name.
- Filter – You can filter templates by their generation frequency, creator, and schedule status.
- Generate Report – Click the ellipsis (***) icon next to a template, and then click **Generate Report** to generate a report using the template. The following two scenarios will occur:
  - If customers have already been defined in the template, reports will be generated and sent to those customers.
  - If customers have not been defined in the template, you need to select customers whose data will be reported and then choose users who will receive the reports.

    > **Note:** To send a report to a customer, make sure the setting for sending service reports is enabled for the customer, otherwise, the customer cannot receive the generated report. If you choose to send a report to customer, after clicking **Generate report**, an email notification will be sent to the customer. The customer needs to verify the email address used to receive the generated report before they can finally view the report.
- Edit Template – Click the ellipsis icon (***) next to a template, and then click **Edit template** to open the template and then make updates to it.
- Pause Schedule – Click the ellipsis icon (***) next to a template, and then click **Pause schedule** to pause the template schedule. Click **Confirm** in the pop-up message to confirm your operation.
- Restart Schedule – Click the ellipsis icon (***) next to a template, and then click **Restart schedule** to restart the template schedule. Click **Confirm** in the pop-up message to confirm your operation.
- Delete Template – Click the ellipsis icon (***) next to a template, and then click **Delete template** to delete the template. Click **Confirm** in the pop-up message to confirm your operation.

Create a Report Template

Refer to the following steps to create a report template:

Procedure

1. Click **Reports** > **Template management** > **Create template**.
2. On the **Basic information** step, complete the following back information, and then click **Continue**:
   - **Template name** – Enter a name for this template.
   - **Description** – Enter a description for future reference.
   - **How to generate the report?** – Select an option to define how you would like to generate the report.
     - **Manually generated** – If you select this option, you need to manually generate a report for customers using this template.
     - **Schedule and automatically generated** – If you select this option, you need to configure a schedule, select customers whose data will be reported, and define users who can access the report.
3. On the **Data selection** step, select the information in the IBM® Storage Protect for Cloud Microsoft™ 365 to be shown in the report. Click **Continue** to proceed.
   - IBM® Storage Protect for Cloud Microsoft™ 365

- **Protected data**
- **Backup status (successful, failed, and finished with exceptions)**
- **Success rate by workspace**

Before selecting data, you can click **View example** to view an example of the report.

4. On the **Schedule** step, define how and when you would like your report to be generated and sent out, and then click **Continue**.
   - **Frequency** – Select a value from the drop-down list: **Weekly**, **Monthly**, **Bi-monthly**, **Quarterly**, and **Annually**.
   - **Send on** – Based on the frequency you selected above, select a value from the drop-down list.
   - **Start date –** Configure a start date.
   - **End date –** Configure an end date. Select the **No end date** checkbox if you don't want to set an end date.
5. On the **Access** step, select customers whose data will be reported and define users who can access the report, and then click **Continue**:
   a. **Customers**– Select customers or customer groups from the drop-down list.
   b. **Send report to customers?** – Choose weather to send a report?
   c. **Also send to internal users** –Choose whether to send a report to internal users. After selecting the checkbox, you need to select internal users from the drop-down list.
6. On the review steps, review your configurations. You can back to the corresponding step if you want to make updates. If everything is fine, click **Create** to create the template.

View Report Statistics on the Dashboard

On the **Dashboard** page, data of service reports to customers is displayed. You can also click **Report center** in the upper-right corner to go to the view and create reports, or click **Create template** to create a service report template.

You can view the data in the following sections. Note that only data in the last 6 months is displayed.

Reports Overview

In this section, you can view the following information:

- **Sent (in the last 30 days)** – The number of reports sent to customers in the last 30 days.
- **Not accessed (in the last 30 days)** – The number of sent reports that have not been opened by customers in the last 30 days.
- **All sent** – The total number of reports sent to customers in the last 6 months.
- **Active templates** – The number of active report templates.
- **Overall report access** – The percentage of reports that have been accessed by customers in the last 6 months.
- **Report access statistics by customer** – The top 5 reports that have been accessed by customers and the percentage of the access rate is displayed for each report.

Schedule

In this section, you can view the following information:

- View data on the calendar – Click the date with a tag to view the number of reports that have been or that will be sent to customers on that date. You can also view the report numbers for each template.
- **Reports sent today** – The number of reports sent today.
- **Monthly template statistics** – The top 5 templates with the reports sent in the current month are displayed. You can also view the numbers of reports for each template.

Activities

In this section, you can view the activities of generating and sending the service reports. To view more activities, click **View report history** to go to the **Reports and history** page.

View Reports and History

On the **Reports and history** page, the generated reports and their generation history are displayed. Only the records of the last 6 months are displayed.

You can perform the following operations:

- Search – You can search for reports by customer name.
- Filter – You can filter reports by generation type – automatically generated or manually generated, report template, report status, and date range.
- View Report – Click the View Report () icon next to a report to view the report details. If you want to share the report with your customers, you can click **Save as PDF** to save the report as a PDF and send it to them offline.

View and Create Reports

This system provides the following built-in reports:

- **Customer operations report** - Allows administrators and users who have the **Customer operations report** permission to view their customers' jobs, request, data collection, and site connection status in their purchased services.
- **Subscription usage** - Allows administrators and users who have the **Subscription usage** permission to view their subscription transaction history report as well as the subscription usage information of their customers, which can also be exported.
- **Subscription expiration** - Allows partners to view customers with expired subscriptions (using IBM® Storage Protect for Cloud storage only).
- **Storage consumption report** - Allows administrators and users who have the **Storage consumption report** permission to view their customer's storage consumption associated with IBM® Storage Protect for Cloud Microsoft™ 365, and export the report.
- **User activity report** - Allows administrators to view user activities in the IBM® Storage Protect for Cloud Partners system and export the report.
- **Insight report** - Allows administrators to view insight reports generated on insight rules configured in this portal.

You can also create custom reports. For details, refer to "Create a Report" on page 48. On the **Reports** page, if you want to pin a custom report to **Dashboard**, click the star icon in the upper-right corner of the report card.

Customer Operations Report

About this task

To access **Customer operations report**, go to the **Reports** page and click **Customer operations report**.

The **Customer operations report** page shows a summary of all customers sorted by online services. You can click a service card to view the details of the summary.

Follow the instructions below to view a **Customer operations report**:

Procedure

Follow the instructions below to view a **Customer operations report**:

1. Click **View details** in the upper-right corner of a customer's card to view the report details. The report about each online service is displayed in the format of line chart.
2. Click the service name to access the tab of each service.
3. By default, the report displays statistics about last week's jobs and requests in all statuses. You can filter the report by job and request status and/or time range.
   a. **Time range** - Select **Yesterday**, **Last week**, **Last month**, or **This month** from the Time Range drop-down list.
   b. **Job status** - Select one or more statues from the drop-down list that is under the service tab, and click **OK**.

Subscription Usage Report

To view the subscription usage report, go to the **Reports** page and click **Subscription usage**. The **Subscription usage** page appears.

- The subscription usage information of the current user appears in the **Current usage** tab. You can click the **Details** link in the **Usage** column to view the usage details of a customer.
- The subscription medication history appears in the **Subscription modification history** tab.
  Follow the instructions below to export the **Subscription modification history** report:

a. Click the **Subscription modification history** tab.

b. Select a month from the calendar to define the time range and click **OK**. The subscription modification history records are displayed in a chart.

c. Click **Export** to export the report to your default download location.

- The usage information of the Enterprise subscriptions of all customers appears in the **Customer current usage** tab.
  Follow the instructions below to export the **Customer current usage** report:

  a. Click the **Customer current usage** tab.

  b. Select **Today** or the first day of any month to view the customer usage information on that day. If you select **Today**, the **Change** column indicates the pool subscription usage changes between today and the first day of the current month. If you select the first day, it will compare the data with the first day of the last month.

  c. Click **Export**, and a window appears. You can select a report format and modify the file name of the report in this window and click **Export** to export the report to your default download location.

Under each tab, you can filter records and manage columns on the page:

- **Filter** – Click **Filter** in the upper-right corner and customize the filter criteria. Click **Filter** to apply the criteria to filter records. All your filter criteria will be displayed at the top of the table, and you can also click the remove ( ) button next to each filter criterion to remove it.
- **Manage columns** – Click **Manage columns** in the upper-right corner to choose the columns you want to display on the page.

