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

User Guide

IBM

Contents

Note:

Before you use this information and the product it supports, read the information in “Notices” on page 163.

Edition Notice (June 2024)

This edition applies to IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID (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 Dynamics 365 in one of the supported environments.

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

What's new

Learn about new features and updates in IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID.

Release Date: November 2, 2025

General Updates

- Geo-Redundant Storage (GRS) is now available for users using Azure default storage.

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

IBM® Storage Protect for Cloud ensures the resiliency of service in the event of a disaster by quickly recovering lost and corrupted content from your backup. IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID offers data recovery capabilities for your **Azure Virtual Machines**, **Microsoft Entra ID**, **Azure Storage** (blob storage and file share), **Admin Portal Settings**, **Azure SQL** (for Azure SQL databases), **Azure DevOps**, and **Azure AD B2C**.

The new redesigned user interface available since the March 2024 release, is now the primary UI of the solution.

IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID is now only available in the following data centers: Canada Central (Toronto), Germany West Central (Frankfurt), East US (Virginia), Switzerland North (Zurich), Australia East (New South Wales), and Brazil South (Sao Paulo State) . In addition, if your browser's first preferred language is French, or German, the IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID interface will be displayed in French, or German. In other cases, the interface will be displayed in English.

Note: To access the user guide, expand the Help & Resources (?) section on the left navigation and click the **User Guide**.

The dashboard on the home page provides a comprehensive overview of the latest activities, job status count, backup object summary, restore job summary, storage space usage, and the storage profile usage rank.

- Job status count – Shows the status of different types of jobs for different services and objects.
- Latest activities – Shows the 5 most recent jobs in IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID.

  To find more jobs, click the arrow (→) icon to navigate to the **Job monitor** page.
- Backup object summary – Shows the ratio of objects in the current backup scope to all the objects detected in your tenant.
- Restore job summary – Shows the total number of restore jobs for each service within a specified date range, as well as the number and ratio of restore jobs for each type of objects in the current service. Use the Date range and service drop-down lists to find the data you need.
- Storage – Shows the storage space used by each service.
- Storage profile usage rank – Shows the top 5 storage profiles by usage.

The **Backup** page shows the **Microsoft Entra ID** tile, the **Virtual Machine** tile, the **Azure Storage** tile, the **Admin Portal Settings** tile, the **Azure Sql** tile, the **Azure DevOps** tile, and the **Azure AD B2C** tile.

Through each service tile, you can view the backup and restore details of its latest jobs, including backup scope name, job duration, operator, latest restore history, etc. Additionally, you can update the backup scopes and frequency. and update the backup scopes and frequency.

If you are in trial, your experience with the IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID will be limited:

- Your trial instance of IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID will use the IBM® Storage Protect for Cloud default storage to store your backup data by default, and the data retention period is one month.
- Virtual Machine backup service in the trial only allows one backup scope and protects up to 5 Azure VMs.
- The Microsoft Entra ID backup service in the trial only allows you to protect one Microsoft Entra tenant, and the backup jobs in trial will not restrict the number of the objects to protect in your Microsoft Entra tenant.
- Azure Storage backup service in the trial only allows one backup scope for Blob storage and file share respectively. You can select up to 5 blob containers or 5 file shares for each backup scope. The backup job

will protect up to 5 folder-level objects within the selected storage and the storage space for backup data can be at most 25 GB.

- Admin Portal Settings service in the trial only allows one backup scope.
- Azure SQL backup service in the trial only allows one backup scope to protect up to 5 databases.
- Azure DevOps backup service in the trial only allows one backup scope to protect up to 5 projects.
- Azure AD B2C backup service in the trial only allows one backup scope.

Enable Backup

To use IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID to protect Microsoft Entra ID, Azure VMs, Azure Storage, Admin Portal Settings, Azure SQL, Azure DevOps, or Azure AD B2C, you must connect your **Microsoft** tenant to IBM® Storage Protect for Cloud. For details, refer to Connect your tenants to IBM Storage Protect for Cloud.

Note the following before you enable the backup:

- Before you enable the backup service for Azure VM, Azure Storage, or Azure SQL, you can register a **Microsoft Delegated** app in your tenant or use a custom Azure app with delegated permissions, and then add this app to the subscriptions where the VM, storage, or database to protect resides and grant the app the **Contributor** role or a custom role with equivalent permissions. For details, refer to "Enable the Backup for Azure Virtual Machines, Azure Storage, and Azure SQL" on page 39.

  > **Note:**
  >
  > - If your storage account has disabled the "**Allow storage account key access**" feature, the app must also have the **Storage Blob Data Contributor** role to the subscription or storage account, in addition to the **Contributor** role to protect the Azure Blob Storage, and in this case the Azure File Storage is not supported.
  > - The Azure virtual machines that can be protected by Virtual Machine service must be hosted by Azure, which may be created with your pre-defined and endorsed settings or using the recommended defaults that match your workload.
  > - If the Azure storage account that you want to protect has enabled the firewall, complete the settings as instructed in "Allow IBM Storage Protect for Cloud Agent Servers to Access Your Storage Account" on page 82. Note that the data in the Azure storage archive tier cannot be protected as the IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID cannot read or download a blob in the Archive tier. You must manually rehydrate the archive data that you want to protect to the online tier (cold, cool, or hot tier).

- Before you use the backup service for Microsoft Entra ID or Admin Portal Settings, you must create a **Service app** for IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID or use a custom Azure app to grant consent with the required permissions. For details, refer to "Enable Backup for Microsoft Entra ID or Admin Portal Settings" on page 42.
  Note the following:

  - If you want to backup and restore **Distribution lists** or **Mail-enabled security groups** in **Microsoft Entra ID**, or protect the Microsoft 365 Defender or Exchange settings through **Admin Portal Settings** service, you can choose to prepare a service account profile with a Global Administrator or Exchange Administrator, or you can go to the Microsoft Entra admin center (Azure portal) to assign the Exchange administrator role to this service app. For details on assigning an app the Exchange administrator role, refer to How to Assign the Exchange Administrator Role to an App?. For details on configuring a service account profile, refer to Create a Service Account Profile. Note that the service account with MFA enabled is currently not supported.

    > **Note:** If you are using a custom Azure app for Microsoft Entra ID or Admin Portal Settings service and you do not want to assign Global administrator or Exchange administrator role to

> the app, refer to the instructions in Create a Custom Role Group to create a role group with the minimum permissions. This configuration is only applicable to the custom app.

  - To restore a temporarily deleted user or group that has access to the Microsoft 365 admin center, the service account or the service app must be assigned with a Global administrator role.
  - To back up and restore the **Self Service Group Management** settings for Microsoft Entra ID > Group General, you must have a service account profile configured in the IBM® Storage Protect for Cloud interface and the service account you use must have the **Cloud Application Administrator** role. Note that if you only want to back up this property, the **Cloud Application Administrator** role is not required.
  - To back up and restore the **Attributes and Claims**, **Identifier (Entity ID)**, **currentSingleSignOnMode**, **ParentAppId**, or **IsCustomApp** the SSO configuration for the enterprise applications, you must have a service account profile configured in the IBM® Storage Protect for Cloud interface and the service account you use must have the **Application Administrator** role. Note that if you only want to back up this property, the **Application Administrator** role is not required.
- Before you use the backup service for Azure DevOps, you must create a service app or use a custom Azure app to grant consent with the required permissions. For details, refer to Enable the Backup for Azure DevOps.
- Before you use the backup service for Azure AD B2C, you must create a service app or use a custom Azure app to grant consent with the required permissions. For details, refer to Enable the Backup for Azure AD B2C

Single Sign-On

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

Beta APIs

Refer to the following table for the beta version API methods of Microsoft Graph that we use in IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID.

Summary for complex table

Category	API Method	Is it available in the 1.0 version?	Then, why do we use the Beta version?
Microsoft Entra ID > Groups	Groups resource type	No	Write back group configurations
Microsoft Entra ID > EnterpriseApplication	Synchronization API	No	For the backup and restore of the Enterprise Applications > Provisioning.
	Delete synchronizationJob	Yes	Currently, there are some missing properties when using the Graph v1.0 endpoint.
	Create synchronizationJob	Yes	Currently, there are some missing properties when using the Graph v1.0 endpoint.
	Update synchronizationSchema	Yes	Currently, there are some missing properties when using the Graph v1.0 endpoint.
	synchronizationJob: pause| start	Yes	Currently, there are some missing properties when using the Graph v1.0 endpoint.

	Add synchronization secrets	Yes	Currently, there are some missing properties when using the Graph v1.0 endpoint.
	Create unifiedRoleAssignment	Yes	Currently, there are some missing properties when using the Graph v1.0 endpoint.
	GetAppDefaultClaim (Internal)	Yes	Currently, there are some missing properties when using the Graph v1.0 endpoint.
	UpdateAppDefaultClaims (Internal)	Yes	Currently, there are some missing properties when using the Graph v1.0 endpoint.
Microsoft Entra ID > SignInLogs	List signIns	Yes	Currently, there are some missing properties when using the Graph v1.0 endpoint.
Microsoft Entra ID > Administrative Unit	Update administrativeUnit	Yes	Currently, there are some missing properties when using the Graph v1.0 endpoint.
Admin Portal Settings	Get authenticationMethodsPolicy	Yes	Currently, there are some missing properties when using the Graph v1.0 endpoint.
	List policies	Yes	Currently, there are some missing properties when using the Graph v1.0 endpoint.
	List deviceCompliancePolicies	Yes	Currently, there are some missing properties when using the Graph v1.0 endpoint.
	Get /deviceManagement/ compliancePolicies	Yes	Currently, there are some missing properties when using the Graph v1.0 endpoint.
	List deviceConfigurations	No	
	GET /deviceManagement/ configurationPolicies?$filter=technologies ne 'mdm,microsoftSense'	No	
	GET /deviceManagement/ configurationPolicies?$filter=technologies eq 'mdm,microsoftSense'	No	
	Get deviceConfigurationAssignment	No	
	List deviceManagementConfigurationPolicyAssignments	No	
	List deviceManagementConfigurationSetting	No	
	List groupPolicyConfigurations	No	
	Get groupPolicyDefinitionValue	No	
	List deviceManagementScripts	No	
	List deviceShellScripts	No	

	Get deviceManagementScriptRunSummary	No	
	Get deviceManagementScriptDeviceState	No	
	List deviceManagementScriptUserStates	No	
	List managedAppPolicies	Yes	Currently, there are some missing properties when using the Graph v1.0 endpoint.
	Get androidManagedAppProtection	No	
	Get iosManagedAppProtection	No	
	Get mdmWindowsInformationProtectionPolicy	No	
	Get windowsManagedAppProtection	No	
	List managedDeviceMobileAppConfigurations	Yes	Currently, there are some missing properties when using the Graph v1.0 endpoint.
	Get managedDeviceMobileAppConfiguration	No	
	Get managedDeviceMobileAppConfigurationAssignment	No	
	List targetedManagedAppConfigurations	Yes	Currently, there are some missing properties when using the Graph v1.0 endpoint.
	GET /deviceManagement/intents?$filter=templateId ne 'e44c2ca3-2f9a-400a-a113-6cc88efd773d'	No	
	GET /deviceManagement/intents?$filter=templateId eq 'e44c2ca3-2f9a-400a-a113-6cc88efd773d'	No	
	Get targetedManagedAppConfiguration	Yes	Currently, there are some missing properties when using the Graph v1.0 endpoint.
	conditionalAccessPolicy resource type	Yes	Currently, there are some missing properties when using the Graph v1.0 endpoint.
	List targetedManagedAppPolicyAssignments	No	
	List deviceManagementIntents	No	
	List deviceManagementIntegerSettingInstances	No	

	Get deviceManagementTemplate	No	
	Get deviceManagementIntent	No	
	Get deviceManagementIntentDeviceStateSummary	No	
	Get deviceManagementIntentUserStateSummary	No	
	List deviceManagementIntentDeviceStates	No	
	List deviceManagementIntentDeviceSettingStateSummaries	No	
	Create conditionalAccessPolicy	No	Currently, there are some missing properties when using the Microsoft Graph v1.0 endpoint.
	Update conditionalAccessPolicy	No	Currently, there are some missing properties when using the Microsoft Graph v1.0 endpoint.
	Create defaultDeviceCompliancePolicy	No	
	assign action	No	
	Update windows10CompliancePolicy	No	
	scheduleActionsForRules action	No	
	Create deviceManagementCompliancePolicy	No	
	setScheduledActions action	No	
	Create conditionalAccessPolicy	No	
	Update conditionalaccesspolicy	No	
	Create windows10CustomConfiguration	No	
	Create deviceManagementScript	No	
	Update deviceManagementScript	No	
	Create deviceManagementScriptAssignment	No	
	Update deviceManagementScriptAssignment	No	
	Create deviceManagementConfigurationPolicy	No	
	Update deviceManagementConfigurationPolicy	No	

	Create androidManagedAppProtection	No	
	Create iosManagedAppProtection	No	
	Create windowsManagedAppProtection	No	
	Create mdmWindowsInformationProtectionPolicy	No	
	Update androidManagedAppProtection	No	
	Update iosManagedAppProtection	No	
	Update windowsManagedAppProtection	No	
	Update mdmWindowsInformationProtectionPolicy	No	
	Create iosMobileAppConfiguration	No	
	Update iosMobileAppConfiguration	No	
	createInstance action	No	
	Update deviceManagementIntent	No	
	updateSettings action	No	
	Create deviceManagementConfigurationPolicy	No	
	Update deviceManagementConfigurationPolicy	No	
	list hardwareconfigurations	No	
	get hardwareconfigurations	No	
	create hardwareconfigurations	No	
	update hardwareconfigurations	No	
	Get Presentation of Definition	No	
	Get Presentation Value	No	
Azure AD B2C > User Flow	List Userflow	No	For the backup and restore of user flows.
	Get Userflow	No	For the backup and restore of user flows.
	Create Userflow	No	For the backup and restore of user flows.
	Update Userflow	No	For the backup and restore of user flows.
	Delete UserFlow	No	For the backup and restore of user flows.

	List Identity provider	No	For the backup and restore of user flows.
	Add Identity provider	No	For the backup and restore of user flows.
	Delete Identity provider	No	For the backup and restore of user flows.
	List user attribute assignment	No	For the backup and restore of user flows.
	Create user attribute assignment	No	For the backup and restore of user flows.
	Delete user attribute assignment	No	For the backup and restore of user flows.

Backup Scope

When configuring the backup scope for Azure VMs, Azure Storage, Azure SQL, or Admin Portal Settings, you can click the Refresh List (🔄) button to retrieve the latest data information and keep your backup scope updated. It may take a long time. The product also provides a timer job to regularly refresh your data list at 0:00 AM every day, in your local time. The last refreshed time will be displayed next to the button.

> **Note:** If it is your first time using a service, you can click the Refresh List (🔄) button to manually initialize the data list that can be added to the backup scope according to your settings.

The backup service for Azure VMs, Azure Storage, and Azure Admin Settings supports you by grouping the backup of Azure VMs, Blob Storage, File Share, or admin portal settings into separate backup scopes. This will protect them with individual backup schedules or data retention settings. Note that the data in the Azure storage archive tier cannot be protected as the IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID cannot read or download a blob in the Archive tier. You must manually rehydrate the archive data that you want to protect to the online tier (cold, cool, or hot tier).

Each backup scope for Microsoft Entra ID can only protect one tenant. In addition, once you have created a backup scope, you cannot add the same tenant to another scope.

The backup services will perform scheduled backups automatically according to the settings of each backup scope. Note that if a backup job for the same backup scope is in progress, the automatic backup job scheduled to run will be skipped.

Storage Location

You can choose to use the default storage hosted by IBM® Storage Protect for Cloud to store your backup data or choose to use your own storage. Currently, you can choose from the following supported storage types for IBM-hosted default storage or for BYOS (bring your own storage).

IBM Default Storage Type	BYOS Storage Type
Microsoft Azure Blob Storage	Microsoft Azure Blob Storage
	Amazon S3 storage
	Amazon S3-Compatible storage
	SFTP
	IBM Storage Protect – S3
	IBM Cloud Object Storage
	Google Cloud Storage

The supported Azure storage account kinds are **Storage** and **StorageV2** of **Standard** performance type. Note that the Azure Blob storage that has enabled Data Lake Storage Gen2 capabilities (a hierarchical namespace) is not supported.

For details on how to change from IBM default storage to BYOS storage and manage your storage profiles, refer to Manage Your Storage.

If you are using your own Microsoft Azure storage and backup retention period is longer than 45 days, your backup data will be automatically stored to the Cold tier for cost savings after the January 2024 release. For existing customers, your former backup data are still stored in the cool tier. To use your Azure blob storage in the most cost-effective manner, you can store your backup data to archive tier. However, IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID currently does not support restoring the backup data from the archive tier automatically. If you want to restore the backup data from the archive tier, you must rehydrate the data first. For details on Azure storage access tiers, refer to the Microsoft article: Access tiers for blob data.

If you use your own Azure storage, IBM® Storage Protect for Cloud recommends using the Azure storage account from the same region as the object you want to back up, otherwise, the backup will incur data transfer costs. Data transfer costs are also incurred if you use IBM® Storage Protect for Cloud default storage and the Azure VMs or storage that is not in the same region as the IBM® Storage Protect for Cloud tenant that you've signed up for. See the information in this Microsoft article for bandwidth pricing that may incur due to the data transferred out of Azure data centers.

If you use IBM-hosted default storage, **Availability Paired Region** is now available as an option to replicate your data. To use availability paired region, go to the IBM® Storage Protect for Cloud and configure your IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID settings by enabling the **Availability Paired Region** option.

Note the following:

- Once enabled, the Availability Paired Region cannot be turned off and will become available for all services.
- If you use IBM Azure storage and enable the Availability Paired Region, the paired region is only available for the storage region, not for the data region.

If you enable the Availability Paired Region, it will be implemented through the Azure Geo- redundant storage functionality. For more details, refer to this Microsoft article. The specific secondary region paired to your primary region is determined by Azure; you can find this mapping in the official Azure regions list.

> **Note:** The Availability Paired Region is not available for data region.

Data Center You Signed Up for in IBM® Storage Protect for Cloud	Available Storage Region for IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID
Australia Southeast (Victoria)	Australia East (Victoria)
Germany West Central (Frankfurt)	Germany North (Frankfurt)

Before you provide your storage information to the IBM® Storage Protect for Cloud interface, you must first add the IBM® Storage Protect for Cloud IP addresses to your storage firewall or configure the firewall to allow IBM® Storage Protect for Cloud servers running on a dedicated ARM Vnet subnet to access your storage location. For details, refer to "Allow IBM Storage Protect for Cloud Agent Servers to Access Your Storage Account" on page 82.

Once you save the storage location for a specific region in a backup scope, you can no longer update the storage for that region in that scope.

The snapshots for managed disks created by IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID will have the following tags: **CreateBy: ACBVM_{tenantId}**; **JobId: {FB or IB}{Date&TimeStamp}**; **VMName: {VMName}**. You can use these tags to filter and manage the snapshots created by IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID.

Backup Retention

The data retention settings can be applied to your backup data to help save your storage costs. You can configure a custom retention period for your backup data up to the retention policy in your subscription.

Once there is backup data of a backup scope approaching the retention period, your tenant owner will receive the **Data Retention Notification**. Once the next full snapshot of your backup scope takes place, we will begin pruning the old backup data that met your retention settings. Your subscription capacity will be released after the backup data is deleted.

Data Restore and Export

The **Restore** page allows you to browse the recovery points of each service type to find the data that you want to restore.

For Microsoft Entra ID and Admin Portal settings, you can also use the **Compare** method to generate a comparison report for the backup data of a specific recovery point against the Azure production data to help you easily locate the changes that you may want to revert. Note that if the properties that you have updated for the user or group are currently not supported by IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID , the user or group will be tagged as **Modified** in the report, though the report cannot show the differences.

After you have found the data at a specific recovery point that you want to restore, you can choose to restore the data to its original location or another destination. The data of specific types also supports being exported to a local location. A monthly export limitation of 500GB/Month has been applied to Azure VM and Azure Storage. Data cannot be exported once the limit has been reached.

Refer to the table below for the data types that you can restore and export or export only:

> **Note:** The data types protected by IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID that are not listed in the table below support being restored only. For the Azure VMs and Azure Storage, you can choose to restore the backup data to their original location or another destination. For the Microsoft Entra ID, only the in-place restore (restore to the original location) is supported.

Data types	**Restore & Export**	**Export Only**
Microsoft Entra ID > Users	You can download the user properties with a script. You can use the script and the downloaded information to bulk import/update the users to a local directory.	/
All data types in Azure Storage	√	/
Azure VMs & Disks	√	/
Azure VMs > files	/	√
Admin Portal Settings	√ For the list of settings supported by restore or export, refer to Admin Portal Settings.	/

Activity and System Auditor

Using the backup statistics of Microsoft Entra ID, Azure VM, Azure Storage, Admin Portal Settings, Azure SQL, and Azure AD B2C on the Backup analysis page and the total used storage space displayed in the **Subscription** page, you will get an overview of the scale of your resources being protected and the storage used for data protection. For details, refer to Reporting.