Subscription Expiration Report

To view the subscription Expiration report, go to the **Reports** page and click **Subscription expiration**. The **Subscription expiration** page appears.

The **Subscription expiration** report lists customers with expired subscriptions, who were using IBM® Storage Protect for Cloud Storage. From the date of expiration, all related data will only be kept for 30 days for Trial subscriptions and 15 days for subscriptions of another type.

In the search box on the right of the **Subscription expiration** page, enter keywords of customer account names and click the search button to search for customers.

Storage Consumption Report

About this task

To access the **Storage consumption report**, go to the **Reports > Report center** page and click **Storage consumption report**. The **Storage consumption report** page appears.

The **Storage consumption report** page displays a summary of all customers sorted by storage type. You can click a card to view the details of the summary.

Procedure

Follow the instructions below:

1. Find a customer card you want to view.
2. Click **View detailis** in the upper-right corner of the customer card to view the report. Click the service name to access the tab of a specific service.
3. Select **This month**, **Last month**, or **All time** from the **Time range** drop-down list.
4. Select the device type you want to view.
5. If you want to include the retention data that has been deleted in the IBM® Storage Protect for Cloud Microsoft™ 365 or IBM® Storage Protect for Cloud Dynamics 365, turn on the **Include retention data** switch.
6. You can change the unit of the storage by selecting an option from the **Unit** drop-down list.

7. Click **Export report**, and a window appears. You can choose whether to include details in the report and modify the file name in this window.
8. Click **Export** to export the report to a location of your choice.

User Activity Report

About this task

To access the **User activity report**, go to the **Report center** page and click **User activity report**. The **User activity report** page appears.

Procedure

Follow the instructions below to view and export user activities in this system:

1. Click the time range and select a month from the calendar to define the time range and click **Apply changes**.
2. Click **Export,** and a window appears. You can modify the file name of the report in this window and click **Export** to export it to a location of your choice. The report contains information about user activities within the selected month.

Insight Report

About this task

To access insight reports, go to the **Reports > Report center** page and click **Insight Report**. The **Insight Report** page appears.

Procedure

You can perform the following to generate an **Insight report**:

1. Use the **Type** and **Customer** filters on the top of the **Insight report** page to filter desired reports.
   a. **Type** – Select an option from the drop-down list to view reports of the selected types.
   b. **Customer** – Select customers from the drop-down list to view reports of the selected customers.
2. Click an insight report to view details.
3. Click the ignore ( ) button to ignore an insight report.

Create a Report

About this task

On the **Reports > Report center** page, click **Create a report**, and then configure the following settings:

Procedure

1. **Report name** – Enter a name for the report.
2. **Description** – Enter a description for the report.
3. If you want IBM® Storage Protect for Cloud Partners to export and send reports to specific recipients in a schedule, select the **Export the report in a schedule** checkbox. Click **Configure export settings**, and then configure the following settings:
   - **Frequency** – Select a frequency from the drop-down list.
   - **File type** – Now only **Excel Workbook** is supported.
   - **Start date** – Click the calendar ( ) button and set a date to start sending the report.

- **End date** – Choose **No end date** or **End by**. If you select **End by**, click the calendar ( ) button to set an end date.
- **Recipients** – Enter one or multiple recipients email addresses and use semicolons (;) to separate them.

> **Note:** The scheduled reports will be exported at UTC 12:00 on the day you configured them.

4. Click **Add a report part**.
5. In the **Add a report rart** window, configure the following settings:
   a. **Report part name** – Enter a name for the report part.
   b. **Template** – Select **Pie chart**, **Line chart**, or **Column chart** from the drop-down list.
   c. **Customer filter** (optional) – You can use this filter to filter customers to be included in this report. Click **Add a filter**, select a rule from the drop-down list, and then select desired values for the rule. Click **OK**. You can add multiple filter rules.
   d. **Horizontal axis** and **Vertical axis** – If you select **Line chart** or **Column chart**, configure the **Horizontal axis** and **Vertical axis** by selecting an option from the drop-down list.
   e. **Legend source** – Select the data as the legend source.
   f. **Legend entry** – Select one or more data values as the legend entries.

   > **Note:** You can select five legend entries at most. If you select the **Column chart**, you do not need to select the legend source and legend entry.

   g. Click **Save** to save your configurations. The report part is displayed.

   You can click the edit ( ) button to edit the report part settings or click the delete ( ) button to delete the report part.
6. You can click **Add a report part** again to add multiple report parts.
7. When you finish all report parts, click **Save** to save the report.

Settings

Configure General Settings

About this task

The **General settings** page is where IBM® Storage Protect for Cloud Partners can configure the time zone, the format to display the date or time, and a session timeout period for their tenant.

Procedure

To configure the general settings, complete the following steps:

1. Go to the **Settings** page, and click **General** in the **System** area to go to the **General settings** page.
2. Configure the following fields in the **Date and time settings** section:
   a. **Time zone** – Select the time zone for the tenant.

      > **Note:** If your country or region uses the Daylight Saving Time, you can select the **Automatically adjust clock for daylight saving time** checkbox to adjust IBM® Storage Protect for Cloud to the correct clock.

   b. **Date format** – Select the format to display the date.
   c. **Time format** – Select the format to display the time.
3. In the **System security policy** section, enter the number of the timeout period in the **Session timeout** text box, and select the unit for the timeout period from the drop-down list.
4. In the **MFA policy** section, you can enable multi-factor authentication for local accounts to sign in to IBM® Storage Protect for Cloud Partners. Once enabled, the MFA policy will be applied to all local accounts within your tenant.
   It is recommended that you use the Microsoft Authenticator app. For detailed instructions on this app, refer to the Microsoft article: Authentication methods in Microsoft Entra ID - Microsoft Authenticator app.
5. If your organization does not allow concurrent sign-ins, go to the **Concurrent sign-in setting** section and deselect the **Allow concurrent sign-ins from multiple locations for the same account** checkbox.
6. Click **Apply** to apply the configurations.

Reset Your Password

Procedure

You can reset the password of your account by completing the following steps:

> **Note:** You can only reset passwords for local users. For more information about user types, refer to "Manage Users" on page 15.

1. Navigate to the IBM® Storage Protect for Cloud Partners sign-in page.
2. Click the **Forgot your password** link under the **Sign in** button.
3. Enter the following information on the **Create new password** page:
   a. Enter the email address that you use to sign in to IBM® Storage Protect for Cloud Partners.
   b. Click **Send verification code**. A verification code will be sent to the email address you entered.
   c. Check the inbox of the email address. Enter the verification code and click **Verify code**.
   d. After your email address is verified, click **Continue**.

e. Enter the following information on this page:

i. **New password** – Enter a new password that you want to use.

ii. **Confirm new password** – Enter the new password again for confirmation.

f. Click **Continue**.

4. The IBM® Storage Protect for Cloud Partners **Dashboard** page appears automatically.

Configure Smart Tags

About this task

Smart tags can be used to label customers so you can categorize or find customers. When you invite new customers or edit customer accounts, you can apply tags to customers. In the **Customers**, you can filter customers by tags.

To manage smart tags, go to the **Settings** page, and click **Tag** in the **System** area.

Procedure

You can perform the following actions:

- **Create a tag** – Click **Add new tag** on the ribbon. In the **Create a tag** window, enter the tag name and description, and then click **Save**.
- **Edit** – Select a tag and click **Edit** on the ribbon, or click the ellipsis (•••) button of the tag and select **Edit** in the drop-down list. You can edit the tag name and description. When you finish the edits, click **Save**.
- **Delete** – To delete a tag, select the tag and click **Delete** on the ribbon, or click the ellipsis (•••) button of the tag and select **Delete** in the drop-down list. To delete multiple tags, select the tags and click **Delete** on the ribbon. A pop-up window appears asking for your confirmation. Click **OK** to confirm your deletion.

Manage Storage Profiles

About this task

Storage profiles are applied in licenses for services that use customers' own storage locations. To manage storage profiles, go to the **Settings** page, and click **Storage profile** in the **System** area.

To enhance security when using your storage device, it is highly recommended that you configure the storage firewall to allow only IBM® Storage Protect for Cloud access to your storage. For detailed instructions, refer to Allow IBM® Storage Protect for Cloud Agent Servers to Access Your Storage Account.

Procedure

You can perform the following actions:

- **Create** – Click **Create** on the ribbon. The **Create a storage profile** window appears. For more information, refer to "Create a Storage Profile" on page 51.
- **Edit** – Select a profile and click **Edit** on the ribbon, or click the edit ( ) button in the **Action** column of a profile. You can edit the name, description, and other settings of different storage types. When you finish the edits, click **Save**.
- **Delete** – To delete a profile, select the profile and click **Delete** on the ribbon, or click the delete ( ) button on the **Action** column of the profile. To delete multiple profiles, select the profiles and click **Delete** on the ribbon. A pop-up window appears asking for your confirmation. Click **OK** to confirm your deletion.

Create a Storage Profile

In the **Create a storage profile** window, enter the profile name and description, select **FTP**, **SFTP**, **Amazon S3**, **Amazon S3-Compatible Storage**, **IBM® Storage Protect - S3**, **IBM® Cloud Object Storage** or **Microsoft Azure Storage** from the **Storage type** drop-down list, and then configure the settings below based on the selected storage type.

- **FTP** or **SFTP -** In a storage profile for an FTP or SFTP server, configure the following settings:
  - **Host** – Enter the IP address of the server.
  - **Port** – Enter the port used to connect to this server. The default port is **1**.
  - **Folder** or **Root folder** – Once this profile is assigned to a customer, a folder named with the customer's registered account will be automatically created.
  - **Username** – Enter the username used to connect to this server.
  - **Password** – Enter the password of the specified username.
  - **Advanced** – If you want to configure extended parameters, select the **Advanced** checkbox, and enter the parameters in the **Extended Parameters** field.
  - **Retain the Data for** – Enter a number between 1 and 99 in this field.
- **Amazon S3** – In a storage profile for Amazon S3, configure the following settings:
  - **Bucket name** – Once this profile is assigned to a customer, a bucket named with the customer's registered account will be automatically created.
  - **Access key ID** – Enter the access key ID used to access the created bucket. You can view the access key ID from your AWS account.

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

  - **Secret access key** – Enter the secret Key ID used to access the created bucket.
  - **Storage region** – Select a storage region from the drop-down list for the created bucket.
  - **Advanced** – If you want to configure extended parameters, select the **Advanced** checkbox, and enter the parameters in the **Extended parameters** field. If you have multiple parameters to enter, press **Enter** on your keyboard to separate the parameters.
  - **Retain the Data for** – Enter a number between 1 and 99 in this field.
- **Amazon S3-Compatible Storage** – In a storage profile for Amazon S3-Compatible Storage, configure the following settings:
  - **Bucket name** – Once this profile is assigned to a customer, a bucket named with the customer's registered account will be automatically created.
  - **Access Key ID** – Enter the access key ID used to access the created bucket.
  - **Secret access key** – Enter the secret Key ID used to access the created bucket.
  - **Endpoint** – Enter the URL used to connect to the place where you want to store the data.

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

  - **Advanced** – If you want to configure extended parameters, select the **Advanced** checkbox, and enter the parameters in the **Extended parameters** field. If you have multiple parameters to enter, press **Enter** on your keyboard to separate the parameters. You can enter the following extended parameters if necessary.
    - **SignatureVersion** – By default, IBM® Storage Protect for Cloud uses V4 authentication to access your storage. If you want to use V2 authentication, add **SignatureVersion=V2** into the extended parameters.
- **IBM® Storage Protect - S3** – In a storage profile for IBM® Storage Protect - S3, configure the following settings:
  - **Bucket name** – Once this profile is assigned to a customer, a bucket named with the customer's registered account will be automatically created.
  - **Access key ID** – Enter the access key ID used to access the created bucket.
  - **Secret access key** – Enter the secret Key ID used to access the created bucket.

- **Endpoint** – Enter the URL used to connect to the place where you want to store the data.

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

- **Advanced** – If you want to configure extended parameters, select the **Advanced** checkbox, and enter the parameters in the **Extended parameters** field. If you have multiple parameters to enter, press **Enter** on your keyboard to separate the parameters. You can enter the following extended parameters if necessary.
  - **Allow_Insecure_SSL** – By default, the storage client expects an SSL certificate issued by a public trusted certificate authority over HTTPS transport to ensure integrity. A self-signed certificate on the storage server side will fail the certificate validation. If you choose to use a self-signed certificate, you can set the **Allow_Insecure_SSL** to **true** in the **Extended parameters** to bypass the certificate validation.
  - **SignatureVersion** – By default, IBM® Storage Protect for Cloud uses V4 authentication to access your storage. If you want to use V2 authentication, add **SignatureVersion=V2** into the extended parameters.
  - **Cert_thumbprint** – If you have a self-signed certificate for S3 server and you want to pass the certificate validation with a specific thumbprint, enter your thumbprint as the value of the parameter.

    > **Note:** The **Allow_Insecure_SSL** and **Cert_thumbprint** parameters cannot be added simultaneously.

- **Retain the Data for** – Enter a number between 1 and 99 in this field.

- **IBM® Cloud Object Storage** – In a storage profile for IBM® Cloud Object Storage, configure the following settings:
  - **Bucket name** – Once this profile is assigned to a customer, a bucket named with the customer’s registered account will be automatically created.
  - **Access key ID** – Enter the access key ID used to access the created bucket.
  - **Secret access key** – Enter the secret Key ID used to access the created bucket.
  - **Endpoint** – Enter the URL used to connect to the place where you want to store the data.

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

  - **Advanced** – If you want to configure extended parameters, select the **Advanced** checkbox, and enter the parameters in the **Extended parameters** field.
    - **SignatureVersion** – By default, IBM® Storage Protect for Cloud uses V4 authentication to access your storage. If you want to use V2 authentication, add **SignatureVersion=V2** into the extended parameters.
  - **Retain the Data for** – Enter a number between 1 and 99 in this field.

- **Microsoft Azure Storage** – In a storage profile for Microsoft™ Azure Storage, configure the following settings:
  - **Access point** – Enter the URL for the Blob Storage Service. The default URL is https://blob.core.windows.net.
  - **Container name** – Once this profile is assigned to a customer, a container named with the customer’s registered account will be automatically created.
  - **Account name** – Enter the account name used to access the created container.
  - **Account key** – Enter the access key used to access the created container.
  - **Enable CDN** – Select this checkbox if the Microsoft™ Azure content delivery network (CDN) is enabled.

- **GUID** – If you select **Enable CDN**, enter a GUID in this field.
- **Advanced** – If you want to configure extended parameters, select the **Advanced** checkbox, and enter the parameters in the **Extended parameters** field.
- **Retain the data for** – Enter a number between 1 and 99 in this field.

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

If the customers are using or plan to use their own storage devices, read the instructions in this section carefully and complete the settings upon their need. Otherwise, skip this topic.

When customers are using their own storage devices, they may have set up the storage firewall to only allow the trusted clients for security concerns. To ensure that IBM® Storage Protect for Cloud products can access the storage, complete the settings as required in the following conditions:

> **Note:** If customers are using a trial license and the storage account they 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 customers are using a storage type other than Microsoft Azure storage, they must add reserved IP addresses to their storage firewall. To get the list of the reserved IP addresses, refer to Download a List of Reserved IP Addresses.
- If customers are using Microsoft Azure storage, refer to the following:
  - **If the storage account is in the same data center as the one they use to sign up for IBM Online Services or the storage account is in itspaired region**, add the Azure Resource Manager (ARM) vNet subnets where the IBM agents are running on to their storage networking. Find additional details in this Microsoft article: Grant access from a virtual network. To get the ARM VNet subnet IDs for the data center, go to IBM® Storage Protect for Cloud > **Advanced Settings** > **Firewalls and Virtual Networks**. For detailed instructions, refer to the Add ARM virtual networks.
  - **Other than the condition above**, they need to add all the reserved IP addresses to the Azure storage firewall. For details, refer to “Add Reserved IP Addresses” on page 54.

Add Reserved IP Addresses

Procedure

Follow the steps below:

1. Navigate to **IBM® Storage Protect for Cloud** interface > **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.
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 Cloud network subnet resource ID
# This variable stores the resource ID of the subnet in the virtual network.
# Replace with the Azure Resource Manager (ARM) VNet ID downloaded from
your IBM® Storage Protect for Cloud tenant.