Through **Job Monitor**, you can monitor job status and download job reports to get a better understanding of your backup scope and performance and take responsive actions. For details, refer to Generate and Download a Job Report.

Use Public APIs for Job Information

You can now use the IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID Public APIs to get the information of backup and restore jobs. For details, refer to "Use Public APIs for Job Information" on page 114.

Configure Date Format

You can configure the date format for the IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID environment and notification emails in **IBM® Storage Protect for Cloud** > **Administration** > **General settings** > **Culture settings**. For details, refer to Culture Settings.

Supported Browsers

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

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

Use Cases

Use Case – Want to Protect Your Business-Critical Azure Application Configurations with Periodic Full Backups and Incremental Backups using Flexible Backup Retention?

Event: Your business runs over Azure assets, including Azure Virtual Machines, Microsoft Entra ID, and Azure Storage. You need a solution to ensure the availability and integrity of the data in these Azure assets.

Resolution: IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID runs periodic full backups and incremental backups to protect the Azure VMs, Microsoft Entra ID, or Azure Storage in your defined backup scopes. You can choose to run incremental backups as frequently as four times a day (Azure VM). Subject to your subscription, the backup data can be stored to your own storage or the IBM® Storage Protect for Cloud default storage and you can apply a flexible backup retention setting upon each of your backup scopes. The retention period can be at least 2 weeks or by month/year.

Use Case – Want to Restore Microsoft Entra Groups with Members, Group Memberships, Licenses, Applications, Roles and Administrators, and Administrative Units?

Event: Tom, one of your IT administrators, discovers that he updated the settings for an important group in your Microsoft Entra ID but accidentally deleted the group.

Problem: Native restore functionality in Microsoft Entra ID cannot revert the changes or restore a group that was deleted more than 30 days ago. Tom cannot recall when he deleted it. He wants to get this group back and revert the changes.

Resolution: You have an IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID account and already have Microsoft Entra ID backup service enabled for the backup of this Microsoft Entra ID. You log into IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID to recover the group that Tom deleted. Tom remembers a keyword that is contained within the group name, but he cannot remember when he deleted the group. You must browse the recovery points for that Azure AD backup scope on the backup calendar that are before he remembers deleting the group or select the recovery points to compare. When viewing the backup data of a recovery point or the comparison report, you can conduct a keyword-based search for the group name to find the backup data of that group. Then, you can perform the restore for the group. The restore job can restore the group with its members, owners, group memberships, licenses, applications, roles and administrators, and the administrative units. For the supported and unsupported properties of restoring groups, refer to **Microsoft Entra ID > Groups**. Note that the object ID cannot be restored if a group with this ID has been permanently deleted.

Use Case – Want to Compare the Recovery Points to Find the Users or Groups to Restore?

Event: Tom is your IT administrator, and he found a user's authentication method and administrative units have been changed.

Problem: Tom wants to know when the changes were made and revert the changes to an ideal recovery point.

Resolution: You have an IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID account and already have Microsoft Entra ID backup service enabled. You log into IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID to compare the recovery points of this user for the differences. For details, refer to Restore Users.

Use Case – Want to Restore Azure Blob Content?

Event: Tom discovers that some blobs were deleted from a folder in an Azure Blob container, which resulted in the corresponding topics appear not found.

Problem: Tom does not know when they were deleted, and it would be difficult to find all the missing blobs that need to be restored among hundreds of topics.

Resolution: You have an IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID account and already have Azure Storage backup service enabled for the backup of this Blob container. You log into IBM® Storage

Protect for Cloud Azure VMs, Storage, and Entra ID to recover the folder where the missing blobs reside. Tom remembers the last released date for this set of documents, and he wants to restore the folder to the state at that recovery point. You must find the recovery point for that backup scope near the release date on the backup calendar. Then, you can drill down to the folder in the Blob container to perform the restore. The restore job supports Merge, Overwrite, or Skip as the conflict resolution. For details, refer to Restore Blob Storage.

Use Case - Want to Export or Restore Admin Portal Settings?

Event: Tom discovers that a conditional access policy was updated with incorrect conditions.

Problem: Tom does not know how many times the policy has been updated and what the exact conditions were configured in this conditional access policy before the updates.

Resolution: You have an IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID account and already have Admin Portal Settings backup service enabled for the backup of the Microsoft Entra ID conditional access. You log into IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID to recover the conditional access policy. Tom knows the last modified time for this policy, and he needs to check the recovery point on the backup calendar before that time. You can drill down to the recovery points and select the policy to export. The conditional access policy will be exported to a JSON file. Then, you can compare the attributes in JSON with the settings on the Azure portal interface for differences. After you confirm the differences, you can either manually update the settings through the Azure portal or go back to IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID to perform a restore job. Before performing the real restore, you can choose to start a dry run first to rehearse the restore action with your defined restore settings.

For details, refer to Restore Admin Portal Settings.

FAQs

Will your backup services incur other costs during backup?

It varies depending upon the backup services. Generally, if you only use the Microsoft Entra ID service and Admin Portal Settings service, you will not experience additional costs for backup.

If your subscription contains Azure VM or Azure Storage, your backup services may incur additional costs on the protected Azure VM and Storage instance for data transfer, snapshots, operations, or API calls, etc. For details, refer to the table below:

Service	**Additional Costs**	**Pricing Reference**
Azure VM	Snapshots The cost could be higher if you perform more backups and keeps more snapshots.	For the snapshots pricing, refer to this Microsoft page.
	Data transfer The cost will increase if the data is transferred out of the region where the Azure VMs reside or out of Azure, especially if you are using different storage types.	For details, refer to this Microsoft page: Bandwidth pricing.
	Index generation for exporting VM files The cost will increase if the Azure VMs to protect are in a region different from where your IBM® Storage Protect for Cloud is signed up for. Additionally, if the data is stored in a storage type other than Microsoft Azure Blob Storage, the expenses will also rise.	
Azure Storage	Read operations and Data retrieval for backup	For details, refer to the following Microsoft pages: Azure Blob Storage pricing Azure Files pricing
Azure SQL	There will be additional costs if you use the Azure SQL backup service. To minimize the impact on production environment databases during Azure SQL backup jobs, the database data is copied to a temporary database before the backup process begins. This approach may incur additional costs.	For details, refer to Azure SQL Database pricing.

How does the retention policy work for Azure VM backups?

The backup process for Azure includes saving snapshots to Microsoft Azure and storing the backup data to your storage location. Snapshots are required to ensure data consistency and enable faster recovery process.

When configuring backup scopes for Azure virtual machines, you can configure the retention policy to set when to prune the snapshots from Azure and the backup data from the storage location.

- ◦ Snapshots in Azure – You can configure the number of snapshots to keep or how long the snapshots will be retained.

- Backup data in storage – You can configure the retention period for daily, hour, and weekly recovery points.

For details on how to configure the retention policy for Azure VMs, refer to Create a New Backup Scope for Azure VM.

Best Practices

Choose the BYOS subscription if the Azure assets to protect are based in a region different from the IBM® Storage Protect for Cloud instance

If your Azure assets (Azure VMs or storage) are not hosted in the same or the paired data center as the IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID product instance that you will access, we strongly recommend that you choose the BYOS subscription with your Microsoft Azure Blob Storage. See the information in this Microsoft article for bandwidth pricing that may incur due to the data transferred out of Azure data centers.

For example, you may register your IBM® Storage Protect for Cloud tenant in Germany West Central data center and want to use IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID to protect the Azure VMs in South Africa. In this case, purchasing the BYOS subscription and using your own Azure storage will be the most cost-effective way and will achieve the best performance. You can contact IBM® Storage Protect for Cloud support for more information.

Azure VM Backup Settings

Index generation for file-level data exportation

When configuring backup scopes for Azure virtual machines,you can select the **Generate index for file-level data export** option if you want to perform file-level data export using the backup data. Note the following:

- Enabling this option will extend the duration of the backup job due to index generation.
- If file-level data export is not required, it is recommended to leave this option deselected to improve backup efficiency.
- You can also generate index for specific disks or VMs in the **Restore** wizard.

Retention policy

When configuring backup scopes for Azure virtual machines, you can choose the number of the latest snapshots to retain or choose for how long the snapshots will be retained after generation. Here are the key points to consider:

- **Rapid restoration**– Restore jobs involving snapshots can be finished within 15 minutes. If rapid restoration is a priority, it is recommended to retain snapshots.
- **Number of snapshots** – You can choose the number of the latest snapshots to retain or choose for how long the snapshots will be retained after generation.
- **Cost consideration** – Snapshots are stored in Microsoft Azure and will incur associated costs. The more snapshots you retain, the higher the cost will be. We recommend balancing your retention requirements with cost constraints.

For details on how to create a new backup scope, refer to Create a New Backup Scope for Azure VM.

Quick Start for Trial Users

Follow the steps below to quickly set up your trial environment and protect key services in IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID:

1. Sign up for IBM® Storage Protect for Cloud to use IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID.
   - Visit IBM Storage Protect for Cloud Azure: Start your 30-day trial.
2. Access IBM® Storage Protect for Cloud
   - Sign in to the IBM® Storage Protect for Cloud environment using the corresponding account. See Sign into IBM® Storage Protect for Cloud for details.
3. Configure Backup Services. Explore and configure the services you want to protect.
   - Microsoft Entra ID Data
   - Admin Portal Settings
   - VMs
   - Azure Storage
   - Azure SQL Databases
   - Azure DevOps Projects
   - Azure AD B2C Data

Microsoft Entra ID Data

To protect your Microsoft Entra ID environment using IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID, follow these steps:

1. Connect your tenant.
   - If you want to protect your Microsoft Entra tenant via IBM® Storage Protect for Cloud, your tenant owner or service administrators must first connect the tenant to IBM® Storage Protect for Cloud. See Connect your Tenants to IBM® Storage Protect for Cloud for details.
2. Configure the service app profile.
   - Set up the app profile for the service app required to protect Microsoft Entra. Use your Microsoft 365 Global Admin Account to consent to the application. See Create a Service App and Grant Consent for details.
3. Configure a service account profile.
   - Create a service account profile if you want to protect the following properties. For details on configuring a service account profile, refer to Create a Service Account Profile.
     - To back up and restore distribution lists or mail-enabled security groups in Microsoft Entra ID, you can choose to configure a service account profile for this tenant with a Global Administrator or Exchange Administrator user role, or you can go to the Azure portal to add this service app with the Exchange Administrators role. For details on assigning an app the Exchange administrator role, refer to How to Assign the Exchange Administrator Role to an App?.
     - To back up and restore the **Attributes and Claims**, **Identifier (Entity ID)**, **currentSingleSignOnMode**, **ParentAppId**, or **IsCustomApp** of the SSO configuration for the enterprise applications, you must have a service account profile configured in the IBM® Storage Protect for Cloud interface and the service account you use must have the **Application Administrator** role.
4. Create the backup scope.
   - Navigate to IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID > **Backup** page and create a backup scope for the Microsoft Entra tenant that you want to protect. Define whether to protect the Sign-in log or Audit log, configure the backup start time, and ensure the data retention

policy meets your organization's needs. The backup job will run once a day. See Create a New Backup Scope for Microsoft Entra ID for details.

> **Note:** During your trial subscription, you can protect one Microsoft Entra tenant without limitations on the number of objects included in the backup.

5. Monitor and manage backups.
    - Regularly monitor the backup status and ensure that backups are running as scheduled. See Monitor Your Backup for details.
    - Use the Backup Analysis report to monitor your backup statistics. See View Backup Analysis Report for details.
6. Test restores.
    - Periodically test the restore process to ensure that you can recover data quickly and accurately. See Microsoft Entra ID for details.
    - Compare backups to ensure you are restoring the correct files. See Use the Compare Method for details.

Admin Portal Settings

To protect your Admin Portal Settings environment using IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID, follow these steps:

1. Connect your tenant.
    - If you want to protect your Microsoft Entra tenant via IBM® Storage Protect for Cloud, your tenant owner or service administrators must first connect the tenant to IBM® Storage Protect for Cloud. See Connect your Tenants to IBM® Storage Protect for Cloud for details.
2. Configure the service app profile.
    - Set up the app profile for the service app required to protect the admin portal settings. Use your Microsoft 365 Global Admin Account to consent to the application. See Create a Service App and Grant Consent for details.
3. Configure a service account profile.
    - Create a service account profile if you want to protect the following properties. For details on configuring a service account profile, refer to Create a Service Account Profile.
        - If you want to back up and restore the Microsoft 365 Defender or Exchange settings through the **Admin Portal Settings** service, you can choose to configure a service account profile for this tenant with a Global Administrator or Exchange Administrator user role, or you can go to the Azure portal to add this service app with the Exchange Administrators role. For details on assigning an app the Exchange administrator role, refer to How to Assign the Exchange Administrator Role to an App?.
        - To back up and restore the **Self Service Group Management** property of the **Groups General** settings for **Microsoft Entra ID** > **Groups**, you must configure a service account profile in the IBM® Storage Protect for Cloud interface with a service account with the **Cloud Application Administrator** role.
4. Create the backup scope.
    - Navigate to the IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID > **Backup** page and create a backup scope for the Microsoft Entra tenant that you want to protect. Define the protected components, configure the backup start time, and ensure the data retention policy meets your organization's needs. The backup job will run once a day. See Create a New Backup Scope for Admin Portal Settings for details.

> **Note:** With a trial subscription, you can only have one backup scope.

5. Monitor and manage backups.

- Regularly monitor the backup status and ensure that backups are running as scheduled. See Monitor Your Backup for details
- Use the Backup Analysis report to monitor your backup statistics. See View Backup Analysis Report for details.

6. Test restores.
    - Periodically test the restore process to ensure that you can recover data quickly and accurately. See Restore Admin Portal Settings for details.
    - Compare backups to ensure you are restoring the correct files. See Use the Compare Method for details.

VMs

Refer to the section below to protect Azure VMs.

- Azure VM

Azure VM

To protect your Azure VMs using IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID, follow these steps:

1. Connect your tenant.
    - If you want to protect your Microsoft Entra tenant via IBM® Storage Protect for Cloud, your tenant owner or service administrators must first connect the tenant to IBM® Storage Protect for Cloud. See Connect your Tenants to IBM® Storage Protect for Cloud for details.
2. Configure the app profile.
    - Set up the app profile for the app required to protect Azure virtual machines. Use your Microsoft 365 Global Admin Account to consent to the application. See Create a Service App and Grant Consent for details.
3. Add to subscription and grant role.
    - After creating the app profile in IBM® Storage Protect for Cloud, add the app to each subscription where the Azure VMs you want to protect belong. See Add to Subscriptions and Assign the Contributor Role for details.
4. Create the backup scope.
    - Navigate to the IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID > **Backup** page and create a backup scope for Azure virtual machines. Define the protected Azure virtual machines, configure the backup start time, and ensure the data retention policy and backup schedule meet your organization’s needs. See Create a New Backup Scope for Azure VM for details.

      > **Note:** With a trial subscription, you can only have one backup scope and protect up to 5 Azure VMs.
5. Monitor and manage backups.
    - Regularly monitor the backup status and ensure that backups are running as scheduled. See Monitor Your Backup for details.
    - Use the Backup Analysis report to monitor your backup statistics. See View Backup Analysis Report for details.
6. Test restores.
    - Periodically test the restore process to ensure that you can recover data quickly and accurately. See Azure Virtual Machines for details.

Azure Storage

To protect your Azure Storage using IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID, follow these steps:

1. Connect your tenant.
   - If you want to protect your Microsoft Entra tenant via IBM® Storage Protect for Cloud, your tenant owner or service administrators must first connect the tenant to IBM® Storage Protect for Cloud. See Connect your Tenants to IBM® Storage Protect for Cloud for details.
2. Configure the app profile.
   - Set up the app profile for the service app required to protect the Azure storage data. Use your Microsoft 365 Global Admin Account to consent to the application. See Create a Service App and Grant Consent for details.
3. Add to subscription and grant role.
   - After creating the app profile in IBM® Storage Protect for Cloud, add the app to each subscription where the Azure storage data you want to protect belongs. See Add to Subscriptions and Assign the Contributor Role for details.
4. Create the backup scope.
   - Navigate to IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID > **Backup** page and create a backup scope for blob storage or file share. Define the protected blobs containers or file shares, configure the backup start time, and ensure the data retention policy and backup schedule meet your organization's needs. See Create a New Backup Scope for Azure Storage for details.

   > **Note:** With a trial subscription, you can only have one backup scope for Blob storage and file share, respectively. You can select up to 5 blob containers or 5 file shares for each backup scope. The backup job will protect up to 5 folder-level objects within the selected storage, and the storage space for backup data can be at most 25 GB.

5. Monitor and manage backups.
   - Regularly monitor the backup status and ensure that backups are running as scheduled. See Monitor Your Backup for details.
   - Use the Backup Analysis report to monitor your backup statistics. See View Backup Analysis Report for details.
6. Test restores.
   - Periodically test the restore process to ensure that you can recover data quickly and accurately. See Azure Storage for details.

Azure SQL Databases

To protect your Azure SQL databases using IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID, follow these steps:

1. Connect your tenant.
   - If you want to protect your Microsoft Entra tenant via IBM® Storage Protect for Cloud, your tenant owner or service administrators must first connect the tenant to IBM® Storage Protect for Cloud. See Connect your Tenants to IBM® Storage Protect for Cloud for details.
2. Configure the app profile.
   - Set up the app profile for the service app required to protect the Azure SQL databases. Use your Microsoft 365 Global Admin Account to consent to the application. See Create a Service App and Grant Consent for details.
3. Add to subscription and grant role.
   - After creating the app profile in IBM® Storage Protect for Cloud, add the app to each subscription where the Azure SQL databases you want to protect belongs. See Add to Subscriptions and Assign the Contributor Role for details.

- If you want to enable the Azure SQL backup service, add a SQL server admin role for the app you want to use to protect Azure SQL databases. See Grant a SQL Server Admin Role for details

4. Create the backup scope.

   - Navigate to IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID > **Backup** page and create a backup scope for native Azure SQL backup monitoring or Azure SQL backup. Define the protected databases, configure the backup start time, and ensure the data retention policy and backup schedule meet your organization's needs. See Create a New Backup Scope for Native Azure SQL Backup Monitoring or Create a New Backup Scope for Azure SQL Backup for details.

   > **Note:** With a Trial subscription, you can create one backup scope to protect up to 5 databases for each service.

5. Monitor and manage backups.

   - Regularly monitor the backup status and ensure that backups are running as scheduled. See Monitor Your Backup for details.

   - Use the Backup Analysis report to monitor your backup statistics. See View Backup Analysis Report for details.

6. Test restores.

   - Periodically test the restore process to ensure that you can recover data quickly and accurately. See Restore Monitored Databases or Restore Backup Databases for details.

Azure DevOps Projects

To protect your Azure DevOps projects using IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID, follow these steps:

1. Connect your tenant.

   - If you want to protect your Microsoft Entra tenant via IBM® Storage Protect for Cloud, your tenant owner or service administrators must first connect the tenant to IBM® Storage Protect for Cloud. See Connect your Tenants to IBM® Storage Protect for Cloud for details.

2. Configure the service app profile.

   - Set up the app profile for the service app required to protect Azure DevOps data. Use your Microsoft 365 Global Admin Account to consent to the application. See Create a Service App and Grant Consent for details.

3. Create the backup scope.

   - Navigate to IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID > **Backup** page and create a backup scope for Azure DevOps. Define the protected organizations, configure the backup start time, and ensure the data retention policy and backup schedule meet your organization's needs. See Create a New Backup Scope for Azure DevOps for details.

   > **Note:** With a trial subscription, you can create one backup scope to protect up to 5 projects

4. Monitor and manage backups.

   - Regularly monitor the backup status and ensure that backups are running as scheduled. See Monitor Your Backup for details.

   - Use the Backup Analysis report to monitor your backup statistics. See View Backup Analysis Report for details.

5. Test restores.

   - Periodically test the restore process to ensure that you can recover data quickly and accurately. See Restore Azure DevOps Organizations for details.

Azure AD B2C Data

To protect your Azure AD B2C using IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID, follow these steps:

1. Connect your tenant.
   - If you want to protect your Microsoft Entra tenant via IBM® Storage Protect for Cloud, your tenant owner or service administrators must first connect the tenant to IBM® Storage Protect for Cloud. See Connect your Tenants to IBM® Storage Protect for Cloud for details.

   > **Note:** The user connecting your tenant must be a member of your tenant's domain, instead of an external user.

2. Configure the service app profile.
   - Set up the app profile for the service app required to protect Azure AD B2C data. Use your Microsoft 365 Global Admin Account to consent to the application. See Create a Service App and Grant Consent for details.