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

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

$DESTRG="customer_resource_group_name"

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

$DESTSTA="customer_storage_account_name"

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

az storage account network-rule add --resource-group $DESTRG --account-name $DESTSTA --
subnet $SUBNETID

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

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

# Step 9 (Optional): Verify that the default action for network rules is set to Deny
# This command shows the network rule set for the specified storage account, including
the default action.

az storage account show --resource-group $DESTRG --name $DESTSTA --query
networkRuleSet.defaultAction
```

- Use the Azure Az PowerShell (https://learn.microsoft.com/en-us/powershell/azure/install-azure-powershell?view=azps-14.2.0)

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

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

Connect-AzAccount

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

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

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

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

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

$DESTRG="customer_resource_group_name"

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

$DESTSTA="customer_storage_account_name"

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

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

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

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

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

Configure Insight Rules

About this task

If some of your customers use the IBM® Storage Protect for Cloud Microsoft™ 365, you can configure insight rules in this portal to monitor the status of IBM® Storage Protect for Cloud Microsoft™ 365 jobs for customers. You can view all insight reports in **Reports** >**Report center** > **Insight report**.

To manage insight rules, go to the **Settings** page, and click **Insight rules** in the **System** area.

Procedure

You can perform the following actions:

- **Create a rule** – Click **Create a rule** on the ribbon. The **Create a rule** window appears. For details, refer to Create an Insight Rule.
- **Edit** – Select a rule and click **Edit** on the ribbon, or click the ellipsis (•••) button of the rule and select **Edit**. For details, refer to Create an Insight Rule.
- **Turn on/off a rule** – Turn on/off the toggle in the **Status** column of a rule to turn on/off that rule.
- **Delete** – To delete a rule, select the rule and click **Delete** on the ribbon, or click the ellipsis (•••) button of the rule and select **Delete** in the drop-down list. To delete multiple rules, select the rules and click **Delete** on the ribbon. A pop-up window appears asking for your confirmation. Click **OK** to confirm your deletion.

Create an Insight Rule

Configure the following fields to create an insight rule:

- **Name** – Enter a required name.
- **Description** – Enter an optional description.
- **Tag** – Select tags from the drop-down list to apply the insight rule to specific customers marked with the selected tags.
- **Criteria** – Configure criteria for this insight rule.
- **Type** – Select **Information** or **Warning** as the type of this insight rule.
- **Automatically submit a support ticket upon a warning** (for **Warning** insight rules only) – With this option selected, once a warning is detected based on the insight rule, an email will be automatically sent to IBM Software Support.
- **Notify the following people about the insight report generated from this rule** – If you want to send email notifications to specific recipients when there are reports generated based on this rule, select this checkbox and enter email addresses in the **Recipients** text box.

Enable Trusted IP Address Settings

About this task

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

> **Note:** Only IPv4 addresses are supported.

Procedure

To enable trusted IP address settings, complete the steps below:

1. Go to the **Settings** page and click **Trusted IP address settings** in the **System** area.
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 an IP address range as trusted, click **New IP address range** in the **Trusted IP address range** field. Then, enter the IP address range. You can set multiple trusted IP address ranges.
3. Click **Save** to save your configurations or click **Cancel** to go back to the **Setting**s page without saving any configurations.

Manage Email Settings

Procedure

In **Settings › Notification › Email settings**, partners can configure the following settings:

- **Email sender** – Select one of the following options to configure the email sender:
  - **Default email address** - By default, all emails will be sent from the following email address: noreply@sp4c.storage-defender.ibm.com
  - **Custom email server and email address** – Select this option, and the emails will be sent from your custom email server and email address. Configure the following fields:
    - **Email server** – Enter the address of the email server.
    - **Port** – Enter the SMTP port.
    - **Email sender display name** – You can specify a display name for the email sender.

      > **Note:** If you specify Microsoft 365 as your email server, and when the email sender and email recipients are in the same tenant, the specified display name of the email sender will not be shown in the emails. Users will see the email sender's display name, which is configured in Microsoft 365.

    - **Email address** – Enter an email address, and the notification emails will be sent from your specified email address.
    - **Username** – Enter the sender's username on the SMTP server.
    - **Password** – Enter the sender's password to log into the SMTP server.
    - **Authentication** (Optional) – You can select **SSL authentication** or **Secure password authentication** according to your email settings.

  Click **Validate** to validate the email sender.
- **Language** – The following display languages are supported in notification emails: English, French, and German. The default display language is set according to a partner's region. To change the display language of notification emails' content, follow the steps below:
  - Select the **Language** tab.
  - In the **Select a display language** drop-down list, select an option.
  - If you want to update the email language for all your customers, select the **Update language settings for all customers' tenants in IBM® Storage Protect for Cloud** checkbox.
- Click **Save** to save the configurations.

Manage Email Templates

IBM® Storage Protect for Cloud Partners allows partners to send out the following email notification:

- After a user is invited to the system, IBM® Storage Protect for Cloud Partners will send an email to the user.
- If you choose to send billing reports to a customer, IBM® Storage Protect for Cloud Partners will send emails based on the schedule in the billing profile.
- If you choose to export the custom report based on a schedule, IBM® Storage Protect for Cloud Partners will send emails to the configured recipients in the report settings.
- If you choose to send service reports to customers, IBM® Storage Protect for Cloud Partners will send emails to customers after you generate the service report.

There is a built-in user invitation template, a built-in customer billing email template, a built-in exported customer report template, and a built-in customer service report template. You can create customized email templates and set them as default ones.

To manage the **Email template**, go to the **Settings** page, and click **Email template** in the **Notification settings** area. The **Email template** page appears. By default, all the email templates are displayed.

You can perform the following actions:

- **Create** – Click **Create** to go to the **Create email template** page. For details, refer to Create Email Templates.
- **View** – Click the email template name to go to the **View email template** page and view the information and preview of the template.
- **Edit** – Select an email template, and click **Edit** to go to the **Edit email template** page to edit the email template. For details, refer to Create Email Templates.

  > **Note:** The built-in email templates cannot be edited.

- **Set as default** – Select an email template, and click **Set as default** to choose the template for sending invitation emails.
- **Delete** – Select one or more email templates, and click **Delete** to delete the selected email templates. A pop-up window appears asking for your confirmation. Click **OK** to confirm your deletion.

  > **Note:** The built-in email templates cannot be deleted.

Create Email Templates

Procedure

On the **Create email template** page, configure the following fields:
If you like to show a custom logo in the notification emails, click the **Branding logo** link to configure it.

- **Email template name** – Enter a name for the new email template. If you want to use this template to send emails, select the **Set as default** checkbox.
- **Email template type** – Select the template type for the email template.
  - **User invitation email** – The email template that is used to invite users to IBM® Storage Protect for Cloud Partners.
  - **Customer billing email** – The email template that is used to send billing reports to customers.
  - **Exported customer report email** – The email template that is used to send exported custom reports.
  - **Customer service report email** - The email template that is used to send service reports to customers.

- **Description** – Enter an optional description.
- **Email subject** - Enter the subject of the emails for this email template. You can insert a reference in the subject by clicking **Insert reference**. A reference is a parameter that will call up the corresponding information for each user, partner, report, etc. For descriptions for the email template references, refer to the "Supported References in Email Templates" on page 61.
- **Email body** – Define the body of the email template. You can insert a reference in the subject by clicking **Insert reference**. A reference is a parameter that will call up the corresponding information for each user, partner, report, etc. For descriptions for the email template references, refer to "Supported References in Email Templates" on page 61.
- Click **Save** to save the configurations.

Supported References in Email Templates

Supported References	Reference Description
Billing Period	The billing period of the billing report sent to the customer.
Customer Organization Name	The organization name of the customer.
Partner Organization Name	The organization name of the partner.
Registered Account	The name of the customer organization's registered account.
Report Name	The name of the report to be sent.
User Email	The email address of the user in Elements for Partners.

Manage Job Notification Profiles

About this task

Job notification profiles allow you to specify recipients for notification emails of different services. To begin with, you must configure job notification profiles for customers. In a job notification profile, you can specify the recipients who will receive notification emails and specify the customers to whom the job notification profile applies.

> **Note:** For customers without a job notification profile applied, the notification emails will be sent to Administrators and users who have the **Receive email notifications** permission.

To manage job notification profiles, go to the **Settings** page, and click **Job notification Profile** in the **Notification settings** area.

Procedure

You can perform the following actions:

- **Create job notification profile** – Click **Create notification profile** and select **Job notification**. The **Create job notification profile** page appears. For more instructions, refer to "Create a Job Notification Profile" on page 62.
- **Create service monitoring notification profile** – Click **Create notification profile** and select **Service monitoring**. The **Create service monitoring notification profile** page appears. For more instructions, refer to Create a Service Monitoring Profile.
- **Edit** – Select a profile and click **Edit** on the ribbon. The **Edit job notification profile** page will appear. Edit the profile settings and click **Save** to save your edits.
- **Delete** – Select one or more profiles and click **Delete** on the ribbon. Click **OK** to confirm your deletion.

Create a Job Notification Profile

About this task

On the **Create job notification profile** page, configure the following fields, and click **Save** to save the configurations:

- **General** – Enter the general information for this job notification profile:
  - **Profile name** – Enter a profile name.
  - **Description** – Enter a description if necessary.
- **Services** – Click the desired service and configure the related settings:
  - For **IBM® Storage Protect for Cloud**, turn on the toggle, and you can configure the following:
    - **Send the email notifications for the jobs in the following statuses** – Select the checkbox next to status to specify the job statuses for auto discovery jobs which will trigger the job notification emails. If the **Finished with exception** status is selected, you can additionally select the **Include finished with exception job reports as attachments** option if you want to attach job reports to notification emails.
    - **Send email notifications to the following email addresses** – Enter email addresses in the text box to specify the recipients who will receive notification emails for all auto discovery jobs of specific statuses.
    - **Out of policy email recipients** – If you want to send notification emails for out-of-policy objects, select the checkbox and specify the recipients by entering their email addresses in the text box.
  - For **IBM® Storage Protect for Cloud Microsoft™ 365**, turn on the toggle, and you can configure the following:

        - **Send the email notifications for the jobs in the following statuses** – Select the checkbox next to status to specify the job statuses for backup jobs which will trigger the job notification emails.
        - **Send email notifications to the following email addresses** – Enter email addresses in the text box to specify the recipients who will receive the notification emails for all backup jobs of specific statuses.
        - **Customize the notification for the restore and export jobs** – If you want to send notification emails to recipients who manage the export and restore jobs, select the checkbox and configure the specific recipients and job statuses.
    - For **IBM® Storage Protect for Cloud Google Workspace**, turn on the toggle, and you can configure the following:
        - **Send the email notifications for the jobs in the following statuses** – Select the checkbox next to status to specify the job statuses for backup jobs which will trigger the job notification emails.
        - **Send email notifications to the following email addresses** – Enter email addresses in the text box to specify the recipients who will receive the notification emails for all backup jobs of specific statuses.
        - **Customize the notification for the restore and export jobs** – If you want to send notification emails to recipients who manage the export and restore jobs, select the checkbox and configure the specific recipients and job statuses.
    - For **IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID**, turn on the toggle, and you can configure the following:
        - **Send the email notifications for the jobs in the following statuses** – Select the checkbox next to status to specify the job statuses for backup jobs which will trigger the job notification emails.
        - **Send email notifications to the following email addresses** – Enter email addresses in the text box to specify the recipients who will receive the notification emails for all backup jobs of specific statuses.
        - **Frequency** – If **Unprotected warning** is enabled above, you need to define the frequency.
- **Customers** – Select customer groups to apply the job notification profile. If you want to choose individual customers to apply, turn on the **Choose individual customers manually** toggle, select the checkboxes next to the customers who will have this profile applied. In addition, you can choose whether to set this job notification profile as default for newly onboarded customers.

> **Note:** After a job notification profile is configured for a customer, notification settings in IBM® Storage Protect for Cloud, IBM® Storage Protect for Cloud Microsoft™ 365, and IBM® Storage Protect for Cloud Google Workspace cannot be updated. If necessary, the customer can contact the managing partner to update the profile in the partner portal.

Create a Service Monitoring Profile

On the **Create service monitoring notification profile** page, configure the following fields, and click **Save** to save the configurations:

- **General** – Enter the general information for this service monitoring notification profile:
    - **Profile name** – Enter a profile name.
    - **Description** – Enter a description if necessary.
- **Services** – Configure the related settings for IBM® Storage Protect for Cloud Microsoft™ 365.
    - **Service monitoring** – The services that will be monitored are listed.
    - **Send email notifications to the following email addresses** – Enter email addresses in the text box to specify the recipients who will receive notification emails for the monitoring services.
- **Customers** – Select customer groups to apply the notification profile. If you want to choose individual customers to apply, turn on the **Choose individual customers manually** toggle, select the checkboxes next

to the customers who will have this profile applied. In addition, you can choose whether to set this notification profile as default for newly onboarded customers.

Manage Billing Profiles

About this task

If you want to send billing reports to customers, you must configure billing profiles. In billing profiles, you can add services' billing information, discount information, and the frequency of sending billing reports.

To manage billing profiles, go to the **Settings** page, and click **Billing profile** in the **Notification settings** area.

Procedure

You can perform the following actions:

- **Create** – Click **Create** on the ribbon. The **Create a profile** page appears. For more instructions, refer to "Create a Billing Profile" on page 65.
- **Edit** – Select a billing profile and click **Edit** on the ribbon. You can edit the billing profile settings, and click **Save** after you finish the edits.
- **Delete** – Select one or more billing profiles and click **Delete** on the ribbon. Click **OK** to confirm your deletion.

Create a Billing Profile

Procedure

On the **Create a profile** page, configure the following fields:

- **Profile name** – Enter a profile name.
- **Description** – Enter a description if necessary.
- **Discount** – If you want to add a discount, select the **Enable discount _ %** checkbox, and then enter an integer between 1 and 100 in the text box.
- **Frequency** – Choose to send billing reports **Monthly** or **Yearly**:
  a. **Monthly** – In the **Send on day _ of every month** text box, enter an integer between 1 and 31.
  b. **Yearly** – Select a month from the **Send on _ _** drop-down list, and enter a day in the text box.
- **Currency** – Select a currency from the drop-down list.
- **Service**, **Billing property**, and **Unit price** – Click **Add a service**, select an option from the **Service** and **Billing property** drop-down lists, and enter a number greater than zero in the **Unit price** text box. If you want to delete a service, click the delete ( ) button.
- Click **Save** to save the configuration.

Configure the Branding Logo

A branding logo is displayed in the service report, risk assessment report, and most notification emails sent from IBM® Storage Protect for Cloud Partners.

Procedure

To configure the branding logo, complete the following steps:

1. In **Setting › Notification › Branding logo**, you can select one of the following options to configure the branding logo:
   - **The default branding logo** – Select this option to display the default logo.
   - **A custom branding logo** – Select this option to display your custom logo. Click **Upload** to upload an image.

     > **Note:** The maximum size of the image is 1 MB, and the type of the image must be PNG, JPG, or JPEG. The recommended size is 160 x 60 pixels.

2. You can click **Reset** to reset the image to the default one.
3. Click **Save** to save the configurations.

Configure Announcement Notification Settings

To ensure important announcements can be received when they are published, you can enable the announcement notification in Elements for Partners. When Elements for Partners publishes an announcement such as service interruption or additional required configurations, the configured recipients will receive a notification email.

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

To configure announcement notification settings, go to the **Settings** page, and click **Announcement notification** in the **Notification** area. Turn on/off the toggle to define if you want to enable the announcement notification.

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

- **Categories**
  - **Service interruption**
  - **Environment updates (product releases)**
  - **Additional configurations required**
  - **Informational (new features)**
- **Select email recipients:**
  - **Tenant Owner in IBM® Storage Protect for Cloud Partners**
  - **Administrators in IBM® Storage Protect for Cloud Partners**
  - **Custom recipients** – You can enter multiple email addresses in the text box and separate them with a semicolon (;).

Click **Save** to save the configuration.

Manage Customer App Profiles

On the **Settings** > **Additional** > **Customer app profile** page, the app profiles that you created for your customers' services are displayed. You can perform the following actions to manage customer app profiles:

- **Create app profile** – You can also create app profiles for customer's IBM® Storage Protect for Cloud Microsoft™ 365 service. For detailed instructions, refer to Create a Customer App Profile.
- **Re-authorize app** – The app profiles with the **Expired** status must be re-authorized. To re-authorize the app for an app profile, select the app profile and click **Re-authorize app**. Enter the credentials of the customer's tenant account, review the required permissions, and click **Accept**.

  > **Note:** Currently, only modern app profiles can be re-authorized on this page. Classic app profiles and custom app profiles need to be re-authorized in IBM® Storage Protect for Cloud. For detailed instructions, refer to Re-authorize an App Profile.

- **Delete** – To delete the app profiles, select the app profiles and click **Delete**.

  > **Note:** If the app type of an app profile is not supported being created in **Customer app profile**, the app profile cannot be deleted.

Create a Customer App Profile

On the **Customer app profile** page, click **Create app profile** and follow the steps below to create an app profile for a customer organization:

1. **Select customer and tenant** – Select the customer and tenant for which you want to create app profiles. Click **Next**.
2. **Select services** – **IBM® Storage Protect for Cloud Microsoft™ 365** is supported. Click **Next**.
3. **Choose setup method** – Now only modern mode is supported. In this mode, the related apps are listed in a service-based view, and you can consent to apps separately for the selected services.
4. **Consent to apps** – Click **Authenticate** next to the app. 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.
   Enter the credentials of the customer's Microsoft 365 Global Administrator account. Review the permissions requested by this app and click **Accept**.

   For the app types of IBM® Storage Protect for Cloud services and required permissions, refer to API Permissions Required by IBM Apps.

   When you finish creating app profiles, click **Save**.
5. After you create app profiles for the apps that will be used to manage Exchange mailboxes and settings / Security and distribution group objects / Microsoft 365 Defender settings, you may need to go to Microsoft Entra admin center (or Microsoft Azure portal) 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?.

Manage Customer Feedback

About this task

Feedback management allows you to manage customer feedback about online services.

To access **Feedback management**, go to the **Settings** page, and select **Feedback management** in the **Additional** area. The **Feedback management** page appears. By default, all feedback from the current year is displayed.

Procedure

You can perform the following actions:

- **Filter feedback** – Filter feedback by year or by service.
  - Select a year from the drop-down list in the upper-left corner.
  - Click **Filter** and select one or more services, then click **Apply**.
- **View details** – To view detailed information about a feedback, click the feedback ID. The **View feedback** page appears.
- **Edit feedback** – To edit a feedback, click the feedback ID, and then click **Edit** on the **View feedback** page. You can edit the following fields:
  a. **Feedback status** – Choose one of the following options:
     a. **Unresolved** – The feedback is not resolved yet.
     b. **Resolved** – The feedback is resolved.
     c. **Won't fix** – The feedback will not be fixed.
  b. **Comment** – Enter a comment for the feedback or your operation.

  Click **Save** to save your changes, or click **Cancel** to go back to the **View feedback** page without saving any changes.
- **Delete feedback** – To delete one or more feedback items, select the checkboxes next to the feedback IDs and click **Delete** on the ribbon. A pop-up window appears asking for your confirmation. Click **OK** to confirm your deletion.

IBM® Storage Protect for Cloud Partners Public API

You can use the IBM® Storage Protect for Cloud Partners Public APIs to retrieve the information of your customers such as services, job details, and scan profile information.

To avoid 429 throttling issues, we recommend limiting API requests to a maximum of 5 per endpoint every 10 seconds from a single IP address.

Deprecation Notice

The legacy API introduced below offers essential capabilities but is slated for deprecation. We are upgrading to a new API for better user experience, stability, and easier integration. Transitioning to the new API is recommended to ensure continued support and access to the latest features.

App Registration

Before using the APIs, you must register an app and grant permissions to the app. With the registered app, you can use the generated application (client) ID for authentication. For details, refer to Configure App Registrations.

Register an App

Complete the following steps to register an app:

1. Go to the **Settings** page and select **API app registration** in the **Additional** area.
2. On the **API app registration** page, click **Create app registration**.
3. Complete the following steps:
   a. Enter a name for the app.
   b. Select the corresponding permissions that you need to grant to this app.
   c. 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 Certificate** to upload a certificate (.cer file). The certificate serves as credentials that allow your application to authenticate as itself, requiring no interaction from a user at runtime. You can refer to Prepare a Certificate for the Custom Azure App to prepare a 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 secret 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.
   d. Click **Save** to save your configurations.

   When you finish the registration, click the app name and you can copy the generated application (client) ID on the app details page.

Edit an App

Complete the following steps to edit an app:

1. On the **API app registration** page, click the app name to access the app details.
2. In the Basics tab, you can update the app name, permissions, and customer scope if required.
3. In the **Certificates and secrets** tab, you can view and manage the certificate and client secret.

Delete Apps

On the **API app registration** page, select the apps and click **Delete** on the ribbon. The selected apps will be deleted.

Get the Access Token

Based on the credentials of an app registration in, refer to the following sections:

- If you want to get access token with a client secret in an app registration, refer to instructions in Client Secret.
- If you want to get access token with a certificate in an app registration, refer to instructions in Certificate.

Client Secret

To obtain an access token using a client secret in an app registration, follow these steps instructions below to submit a POST request:

1. Set the access token URL: **https://identity.sp4c.storage-defender.ibm.com/connect/token**.
2. Set the header to **Content-Type: application/x-www-form-urlencoded**.
3. Set the following parameters in the request body:
   - **grant_type** – Set this value to **client_credentials**.
   - **client_id** – Copy the **Application (Client) ID** value in the app registration and paste the value here.
   - **client_secret** – Copy the **Client Secret** value that has been saved upon the creation of the app registration, and paste the value here.
4. In the response, the **access_token** node represents the token value, the **expires_in** node represents the token will be expired in how many seconds, and the **scope** node lists the assigned permissions of the app registration.

Certificate

Once you have the application (client) ID, get the access token via the application (client) ID to authenticate with IBM® Storage Protect for Cloud Partners APIs

The following information is required to get an access token:

Element	Description
Identity Service URL	https://identity.sp4c.storage-defender.ibm.com
Application (Client) ID	The application (client) ID you have retrieved.
Certificate	The corresponding .pfx certificate file of the .cer certificate you used when registering the app.

To get the access token using the above information, create a JSON web token using the Client ID and certificate first, and then use the JSON web token to request an access token of the defined scope from Identity Service.

Below is an example for getting the access token.