   > **Note:** The user creating the service app profile and granting consent must be a member of your tenant's domain, instead of an external user.

3. Create the backup scope.
   - Navigate to IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID > **Backup** page and create a backup scope for Azure AD B2C. Define the protected data, configure the backup start time, and ensure the data retention policy meets your organization's needs. The backup job will run once a day. See Create a New Backup Scope for Azure AD B2C for details.

   > **Note:** With a trial subscription, you can only have one backup scope.

4. Monitor and manage backups.
   - Regularly monitor the backup status and ensure that backups are running as scheduled. See Monitor Your Backup for details.
   - Use the Backup Analysis report to monitor your backup statistics. See View Backup Analysis Report for details.

5. Test restores.
   - Periodically test the restore process to ensure that you can recover data quickly and accurately. See Azure AD B2C for details.

Quick Setup

Entra ID Initial Activation

Follow these steps to set up and manage Entra ID activation for IBM® Storage Protect for Cloud:

1. Sign up for IBM® Storage Protect for Cloud to use IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID.
   - Visit the IBM® Storage Protect for Cloud trial page for IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID and sign up for a free 30 day trial.
2. Access IBM® Storage Protect for Cloud.
   - Sign in to the IBM® Storage Protect for Cloud environment using the corresponding account. See Sign into IBM® Storage Protect for Cloud for details.
3. Connect your tenant.
   - If you want to protect your Microsoft Entra tenant via IBM® Storage Protect for Cloud, your tenant owner or service administrators must first connect the tenant to IBM® Storage Protect for Cloud. See Connect your Tenants to IBM® Storage Protect for Cloud for details.
4. Configure the service app profile.
   - Set up the app profile for the service app required to protect the Microsoft Entra. Use your Microsoft 365 Global Admin Account to consent to the application. See Create a Service App and Grant the Consent for details.
5. Configure a service account profile.
   - Create a service account profile if you want to protect the following properties. For details on configuring a service account profile, refer to Create a Service Account Profile.
     - To back up and restore distribution lists or mail-enabled security groups in Microsoft Entra ID, you can choose to configure a service account profile for this tenant with a Global Administrator or Exchange Administrator user role, or you can go to the Azure portal to add this service app as Exchange Administrators role. For details on assigning an app the Exchange administrator role, refer to How to Assign the Exchange Administrator Role to an App?.
     - To back up and restore the **Attributes and Claims**, **Identifier (Entity ID)**, **currentSingleSignOnMode**, **ParentAppId**, or **IsCustomApp**of the SSO configuration for the enterprise applications, you must have a service account profile configured in the IBM® Storage Protect for Cloud interface and the service account you use must have the **Application Administrator** role.
6. Create the backup scope.
   - Navigate to IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID > **Backup** page and create a backup scope for the Microsoft Entra tenant that you want to protect. Define whether to protect the Sign-in log or Audit log, configure the backup start time, and ensure the data retention policy meets your organization's needs. The backup job will run once a day. See Create a New Backup Scope for Microsoft Entra ID for details.
7. Monitor and manage backups.
   - Regularly monitor the backup status and ensure that backups are running as scheduled. See Monitor Your Backup for details.
   - Use the Subscription Consumption report and Backup Analysis report to track your subscription utilization and backup statistics. See Reports for details.
8. Test restores.
   - Periodically test the restore process to ensure that you can recover data quickly and accurately.
   - Compare backups to ensure you are restoring the correct files. See Use the Compare Method for details.

Admin Portal Settings Initial Activation

Follow these steps to set up and manage Admin Portal Settings activation for IBM® Storage Protect for Cloud:

1. Sign up for IBM® Storage Protect for Cloud to use IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID.
    - Visit the IBM® Storage Protect for Cloud trial page for IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID and sign up for a free 30 day trial.
2. Access IBM® Storage Protect for Cloud.
    - Sign into the IBM® Storage Protect for Cloud environment using the corresponding account. See Sign into IBM® Storage Protect for Cloud for details.
3. Connect your tenant.
    - If you want to protect your Microsoft Entra tenant via IBM® Storage Protect for Cloud, your tenant owner or service administrators must first connect the tenant to IBM® Storage Protect for Cloud. See Connect your Tenants to IBM® Storage Protect for Cloud for details.
4. Configure the service app profile.
    - Set up the app profile for the service app required to protect the admin portal settings. Use your Microsoft 365 Global Admin Account to consent to the application. See Create a Service App and Grant the Consent for details.
5. Configure a service account profile.
    - Create a service account profile if you want to protect the following properties. For details on configuring a service account profile, refer to Create a Service Account Profile.
        - If you want to back up and restore the Microsoft 365 Defender or Exchange settings through **Admin Portal Settings** service, you can choose to configure a service account profile for this tenant with a Global Administrator or Exchange Administrator user role, or you can go to the Azure portal to add this service app as Exchange Administrators role. For details on assigning an app the Exchange administrator role, refer to How to Assign the Exchange Administrator Role to an App?.
        - To back up and restore the **Self Service Group Management** property of the **Groups General** settings for **Microsoft Entra ID** > **Groups**, you must configure a service account profile in the IBM® Storage Protect for Cloud interface with the service account in **Cloud Application Administrator** role.
6. Create the backup scope.
    - Navigate to IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID > **Backup** page and create a backup scope for the Microsoft Entra tenant that you want to protect. Define whether to protect the Sign-in log or Audit log, configure the backup start time, and ensure the data retention policy meets your organization’s needs. The backup job will run once a day. See Create a New Backup Scope for Admin Portal Settings for details.
7. Monitor and manage backups.
    - Regularly monitor the backup status and ensure that backups are running as scheduled. See Monitor Your Backup for details.
    - Use the Subscription Consumption report and Backup Analysis report to track your subscription utilization and backup statistics. See Reports for details.
8. Test restores.
    - Periodically test the restore process to ensure that you can recover data quickly and accurately.
    - Compare backups to ensure you are restoring the correct files. See Use the Compare Method for details.

Azure Virtual Machine Initial Activation

Follow these steps to set up and manage Azure virtual machine activation for IBM® Storage Protect for Cloud:

1. Sign up for IBM® Storage Protect for Cloud to use IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID.

- Visit the IBM® Storage Protect for Cloud trial page for IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID and sign up for a free 30 day trial.

2. Access IBM® Storage Protect for Cloud.
    - Sign in to the IBM® Storage Protect for Cloud environment using the corresponding account. See Sign into IBM® Storage Protect for Cloud for details.
3. Connect your tenant.
    - If you want to protect your Microsoft Entra tenant via IBM® Storage Protect for Cloud, your tenant owner or service administrators must first connect the tenant to IBM® Storage Protect for Cloud. See Connect your Tenants to IBM® Storage Protect for Cloud for details.
4. Configure the service app profile.
    - Set up the app profile for the service app required to protect the Microsoft Entra. Use your Microsoft 365 Global Admin Account to consent to the application. See Create a Service App and Grant the Consent for details.
5. Add to subscription and grant role.
    - After creating the app profile in IBM® Storage Protect for Cloud, add the app to each subscription where the Azure VMs you want to protect belong. See Add to Subscriptions and Assign the Contributor Role for details.
6. Create the backup scope.
    - Navigate to IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID > **Backup** page and create a backup scope for the Microsoft Entra tenant that you want to protect. Define whether to protect the Sign-in log or Audit log, configure the backup start time, and ensure the data retention policy meets your organization’s needs. The backup job will run once a day. See Create a New Backup Scope for Azure VM for details.
7. Monitor and manage backups.
    - Regularly monitor the backup status and ensure that backups are running as scheduled. See Monitor Your Backup for details.
    - Use the Subscription Consumption report and Backup Analysis report to track your subscription utilization and backup statistics. See Reports for details.
8. Test restores.
    - Periodically test the restore process to ensure that you can recover data quickly and accurately.

Azure Storage Initial Activation

Follow these steps to set up and manage Azure storage activation for IBM® Storage Protect for Cloud:

1. Sign up for IBM® Storage Protect for Cloud to use IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID.
    - Visit the IBM® Storage Protect for Cloud trial page for IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID and sign up for a free 30 day trial.
2. Access IBM® Storage Protect for Cloud.
    - Sign in to the IBM® Storage Protect for Cloud environment using the corresponding account. See Sign into IBM® Storage Protect for Cloud for details.
3. Connect your tenant.
    - If you want to protect your Microsoft Entra tenant via IBM® Storage Protect for Cloud, your tenant owner or service administrators must first connect the tenant to IBM® Storage Protect for Cloud. See Connect your Tenants to IBM® Storage Protect for Cloud for details.
4. Configure the app profile.
    - Set up the app profile for the service app required to protect the Azure storage data. Use your Microsoft 365 Global Admin Account to consent to the application. See Create a Service App and Grant the Consent for details.
5. Add to subscription and grant role.

- After creating the app profile in IBM® Storage Protect for Cloud, add the app to each subscription where the Azure storage data you want to protect belongs to. See Add to Subscriptions and Assign the Contributor Role for details.

6. Create the backup scope.
   - Navigate to IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID > **Backup** page and create a backup scope for the Microsoft Entra tenant that you want to protect. Define whether to protect the Sign-in log or Audit log, configure the backup start time, and ensure the data retention policy meets your organization’s needs. The backup job will run once a day. See Create a New Backup Scope for Azure Storage for details.
7. Monitor and manage backups.
   - Regularly monitor the backup status and ensure that backups are running as scheduled. See Monitor Your Backup for details.
   - Use the Subscription Consumption report and Backup Analysis report to track your subscription utilization and backup statistics. See Reports for details.
8. Test restores.
   - Periodically test the restore process to ensure that you can recover data quickly and accurately.

Azure SQL Initial Activation

Follow these steps to set up and manage Azure SQL activation for IBM® Storage Protect for Cloud:

1. Sign up for IBM® Storage Protect for Cloud to use IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID.
   - Visit the IBM® Storage Protect for Cloud trial page for IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID and sign up for a free 30 day trial.
2. Access IBM® Storage Protect for Cloud.
   - Sign in to the IBM® Storage Protect for Cloud environment using the corresponding account. See Sign into IBM® Storage Protect for Cloud for details.
3. Connect your tenant.
   - If you want to protect your Microsoft Entra tenant via IBM® Storage Protect for Cloud, your tenant owner or service administrators must first connect the tenant to IBM® Storage Protect for Cloud. See Connect your Tenants to IBM® Storage Protect for Cloud for details.
4. Configure the app profile.
   - Set up the app profile for the service app required to protect the Azure SQL databases. Use your Microsoft 365 Global Admin Account to consent to the application. See Create an App Profile and Grant Consent for details.
5. Add to subscription and grant role.
   - After creating the app profile in IBM® Storage Protect for Cloud, add the app to each subscription where the Azure storage data you want to protect belongs to. See Add to Subscriptions and Assign the Contributor Role for details.
   - If you want to enable the Azure SQL backup service, add a SQL server admin role for the app you want to use to protect Azure SQL databases. See Grant a SQL Server Admin Role for details.
6. Create the backup scope.
   - Navigate to IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID > **Backup** page and create a backup scope for native Azure SQL backup monitoring or Azure SQL backup. Define the protected databases, configure the backup start time, and ensure the data retention policy and backup schedule meet your organization’s needs. See Create a New Backup Scope for Native Azure SQL Backup Monitoring or Create a New Backup Scope for Azure SQL Backup for details.
7. Monitor and manage backups.
   - Regularly monitor the backup status and ensure that backups are running as scheduled. See Monitor Your Backup for details.

- Use the Subscription Consumption report and Backup Analysis report to track your subscription utilization and backup statistics. See Reports for details.

8. Test restores.
   - Periodically test the restore process to ensure that you can recover data quickly and accurately.

Azure DevOps Initial Activation

Follow these steps to set up and manage Azure DevOps activation for IBM® Storage Protect for Cloud:

1. Sign up for IBM® Storage Protect for Cloud to use IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID.
   - Visit the IBM® Storage Protect for Cloud trial page for IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID and sign up for a free 30 day trial.
2. Access IBM® Storage Protect for Cloud.
   - Sign in to the IBM® Storage Protect for Cloud environment using the corresponding account. See Sign into IBM® Storage Protect for Cloud for details.
3. Connect your tenant.
   - If you want to protect your Microsoft Entra tenant via IBM® Storage Protect for Cloud, your tenant owner or service administrators must first connect the tenant to IBM® Storage Protect for Cloud. See Connect your Tenants to IBM® Storage Protect for Cloud for details.
4. Configure the service app profile.
   - Set up the app profile for the service app required to protect the Azure DevOps data. Use your Microsoft 365 Global Admin Account to consent to the application. See Create a Service App and Grant the Consent for details.
5. Create the backup scope.
   - Navigate to IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID > **Backup** page and create a backup scope for the Microsoft Entra tenant that you want to protect. Define whether to protect the Sign-in log or Audit log, configure the backup start time, and ensure the data retention policy meets your organization's needs. The backup job will run once a day. See Create a New Backup Scope for Azure DevOps for details.
6. Monitor and manage backups.
   - Regularly monitor the backup status and ensure that backups are running as scheduled. See Monitor Your Backup for details.
   - Use the Subscription Consumption report and Backup Analysis report to track your subscription utilization and backup statistics. See Reports for details.
7. Test restores.
   - Periodically test the restore process to ensure that you can recover data quickly and accurately.

Azure AD B2C Initial Activation

Follow these steps to set up and manage Azure AD B2C activation for IBM® Storage Protect for Cloud:

1. Sign up for IBM® Storage Protect for Cloud to use IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID.
   - Visit the IBM® Storage Protect for Cloud trial page for IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID and sign up for a free 30 day trial.
2. Access IBM® Storage Protect for Cloud.
   - Sign in to the IBM® Storage Protect for Cloud environment using the corresponding account. See Sign into IBM® Storage Protect for Cloud for details.
3. Connect your tenant.
   - If you want to protect your Microsoft Entra tenant via IBM® Storage Protect for Cloud, your tenant owner or service administrators must first connect the tenant to IBM® Storage Protect for Cloud. See Connect your Tenants to IBM® Storage Protect for Cloud for details.

> **Note:** The user connecting your tenant must be a member of your tenant's domain, instead of an external user.

4. Configure the service app profile.

    - Set up the app profile for the service app required to protect the Azure AD B2C data. Use your Microsoft 365 Global Admin Account to consent to the application. See Create a Service App and Grant the Consent for details.

    > **Note:** The user creating the service app profile and granting consent must be a member of your tenant's domain, instead of an external user.

5. Create the backup scope.

    - Navigate to IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID > **Backup** page and create a backup scope for Azure AD B2C. Define whether to protect the Sign-in log or Audit log, configure the backup start time, and ensure the data retention policy meets your organization's needs. The backup job will run once a day. See Create a New Backup Scope for Azure AD B2C for details.

6. Monitor and manage backups.

    - Regularly monitor the backup status and ensure that backups are running as scheduled. See Monitor Your Backup for details.

    - Use the Subscription Consumption report and Backup Analysis report to track your subscription utilization and backup statistics. See Reports for details.

7. Test restores.

    - Periodically test the restore process to ensure that you can recover data quickly and accurately.

Quick Start Guide

Refer to the following guide to get started with IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID.

IBM Storage Protect for Cloud Azure VMs, Storage, and Entra ID Quick Start Guide

Get Started

Before you start using IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID, you must at first obtain a trial or enterprise subscription.

To use IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID to protect Microsoft Entra ID, Azure VMs, Azure Storage, Admin Portal Settings, Azure SQL, or Azure AD B2C, you must connect your **Microsoft** tenant to IBM® Storage Protect for Cloud. For details, refer to Connect your tenants to IBM Storage Protect for Cloud.

Note the following:

- If you want to connect a tenant which will be used to back up Azure AD B2C, the user creating the service app profile and granting consent must be a member of your tenant's domain , instead of an external user.
- The Azure SQL service only supports protecting SQL databases. The SQL managed instances and SQL virtual machines are currently unsupported.
- If you are a customer from a distributor with the subscription to use the IBM® Storage Protect for Cloud default storage, you can choose either to use the IBM® Storage Protect for Cloud default storage or use your own storage to store the backup data for the first time you sign into IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID.

Refer to the sections below to enable the backup services:

Enable the Backup for Azure Virtual Machines, Azure Storage, and Azure SQL

Before you enable the backup service for Azure VM, Azure Storage, or Azure SQL, go to IBM® Storage Protect for Cloud to configure an app profile to register an app for **Microsoft™ Delegate** purposes. You can choose to register a delegated app or use a custom Azure app with the required Delegated permissions. After registering the app to your tenant, the owner of each subscription where the VMs or storages to protect are running must add the **IBM® Storage Protect for Cloud - Delegated App** with **Contributor** role to the subscription.

Before you begin

Note that if you have concerns about granting this app the **Contributor** role, you can create a custom role for this app. For details, refer to “Add a Custom Role Using Azure Portal, CLI, or PowerShell” on page 41.

Procedure

Complete the following steps:

1. Go to **Management** > **App Management** in the IBM® Storage Protect for Cloud interface to create an app profile for Microsoft™ Delegate. For details, refer to “Create an App Profile and Grant Consent” on page 40.
2. Add this app to all the subscriptions where the VMs, storages, or databases that you want to protect are running and grant this app the Contributor role. For details, refer to “Add to Subscriptions and Assign the Contributor Role” on page 41. This guide introduces only the steps of adding a role to a subscription through the Microsoft™ Azure Portal.

> **Note:** The user to add the app to the subscription and grant it the Contributor role must be the subscription owner or the User access administrator of your tenant, and if your tenant has new subscriptions to protect after the initialization, you must follow the same steps to add this app as Contributor as well.

If you are going to protect Azure storage or use your own storage device to store the backup data, read the instructions in “Allow IBM Storage Protect for Cloud Agent Servers to Access Your Storage Account” on page 82 section carefully and complete the settings upon your need.

If the storage account has disabled the “**Allow storage account key access**” feature, the app must also have the **Storage Blob Data Contributor** role to the subscription or storage account, in addition to the **Contributor** role. Additionally, in this case, only the Azure Blob Storage is supported; the Azure File Storage is not supported.

If you want to protect databases with the Azure SQL backup service, read the instructions in Grant a SQL Server Admin Role.

3. After you completed all the settings above, go to the **Backup** page of IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID, and then configure backup scopes for Azure Virtual Machine, Azure Storage, or Azure SQL. Note that before you start creating a backup scope, you can click the **Refresh** (🔄) button in the upper-right corner of the service page to retrieve the latest status for the data to protect. The Last refreshed time is displayed next to the **Refresh** (🔄) button.
For details on configuring the backup scope, refer to:
    - Create a New Backup Scope for Azure VM
    - Create a New Backup Scope for Azure Storage
    - Create a New Backup Scope for Native Azure SQL Backup Monitoring
    - Create a New Backup Scope for Azure SQL

Create an App Profile and Grant Consent

To use backup and restore services for Azure VM, Azure Storage, or Azure SQL, it is necessary to create a delegated app or a custom Azure app with delegated permissions. This app must connect to your tenant and receive consent for the requested permissions.

Before you begin

Creating a delegated profile requires a Microsoft 365 Global Administrator account to consent. However, to re-authorize an app with delegated permission, you can choose to end-user consent. For details, refer to Re-authorize an App Profile.

Procedure

To create the delegated app, complete the following steps:

1. On the **App Management** page, click **Create** on the action bar.
2. In the **Select services** step, select **IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID**.
3. In the **Choose setup method** step, select **Modern mode** if you want to consent a delegated app directly. You can also select **Custom Mode** if you want to manually create and maintain a custom app with delegated permissions in your tenant. For details on creating a custom app with delegated permission for IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID, refer to Create a Custom Azure App.
4. Click **Next**
5. In the **Consent to apps** step for a Microsoft tenant, click**Consent** next to the **IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID– Delegated App**.
6. On the Microsoft 365 sign-in page, sign in with a Microsoft 365 Global Administrator account.
7. On the **Permissions required** page, review the permissions required and click **Accept** to continue. This delegated app must have the following Microsoft Azure API permissions:
    - **Access Azure Service Management as you (Preview)** – Allows the application to access Azure Service Management as you.
    - **View your basic profile**– Allows the app to see your basic profile (name, picture, username).
    - **Maintain access to data you have given it access to** – Allows the app to see and update the data that you gave access to, even when you are not currently using the app. This does not give the app any additional permissions. For example, for the functioning of IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID, you also need to add this app to the subscription where the VMs you want to protect are running as Contributor. The Contributor role in subscription allows the app to access and manage resources. This permission allows IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID to access and manage the resources via this app.

8. The app profile you created will be displayed on the **App Management** page, and the **IBM® Storage Protect for Cloud– Delegated App** will be added to your Azure enterprise applications.