```
var identityServiceUrl = "{https://identity.sp4c.storage-defender.ibm.com}";
var client = new HttpClient();
var disco = await client.GetDiscoveryDocumentAsync(identityServiceUrl);
if (disco.IsError)
{
return;
}
var tokenResponse = await client.RequestClientCredentialsTokenAsync(new
ClientCredentialsTokenRequest
{
Address = disco.TokenEndpoint,
ClientAssertion = new ClientAssertion()
{
```

```
Type = OidcConstants.ClientAssertionTypes.JwtBearer,
Value = CreateClientAuthJwt(disco)
}
}
if (tokenResponse.IsError)
{
return;
}
return tokenResponse.Json
private static string CreateClientAuthJwt(DiscoveryDocumentResponse response)
{
var clientId = "{Client ID}";
var certificateThumbprint = "{Certificate Thumbprint}";

// set exp to 5 minutes
var tokenHandler = new JwtSecurityTokenHandler { TokenLifetimeInMinutes = 60 };

var securityToken = tokenHandler.CreateJwtSecurityToken(
// iss must be the client_id of our application
issuer: clientId,
// aud must be the identity provider (token endpoint)
audience: response.TokenEndpoint,
// sub must be the client_id of our application
subject: new ClaimsIdentity(
new List<Claim> { new Claim("sub", clientId),
new Claim("jti", Guid.NewGuid().ToString())}),
// sign with the private key (using RS256 for IdentityServer)
signingCredentials: new SigningCredentials(
new X509SecurityKey(new X509Certificate2(LoadCertificate(certificateThumbprint))), "RS256")
);
return tokenHandler.WriteToken(securityToken);
}
private static X509Certificate2 LoadCertificate(string certificateThumbprint)
{
var store = new X509Store(StoreName.My, StoreLocation.LocalMachine);
store.Open(OpenFlags.ReadOnly);
var vCloudCertificate = store.Certificates.Find(
X509FindType.FindByThumbprint,
certificateThumbprint,
false)[0];
return vCloudCertificate;
}
```

Note: The token you get will expire in one hour, and you need to get the token again after the expiration.

Supported APIs

The API URL of IBM® Storage Protect for Cloud Partners is **https://graph.sp4c.storage-defender.ibm.com/partner**.

GET api/v1.1/customers

Get the general information of the customers that you manage.

Required Permission: partner.customers.read.all

Response Information:

Element	Description	Type
id	The tenant owner ID of the customer.	string
organization	The organization name of the customer.	string
ownerEmail	The tenant owner email address of the customer.	string
jobStatus	The status of the customer's tenant.	string
countryOrRegion	The country or region name of the customer.	string

GET api/v1.1/customers('id')

Get the general information of a specific customer that you manage.

Required Permission: partner.customers.read.all

Response Information:

Element	Description	Type
id	The tenant owner ID of the customer.	string
organization	The organization name of the customer.	string
ownerEmail	The tenant owner email address of the customer.	string
jobStatus	The status of the customer's tenant.	string
countryOrRegion	The country or region name of the customer.	string

GET api/v1.1/customers('id')/protected

Get your customers' protected data information of IBM® Storage Protect for Cloud Microsoft™ 365.

> **Note:** Only the IBM® Storage Protect for Cloud Microsoft™ 365 service that customers have the subscription for is supported.

Required Permission: partner.cbprotected.read.all

Response Information:

Element	Description	Type
customerId	The tenant owner ID of the customer.	string
customer	The tenant owner email address of the customer.	string
serviceType	The IBM® Storage Protect for Cloud Microsoft™ 365 service that the customer has subscriptions for.	string
serviceModule	The module of the customer's service.	string
totalScannedObjects	The number of the scanned objects.	integer
totalProtectedObjects	The number of the backed-up objects	integer
dataSizeStoredInIBM	The size of the backed-up objects stored in the IBM storage.	string
dataSizeStoredInBYOS	The size of the backed-up objects stored in BYOS.	string

GET api/v1.1/services

Get the license details of different services for the customers that you manage.

> **Note:** Only services that customers have the **Enterprise** subscription for are supported.

Required Permission: partner.license.read.all

Response Information:

Element	Description	Type
customerId	The tenant owner ID of the customer.	string
organization	The organization name of the customer.	string
customer	The tenant owner of the customer.	string

Element	Description	Type
tenantId	The tenant ID of the customer.	string
products	A list of products that the customer has subscribed to.	list

Product subscriptions:

Element	Description	Type
service	The service that the customer has subscriptions for.	string
subscriptionModel	The subscription model of the customer's service.	string
purchasedUserSeats	The number of purchased user seats of the customer.	string
microsoftLicenseAssigned	The number of assigned Microsoft licenses of the customer.	string
microsoftLicenseAvailable	The number of available Microsoft licenses of the customer.	string
purchasedCapacity	The purchased capacity of the customer.	string
protectedCapacity	The protected data size of the customer.	string
storage	The storage type of the customer.	string
retention	The data retention period of the customer.	string
consumedStorage	The consumed storage size of the customer.	string
expirationDate	The expiration date of the customer's service.	string
change	The user seats changes in the pool license compared with the first day of the current month.	string
source	The source of the subscription.	string

GET api/v1.1/services('CustomerId')

Get the license details of different services for a specific customer that you manage.

> **Note:** Only services that customers have the **Enterprise** subscription for are supported.

Required Permission: partner.license.read.all

Response Information:

Element	Description	Type
customerId	The tenant owner ID of the customer.	string
organization	The organization name of the customer.	string
customer	The tenant owner email address of the customer.	string
tenantId	The tenant ID of the customer.	string
product	A list of products that the customer has subscribed to.	list

Product subscriptions:

Element	Description	Type
service	The service that the customer has subscriptions for.	string
subscriptionModel	The subscription model of the customer's service.	string
purchasedUserSeats	The number of purchased user seats of the customer.	string
microsoftLicenseAssigned	The number of assigned Microsoft licenses of the customer.	string
microsoftLicenseAvailable	The number of available Microsoft licenses of the customer.	string
purchasedCapacity	The purchased capacity of the customer.	string
storage	The storage type of the customer.	string
retention	The data retention period of the customer.	string
consumedStorage	The consumed storage size of the customer.	string
expirationDate	The expiration date of the customer's service.	string

GET api/v1.1/customers('id')/jobs

Get the job details of backup services of a specific customer that you manage.

> **Note:** Only job details of the service that the customer has the subscription for are supported.

Required Permission: partner.jobs.read.all

Response Information:

Element	Description	Type
jobType	The service type of the job.	string
jobModule	The service module of the job.	string
status	The job status.	string
jobId	The job ID.	string
name	The job name.	string
totalCount	The count of the objects that have been processed by the job.	string
failedCount	The count of the failed objects.	string
successfulCount	The count of the successful objects.	string
skippedCount	The count of the skipped objects.	string
warningCount	The count of the warning objects.	string
backupSize	The size of the backed-up objects.	string
startTime	The start time of the job	string
endTime	The end time of the job.	string
jobDuration	The job duration.	string
lastModifyTime	The last modified time of the job.	string

GET api/v1.1/customers('id')/jobs(JobType='job type',JobModule='job module')

Get the job details of a specific job type and module of backup service for a customer that you manage.

> **Note:** Only job details of the service that the customer has the subscription for are supported
> **Supported job type values**: Microsoft 365, Google Workspace, Azure, Dynamics 365, or Salesforce

Supported job module values:

- Microsoft 365: SharePoint Online, Exchange Online, Microsoft 365 Group, OneDrive, Project Online, Exchange Online Public Folders, Microsoft Teams, Microsoft Teams Chat, Viva Engage, Power BI, Power Automate, or Power Apps
- Google Workspace: Gmail, Calendar, Contacts, Drive, or Shared Drives
- Azure: Virtual Machine, Microsoft Entra ID, Storage, or Admin Portal Setting
- Dynamics 365: Dynamics Customer Engagement or Dynamics Unified Operations
- Salesforce: Salesforce

Required Permission: partner.jobs.read.all

Response Information:

Element	Description	Type
jobType	The service type of the job.	string
jobModule	The service module of the job.	string
status	The job status.	string
jobId	The job ID.	string
name	The job name.	string
totalCount	The count of the objects that have been processed by the job.	string
failedCount	The count of the failed objects.	string
successfulCount	The count of the successful objects.	string
skippedCount	The count of the skipped objects.	string
warningCount	The count of the warning objects.	string
backupSize	The size of the backed-up objects.	string
startTime	The start time of the job	string
endTime	The end time of the job.	string
jobDuration	The job duration.	string
lastModifyTime	The last modified time of the job.	string

GET api/v1.1/customers('id')/scanprofiles

Get the information of all scan profiles configured in IBM® Storage Protect for Cloud for a customer.

Required Permission: partner.scanprofiles.read.all

Response Information:

Element	Description	Type
profileName	The name of the scan profile.	string
profileId	The ID of the scan profile.	string

Element	Description	Type