Add to Subscriptions and Assign the Contributor Role

After you complete the app profile creation in IBM® Storage Protect for Cloud, navigate to the Entra Admin Center **> Subscriptions**. Follow the steps below to add the **IBM® Storage Protect for Cloud - Delegated App** or the custom app you created with delegated permissions, to each subscription that includes the VM you intend to protect.

Before you begin

> **Note:** To add this app to the subscription and grant it the Contributor role, the user must be either the **Owner** of the subscription or the User access administrator of your tenant. If you have concerns about granting this app the **Contributor** role, you can create a custom role for this app. For details, refer to "Add a Custom Role Using Azure Portal, CLI, or PowerShell" on page 41.

If your storage account to protect has disabled the "**Allow storage account key access**" feature, the app must also have the **Storage Blob Data Contributor** role to the subscription or storage account, in addition to the **Contributor** role to protect the Azure Blob Storage, and in this case the Azure File Storage is not supported.

Procedure

1. On the **Subscriptions** page, find the list of subscriptions. You can filter the subscriptions in the list or search for subscriptions via keywords.
2. Click a subscription.
3. Click **Access control (IAM)** on the left pane.
4. On the **Access control (IAM)** page, click **Add** on the action bar and select **Add role assignment** from the drop-down list.
5. In the **Add role assignment** pane, go to the **Privileged administrator roles** tab, click **Contributor** from the **Role**tab, and then click **Next**.
6. In the **Members** list, find the **Members** field, and click **Select members**.
7. In the **Select members** pane, enter a keyword in the **Select** box to search for the **IBM® Storage Protect for Cloud - Delegated App** or the custom app that was created with delegated permissions. Click the app to add it to the **Selected members** field and click the **Select** button.
8. Click the **Review + assign** button to review the role assignment and click this button again to add this app as **Contributor** for your subscription.

Add a Custom Role Using Azure Portal, CLI, or PowerShell

About this task

Follow the steps below to add a custom role for the app that you want to use to protect Azure Virtual Machines and Azure Storage:

Procedure

1. Download the template from this link: Custom_Role_Template.zip.
2. In the extracted folder, open the file that you want to use to add the custom role.
3. Find the entry "AssignableScopes":["/subscriptions/#SubscriptionID#"] and replace #SubscriptionID# with your subscription ID.
4. For the examples of creating a custom role using the Azure Portal, CLI, or PowerShell, refer to Azure custom roles.

Grant a SQL Server Admin Role

About this task

To enable Azure SQL backup service, the SQL server admin role is required to grant to the delegated app. Follow the steps below to add a SQL server admin role for the app you want to use to protect Azure SQL databases.

Procedure

1. Go to Azure portal > **Azure SQL**.
2. Click your app name and navigate to **Settings** > **Microsoft Entra ID**.
3. In the Microsoft Entra ID page, click **Set admin**.
4. Select your admin group and then click **Select**.
5. After selecting, click **Save**tosave changes.
6. Navigate to **Security** > **Networking** > **Public access** tab.
7. In the Public network access field, select **Selected networks** to enable public network access.
8. In the Exceptions field, select the **Allow Azure services and resources to access this server** option.

Enable Backup for Microsoft Entra ID or Admin Portal Settings

About this task

To back up the Microsoft Entra ID or Admin Portal Settings, you can choose to create a service app, or use a custom Azure app with required permissions. For details on creating a custom Azure app, refer to Create a Custom Azure App. You can go to the Default Permissions Granted to the Service App section to find the permissions that you can grant to your custom app.

Procedure

Complete the following steps:

1. Before you enable the backup service for Microsoft Entra ID or Admin Portal Settings, go to IBM® Storage Protect for Cloud to configure a service app profile for that Microsoft 365 tenant. For detailed instructions on creating a service app profile, refer to "Create a Service App and Grant Consent" on page 43.
2. After the service app is ready, go to the **Backup** page of the IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID to configure the backup scope for the Microsoft Entra ID or Admin Portal Settings. Note that if you have multiple tenants to protect, you must create a service app for each of them.
   For details on configuring the backup scope, refer to:
   - Create a New Backup Scope for Microsoft Entra ID
   - Create a New Backup Scope for Admin Portal Settings

   Note the following:

   - If you want to protect distribution lists or mail-enabled security groups in **Microsoft Entra ID**, or protect the Microsoft 365 Defender or Exchange settings through **Admin Portal Settings** service, you can choose to configure a service account profile for this tenant with a Global Administrator or Exchange Administrator user role, or you can go to the Azure portal to add this service app as Exchange Administrators role. For details on assigning an app the Exchange administrator role, refer to How to Assign the Exchange Administrator Role to an App?. For details on configuring a service account profile, refer to Create a Service Account Profile.
   - A service account with MFA enabled is currently not supported. In addition, due to API limitations, the backup service of Microsoft Entra ID will perform full backups on the distribution lists and mail-enabled security groups each time. This can be determined by the number of successful objects in each backup job.
   - If you are using custom Azure app for Microsoft Entra ID or Admin Portal Settings service and you do not want to assign Global administrator or Exchange administrator role to the app, refer to the instructions in Create a Custom Role Group to create a role group with the minimum permissions. This configuration is only applicable to the custom app.

- If you want to restore a temporarily deleted user or group, the service account or the service app must be assigned with the **Global administrator** role.
- If you want to protect the **Self Service Group Management** property of the **Groups General** settings for **Microsoft Entra ID** > **Groups**, you must configure a service account profile in IBM® Storage Protect for Cloud interface with the service account in **Groups Administrator** role. Note that if you only want to back up this property, the **Cloud Application Administrator** role is not required.
- To back up and restore the **Attributes and Claims**, **Identifier (Entity ID)**,**currentSingleSignOnMode**, **ParentAppId**, or **IsCustomApp** of the SSO configuration for the enterprise applications, you must have a service account profile configured in IBM® Storage Protect for Cloud interface and the service account you use must have the **Application Administrator** role. Note that if you only want to back up this property, the **Application Administrator** role is not required.

For details on the support list, refer to Microsoft Entra ID and Admin Portal Settings.

Create a Service App and Grant Consent

The use Microsoft Entra ID's backup and restore services, create a service app to connect to your tenant and grant the requested permissions.

Before you begin

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

> **Note:** If you want to restore temporarily deleted users or groups, this service app must also be added as Global Administrator.

Procedure

Follow the steps below to create the service app:

1. On the **App Management** page, click **Create** on the action bar.
2. In the **Select services** step, select IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID.
3. In the **Choose setup method** step, select **Modern mode** and click **Next**.
4. In the **Consent to apps** step, click **Consent** next to the IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID.
5. On the Microsoft 365 sign-in page, sign in with a Microsoft 365 Global Administrator account.
6. On the **Permissions required** page, review the permissions required and click **Accept** to continue. For the API permissions that this app requests, refer to “Default Permissions Granted to the Service App” on page 43.
7. The app profile you created will be displayed on the **App Management** page, and the IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID app will be added to your **Microsoft Entra admin center › enterprise applications**.

Default Permissions Granted to the Service App

From January 2024 release, you can choose to use a custom Azure app with specific permissions for the data that you only want to protect.

All the API permissions required for Microsoft Entra ID and Admin Portal Settings services are listed in this table and they are automatically added to the service app after consent. For custom app permissions, you can choose to only add the corresponding permissions to protect the specific data types or add their alternative permissions (if available) for backup only purpose.

If you want to protect Microsoft Entra ID or the Admin Portal Settings, you can choose to create a **IBM® Storage Protect for Cloud** Azure service app profile or create a custom Azure app profile with **delegated permissions**through IBM® Storage Protect for Cloud > **App management** page. Note that if you do not use the

Microsoft Entra ID backup service to protect the BitLocker recovery keys for the devices, you can choose to create any types of custom Azure app.

The following API permissions will be automatically added to the service app with consent from your **Global administrator** account. You can also choose the specific permissions to grant your custom Azure app for the services or data types that you want to protect.

> **Note:** If you remove the **Global administrator** role for the user after consenting, to ensure the protection of BitLocker keys, the consent user must be in one of the following roles: Cloud device administrator, Helpdesk administrator, Intune service administrator, Security administrator, Security reader, or Global reader. Otherwise, the user must be the registered owner of the device that the BitLocker recovery key was originally backed up from.

Summary for complex table

API	Permissions	Type	Why You Need	Permission Catagory	Alternative Permission for backup only
Microsoft Graph Microsoft Graph	**AdministrativeUnit.ReadWrite.All** (Read and write administrative units.)	Application	Allows the app to create, read, update, and delete administrative units and manage administrative unit membership on behalf of the signed-in user.	Microsoft Entra ID > backup and restore of Administrative Units.	**AdministrativeUnit.Read.All** (Read all administrative units.)
	Application.ReadWrite.All (Read and write all apps.)	Application	Allows the app to create, read, update and delete applications and service principals on behalf of the signed-in user.	Microsoft Entra ID > backup and restore of applications.	**Application.Read.All** (Read all applications)
	AppRoleAssignment.ReadWrite.All (Manage app permission grants and app role assignments.)	Application	Allows the app to manage permission grants for application permissions to any API (including Microsoft Graph) and application assignments for any app, on behalf of the signed-in user.	Microsoft Entra ID > backup and restore of application role assignment.	
	AuditLog.Read.All (Read all audit log data.)	Application	Allows the app to read and query your audit log activities, without a signed-in user.	Microsoft Entra ID > backup of the Audit Logs and Sign-in Logs.	
	BitLockerKey.Read.All (Read BitLocker keys)	Application	Allows an app to read BitLocker keys for all devices, without a signed-in user. Allows read of the recovery key.	Microsoft Entra ID > backup of Device BitLocker keys.	
	BitLockerKey.Read.All (Read BitLocker keys)	Delegated	Allows an app to read BitLocker keys for all devices, without a signed-in user. Allows read of the recovery key.	Microsoft Entra ID > backup of Device BitLocker keys.	
	DeviceManagementApps.Read.All (Read Microsoft Intune apps.)	Application	Allows the app to read the properties, group assignments, and status of apps, app configurations, and app protection policies managed by Microsoft Intune.	Admin Portal Settings > backup of the app configuration policies in Microsoft Intune.	
	DeviceManagementApps.ReadWrite.All (Read and write Microsoft Intune apps.)	Delegated	Allows the app to read and write the properties, group assignments and status of apps, app configurations and app protection policies managed by Microsoft Intune, without a signed-in user.	Admin Portal Settings > restore of the supported Intune settings, such as apps properties, app configurations, and app protection policies.	**DeviceManagementApps.Read.All**

API	Permissions	Type	Why You Need	Permission Catagory	Alternative Permission for backup only
	DeviceManagementConfiguration.Read.All (Read Microsoft Intune device configuration and policies.)	Application	Allows the app to read properties of Microsoft Intune-managed device configuration and device compliance policies and their assignment to groups.	Admin Portal Settings > backup of device policies in Microsoft Intune.	
	DeviceManagementConfiguration.ReadWrite.All (Read and write all Microsoft Intune device configuration and policies.)	Application	Allows the app to read and write properties of Microsoft Intune-managed device configuration and device compliance policies and their assignment to groups, without a signed-in user.	Admin Portal Settings > restore of device policies in Microsoft Intune	
	DeviceManagementRBAC.Read.All (Read Microsoft Intune RBAC settings)	Application	Allows the app to read the properties relating to the Microsoft Intune Role-Based Access Control (RBAC) settings, without a signed-in user.	Admin Portal Settings > backup of the supported Intune settings, such as policy properties.	
	DeviceManagementScripts.ReadWrite.All (Read and write Microsoft Intune Scripts)	Application	Allows the app to read and write Microsoft Intune device compliance scripts, device management scripts, device shell scripts, device custom attribute shell scripts and device health scripts, without a signed-in user.	Admin Portal Settings > backup and restore of Intune Devices Scripts settings.	**DeviceManagementScripts.Read.All** (Allows the app to read Microsoft Intune device compliance scripts, device management scripts, device shell scripts, device custom attribute shell scripts and device health scripts, without a signed-in user.)

API	Permissions	Type	Why You Need	Permission Catagory	Alternative Permission for backup only
	Directory.ReadWrite.All (Read and write directory data.)	Application	Allows the app to read and write data in your organization's directory, such as users, and groups. It does not allow the app to delete users or groups, or reset user passwords.	Microsoft Entra ID > backup and restore of users and groups.	**Directory.Read.All** (Read directory data.)
	Domain.Read.All (Read domains)	Application	Allows the app to read all domain properties without a signed-in user.	Microsoft Entra ID > restore users.	
	Group.ReadWrite.All (Read and write all groups.)	Application	Allows the app to create groups and read all group properties and memberships on behalf of the signed-in user. Also allows the app to read and write calendar, conversations, files, and other group content for all groups the signed-in user can access. Additionally allows group owners to manage their groups and allows group members to update group content.	Microsoft Entra ID > backup and restore of groups.	**Group.Read.All** (Read all groups.)
	Organization.Read.All (Read organization information)	Application	Retrieves all the organizational brandings.	Admin Portal Settings > backup of Company Branding Settings.	
	Policy.Read.All (Read your organization's policies)	Application	Allows the app to read all your organization's policies without a signed in user.Retrieves all the named locations.	Microsoft Entra ID > restore users to another tenant. Admin Portal Settings > backup of Conditional Access and Named Locations.	
	Policy.ReadWrite.ApplicationConfiguration (Read and write your organization’s application configuration policies.)	Application	Allows the app to read and write your organization’s application configuration policies on behalf of the signed-in user.	Microsoft Entra ID > backup and restore for the SSO configurations of Enterprise applications.	
	Policy.ReadWrite.AuthenticationMethod (Read and write all authentication method policies)	Application	Retrieves all the authentication method policies and configurations.	Admin Portal Settings > backup of Authentication Methods.	
	UserAuthenticationMethod.ReadWrite.All (Read and write all users' authentication methods)	Application	Allows the application to read and write authentication methods of all users in your organization without a signed-in user. Authentication methods include information like a user’s phone number and Authenticator app settings. This does not allow the app to see sensitive information, such as the password, or to sign in or use the authentication methods.	Microsoft Entra ID > backup and restore of User Authentication Methods.	**UserAuthenticationMethod.Read.All** (Read all users’ authentication methods.)
	RoleManagement.ReadWrite.Directory (Read and write all directory RBAC settings.)	Application	Allows the app to read and manage the role-based access control (RBAC) settings for your company's directory, on behalf of the signed-in user. This includes instantiating directory roles and managing directory role membership, and reading directory role templates, directory roles and memberships.	Microsoft Entra ID > backup and restore of roles and administrators.	
	User.ReadWrite.All (Read and write all users’ full profiles.)	Application	Allows the app to read and write the full set of profile properties, reports, and managers of other users in your organization, on behalf of the signed-in user. Also allows the app to create and delete users as well as reset user passwords on behalf of the signed-in user.	Microsoft Entra ID > backup and restore of users.	**User.Read.All** (Read all users' full profiles)

API	Permissions	Type	Why You Need	Permission Catagory	Alternative Permission for backup only
	Policy.ReadWrite.Authorization (Read and write your organization’s authorization policy.)	Application	Allows the app to update the group general settings to enable or disable the capability for users to create security groups.	Admin Portal Settings > backup and restore of the group general settings.	
	Policy.ReadWrite.ConditionalAccess (Read and write your organization's conditional access policies.)	Application	Allows the app to read and write your organization's conditional access policies, without a signed-in user.	Admin Portal Settings > backup and restore of the conditional access.	**Policy.Read.ConditionalAccess** (Read your organization's conditional access policies)
	RoleManagement.ReadWrite.Directory (Read and write all directory RBAC settings.)	Application	Allows the app to read and manage the role-based access control (RBAC) settings for your company's directory, on behalf of the signed-in user. This includes instantiating directory roles and managing directory role membership, and reading directory role templates, directory roles and memberships.	Microsoft Entra ID > backup and restore of roles and administrators.	
	User.Read (Sign in and read user profile.)	Delegated	Allows users to sign into IBM® Storage Protect for Cloud with Microsoft 365 accounts.	Sign into IBM® Storage Protect for Cloudwith Microsoft 365 accounts.	
	User.ReadWrite.All (Read and write all users’ full profiles.)	Application	Allows the app to read and write the full set of profile properties, reports, and managers of other users in your organization, on behalf of the signed-in user. Also allows the app to create and delete users as well as reset user passwords on behalf of the signed-in user.	Microsoft Entra ID > backup and restore of users.	**User.Read.All** (Read all users' full profiles)
	UserAuthenticationMethod.ReadWrite.All (Read and write all users' authentication methods)	Application	Allows the application to read and write authentication methods of all users in your organization without a signed-in user. Authentication methods include information like a user’s phone number and Authenticator app settings. This does not allow the app to see sensitive information, such as the password, or to sign in or use the authentication methods.	Microsoft Entra ID > backup and restore of User Authentication Methods.	**UserAuthenticationMethod.Read.All** (Read all users’ authentication methods.)
Office 365 Exchange Online	**Exchange.ManageAsApp** (Manage Exchange as application)	Application	Allows the backup and restore of the distribution lists.	Microsoft Entra ID >Allows the backup and restore of distribution lists. Admin Portal Settings > backup and restore of Exchange and Defender settings.	

Create a Custom Role Group

If you want to protect **distribution lists** or **mail-enabled security groups** in Microsoft Entra tenant through the **Microsoft Entra ID** service, or to protect Microsoft 365 Defender or Exchange admin center settings through the **Admin Portal Settings** service, you can choose to assign the Exchange administrator role to the app that you created for Microsoft Entra ID and Admin Portal Settings services. If you are using a custom app and you do not want to assign the Exchange administrator role to the app in this case, you can now create a role group through Exchange admin center with minimum permissions and add the app as the group member.

Note that this configuration is only applicable to the custom app.

Follow the steps below:

1. Sign into the Exchange admin center with an administrator account.
2. Navigate to **Roles** > **Admin roles**.
3. Click **Add role group**.
4. Provide the basic information for the role group and go to the **Permission** step.
5. In the **Add permissions** page, select the following permissions:
   - Mail Recipients
   - View-Only Configuration
   - View-Only Recipients
6. Click **Next**, continue to complete the other settings, and click **Add role group** to finish.
7. After the role group with the required permissions has been added, follow the steps below to add the app to the role group as a group member:
   a. Run PowerShell as an administrator on your computer.

   b. Install Exchange Online via PowerShell using the following command lines:

```
Install-Module -Name ExchangeOnlineManagement -RequiredVersion 3.4.0

Set-ExecutionPolicy RemoteSigned
```

   c. Execute the following command lines to add the app as a member of the role group that you have created:

> **Note:** You must provide the **Application ID**, **Object ID**, and the **Display Name** of the app. You can go to the Azure portal > **Enterprise applications** page for the app information.

```
Connect-ExchangeOnline

New-ServicePrincipal -AppId <Application ID on Azure Portal> -ObjectId <Object ID
on Azure Portal> -DisplayName <Same name as in Azure Portal>

Add-RoleGroupMember "<Roles Groups Name on Exchange Admin page>" -Member
<ServicePrincipal Object ID>
```

Enable Backup for Azure DevOps

Before you begin

To back up the Azure DevOps, you can choose to create a service app, or use a custom Azure app with **Azure DevOps API user_impersonation** permission. For details on creating a custom Azure app in your tenant, refer to Create a Custom Azure App.

Procedure

Complete the steps below:

1. Before you enable the backup service for Azure DevOps, go to IBM® Storage Protect for Cloud to configure a service app profile for that Microsoft 365 tenant. For detailed instructions on creating a service app profile, refer to Create a Service App and Grant the Consent.
2. After the service app is ready, go to the **Backup** page of the IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID to configure the backup scope for the Azure DevOps. Note that if you have multiple tenants to protect, you must create a service app for each of them.
   For details on configuring the backup scope, refer to Create a New Backup Scope for Azure DevOps.

   > **Note:** Before you back up your organizations in IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID, you must first log into your organizations with the account for which the app profile was configured.

Create a Service App and Grant Consent

For the backup and restore services of Azure DevOps, you must create a service app to connect to your tenant and grant consent for the permissions this app requests.

Before you begin

To create an app profile and grant consent, a Project Collection Administrator of the Azure DevOps organization account account is required, and your tenant must have previously created or connected to an organization in Azure DevOps. For details on how to add users to the Project Collection Administrator group, refer to the Microsoft article: Look up a project collection administrator.

Procedure

Follow the steps below to create the service app:

1. On the **Management** > **App management** page, click **Create** on the action bar.
2. In the **Select services** step, select **IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID**.
3. In the **Choose setup method** step, select **Modern mode** and click **Next**.
4. In the **Consent to apps** step, click **Consent** next to the **IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID DevOps**.
5. On the Microsoft 365 sign-in page, sign in with a Microsoft 365 Global Administrator account.
6. On the **Permissions required** page, review the permissions required and click **Accept** to continue. For the API permissions that this app requests, refer to Default Permissions Granted to the Service App.
7. The app profile you created will be displayed on the **App management** page, and the **IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID DevOps** app will be added to your Microsoft Entra admin center > enterprise applications.