scanMode	The scan mode of the scan profile. • 0 – Express mode • 1 – Advance mode	integer
modifiedTime	The last modified time of the scan profile.	string

GET api/v1.1/customers('id')/ScanProfilesDetails(ProfileId='ProfileId')

Get a scan profile information configured in IBM® Storage Protect for Cloud for a customer.

Required Permission: partner.scanprofiles.read.all

Response Information:

Element	Description	Type
profileId	The ID of the scan profile.	string
profileName	The name of the scan profile.	string
description	The description of the scan profile.	string
tenantId	The tenant ID the scan profile.	string
tenantDomain	The tenant domain of the scan profile.	string
scanMode	The scan mode of the scan profile. 0 – Express mode 1 – Advance mode	string
modifiedTime	The last modified time of the scan profile.	string
createdTime	The created time of the scan profile.	string
impersonationAccount	The impersonation account configured in the scan profile.	string
scanInplaceArchivedMailboxes	Whether or not the **Scan in-place archived mailboxes**setting is enabled in the scan profile. True – Scan in-place archived mailbox False – Do not scan in-place archived mailbox	boolean
isIgnoreLockedSiteEnabled	Whether or not the **Ignore the locked objects when updating the job status** setting is enabled in the scan profile. True – Enabled False – Disabled	boolean
enableDailyScan	Whether or not the **Enable daily scan** setting is enabled in the scan profile. No – Daily scan is not enabled. hh:mm – The time of the daily scan. For example: 01:59.	string

Element	Description		Type
isSendOutOfPolicy Notification	Whether or not the **Send an email notification to the following recipients when objects are moved to other containers or removed from any containers** setting is enabled in the scan profile. True – Enabled False – Disabled		boolean
containers	The container details of the scan profile.	ContainersName	string
		ObjectType	string

Note: To improve the experience, we've added **isIgnoreLockedSiteEnabled** to replace **ignoreTheLockedObjectsWhenUpdatingTheJobStatus** and added **isSendOutOfPolicyNotification** to replace **sendAnemailNotificationToTheFollowIngRecipientsWhenObjectsAreMovedTooTherContainerOrRemovedFromAnyCont**

GET api/v1.1/Customers('id')/ScanProfilesDailyNew(ProfileId='ProfileId')

Get the daily scan profile changes in IBM® Storage Protect for Cloud for a customer.

Required Permission: partner.scanprofiles.read.all

Response Information:

Element	Description	Type
profileName	The name of the scan profile.	string
profileID	The ID of the scan profile.	string
tenantDomain	The tenant domain of the scan profile.	string
tenantID	The tenant ID the scan profile.	string
description	The description of the scan profile.	string
scanMode	The scan mode of the scan profile. 0 – Express mode 1 – Advance mode	integer
modifiedTime	The last modified time of the scan profile.	string
lastUpdateTime	The time of generating the daily report for the scan profile. If no daily report has been generated, the time is the last modified time of the scan profile.	string

Element	Description	Type
lastScanStatus	The last scan job status of the scan profile. 1 – In progress 2 – Finished 3 – Failed 4 – Finished with exception 5 – Skipped 10 – Stopped	integer
newRegisteredContentCount	The number of newly registered contents in the daily report of the scan profile.	integer
movedToAnotherContainerObjects	The number of objects moved to another container in the daily report of the scan profile.	integer
removedFromMicrosoft365OrOutofPolicy	The number of objects removed from Microsoft 365 or out of policy in the daily report of the scan profile.	integer

Note: To improve the experience, we've added **newRegisteredContentCount** to replace **newRegistedContentCount**.

GET api/v1.1/Customers('id')/ScanProfilesDailyNewDetail(ProfileId='ProfileId')

Get the daily scan profile change details in IBM® Storage Protect for Cloud for a customer.

Required Permission: partner.scanprofiles.read.all

Response Information:

Element	Description	Type
profileName	The name of the scan profile.	string
profileID	The ID of the scan profile.	string
tenantDomain	The tenant domain of the scan profile.	string
tenantID	The tenant ID the scan profile.	string
lastUpdateTime	The time of generating the daily report for the scan profile. If no daily report has been generated, the time is the last modified time of the scan profile.	string

Element	Description	Type	
newRegisteredContent	The details of newly registered contents in the daily report of the scan profile.	objectName	string
		containerName	string
removedFromMicrosoft365OrOutOfPolicyObjects	The details of objects moved to another container in the daily report of the scan profile.	objectName	string
		containerName	string
movedToAnotherContainerObjects	The details of objects removed from Microsoft 365 or out of policy in the daily report of the scan profile.	objectName	string
		containerName	string

Note: To improve the experience, we've added **newRegisteredContent** to replace **newRegistedContent**.

Access the Help Page

IBM® Storage Protect for Cloud Partners provides the **Help** page, which allows you to quickly access the user guide and FAQs of IBM® Storage Protect for Cloud Partners, submit feedback, and invite support. You can access this page by clicking **Help** in the left navigation.

View the User Guide and FAQs

On the **Help** page, click the **User guide** card to view the IBM® Storage Protect for Cloud Partners User Guide. Click the **FAQs** card to view the "FAQs" on page 11.

Submit Feedback

About this task

The system provides a platform to collect feedback where you can provide suggestions for service features from your experience of this system. Refer to the following steps to submit feedback:

Procedure

Refer to the following steps to submit feedback:

1. On the **Help** page, click the **Submit feedback** card.
2. On the **Submit feedback** page, configure the following settings:
   a. **Rate Your IBM® Storage Protect for Cloud Partners Experience** – Click the stars to evaluate your IBM® Storage Protect for Cloud Partners experience.
   b. **Your suggestion** – Enter your suggestions about IBM® Storage Protect for Cloud Partners features.

   > **Note:** You can enter up to 500 characters.

3. Click **Submit** to submit the feedback, or click **Cancel** to return to the **Help** page without submitting your feedback.

Prepare a Certificate

This section details how to prepare certificate files (.cer file and .pfx file).

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 82
- "Use Windows PowerShell to Prepare Certificates" on page 84

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" on page 82. Then follow the instructions below to prepare the certificate.

Procedure

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

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

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

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

      > **Note:** The .pfx file contains your private key.

Create a Key Vault in Azure

You can create a key vault in Azure.

Procedure

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

1. Create an application. This application is only used for Azure Key Vault.

a. In the Microsoft Entra admin center (or Microsoft Azure portal), navigate to **Microsoft Entra ID › App registrations**.
b. Click **New registration** on the ribbon.
c. On the **Register an application** page, configure the application settings.
d. Click **Register** to create your application.
e. After the application is created successfully, copy the application ID. The application ID is the client ID that will be used in the encryption profile.

2. Add a client secret for the application.
   a. After creating the application, click **Certificates & secrets** in the left menu.
   b. In the **Client secrets** field, click **New client secret**.
   c. In the **Add a client secret** pane, enter a description for the client secret and select a duration.
   d. Click **Add**. The value of the client secret is automatically generated and displayed.
   e. Copy the client secret value. You will need to provide the value when configuring the encryption profile.

> **Note:** The value will be hidden after you leave or refresh the page.

3. Create a key vault.
   a. In the Microsoft Azure portal, enter **Key vaults** in the search box on the top, and then select the first result to access the **Key vaults** page.
   b. Click **Add**. The **Create key vault** page appears.
   c. In the **Basics** tab, provide the basic information for the key vault, and then click the **Access policy** tab.
   d. Click **Add Access Policy**.
   e. On the **Add access policy** page, select the following **Key permissions** from the drop-down list.
      - In the **Key Management Operations** field, select **Get**.
      - In the **Cryptographic Operations** field, select **Decrypt** and **Encrypt**.
   f. Click the select button in the **Select principal** field.
   g. In the **Principal** pane, enter the application name or application ID in the search box.
   h. Select the application and click **Select** at the bottom.
   i. Click **Add** to add the access policy.
   j. Click the **Networking** tab.
   k. Select **Public endpoint (all networks)** which allows all networks to connect to this key vault.
   l. Click the **Tags** tab and you can add tags to categorize your key vault.
   m. Click **Review + create** to review all of your configurations first, and then click **Create** at the bottom to create the key vault.

> **Note:** If you need to change some settings before creating the key vault, you can click the Previous button to change previous settings.

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

Use Windows PowerShell to Prepare Certificates

Procedure

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.

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' -NotAfter (Get-Date).AddMonths(60)
   ```

   Press **Enter** on the keyboard.
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
   ```

   Note the following:

   - The .pfx file contains your private key.
   - 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-PfxCertificate -Password $(Read-Host -AsSecureString -Prompt "Enter a
     password to protect the certificate") -Cert $cert -FilePath "C:
     \Temp\IBMCustomApp.pfx"
     ```

     Press **Enter** on the keyboard.

   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)”
   ```

Appendix B - Accessibility features for the IBM® Storage Protect for Cloud

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

Overview

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

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

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

The product documentation in IBM® Documentation is enabled for accessibility.

Keyboard navigation

This product uses standard navigation keys.

Interface information

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

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

Related accessibility information

In addition to standard IBM® help desk and support websites, IBM® has a TTY telephone service for use by deaf or hard of hearing customers to access sales and support services:
TTY service
800-IBM®-3383 (800-426-3383)
(within North America)

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

Notices

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

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

IBM® may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:
IBM® Director of Licensing
IBM® Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM® Intellectual Property Department in your country or send inquiries, in writing, to:
Intellectual Property Licensing
Legal and Intellectual Property Law
IBM® Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

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

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

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

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

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:
IBM® Director of Licensing
IBM® Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

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

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

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

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

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

COPYRIGHT LICENSE:

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

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

Trademarks

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

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

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

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

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

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

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

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

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

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

Terms and conditions for product documentation

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

Applicability

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

Personal use

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

Commercial use

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

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.
IBM® reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM®, the above instructions are not being properly followed.

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

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

Privacy policy considerations

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

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

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

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