Default Permissions Granted to the Service App

If you want to protect **Azure DevOps**, you can choose to create a **IBM® Storage Protect for Cloud AzureDevOps** service app profile or create a custom Azure app profile with **delegated permissions** through IBM® Storage Protect for Cloud > **Management** >**App management** page.

The following API permissions will be automatically added to the service app with consent from your **Global administrator** account. You can also choose the specific permissions to grant your custom Azure app for the services or data types that you want to protect upon the usage purpose. Currently, the required permissions don’t have any alternative permissions.

API	Permissions	Type	Why You Need	Permissions Category
Azure DevOps	**user_impersonation** (Have full access to Visual Studio Team Services REST APIs)	Delegated	Have full access to Visual Studio Team Services REST APIs.	Azure DevOps
Microsoft Graph	**User.Read.All** (Read all user's full profile)	Delegated	Allows the app to read the full set of profile properties, reports, and managers of other users in your organization, on behalf of the signed-in user.	Sign into IBM® Storage Protect for Cloud with Microsoft 365 accounts.

Enable Backup for Azure AD B2C

To back up Azure AD B2C data, you can choose to create a service app, or use a custom Azure app with required permissions. For details on creating a custom Azure app in your tenant, refer to Create a Custom Azure App.

Complete the steps below:

1. Before you enable the backup service for Azure AD B2C, go to IBM® Storage Protect for Cloud to configure a service app profile for that Microsoft 365 tenant. For detailed instructions on creating a service app profile, refer to Create a Service App and Grant the Consent.

   > **Note:** The user creating the service app profile and granting consent must be a member of your tenant's domain, instead of an external user.

2. After the service app is ready, go to the **Backup** page of the IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID to configure the backup scope for the Azure AD B2C. Note that if you have multiple tenants to protect, you must create a service app for each of them.
   For details on configuring the backup scope, refer to Create a New Backup Scope for Azure AD B2C.

For details on the support list, refer to Azure AD B2C.

Create a Service App and Grant Consent

The use Azure AD B2C backup and restore services, create a service app to connect to your tenant and grant the requested permissions for this app.

> **Note:** The user creating the service app profile and granting consent must be a member of your tenant's domain, instead of an external user.

Follow the steps below to create the service app:

1. On the **Management > App management** page, click **Create** on the action bar.
2. In the **Select services** step, select **IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID**.
3. In the **Choose setup method** step, select **Modern mode** and click **Next**.
4. In the **Consent to apps** step, click **Consent** next to the **IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID AD B2C**.
5. On the Microsoft 365 sign-in page, sign in with a Microsoft 365 Global Administrator account.

6. On the **Permissions required** page, review the permissions required and click **Accept** to continue. For the API permissions that this app requests, refer to Default Permissions Granted to the Service App.
7. The app profile you created will be displayed on the **App management** page, and the **IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID AD B2C** app will be added to your Microsoft Entra admin center > enterprise applications.

Default Permissions Granted to the Service App

If you want to protect Azure AD B2C data, you can choose to create a **IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra IDAD B2C**service app profile or create a custom Azure app profile with **delegated permissions** through IBM® Storage Protect for Cloud > **Management > App management** page.

The following API permissions will be automatically added to the service app with consent from your **Global administrator** account. You can also choose the specific permissions to grant your custom Azure app for the services or data types that you want to protect upon the usage purpose.
Summary for complex table

API	Permissions	Type	Why You Need	Permission Category	Alternative Permission for backup only
Microsoft Graph	**AppRoleAssignment.ReadWrite.All** (Manage app permission grants and app role assignments)	Application	Allows the app to manage permission grants for application permissions to any API (including Microsoft Graph) and application assignments for any app, without a signed-in user.	Azure AD B2C > backup and restore user > app role assignment	**Directory.Read.All**
	Application.ReadWrite.All (Read and write all applications)	Application	Allows the app to create, read, update and delete applications and service principals without a signed-in user. Does not allow management of consent grants	Azure AD B2C > backup and restore app registration	**Application.Read.All**
	AuditLog.Read.All (Read all audit log data)	Application	Allows the app to read and query your audit log activities, without a signed-in user.	Azure AD B2C > backup and restore userflow and userattribute Azure AD B2C > backup and restore identity provider Azure AD B2C > backup and restore app registration	

API	Permissions	Type	Why You Need	Permission Category	Alternative Permission for backup only
	Directory.Read.All (Read directory data)	Application	Allows the app to read data in your organization's directory, such as users, groups and apps, without a signed-in user.	Azure AD B2C > create plan Azure AD B2C > backup and restore userflow and userattribute Azure AD B2C > backup and restore identity provider Azure AD B2C > backup and restore app registration	
	GroupMember.ReadWrite.All (Read and write all group memberships)	Application	Allows the app to list groups, read basic properties, read and update the membership of the groups this app has access to without a signed-in user. Group properties and owners cannot be updated and groups cannot be deleted.	Azure AD B2C > backup and restore user > member of group	**User.Read.All**
	IdentityProvider.ReadWrite.All (Read and write identity providers)	Application	Allows the app to read and write your organization's identity (authentication) providers' properties without a signed in user.	Azure AD B2C > backup and restore identity provider	**IdentityProvider.Read.All**
	IdentityUserFlow.ReadWrite.All (Read and write all identity user flows)	Application	Allows the app to read or write your organization's user flows, without a signed-in user.	Azure AD B2C > backup and restore userflow and userattribute	**IdentityUserFlow.Read.All**

API	Permissions	Type	Why You Need	Permission Category	Alternative Permission for backup only
	RoleManagement.ReadWrite.Directory (Read and write all directory RBAC settings)	Application	Allows the app to read and manage the role-based access control (RBAC) settings for your company's directory, without a signed-in user. This includes instantiating directory roles and managing directory role membership, and reading directory role templates, directory roles and memberships.	Azure AD B2C > backup and restore user > unified role assignment	**RoleManagement.Read.Directory**
	UserAuthenticationMethod.ReadWrite.All (Read and write all users' authentication methods)	Application	Allows the application to read and write authentication methods of all users in your organization, without a signed-in user. Authentication methods include things like a user's phone numbers and Authenticator app settings. This does not allow the app to see secret information like passwords, or to sign-in or otherwise use the authentication methods.	Azure AD B2C > backup and restore user > authentication user	**User.Read.All**
	User.EnableDisableAccount.All (Enable and disable user accounts)	Application	Allows the app to enable and disable users' accounts, without a signed-in user.	Azure AD B2C > backup and restore user > accountEnabled	**User.Read.All**

API	Permissions	Type	Why You Need	Permission Category	Alternative Permission for backup only
	User.ManageIdentities.All (Manage all users' identities)	Application	Allows the app to read, update and delete identities that are associated with a user's account, without a signed in user. This controls the identities users can sign-in with.	Azure AD B2C > backup and restore user > identities	**User.Read.All**
	User.ReadWrite.All (Read and write all users' full profiles)	Application	Allows the app to read and update user profiles without a signed in user.	Azure AD B2C > backup and restore user	**User.Read.All**
	User-Mail.ReadWrite.All (Read and write all secondary mail addresses for users)	Application	Allows the app to read and write secondary mail addresses for all users, without a signed-in user.	Azure AD B2C > backup and restore user > otherMails	**User.Read.All**
	User-Phone.ReadWrite.All (Read and write all user mobile phone and business phones)	Application	Allows the app to read and write the mobile phone and business phones for all users, without a signed-in user.	Azure AD B2C > backup and restore user > businessPhones/mobilePhone	**User.Read.All**

Monitor Your Backup

You can monitor backup job details and generate a backup job report.

Procedure

To view backup job details and generate a backup job report, complete the following steps:

1. On the **Backup** page, click the More actions (•••) button on a service tile and click **View job history** from the list.
2. In the **View job details** page, you will find the **Backup details** tab and the **Restore details** tab. In the **Backup details** tab, the backup jobs are listed in descending.
3. Click a backup job to view its summary on the right panel including the job ID, job start time and finish time, the backup data size, the total number of objects that are backed up in this job, and the number of successful, skipped, and failed objects. You can also click the More actions (•••) button to generate and download job report.

> **Note:** The failed objects in the backup job will be included in the subsequent backup jobs until they are successfully backed up.

Configure Notifications

With IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID, you can define define certain statuses of jobs that will trigger alerts, including backup, restore, export, retention, index generation, and unprotected warning.

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

1. Navigate to **Settings** > **Notification**.
2. Click the **+Create** button. The **Create a new notification profile** panel appears.
3. In the **Create a new notification profile** panel, complete the following settings:
   - Profile information – Enter a name and description for the profile you are creating. The description is optional.
   - Send email notifications to the following email addresses – Enter the email addresses in the text box to configure the recipients for the email notifications. You can enter the email addresses of users or groups. For groups, you must ensure the group you entered can receive emails. Otherwise, the group members will not be notified of the activities in IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID.
   - Notification condition – Configure whether to apply the notification profile to specific backup scopes. You can turn on the switch for **Apply the notification profile to specific backup scopes** and then select backup scopes from the drop-down list to configure the backup scopes to which the notification profile will be applied.
   - Send email notifications for the jobs in the following statuses – Select the job status for the Backup, Restore, Export, Retention, and Generate index jobs which will trigger the notification. Note that you can configure whether to attach the Azure virtual machine backup job report in email notifications through **Advanced settings** in the **Backup** section.
   - Unprotected virtual machines notification – Configure whether to send email notifications for the unprotected virtual machines. You can turn on the switch for **Send warning notification for unprotected virtual machines** and then configure the frequency of sending this notification. In the **Frequency** section, enter a number in the text box and then select **Days** or **Weeks** from the drop-down list to configure an interval of sending this notification.
4. Click **Save** when you finish configuring the profile.

Job Notification

Procedure

To configure job notification settings, follow the steps below:

1. Navigate to **Settings** > **Notification settings**.
2. Click **Job notification**.
3. To enable the job notification, turn on the switch and configure the following notification settings:
   a. **Send email notifications to the following email addresses** – Enter the email addresses in the text box to configure the recipients for the email notifications. You can enter the email addresses of users or groups. For groups, you must ensure the group you entered can receive emails. Otherwise, the group members will not be notified of the activities in IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID.

   b. **Send the email notifications for the jobs in the following status** – Select the job status (**Finished**, **Finished with exception**, or **Failed**), which will trigger the notification. When the job completes with the selected status, the email notification will be sent to the email addresses that you configured in the last step.
4. If you have a separate team to manage the export and restore jobs, you can select the **Customize the notification for the restore and export jobs** option and then configure the recipients who will receive the email notification, particularly for the restore and export jobs of specific statuses.

5. Click **Save** when finished configuring the settings. The notification settings will take effect immediately.

Unprotected Warning

Procedure

To configure unprotected warning settings, follow the steps below:

1. Navigate to **Settings** > **Notification settings**.
2. Click **Unprotected warning**.
3. Turn on the switch for **Send warning notification for unprotected virtual machines** and configure the following notification settings:
    a. **Send email notifications to the following email addresses** – Enter the email addresses in the text box to configure the recipients for the email notifications. You can enter the email addresses of users or groups. For groups, you must ensure the group you entered can receive emails. Otherwise, the group members will not be notified of the activities in IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID.

    b. In the **Frequency** section, enter a number in the text box and then select **Days** or **Weeks** from the drop-down list to configure an interval of sending this notification.
4. Click **Save**.

Manage the Backup Scopes for Virtual Machines

You can configure backup scopes for Azure VMs instances under the **Virtual Machines** service tile.

> **Note:** Backup for Azure VMs may incur additional costs on data transfer, snapshots, operations, or API calls, etc. For more details, refer to FAQs.

The backup scopes can be used as virtual tenants. The Azure VMs instances in the same backup scope are protected in the same backup frequency and applied with the same data retention policy.

You can create multiple backup scopes and also update each of the backup scopes to change their protected VMs, backup schedule, and data retention settings.

- To create a new backup scope, refer to:
  - Create a New Backup Scope for Azure VM
- For the existing backup scopes, you can perform the following actions:
  - Edit – To edit a backup scope, you can select a backup scope and click **Edit** button on the command bar, or you can click the **Edit** button when you are viewing the backup scope details.
    If an Azure VM instance has been added to a backup scope, it cannot be added to another

    When you are editing a backup scope and the VMs that are newly selected to protect are from the region that has a storage location configured in this backup scope, the storage location will be automatically populated and cannot be changed. If you select VMs from a new region to protect, you must configure a storage profile for this new region by selecting an existing storage profile or creating a new one. We strongly recommend using a storage account from the same region for the best traffic. For details on configuring storage, refer to Manage Your Storage.
  - Delete – To delete a backup scope, you can select a backup scope and click the **Delete** button on the command bar, or you can click the **Delete** option from the More actions (•••) list when you are viewing the details of a backup scope. You can also select multiple backup scopes to delete. When deleting backup scopes, you can select how to handle your backup data: keep the data and follow the configured retention policy, keep the data for 30 days before deletion, or delete the backup data immediately.
  - Run backup now – If you want to start a backup immediately, you can select a backup scope and click **Run backup now**, or you can click the **Run backup now** from the More actions (•••) list when you are viewing the details of a backup scope.

Create a New Backup Scope for Azure VM

The Azure VM service supports the following for backup scope configuration

- SaaS infrastructure mode – Provides centralized management, automation, and robust data protection to empower organizations with scalable, policy-driven backup solutions. For details, refer to Use the SaaS Infrastructure Mode.

Use the SaaS Infrastructure Mode

Procedure

To create a new backup scope, follow the steps below:

1. Go to the **Backup** page.
2. Click on the **Virtual Machine** service tile or click the More actions (•••) button on the upper-right corner of the **Virtual Machine** service tile and click **Configure backup scope** from the drop-down list.

3. In the **Configure backup scope for virtual machines** page, all the existing backup scopes for Azure virtual machines instance are listed in the table. You can use the search box to search for the backup scopes by name and manage the columns to adjust the view of the backup scopes.

   > **Note:** You can click the Refresh (⟳) button in the upper-right corner of this page to retrieve the latest data list for Azure VMs instances. The **Last refreshed time** is displayed next to the Refresh (⟳) button. Additionally, the data list will be automatically refreshed daily at 00:00 local time.

4. Click the **Create** button and select **Azure virtual machines**.
5. In the **Choose a method** page, you can choose to manually select the VMs that you want to add to the backup scope, or you can configure a dynamic scope to use attribute-based rules to include the VMs that meet your conditions to the backup.
   - **Manually Select** – In the **Select virtual machines** step, select the VMs that you want to add to the backup scope that you are creating. You can click the link in the **Selected disks/total disks** column next to the virtual machine name to select disks under the selected virtual machine to protect.

     > **Note:** The OS disk is mandatory and cannot be deselected.

     You can use the Search box (🔍) to search for the VMs via the keywords in the name or use the **Filters** to find the VMs with specific properties.

     The VMs are grouped by tenants. Selecting the checkbox in the column header will select all the VMs and disks on the current page. You can turn to the next page and select more VMs. Your selection will be kept, and the number of your selection will be displayed next to the tenant’s name.
   - **Dynamic rules** – In the **Select virtual machines** step, define the rule conditions for the VMs that you want to include in this backup scope. You can add multiple rules to filter the **Tag name**, **Tag value**, **Virtual machine name**, **Region**, **Resource group**, or **Subscription name of the VMs**. Click **Apply** when you complete the rule configuration, and then the VMs that meet your rules will be displayed in the table and included for backup. The dynamic scope will automatically add or remove the VMs according to your rules. The new VMs that meet the configured rule conditions will also be automatically added to the backup scope.
6. Click **Next**, and you will go to the **Configure storage based on region** step to configure a storage profile for each region. You can select a storage type and then select storage profiles. You can use an existing storage profile or create a new storage profile to store the backup data for the VMs in the same region. For details on configuring storage location, refer to Manage Your Storage.

   > **Note:** If you have enabled a firewall for your Azure storage, you need to add the IBM® Storage Protect for Cloud IP addresses to your Azure storage account firewall or configure the firewall to allow IBM® Storage Protect for Cloud agent servers running on a dedicated ARM Vnet subnet to access your storage location. For details, refer to “Allow IBM Storage Protect for Cloud Agent Servers to Access Your Storage Account” on page 82.

7. After you finish the storage configuration for each region, click **Next** to configure the scope information, schedule, and data retention settings. Refer to the following:
   - **Scope information** – Enter a name and description for the scope you are creating. The description is optional.
   - **Snapshots and index** – Configure which resource group to keep the snapshots and whether to generate index during backup.
     - **Which resource group do you want to keep the snapshots?** – If the VMs to protect in this backup scope are in the same subscription, you can choose to store the snapshots in another resource group.

    - **Generate index for file-level data export** – Select this option if you want to perform file-level data export using the backup data. Otherwise, keep this option deselected. The backup job will take longer to finish to generate an index. The retention period to keep the index will follow the retention policy configured for the backup data. Note that generating index for the disks with over 8 TB size is also supported.

    > **Note:** Running index generation on the following file systems will result in folders without indexes in restore recovery points.: **UFS – BSD default fs**, **ZFS – BSD alternative fs**, **BitLocker – Windows encrypted fs**, **LUKS – Linux encrypted fs**, **ReFS – Windows new fs**. Therefore, the file-level data exportation is unsupported for disks with the file systems.

- **Schedule** – Select **hours**, **days**, **weeks**, or **months** from the **Interval** drop-down list as the unit of time for the backup interval, enter a number in the text box after **Every**, and then configure the start time for your first backup job. By default, the VM backup job will run once a day. Backing up VMs at the same time may cause traffic jams. You are recommended to configure different backup schedules for the backup scopes and make sure the times do not overlap.
- **Notification** – Check the notification profiles which will be applied to the backup scope.
- **Retention policy** – Configure when to prune the snapshots from Azure and the backup data from the storage location. Note that if you are using IBM storage, the retention policy for backup data is subject to your agreement and you can configure a retention period up to the retention policy in your subscription.
    - For snapshots in Azure – You can choose the number of the latest snapshots to retain or choose for how long the snapshots will be retained after generation.

    > **Note:** The number of the latest snapshots to retain must be less than 500.

    - For backup data in storage – Configure the retention period to keep the backup data in the storage.

    > **Note:** For existing backup scopes with the legacy retention policy, you can click **Switch to modern retention policy** to configure the new retention period.
    >
    > - **Daily/Hourly recovery point** – Enter a number in the text box and select **days** or **weeks** from the drop-down list. The retention period must be between 7 and 28 days.
    > - **Weekly recovery point** – Enter a number in the text box and select **weeks** or **months** from the drop-down list. The retention period must be between 2 and 12 weeks.
    > - **Monthly recovery point** – Enter a number in the text box. The retention period must be between 1 and 12 months.
    > - **Yearly recovery point** – If you are using **IBM default storage** with unlimited retention period, the **Unlimited** option is selected automatically. If you want to use a custom retention period, select **Custom**.

8. Click **Next** to review your settings.

9. Click **Save** to save this backup scope. The backup for the VMs in this backup scope will roll out as scheduled. You can also click **Save** and run to save the backup scope and start the backup job immediately. For more details about monitoring the backups, refer to Monitor Your Backup.

Manage the Backup Scopes for Microsoft Entra ID

You can only define a single backup scope for a Microsoft Entra ID. Once you have created a scope, you cannot add this directory to another one. The backup service for Microsoft Entra ID will perform one backup job a day. Backup job frequency is currently not editable.

- To create a new backup scope for Microsoft Entra ID, refer to Create a New Backup Scope for Microsoft Entra ID.
- For the existing backup scopes, you can perform the following actions:
    - Edit – To edit a backup scope, you can select a backup scope and click **Edit** button on the command bar, or you can click the **Edit** button when you are viewing the backup scope details. For details on the backup scope settings, refer to Create a New Backup Scope for Microsoft Entra ID.
    - Delete – To delete a backup scope, you can select a backup scope and click **Delete** button on the command bar, or you can click the **Delete** option from the More actions (•••) list when you are viewing the details of a backup scope. You can also select multiple backup scopes to delete. When deleting backup scopes, you can select how to handle your backup data: keep the data and follow the configured retention policy, keep the data for 30 days before deletion, or delete the backup data immediately.
    - Run backup now – If you want to start a backup immediately, you can select a backup scope and click **Run backup now**, or you can click the **Run backup now** from the More actions (•••) list when you are viewing the details of a backup scope.

Create a New Backup Scope for Microsoft Entra ID

Procedure

To create a new backup scope, follow the steps below:

1. Go to the **Backup** page on the new UI.
2. Click on the **Microsoft Entra ID** service tile or click the More actions (•••) button on the upper-right corner of the **Microsoft Entra ID**service tile and click **Configure backup scope** from the drop-down list.
3. In the **Configure backup scope for Microsoft Entra ID** page, all the existing backup scopes for Microsoft Entra ID are listed in the table. You can use the search box to search for the backup scopes by name and manage the columns to adjust the view of the backup scopes.
4. Click the **Create** button. The Create a new backup scope panel appears.
5. In the **Define scope** step, select the service app profile from the drop-down list for the Microsoft Entra tenant that you want to protect in this backup scope. For details on configuring the app profile, refer to Create a Service App and Grant the Consent.
6. Select the directory objects and logs that you want to include into this backup scope. You can select specific users or groups to protect.
    - If you select all data to protect, click **Next** to configure the backup setting in **Setting** step.
    - If you select specific users or groups to protect in the **Define scope** step, click **Next** and you will go to the **Define conditions** step to configure the rule conditions for the groups or users that you want to include in this backup scope. In the **Define conditions** step, you can add multiple rules to filter the **Display name**, **Group email address**, or **Group type** of the groups. You can also add multiple rules to filter the **Department**, **Display name**, **User principal name**, or **User type** of the users. When finished, click **Next**.
7. In the **Settings** step, complete the following settings:
    - **Scope information** – Enter a name and description for the scope you are creating. The description is optional.

- **Storage profile** – You can select a storage profile from the drop-down list to use or click the **+Create storage profile** link from the list to create a new storage profile for this backup scope. For details on configuring storage profiles, refer to Manage Your Storage.
- **Schedule** – The backup job will run once a day. Configure the start time for your first backup job.
- **Notification** – Check the notification profiles which will be applied to the backup scope.
- **Retention policy** – Configure when to prune the backup data from the storage location. Note that if you are using IBM storage, the retention policy for backup data is subject to your agreement and you can configure a custom retention period up to the retention policy in your subscription. If you are using **IBM default storage** with **unlimited** retention period, the **Unlimited** option is selected automatically in the list. If you want to use a custom retention period, select **Custom** from the list, enter a number in the text box and select **weeks**, **months**, or **years** from the drop-down list. The retention period cannot be less than 2 weeks. Note that if you have a retention policy with a fixed year in your subscription, the maximum retention period that you can configure will be displayed under this field.

  > **Note:** When you configure the retention period for backup data using the Year unit, the **Configure Full Backup Frequency** section will appear. You can then select a number from the drop-down list to set the full backup frequency. If the retention period is set to more than three months using the Month or Week unit, the full backup frequency will automatically be set to three months and cannot be changed. For retention periods of less than three months, the full backup frequency will be adjusted accordingly and cannot be modified.

8. Click **Next** to review your settings.
9. Click **Save**.
10. In the **Check permissions** panel, the required app profile, service account, Exchange Administrator role, and premium license will be checked based on the selected object types.
    If all required permissions are valid, click **Continue** to save this backup scope.

    If any permissions fail, you can follow the provided instructions to update them, then return here to click **Check again** to re-verify the updated permissions. You can also select the **Ignore this error in any jobs** checkbox for the failed permission and then click **Skip and continue** to ignore the failed permissions and save this backup scope.

    > **Note:** Before clicking **Skip and continue** to ignore failed permissions, if you select the **Ignore this error in any jobs** checkbox, the related objects in the backup scope will be skipped when running backup jobs for the scope. If you don’t select the checkbox and instead click **Skip and continue** to save the backup scope and run backup jobs, the related objects in the backup scope will fail to be backed up.

11. After saving this backup scope, the The backup for the Microsoft Entra tenant in this backup scope will roll out as scheduled. For more details about monitoring the backups, refer to Monitor Your Backup.

Manage the Backup Scopes for Azure Storage

The backup scopes can be used as virtual tenants. To protect Azure Blob Storage and Azure File Share, you must define the backup scopes separately for the two storage types, and the storage in the same backup scope are from the same tenant.

> **Note:** Backup for Azure Storage may incur additional costs on data transfer, snapshots, operations, or API calls, etc. For more details, refer to FAQs.

The storages in the same backup scope will be protected in the same backup frequency and applied with the same data retention policy.

Note that each storage can only be included in one backup scope. Additionally, if the Azure storage account that you want to protect has enabled a firewall, ensure you have read and completed the settings in“Allow IBM Storage Protect for Cloud Agent Servers to Access Your Storage Account” on page 82 .

- To create a new backup scope for Azure Storage, refer to Create a New Backup Scope for Azure Storage
- For the existing backup scopes, you can perform the following actions:
    - Edit – To edit a backup scope, you can select a backup scope and click **Edit** button on the command bar, or you can click the **Edit** button when you are viewing the backup scope details. For details on the backup scope settings, refer to Create a New Backup Scope for Azure Storage.
    - Delete – To delete a backup scope, you can select a backup scope and click **Delete** button on the command bar, or you can click the **Delete** option from the More actions (•••) list when you are viewing the details of a backup scope. You can also select multiple backup scopes to delete. When deleting backup scopes, you can select how to handle your backup data: keep the data and follow the configured retention policy, keep the data for 30 days before deletion, or delete the backup data immediately.
    - Run backup now – If you want to start a backup immediately, you can select a backup scope and click **Run backup now**, or you can click the **Run backup now** from the More actions (•••) list when you are viewing the details of a backup scope.

Create a New Backup Scope for Azure Storage

The Azure Storage service supports the following for backup scope configuration:

- SaaS infrastructure mode – Provides centralized management, automation, and robust data protection to empower organizations with scalable, policy-driven backup solutions. For details, refer to Use the SaaS Infrastructure Mode.

Use the SaaS Infrastructure Mode

Procedure

To create a new backup scope, follow the steps below:

1. Go to the **Backup** page.
2. Click on the **Azure Storage** service tile or click the More actions (•••) button on the upper-right corner of the **Azure Storage** service tile and click **Configure backup scope** from the drop-down list.
3. In the **Configure backup scope for Azure Storage** page, all the existing backup scopes for Azure Storage are listed in the table. You can use the search box to search for the backup scopes by name and manage the columns to adjust the view of the backup scopes.

> **Note:** You can click the Refresh (🔄) button in the upper-right corner of this page to retrieve the latest data list for Azure Storage. The **Last refreshed time** is displayed next to the Refresh (🔄) button. Additionally, the data list will be automatically refreshed daily at 00:00 local time.

4. Click the **Create** button and select **Blob Storage** or **File Share** from the drop-down list.
5. In the **Choose a mode for blob storage**/**Choose a mode for file shares** page, select **SaaS infrastructure mode**.
6. Then, choose a method. You can choose to manually select the blob containers/files shares that you want to add to the backup scope, or you can configure a dynamic scope to use attribute-based rules to include the blob containers/files shares that meet your conditions to the backup.
   - **Manually Select** - In the **Select blob containers**/**Select file shares** step, select the tenant and the storages (blob containers or file shares) that you want to add to the backup scope. You can use filters to find the storage you want to protect.
     The number of your selection will be displayed on the storage account row.
   - **Dynamic rules** – In the **Select blob containers**/**Select file shares** step, define the rule conditions for the blob containers/file shares that you want to include in this backup scope. You can add multiple rules to filter the Subscription name, Resource group, Name, Storage account, or Region of the blob containers/file shares. Click Apply when you complete the rule configuration, and then the blob containers/file shares that meet your rules will be displayed in the table and included for backup. The dynamic scope will automatically add or remove the blob containers/file shares according to your rules. The new blob containers/file shares that meet the configured rule conditions will also be automatically added to the backup scope.
7. Click **Next**, and you will go to the **Configure storage based on region** step to configure a storage profile for each region. You can select a storage type and then select storage profiles. You can use an existing storage profile or create a new storage profile to store the backup data for the storages in the same region. For details on configuring storage location, refer to Manage Your Storage.

> **Note:** If you have enabled a firewall for your Azure storage, you need to add the IBM® Storage Protect for Cloud IP addresses to your Azure storage account firewall or configure the firewall to allow IBM® Storage Protect for Cloud agent servers running on a dedicated ARM Vnet subnet to access your storage location. For details, refer to “Allow IBM Storage Protect for Cloud Agent Servers to Access Your Storage Account” on page 82.

8. After you finish the storage configuration for each region, click **Next** to configure the scope information, schedule, and data retention settings. Refer to the following:
   - Scope information – Enter a name and description for the scope you are creating. The description is optional.
   - Schedule – Select **days**, **weeks**, **months**, or **years** as the unit of time for the backup interval, enter a number in the text box after **Every**, and then configure the start time for your first backup job.
   - Notification – Check the notification profiles which will be applied to the backup scope.
   - Retention policy – Configure when to prune the backup data from the storage location. Note that if you are using IBM® Storage Protect for Cloud storage, the retention policy for backup data is subject to your agreement and you can configure a custom retention period up to the retention policy in your subscription. If you are using **IBM default storage** with **unlimited** retention period, the **Unlimited** option is selected automatically in the list. If you want to use a custom retention period, select **Custom** from the list, enter a number in the text box and select **weeks**, **months**, or **years** from the drop-down list. The retention period cannot be less than 2 weeks. Note that if you have a retention policy with a fixed year in your subscription, the maximum retention period that you can configure will be displayed under this field.

> **Note:** When you configure the retention period for backup data using the Year unit, the **Configure Full Backup Frequency** section will appear. You can then select a number from the drop-down list to set the full backup frequency. The default full backup frequency is 3 months. If the retention period for the backup data is less than 3 months, the full backup frequency will match the retention period.

9. Click **Next** to review your settings.
10. Click **Save** to save this backup scope. The backup for the storages in this backup scope will roll out as scheduled. For more details about monitoring the backups, refer to Monitor Your Backup.

Manage the Backup Scopes for Admin Portal Settings

The Admin Portal Settings service is generally available after August 2023 release. You can use the Admin Portal Settings service to protect the Azure portal settings, Microsoft 365 Defender admin settings, Exchange admin portal settings, and the Intune settings. For additional details, refer to Admin Portal Settings.

- To create a new backup scope for Admin Portal Settings, refer to Create a New Backup Scope for Admin Portal Settings.
- For the existing backup scopes, you can perform the following actions:
  - Edit – To edit a backup scope, you can select a backup scope and click **Edit** button on the command bar, or you can click the **Edit** button when you are viewing the backup scope details. For details on the backup scope settings, refer to Create a New Backup Scope for Admin Portal Settings.
  - Delete – To delete a backup scope, you can select a backup scope and click **Delete** button on the command bar, or you can click the **Delete** option from the More actions (•••) list when you are viewing the details of a backup scope. You can also select multiple backup scopes to delete. When deleting backup scopes, you can select how to handle your backup data: keep the data and follow the configured retention policy, keep the data for 30 days before deletion, or delete the backup data immediately.
  - Run backup now – If you want to start a backup immediately, you can select a backup scope and click **Run backup now**, or you can click the **Run backup now** from the More actions (•••) list when you are viewing the details of a backup scope.

Create a New Backup Scope for Admin Portal Settings

Procedure

To create a new backup scope, follow the steps below:

1. Go to the **Backup** page on the new UI.
2. Click on the **Admin Portal Settings** service tile or click the More actions (•••) button on the upper-right corner of the **Admin Portal Settings** service tile and click **Configure backup scope** from the drop-down list.
3. In the **Configure backup scope forAdmin Portal Settings** page, all the existing backup scopes for Admin Portal Settings are listed in the table. You can use the search box to search for the backup scopes by name and manage the columns to adjust the view of the backup scopes.

> **Note:** You can click the Refresh (↻) button in the upper-right corner of this page to retrieve the latest data list for Admin Portal Settings. The **Last refreshed time** is displayed next to the Refresh (↻) button. Additionally, the data list will be automatically refreshed daily at 00:00 local time.

4. Click the **Create** button. The **Create a new backup scope** panel appears.
5. In the **Define scope** step, select the service app profile from the drop-down list for the tenant that you want to protect in this backup scope. For details on configuring the app profile, refer to Create a Service App and Grant the Consent.
6. Select the components that you want to include into this backup scope for **Microsoft Entra ID**, **Microsoft 365 Defender**, **Exchange**, and **Intune**.
7. Click **Next**.
8. In the **Settings** step, complete the following settings:

- **Scope information** – Enter a name and description for the scope you are creating. The description is optional.
- **Storage profile** – You can select a storage profile from the drop-down list to use or click the **+Create storage profile** link next to the list to create a new storage profile for this backup scope. For details on configuring storage profiles, refer to Manage Your Storage.
- **Schedule** – The backup job will run once a day. Configure the start time for your first backup job.
- **Notification** – Check the notification profiles which will be applied to the backup scope.
- **Retention policy** – Configure when to prune the backup data from the storage location. Note that if you are using IBM® Storage Protect for Cloud storage, the retention policy for backup data is subject to your agreement. You can configure a custom retention period up to the retention policy in your subscription. If you are using **IBM default storage** with **unlimited** retention period, the **Unlimited** option is selected automatically in the list. If you want to use a custom retention period, select **Custom** from the list, enter a number in the text box and select **weeks**, **months**, or **years** from the drop-down list. The retention period cannot be less than 2 weeks. Note that if you have a retention policy with a fixed year in your subscription, the maximum retention period that you can configure will be displayed under this field.

> **Note:** When you configure the retention period for backup data using the Year unit, the **Configure Full Backup Frequency** section will appear. You can then select a number from the drop-down list to set the full backup frequency. If the retention period is set to more than three months using the Month or Week unit, the full backup frequency will automatically be set to three months and cannot be changed. For retention periods of less than three months, the full backup frequency will be adjusted accordingly and cannot be modified.

9. Click **Next** to review your settings.
10. Click **Save**.
11. In the **Check permissions** panel, the required app profile, service account, Exchange Administrator role, and Microsoft Intune license will be checked based on the selected object types.
    If all required permissions are valid, click **Continue** to save this backup scope.

    If any permissions fail, you can follow the provided instructions to update them, then return here to click **Check again** to re-verify the updated permissions. You can also click **Skip and continue** to ignore the failed permissions and save this backup scope.

    > **Note:** Before clicking **Skip and continue** to ignore failed permissions, if you select the **Ignore this error in any jobs** checkbox, the related objects in the backup scope will be skipped when running backup jobs for the scope. If you don’t select the checkbox and instead click **Skip and continue** to save the backup scope and run backup jobs, the related objects in the backup scope will fail to be backed up.

12. After saving this backup scope. The backup for the Admin Portal Settings in this backup scope will roll out as scheduled. For more details about monitoring the backups, refer to Monitor Your Backup.

Manage the Backup Scopes for Azure SQL

The Azure SQL service has been generally available since the March 2025 release. With Azure SQL service enabled, you can:

- **Monitoring jobs**: Perform monitoring jobs to retrieve the native Azure backups for databases and update the backup schedule and data retention settings to Azure. Both the point-in-time restore and long-term retention recovery points can be synced to Azure SQL service.
- **Direct backup jobs**: You can also perform direct backup jobs with Azure SQL backup service to protect Azure SQL databases.

The Azure SQL service trial only allows one backup scope to protect up to 5 databases.

- To create a new monitoring backup scope for Azure SQL, refer to Create a New Backup Scope for Native Azure SQL Backup Monitoring.
- To create a new backup scope for Azure SQL, refer to Create a New Backup Scope for Azure SQL.
- For the existing backup scopes, you can perform the following actions:
    - Edit – To edit a backup scope, you can select a backup scope and click **Edit** button on the command bar, or you can click the **Edit** button when you are viewing the backup scope details. For details on the backup scope settings, refer to Create a New Backup Scope for Native Azure SQL Backup Monitoring or Create a New Backup Scope for Azure SQL.
    - Delete – To delete a backup scope, you can select a backup scope and click **Delete** button on the command bar, or you can click the **Delete** option from the More actions (•••) list when you are viewing the details of a backup scope. You can also select multiple backup scopes to delete. When deleting backup scopes, you can select how to handle your backup data: keep the data and follow the configured retention policy, keep the data for 30 days before deletion, or delete the backup data immediately.
    - Run backup now – If you want to start a backup immediately, you can select a backup scope and click **Run backup now**, or you can click the **Run backup now** from the More actions (•••) list when you are viewing the details of a backup scope.

Create a New Backup Scope for Native Azure SQL Backup Monitoring

About this task

To create a new backup scope for Azure SQL, follow the steps below:

Procedure

1. Go to the **Backup** page.
2. Click on the **Azure SQL** service tile or click the More actions (•••) button on the upper-right corner of the **Azure SQL** service tile and click **Configure backup scope** from the drop-down list.
3. In the **Configure backup scope for Azure SQL** page, all the existing backup scopes for Azure SQL are listed in the table. You can use the search box to search for the backup scopes by name and manage the columns to adjust the view of the backup scopes.

    > **Note:** You can click the Refresh (↻) button in the upper-right corner of this page to retrieve the latest data list for Azure SQL databases. The **Last refreshed time** is displayed next to the Refresh (↻) button. Additionally, the data list will be automatically refreshed daily at 00:00 local time.

4. Click the **Create** button and select **Native Azure SQL backup monitoring**. The **Create backup scope** panel appears.

5. In the **Select databases** step, select the tenant and the databases that you want to add to the backup scope. You can use **Filters** to find the databases you want to protect or use the **Search** box to search for the databases via the keywords in the name. The number of your selection will be displayed on the row of the tenant name.

6. Click **Next**, and you will go to the **Configure storage based on region** step to configure a storage profile for each region. You can select a storage type and then select storage profiles. You can use an existing storage profile or create a new storage profile to store the backup data for the databases in the same region. For details on configuring storage location, refer to Manage Your Storage.

   > **Note:** If you have enabled a firewall for your Azure SQL databases, you need to add the IBM IP addresses to your Azure SQL databases account firewall or configure the firewall to allow IBM agent servers running on a dedicated ARM Vnet subnet to access your storage location. For details, refer to Allow IBM Storage Protect for Cloud Agent Servers to Access Your Storage Account.

7. After you finish the storage configuration for each region, click **Next** to configure the scope information, schedule, and data retention settings. Refer to the following:

   - **Scope information** – Enter a name and description for the scope you are creating. The description is optional.
   - **Schedule** – Click **hours**, **days**, **weeks**, **or months** as the unit of time for the monitoring job interval, enter a number in the text box after **Run a monitoring job every**, and then configure the start time for your first monitoring job. The monitoring jobs will retrieve the information of the native Azure backups (both PITR and LTR) and provide them as recovery points that you can use to perform restore.
   - **Notification** – Check the notification profiles which will be applied to the backup scope.
   - **Retention policy** – You can change the backup frequency for the differential backups and update the retention policy for the native Azure backups (PITR and LTR).
     - **Change differential backup frequency** – You can change the differential backup frequency for the selected databases in this backup scope. You can select **12** or **24** from the drop-down list to perform the differential backups in Azure every 12 or 24 hours.
     - **How many days would you like to keep the point-in-time restore (PITR) backups?** – You can keep the PITR backups up to 35 days. Enter a number for the PITR backups that you want to keep for the databases in this backup.
     - **How long do you want to keep the long-term retention (LTR) backups?** – Configure the data retention policy for the LTR backups, including weekly LTR backups, monthly LTR backups, and yearly LTR backups. In the corresponding section, select days, weeks, months, and years from the drop-down list and enter a number in the text box. The LTR backups can be kept for up to 10 years.
       - **Weekly LTR Backups** – Configure for how long you want to keep the weekly backups in Azure.
       - **Monthly LTR Backups** – The first backup of each month will be kept as the monthly LTR backups. You can configure for how long you want to keep the monthly backups in Azure.
       - **Yearly LTR Backups** – You can select a weekly backup as the backup of the year and configure for how long you want to keep this yearly backup.

8. Click **Next** to review your settings.

9. Click **Save** to save this backup scope. The backup for the databases in this backup scope will roll out as scheduled. For more details about monitoring the backups, refer to Monitor Your Backup.

Create a New Backup Scope for Azure SQL Backup

Procedure

To create a new backup scope for Azure SQL, follow the steps below:

1. Go to the **Backup** page on the new UI.

2. Click on the **Azure SQL** service tile or click the More actions (•••) button on the upper-right corner of the **Azure SQL** service tile and click **Configure backup scope** from the drop-down list.

3. In the **Configure backup scope for Azure SQL** page, all the existing backup scopes for Azure SQL are listed in the table. You can use the search box to search for the backup scopes by name and manage the columns to adjust the view of the backup scopes.

   > **Note:** You can click the Refresh (↻) button in the upper-right corner of this page to retrieve the latest data list for Azure SQL databases. The **Last refreshed time** is displayed next to the Refresh (↻) button.

4. Click the **Create** button and select **Azure SQL backup**. The **Create backup scope** panel appears.

5. In the **Select databases** step, select the tenant and the databases that you want to add to the backup scope.

   - Manually select – Select the databases that you want to add to the backup scope. You can use **Filters** to find the databases you want to protect or use the **Search** box to search for the databases via the keywords in the name. The number of your selection will be displayed on the row of the tenant name.

   - Copy from existing native Azure SQL backup monitoring backup scope – Select the backup scopes from the native Azure SQL backup monitoring backup scopes drop-down list.

6. Click **Next**, and you will go to the **Configure storage based on region** step to configure a storage profile for each region. You can select a storage type and then select storage profiles. You can use an existing storage profile or create a new storage profile to store the backup data for the databases in the same region. For details on configuring storage location, refer to Manage Your Storage.

   > **Note:** If you have enabled a firewall for your Azure SQL databases, you need to add the IBM® Storage Protect for Cloud IP addresses to your Azure SQL database account firewall or configure the firewall to allow IBM® Storage Protect for Cloud agent servers running on a dedicated ARM Vnet subnet to access your storage location. For details, refer to "Allow IBM Storage Protect for Cloud Agent Servers to Access Your Storage Account" on page 82.

7. After you finish the storage configuration for each region, click **Next** to configure the scope information, schedule, and data retention settings. Refer to the following:

   - **Scope information** – Enter a name and description for the scope you are creating. The description is optional.

   - **Schedule** – Select days, **weeks**, **months**,or**years** as the unit of time for the backup interval, enter a number in the text box after **Every**, and then configure the start time for your first backup job.

     > **Note:** The **days** option is only available if you use your own storage to store backup data.

   - **Notification policy** – Check the notification profiles which will be applied to the backup scope.

   - **Retention policy** – Configure the retention period to keep the backup data in the storage.

     > **Note:** For existing backup scopes with the legacy retention policy, you can click **Switch to modern retention policy** to configure the new retention period.

     - **Daily recovery point** – Enter a number in the text box and select **days** or **weeks** from the drop-down list. The retention period must be between 7 and 28 days.

- **Weekly recovery point** – Enter a number in the text box and select **weeks** or **months** from the drop-down list. The retention period must be between 2 and 12 weeks.
- **Monthly recovery point** – Enter a number in the text box. The retention period must be between 1 and 12 months.
- **Yearly recovery point** – If you are using **IBM default storage** with unlimited retention period, the **Unlimited** option is selected automatically. If you want to use a custom retention period, select **Custom**.

8. Click **Next** to review your settings.
9. Click **Save** to save this backup scope. The backup for the databases in this backup scope will roll out as scheduled. For more details about monitoring the backups, refer to Monitor Your Backup.

Manage the Backup Scopes for Azure DevOps

The Azure DevOps service is currently available now from August 2024 release. You can use the Azure DevOps service to protect the Azure DevOps organizations. An organization can only be added to one backup scope.

If you want to try this service, contact your IBM representative for assistance. The Azure DevOps service trial only allows one backup scope.

- To create a new backup scope for Azure DevOps, refer to Create a New Backup Scope for Azure DevOps.
- For the existing backup scopes, you can perform the following actions:
  - Edit – To edit a backup scope, you can select a backup scope and click **Edit** button on the command bar, or you can click the **Edit** button when you are viewing the backup scope details. For details on the backup scope settings, refer to Create a New Backup Scope for Azure DevOps.
  - Delete – To delete a backup scope, you can select a backup scope and click **Delete** button on the command bar, or you can click the **Delete** option from the More actions (•••) list when you are viewing the details of a backup scope. You can also select multiple backup scopes to delete. When deleting backup scopes, you can select how to handle your backup data: keep the data and follow the configured retention policy, keep the data for 30 days before deletion, or delete the backup data immediately.
  - Run backup now – If you want to start a backup immediately, you can select a backup scope and click **Run backup now**, or you can click the **Run backup now** from the More actions (•••) list when you are viewing the details of a backup scope.

Create a New Backup Scope for Azure DevOps

Procedure

To create a new backup scope for Azure DevOps, follow the steps below:

1. Go to the **Backup** page on the new UI.
2. Click on the **Azure DevOps** service tile or click the More actions (•••) button on the upper-right corner of the Azure DevOps service tile and click Configure backup scope from the drop-down list.
3. In the **Configure backup scope for Azure DevOps** page, all the existing backup scopes for Azure DevOps are listed in the table. You can use the search box to search for the backup scopes by name and manage the columns to adjust the view of the backup scopes.
4. Click the **Create** button. The **Create backup scope** panel appears.
5. In the **Define scope** step, select the custom Azure app profile from the drop-down list for the tenant that you want to protect in this backup scope and then click the organizations to drill down to the items that you want to include into this backup scope.
6. Click **Next**.
7. In the **Settings** step, complete the following settings:
   - **Scope information** – Enter a name and description for the scope you are creating. The description is optional.
   - **Storage profile** – You can select a storage profile from the drop-down list to use or click the **+ Create a storage profile** link next to the list to create a new storage profile for this backup scope. For details on configuring storage profiles, refer to Manage Your Storage.
   - **Schedule** - Select **days**, **weeks**, **months**, or **years** as the unit of time for the backup interval, enter a number in the text box after **Every**, and then configure the start time for your first backup job.
   - **Notification** – Check the notification profiles which will be applied to the backup scope.

- **Retention policy** – Configure when to prune the backup data from the storage location. Note that if you are using IBM storage, the retention policy for backup data is subject to your agreement. You can configure a custom retention period up to the retention policy in your subscription. If you are using **IBM default storage** with **unlimited** retention period, the **Unlimited** option is selected automatically in the list. If you want to use a custom retention period, select **Custom** from the list, enter a number in the text box and select **weeks**, **months**, or **years** from the drop-down list. The retention period cannot be less than 2 weeks. Note that if you have a retention policy with a fixed year in your subscription, the maximum retention period that you can configure will be displayed under this field.

> **Note:** When you configure the retention period for backup data using the Year unit, the **Configure Full Backup Frequency** section will appear. You can then select a number from the drop-down list to set the full backup frequency. If the retention period is set to more than three months using the Month or Week unit, the full backup frequency will automatically be set to three months and cannot be changed. For retention periods of less than three months, the full backup frequency will be adjusted accordingly and cannot be modified.

8. Click **Next** to review your settings.

9. Click **Save** to save this backup scope. The backup for the organizations in this backup scope will roll out as scheduled. For more details about monitoring the backups, refer to Monitor Your Backup.

Manage the Backup Scopes for Azure AD B2C

You can use the Azure AD B2C service to protect the app registration, identity provider, user attribute, and user flow.

The Azure AD B2C service trial only allows one backup scope.

- To create a new backup scope for Azure AD B2C, refer to Create a New Backup Scope for Azure AD B2C.
- For the existing backup scopes, you can perform the following actions:
  - Edit – To edit a backup scope, you can select a backup scope and click **Edit** button on the command bar, or you can click the **Edit** button when you are viewing the backup scope details. For details on the backup scope settings, refer to Create a New Backup Scope for Azure AD B2C.
  - Delete – To delete a backup scope, you can select a backup scope and click **Delete** button on the command bar, or you can click the **Delete** option from the More actions (•••) list when you are viewing the details of a backup scope. You can also select multiple backup scopes to delete. When deleting backup scopes, you can select how to handle your backup data: keep the data and follow the configured retention policy, keep the data for 30 days before deletion, or delete the backup data immediately.
  - Run backup now – If you want to start a backup immediately, you can select a backup scope and click **Run backup now**, or you can click the **Run backup now** from the More actions (•••) list when you are viewing the details of a backup scope.

Create a New Backup Scope for Azure AD B2C

About this task

To create a new backup scope for Azure AD B2C, follow the steps below:

1. Go to the **Backup** page on the new UI.
2. Click on the **Azure AD B2C** service tile or click the More actions (•••) button on the upper-right corner of the Azure AD B2C service tile and click Configure backup scope from the drop-down list.
3. In the **Configure backup scope for Azure AD B2C** page, all the existing backup scopes for Azure AD B2C are listed in the table. You can use the search box to search for the backup scopes by name and manage the columns to adjust the view of the backup scopes.
4. Click the **Create** button. The **Create backup scope** panel appears.
5. In the **Define scope** step, select the custom Azure app profile from the drop-down list for the tenant that you want to protect in this backup scope and then select the data type that you want to include into this backup scope.
6. Click **Next**.
7. In the **Settings** step, complete the following settings:
   - **Scope information** – Enter a name and description for the scope you are creating. The description is optional.
   - **Storage profile** – You can select a storage profile from the drop-down list to use or click the **+ Create a storage profile** link next to the list to create a new storage profile for this backup scope. For details on configuring storage profiles, refer to Manage Your Storage.
   - **Schedule** – The backup job will run once a day. Configure the start time for your first backup job.
   - **Notification** – Check the notification profiles which will be applied to the backup scope.
   - **Retention policy** – Configure when to prune the backup data from the storage location. Note that if you are using IBM storage, the retention policy for backup data is subject to your agreement. You can configure a custom retention period up to the retention policy in your subscription. If you are using **IBM default storage** with **unlimited** retention period, the **Unlimited** option is selected automatically in the list. If you want to use a custom retention period, select **Custom** from the list,

enter a number in the text box and select **weeks**, **months**, or **years** from the drop-down list. The retention period cannot be less than 2 weeks. Note that if you have a retention policy with a fixed year in your subscription, the maximum retention period that you can configure will be displayed under this field.

> **Note:** When you configure the retention period for backup data using the Year unit, the **Configure Full Backup Frequency** section will appear. You can then select a number from the drop-down list to set the full backup frequency. If the retention period is set to more than three months using the Month or Week unit, the full backup frequency will automatically be set to three months and cannot be changed. For retention periods of less than three months, the full backup frequency will be adjusted accordingly and cannot be modified.

8. Click **Next** to review your settings.
9. Click **Save** to save this backup scope. The backup for the organizations in this backup scope will roll out as scheduled. For more details about monitoring the backups, refer to Monitor Your Backup.

Manage Your Storage

About this task

Navigate to **Settings** > **Storage profiles** > **Backup storage**, and all the backup storage profiles are displayed in the table.

If you are using your own storage, you can choose to use the following storage type: Amazon S3, Amazon S3-Compatible, Microsoft Azure Blob Storage, IBM Storage Protect – S3, IBM Cloud Object Storage, and Google Cloud Storage. In addition, if you may have set up the storage firewall to only allow trusted clients to access your storage, read the instructions in the "Allow IBM Storage Protect for Cloud Agent Servers to Access Your Storage Account" on page 82 section carefully and complete the settings upon your need.

If you have updated your subscription from using default storage to your own storage, you must navigate to this page, click **Storage**, and click the **Change to my own storage** link to configure the storage profiles connecting to your own storage. Otherwise, the backup will be interrupted.

If you updated the subscription by using your own storage to default IBM® Storage Protect for Cloud storage, the backup service will force a full backup for the subsequent backup job in the schedule and automatically store the backup data to the default IBM® Storage Protect for Cloud storage. The legacy backup data stored on your own storage can still be used for restoring until it expires the retention period.

You can click the storage profile name to view the details of the storage location and click **Edit** to update the profile information. The storage information, apart from its path information, can be modified.

Follow the instructions below to create a storage profile:

1. In the **Backup storage**tab, click the **Create** button. The **Create a storage profile** pane appears on the right.

2. Enter a profile name for the storage location that you want to connect to and provide an optional description.

3. In the **Storage Type** field, select a storage type from the list and then refer to the following sections for the storage configuration.

Microsoft Azure Storage

You can configure the Azure Blob storage location by referring the information given in this topic.

Before you begin

Note the following before configuring Azure Blob storage location:

- The supported Azure account kinds are **Storage** and **StorageV2** of **Standard** performance type. For details on creating a storage account, refer to the Microsoft article: Create a storage account.

- Before you add the Azure storage account to the IBM® Storage Protect for Cloud interface, you must ensure your storage can be accessed by IBM® Storage Protect for Cloud products. For details, refer to "Allow IBM Storage Protect for Cloud Agent Servers to Access Your Storage Account" on page 82.

- If you use Microsoft Azure Blob Storage to store backup data for **Azure VM** and **Azure Storage**, navigate to **Storage account** > **Settings** > **Configuration** > **Permitted scope for copy operations**, and ensure the permitted scope for copy operations of the storage account used by the storage profile is properly configured as follows:

  - For the storage account within the same Microsoft Entra tenant, you can select the **From storage accounts in the same Microsoft Entra tenant** option.

  - For the storage account from a different Microsoft Entra tenant, ensure the **From any storage account** option is selected.

- To help reduce storage costs, the backup data generated after October 2023 release will be automatically stored to the Microsoft Azure storage cold tier, if the retention period is more than 45 days.

Procedure

Complete the following steps:

1. **Storage Type** – Select **Microsoft Azure Blob Storage** from the drop-down list.
2. Access point – Enter the URL for the Blob Storage Service. The default URL is https://blob.core.windows.net.
3. > **Note:** The entered name must match an existing container.

   Container name – Enter the container name you wish to access.
4. **Account name** – Enter the corresponding account name to access the specified container.
5. **Account key** – Enter the corresponding account key to access the specified container.
6. **Advanced** – Enter the following extended parameters if necessary. If you have multiple parameters to enter, use a semicolon (;) to separate the parameters. Refer to the instructions below to add parameters.
   - **RetryInterval** – Customize the retry interval when the network connection is interrupted. You are allowed to enter any positive integer between 0 and 2147483646 (the unit is in milliseconds). For example, RetryInterval=30000 means that it will try to reconnect every 30000 milliseconds.
     If you do not configure this parameter, the value is 30000 milliseconds by default.
   - **RetryCount** – Customize the reconnection times after the network connection is interrupted. You are allowed to enter any positive integer between 0 and 2147483646. For example, RetryCount=10 represents when the network connection is interrupted, it can reconnect at most 10 times.
     If you do not configure this parameter, the value is 6 by default.
7. Click **Save** to save your storage. The storage path cannot be changed once saved, and the storage profile cannot be deleted once the storage has been applied to store the backup data for a region.

Amazon S3

IBM® Storage Protect for Cloud will by default use HTTPS (SSL) communication to access your Amazon S3 storage and store your backup data to the S3 Glacier Instant Retrieval / Standard-IA storage class automatically. You can move the backup data from S3 Standard-IA to S3 Standard, S3 One Zone-IA, or S3 Intelligent-Tiering, and IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID can restore the backup data of those storage classes.

Procedure

Follow the instructions below:

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

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

5. **Storage Region** – Select the **Storage region** of this bucket from the drop-down menu. You can use the **Search** box to search for region via keywords.
6. **Extended parameters** – Enter the following extended parameters if necessary. If you have multiple parameters to enter, use a semicolon (;) to separate the parameters. Refer to the instructions below to add parameters.
   - **RetryInterval** – Customize the retry interval when the network connection is interrupted. Enter any positive integer between 0 and 2147483646 (the unit is millisecond). For example, RetryInterval=30000 means that it will try to reconnect every 30000 milliseconds.
     If you do not configure this parameter, the value is 30000 milliseconds by default.
   - **RetryCount** – Customize the reconnection times after the network connection is interrupted. Enter any positive integer between 0 and 2147483646. For example, RetryCount=6 represents when the network connection is interrupted, and it can reconnect at most 6 times.
     If you do not configure this parameter, the value is 6 by default.
   - **RetryMode** – Customize the retry mode for the requests not being completed successfully. If this parameter is not configured or configured incorrectly, the **Legacy** will be applied as the default value. You can also set the value to **Standard** or **Adaptive**. **Standard** represents the standardized request retry strategy which is consistent across all SDKs; **Adaptive** represents an experimental request retry strategy that builds on the Standard strategy and introduces congestion control through client-side rate limiting.
7. Click **Save** to save your storage profile. The storage path cannot be changed once saved, and the storage profile cannot be deleted once the storage has been applied to store the backup data for a region.

Amazon S3-Compatible

You can configure the Amazon S3-Compatible storage by referring the information given in this topic.

Procedure

Follow the instructions below:

1. **Storage Type** – Select Amazon S3-Compatible Storage from the drop-down list.
2. **Bucket name** – Enter the bucket name you wish to access.
   Note the following:
   - The entered name must match an existing bucket. If no bucket is available, refer to Creating a bucket to create one. Note that it’s a general guidance, the exact steps may vary depending on the specific product, refer to your specific product documentation for any additional configurations required.
   - Ensure the bucket policy in Amazon S3-compatible storage applied to your account contains the following required permissions:
     - Read: Get Object
     - List: ListBucket
     - Write: DeleteObject; PutObject; DeleteObjectVersion
3. **Access key ID** – Enter the corresponding access key ID to access the specified bucket.
4. **Secret access key** – Enter the corresponding secret key ID to access the specified bucket.
5. **Endpoint**– Enter the URL used to connect to the place where you want to store the data.

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

6. **Extended parameters**– Enter the following extended parameters if necessary. If you have multiple parameters to enter, use a semicolon (;) to separate the parameters. Refer to the instructions below to add parameters.

- **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.
- **RetryInterval**– Customize the retry interval when the network connection is interrupted. Enter any positive integer between 0 and 2147483646 (the unit is millisecond). For example, RetryInterval=30000 means that it will try to reconnect every 30000 milliseconds.
  If you do not configure this parameter, the value is 30000 milliseconds by default
- **RetryCount**– Customize the reconnection times after the network connection is interrupted. Enter any positive integer between 0 and 2147483646. For example, RetryCount=6 represents when the network connection is interrupted, it can reconnect at most 6 times.
  If you do not configure this parameter, the value is 6 by default.
- **RetryMode** – Customize the retry mode for the requests not being completed successfully. If this parameter is not configured or configured incorrectly, the **Legacy** will be applied as the default value. You can also set the value to **Standard** or **Adaptive**. **Standard** represents the standardized request retry strategy which is consistent across all SDKs. **Adaptive** represents an experimental request retry strategy that builds on the Standard strategy and introduces congestion control through client-side rate limiting.
- **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.
- **Cert_thumbprint** – If you have a self-signed certificate for storage server and only want to pass the certificate validation with a specific thumbprint, enter your thumbprint as the value of this parameter.
- **Use_PathStyle=true** – This parameter is required to ensure the IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID can work with your storage properly.
- **Use_ClientMultiUpload=true** – This parameter is required to ensure theIBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID can work with your storage properly.

7. Click **Save** to save your storage profile. The storage path cannot be changed once saved, and the storage profile cannot be deleted once the storage has been applied to store the backup data for a region.

IBM Storage Protect - S3

Before you begin

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

Procedure

Follow the instructions below:

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

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

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

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

6. **Extended parameters** – Enter the following extended parameters if necessary. If you have multiple parameters to enter, use a semicolon (;) to separate the parameters. Refer to the instructions below to add parameters.

   - ***Use_PathStyle=true** – This parameter is required to ensure the IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID can work with your storage properly.

   - **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.

   - **Cert_thumbprint** – If you have a self-signed certificate for S3 server and only want to pass the certificate validation with a specific thumbprint, enter your thumbprint as the value of this parameter.

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

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

   - **RetryMode** – Customize the retry mode for the requests not being completed successfully. If this parameter is not configured or configured incorrectly, the **Legacy** will be applied as the default value. You can also set the value to **Standard** or **Adaptive**. **Standard** represents the standardized request retry strategy which is consistent across all SDKs; **Adaptive** represents an experimental request retry strategy that builds on the Standard strategy and introduces congestion control through client-side rate limiting.

7. Click**Save** to save your storage. The storage path cannot be changed once saved, and the storage profile cannot be deleted once the storage has been applied to store the backup data for a region.

IBM Cloud Object Storage

You can configure the IBM Cloud Object Storage location by referring the information given in this topic.

Procedure

Follow the instructions below:

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

   > **Note:** The entered name must match an existing bucket. If no bucket is available, refer to Create some buckets to store your data to create one.

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

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

6. **Extended parameters** – Enter the following extended parameters if necessary. If you have multiple parameters to enter, use a semicolon (;) to separate the parameters. Refer to the instructions below to add parameters.

- **RetryInterval** – Customize the retry interval when the network connection is interrupted. Enter any positive integer between 0 and 2147483646 (the unit is millisecond). For example, RetryInterval=30000 means that it will try to reconnect every 30000 milliseconds.
  If you do not configure this parameter, the value is 30000 milliseconds by default.
- **RetryCount** – Customize the reconnection times after the network connection is interrupted. Enter any positive integer between 0 and 2147483646. For example, RetryCount=6 represents when the network connection is interrupted, and it can reconnect at most 6 times.
  If you do not configure this parameter, the value is 6 by default.
- **RetryMode** – Customize the retry mode for the requests not being completed successfully. If this parameter is not configured or configured incorrectly, the **Legacy** will be applied as the default value. You can also set the value to **Standard** or **Adaptive**. **Standard** represents the standardized request retry strategy which is consistent across all SDKs; **Adaptive** represents an experimental request retry strategy that builds on the Standard strategy and introduces congestion control through client-side rate limiting.

7. Click**Save** to save your storage. The storage path cannot be changed once saved, and the storage profile cannot be deleted once the storage has been applied to store the backup data for a region.

Google Cloud Storage

You can configure the Google Cloud Storage location by referring the information given in this topic.

About this task

Note the following before creating a Google Cloud Storage:

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

Procedure

Follow the instructions below:

1. **Storage type** – Select **Google Cloud Storage** from the drop-down list.
2. **Service account email address** – Enter the corresponding client email to access the specified service account.
3. **Private key** – Enter the corresponding private key to access the specified service account.
4. **Project ID** – Enter the corresponding project ID to access the specified service account.
5. **Bucket name** – Enter the bucket name you wish to access.

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

6. Click**Save** to save your storage. The storage path cannot be changed once saved, and the storage profile cannot be deleted once the storage has been applied to store the backup data for a region.

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

If you are going to protect Azure storage or use your own storage device to store the backup data, read the instructions in this section carefully and complete the settings upon your need. Otherwise, you can skip this topic.

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

> **Note:** If you are in trial and the storage account you want to use in the trial has a firewall enabled, read the conditions below and contact IBM® Storage Protect for Cloud Support for the corresponding reserved IP addresses or ARM VNet IDs.
>
> - If you use a storage type other than Microsoft Azure storage, you must add reserved IP addresses to your storage firewall. To get the list of the reserved IP addresses, refer to Download a List of Reserved IP Addresses.
> - If you are using Microsoft Azure storage, refer to the following:
>   - If your storage account is in the same data center as the one you use to sign up for IBM® Storage Protect for Cloud or your storage account is in its paired region, you must add the Azure Resource Manager (ARM) vNet subnets where the IBM® Storage Protect for Cloud agents are running on to your storage networking. You can find additional details in this Microsoft article: Grant access from a virtual network, and get the subnet ID of IBM® Storage Protect for Cloud cloud products for your data center from Download ARM VNet IDs. For detailed instructions, refer to "Add ARM virtual networks" on page 82.
>   - Other than the condition above, you need to add all the reserved IP addresses to the Azure storage firewall. For details, refer to Add reserved IP addresses.

Add reserved IP addresses

You can add reserved IP addresses to IBM® Storage Protect for Cloud.

Procedure

Follow the steps below:

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

Add ARM virtual networks

You can add ARM virtual networks to the IBM® Storage Protect for Cloud.

About this task

There are two ways to grant access to a subnet in a virtual network belonging to another tenant:

- 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 the Azure Az PowerShell

# # 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: Verify the newly added network rule.
# This cmdlet retrieves the network rule set for the specified storage account.
Get-AzStorageAccountNetworkRuleSet -ResourceGroupName $DESTRG -AccountName $DESTSTA
```

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

Restore and Recover Your Data

IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID provides robust solutions for quickly recovering or exporting your backup data of various Azure services. Whether it's Azure VMs, Microsoft Entra ID, Azure Storage, Admin Portal Settings, Azure SQL, Azure DevOps, or Azure AD B2C.

Azure VM and Azure Storage

- You can choose to restore the backup data to its original location or another place.
- You can also choose to export the backup data of the folders and files in Azure VM and Azure storage. For details, refer to Export and Download Your Data.
- If the disk snapshots of Azure VM exist, both the in-place and out-of-place restore jobs for Azure VMs can restore data from snapshots. For details, refer to Azure Virtual Machines.

Microsoft Entra ID

- For Microsoft Entra ID data recovery, you can perform both in-place and out-of-place restores for groups and users. However, for other data types, only the in-place restore is supported.
- You can restore app registrations, enterprise applications, groups, users, administrative units, or roles and administrators. The restore job can keep the object ID for the users or groups that have not yet been permanently deleted and the Overwrite, Merge, and Skip are the available options for conflict resolution during restore.
- You can download the properties of the Microsoft Entra users at specific recovery points to a local location and use the downloaded script to import the users with the downloaded properties.
- You can copy the BitLocker key from the backup. For details, refer to Copy BitLocker Recovery Keys.
- You can export the backup data of sign-in logs and audit logs. For details, refer to Export and Download Your Data.

Admin Portal Settings

- For Admin Portal Settings, you can not only export the backup data of the components to a JSON file, but also restore some settings to their original location. For the settings you can export or restore, refer to “Admin Portal Settings” on page 128. For details on exporting data, refer to Export and Download Your Data.

Azure SQL

- For Azure SQL databases, the restoration of both monitored databases and backup databases is supported. To restore the retrieved native Azure backups for databases, refer to Restore Monitored Databases.

  To restore the directly backup databases and Restore Backup Databases.
- You can choose to replace the existing database using the backup data or restoring the database to the same SQL server by creating a database with a new name.

Azure DevOps

- For Azure DevOps organizations, you can restore the backup items to its original location.

Azure AD B2C

- For Azure AD B2C data, you can restore the backup data to its original location.

To find the data you want to restore through the **Restore** wizard, you can choose to use the classic Recovery Point method to search in a backup job for the data you want to restore, or you can now use the **Compare** method to compare the backup data with the data in a production environment for the differences. Note that the **Compare** method is available in the**Microsoft Entra ID** service and **Admin Portal Settings** service, and only supports comparing for Microsoft Entra ID users and groups.

- Using the **Recovery Point** method, you will select the service that you want to restore and then a calendar appears displaying all the data recovery points of this service. You can switch the display of recovery points between **Month** view and **Day** view and choose whether to display the finished with the exception or failed jobs in the calendar by selecting the **Include jobs with only partial backup data**option.
  Hover over the data recovery point to view the job details, including the backup scope name, scope ID, job status, job finished time, job ID, backup size, and the number of objects in a backup.

- The **Compare** method now only supports comparing the backup data with the data in your Microsoft Entra ID production environment. You need to first provide the comparison conditions, such as the tenant's name and the data type to compare, and the recovery point that you want to compare against the production environment. Then, generate a comparison report. You can go to the **View Compared Results** tile to check the comparison job progress and continue with the restore using the comparison report. For details, refer to "Use the Compare Method" on page 86.

Use the Compare Method

IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID supports comparing for Microsoft Entra ID users or groups and Admin Portal Settings. Follow the instructions below to use the **Compare** method to find the data that you want to restore.

Microsoft Entra ID

Before restoration, you can choose to compare all items or specific objects.

Compare All Data

To compare all data, follow the steps below:

1. In the **Restore** page, click **Microsoft Entra ID**, and then click the **Compare** tile. All the existing comparison reports are displayed in the **Compare** page.
2. Click the **Create** button to create a comparison report. Complete the settings below:
    - **Report name** – Enter a report name for the comparison report that you are about to create.
    - **Compare type** – Choose to compare two recovery points or compare the selected recovery point with the current state of Microsoft Entra ID.
    - **App profile** – Select the app profile from the list.
    - **Object type** – Currently, the Compare feature only supports comparing the backup data for users or groups in the Microsoft Entra tenant.
    - **Recovery points** – Select the recovery point from the calendar according to the compare type that you have configured.
    - **What data do you want to compare** – Select **All** to compare all data.
3. Click **Compare**. The comparison job will start, and you can view the job progress in the **Compare** page.
4. After the comparison job is finished, click the report name to open the comparison report.
5. In the **View comparison report** page, you can get the basic information of this comparison report, including the tenant name and the recovery points selected to compare. If only one recovery point is displayed, this comparison report was generated for comparing the backup data against the current state of the Microsoft Entra environment. In the **Summary** section, you can also get a summary of the report for the total number in the scope and the number of users or groups being added, modified, not found, or unchanged.
6. You can use the **Name** or **Object ID** to search for the data or use the Filters (such as, **Company**, **Office location**, **Department**, or **Status**) to find the data. Note that if the properties that have been updated for the user or group are currently not supported by IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID, the user or group will be tagged as **Modified** in the report, though the report cannot show the differences. To view the differences, click the object ID on the row.
7. You can select the data that you want to restore and click **Restore**. Users or groups can be restored to the original location or a new location. For details, refer to Restore Users or Restore Groups.

Compare Specific Items

To compare specific items, follow the steps below:

1. In the **Restore** page, click **Microsoft Entra ID**, and then click the **Compare** tile. All the existing comparison reports are displayed in the **Compare** page.
2. Click the **Create** button to create a comparison report. Complete the settings below:
    - **Report name** – Enter a report name for the comparison report that you are about to create.

- **Compare type** – Choose to compare two recovery points or compare the selected recovery point with the current state of Microsoft Entra ID.
- **App profile** – Select the app profile from the list.
- **Object type** – Currently, the Compare feature only supports comparing the backup data for users or groups in the Microsoft Entra tenant.
- **Recovery points** – Select the recovery point from the calendar according to the compare type that you have configured.
- **What data do you want to compare** – Select **Specific items** to compare specific users or groups.

3. Click **Next**.
4. In the **Select objects** step, select the users or groups you want to compare. You can select at most 100 users or groups to compare.
5. Click **Compare**. The comparison job will start, and you can view the job progress in the **Compare** page.
6. After the comparison job is finished, click the report name to open the comparison report.
7. In the **View comparison report** page, you can get the basic information of this comparison report, including the tenant name and the recovery points selected to compare. If only one recovery point is displayed, this comparison report was generated for comparing the backup data against the current state of the Microsoft Entra environment. On the **Summary** section, you can also get a summary of the report for the total number in the scope and the number of users or groups being added, modified, not found, or unchanged.
8. You can use the **Name** or **Object ID** to search for the data or use the Filters (such as, **Company**, **Office location**, **Department**, or **Status**) to find the data. Note that if the properties that have been updated for the user or group are currently not supported by IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID, the user or group will be tagged as **Modified** in the report, though the report cannot show the differences. To view the differences, click the object ID on the row.
9. You can select the data that you want to restore and click **Restore**. For details on restoring the users or groups, refer to Restore Users or Restore Groups.

Admin Portal Settings

The Admin Portal Settings service supports comparing two modules: Microsoft Entra ID (Conditional Access, General, Expiration, Naming Policy, and Named Locations) and Intune (Configuration Profile, Conditional Access, and Compliance Policies). To compare all data, follow the steps below:

1. In the **Restore** page, click **Admin Portal Settings**, and then click the **Compare** tile. All the existing comparison reports are displayed in the **Compare** page.
2. Click the **Create** button to create a comparison report. Complete the settings below:
   - **Report name** – Enter a report name for the comparison report that you are about to create.
   - **Compare type** – Choose to compare two recovery points or compare the selected recovery point with the current state of Microsoft Entra ID.
   - **App profile** – Select the app profile from the list.
   - **Module** – Select the module you want to compare.
   - **Object type** – Select the object type you want to compare.
   - **Recovery points** – Select the recovery point from the calendar according to the compare type that you have configured.
3. Click **Compare**. The comparison job will start, and you can view the job progress in the **Compare** page.
4. After the comparison job is finished, click the report name to open the comparison report.
5. In the **View comparison report** page, you can get the basic information of this comparison report, including the tenant name and the recovery points selected to compare. If only one recovery point is displayed, this comparison report was generated for comparing the backup data against the current state of the Microsoft Entra environment. On the **Summary** section, you can also get a summary of the report

for the total number in the scope and the number of policies being added, modified, not found, or unchanged.

6. You can use the **Name** to search for the data or use the Filters (such as, **Data from**, **Component**, **Category**, or **Status**) to find the data.
7. You can select the data that you want to restore and click **Restore**. For details, refer to Restore Admin Portal Settings.

Azure Virtual Machines

Azure Virtual Machines restore service supports restoring the VMs and disks to original locations, or to another location with different settings. The specific folders or files can be restored to original locations. The file-level restore job supports both VMs of Linux system and Windows system. For the instructions on restoring folders or files, refer to Restore Folders/Files. The file level export job for Azure VMs supports both VMs of Linux System and Windows system. For the instructions on exporting your data, refer to Export and Download Your Data.

A faster in-place or out-of-place restore job will be performed from snapshots automatically if the disk snapshots exist and reside within the same subscription and region as the destination snapshots. Otherwise, the VMs will be restored from the backup storage, which takes more time than snapshot restoration.

Follow the instructions below to perform the restore and you can also refer to Azure VM for the supported and unsupported properties or settings in the data recovery.

Restore VM

To restore a VM, complete the steps in the below procedure.

Procedure

1. Go to the **Restore** page, and click the **Virtual Machine** tile.
2. In the **Restore** wizard, a calendar displays all the data recovery points. Click **Azure Virtual Machines**. You can switch the display of recovery points between the **Month** view and **Day** view and choose whether to display the finished with the exception jobs in the calendar by selecting the **Include jobs with only partial backup data** option.
3. Hover over the data recovery point to view the job details, including the job status, job start time, scope name, scope ID, job ID, backup size, and the number of objects in a backup.
4. Click the data recovery point in the calendar. The VMs backed up in the selected backup job are displayed in the table.
5. You can use the **Tenant** filter, **Subscription** filter, and **Resource Group** filter to find the VMs of specific properties or use the **Search** box to search for VMs via keywords in the name. You can also manage the columns to adjust the view of VMs.
6. Select the VM that you want to restore and click **Restore**.
7. In the **Restore Options** step, select where you would like to restore the VM data and provide an optional description for further reference.
    - **Restore the data to the original location** – To restore the data to its original location, you must note that the VM in the original location will be overwritten, and the VM will be stopped (deallocated) if it is running. If the network at the recovery point is no longer connected, but the backend pool related to the VM still exists, you can choose to add this VM to the load balancer.
    - **Restore the data to a new location, or with different settings** – Follow the steps below to choose the subscription for the VM being restored, and configure the properties, disks, and network settings for the target VM.
        a. **Subscription** – In the Subscription step, select a destination subscription for the VM being restored. You can choose to restore this VM to the same subscription when it is being backed up or select a new subscription, and then select a region as well.

> **Note:** If your subscription is added to your tenant after the initialization of IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID, you must follow the steps in Add to the Subscription and Grant Contributor Role to add the consent user of the IBM® Storage Protect for Cloud – Delegated App to your subscription and grant this user the Contributor role at the same time.

b. **Properties** – Configure the properties for the destination VM, including the VM name, resource group, disk type, availability options, storage account, and VM size.
Note the following:
   - The VM name cannot be a duplicate with VMs already in the target resource group.
   - If you choose **Availability set** or **Virtual machine scale set** from the **Availability options** drop-down list, you can then select a specific availability set or virtual machine scale set from the corresponding drop-down list.

c. **Disk** – All the disks in this VM are displayed. By default, the disk name in the backup will be populated. You can use the same disk name or use a new name, but you must ensure the name is unique in the destination.

d. **Network** – Configure a virtual network for this VM to access. Select the network, subnet, and network interface from the lists. You can configure whether to restore the VM to an existing network interface or create a new one for this VM. If you leave the **Public IP Address Name** field empty, no public IP addresses will be assigned to this restored VM.

8. Click **Next** to continue.
9. Review the restore settings in the **Overview** step.
10. Click **Restore** to perform the restore job.

Restore Disks

To restore disks, follow the steps below:

About this task

> **Note:** When a **VM** disk of Windows system has **Data Deduplication** enabled, the restore of the duplicate files in the disk is unsupported even though the backup and index generation jobs complete successfully.

Procedure

1. Go to the **Restore** page, and click the **Virtual Machine** tile.
2. In the**Restore** wizard, a calendar displays all the data recovery points. Click **Azure virtual machines**.
3. You can choose whether to display the finished with the exception jobs in the calendar by selecting the **Include jobs with only partial backup data** option.
4. Hover over the data recovery point to view the job details, including the job status, job finished time, scope name, scope ID, job ID, backup size, and the number of objects in a backup.
5. Click the data recovery point in the calendar. The VMs backed up in the selected backup job are displayed in the table.
6. You can use the **Tenant** filter, **Subscription** filter, and **Resource group** filter to find the VMs of specific properties or use the **Search** box to search for VMs via keywords in the name. You can also manage the columns to adjust the view of VMs.
7. Click the VM where the disks that you want to restore reside in. All the disks in this VM are displayed. You can search for disks by name or manage the columns to adjust the view of the disks.
8. Select the disks that you want to restore and click **Restore**.
9. In the **Restore options** step, select where you would like to restore the disk data and provide an optional description for further reference.

- **Restore the data to the original location** – To restore the data to its original location, the disks in the original location will be overwritten, and the VM will be stopped (deallocated) if it is running.
- **Restore the data to a new location or with different settings** – Follow the steps below to choose the subscription for the disk being restored and configure the properties of the destination disk.
    - **Subscription** – In the Subscription step, select a destination subscription for the disk being restored. You can choose to restore this disk to the same subscription when it is being backed up or select a new subscription, and then select a region as well.

      > **Note:** If the subscription is added to your tenant after the initialization of IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID, you must follow the steps in Add to the Subscription and Grant Contributor Role to add the consent user of the IBM® Storage Protect for Cloud– Delegated App to your subscription and grant this user the Contributor role at the same time.

    - **Disk** – Configure the properties for the destination disk, including the resource group, the VM to attach the restored disk (optional), the disk type, the availability zone (for Managed disk), and the storage account (for Unmanaged disk).

      > **Note:** You can restore the unmanaged disks (data disks) to managed types (OS disks), but the managed disks cannot be converted to unmanaged types.

10. Click **Next** to continue.
11. Review the restore settings in the **Overview** step.
12. Click **Restore** to perform the restore job.

Restore Folders/Files

Procedure

To restore folder/files to original locations, follow the steps below:
Note the following:

- The restoration of signed scripts is now supported. To ensure the security and integrity of signed scripts, you can verify the scripts after restoring. For details, refer to Verify Windows Signed Scripts and Verify Linux Signed Scripts.
- The file-level restore job for Azure VMs supports both VMs of Linux system and Windows system. If you would like to perform file-level data restoration of Azure VM backup data, you must have generated an index for the backup data.
- The index generation for the following file systems is unsupported: **UFS – BSD default fs**, **ZFS – BSD alternative fs**, **BitLocker – Windows encrypted fs**, **LUKS – Linux encrypted fs**, **ReFS – Windows new fs**. Running index generation on these file systems will result in folders without indexes in restore **recovery** points.

1. Go to the **Restore** page, and click the **Virtual Machine** tile.
2. In the**Restore** wizard, a calendar displays all the data recovery points. Click **Azure virtual machines**. You can choose whether to display the finished with the exception or failed jobs in the calendar by selecting the **Include jobs with only partial backup data** option.
3. Hover over the data recovery point to view the job details, including the job status, job finished time, scope name, scope ID, job ID, backup size, and the number of objects in a backup.
4. Click the data recovery point in the calendar. The VMs backed up in the selected backup job are displayed in the table.
5. You can use the **Tenant** filter, **Subscription** filter, and **Resource group** filter to find the VMs of specific properties or use the **Search** box to search for VMs via keywords in the name. You can also manage the columns to adjust the view of VMs.

6. Click the VM to drill down to the folder/files that you want to restore, select the object, and click **Restore**.
7. In the **Restore options** step, provide an optional description for further reference and click **Next** to continue.
8. In the **Destination** step, configure the destination path and click **Next**.
9. Review the restore settings in the **Overview** step and click **Restore**.
10. In the **Check destination virtual machine** panel, the custom script extension, running status, and agent service of the destination virtual machine will be checked. Note that restoring files/folders in Azure VMs will create custom script extensions in your environment. To run the created custom script extensions, the agent service of the destination virtual machine must be available.
    If all required conditions are valid, click **Continue** to perform the restore job.

    If any conditions fail, you can follow the provided instructions to update them, then , then return here to click **Check again** to re-verify.

Verify Windows Signed Scripts

Procedure

Follow the steps below to verify the signed script of Windows system:

1. Run PowerShell on your computer.
2. Execute the following command lines in PowerShell:

   ```
   Get-AuthenticodeSignature –FilePath “{Restore destination path}\{RestoreJobId}
   _Script.ps1”
   ```

   If the command status is valid, the signed script has passed verification.

   Example:

   ```
   Restore destination path: C:\temp\VMBackup
   Restore Job ID: RS SerialNumber
   ```

   Follow the steps below to verify the signed script:

   a. Run PowerShell on your computer.

   b. Execute the following command lines in PowerShell:

      ```
      Get-AuthenticodeSignature –FilePath “C:\temp\VMBackup\RS SerialNumber_Script.ps1”
      ```

   If the command status is valid, the signed script has passed verification.

Verify Linux Signed Scripts

Procedure

Follow the steps below to verify the signed script of Linux system:

1. Copy the signed script from Linux system to Windows system.
2. Download and save the signed script to Windows system as a “.ps1” file.
3. Run PowerShell and execute the following command in PowerShell:

   ```
   Get-AuthenticodeSignature –FilePath “{root path where the script file is saved}\
   {RestoreJobId} _Script.ps1”
   ```

   If the command status is valid, the signed scripts have passed verification.

   Example:

   ```
   Root path where the script file is saved: D:\TestFolder
   Restore Job ID: RS SerialNumber
   ```

Follow the steps below to verify the signed scripts:

a. Copy the signed scripts from Linux system to Azure storage.

b. Download and save the script as a ".ps1" file.

c. Execute the following command lines in PowerShell:

```
Get-AuthenticodeSignature –FilePath "D:\TestFolder\RS SerialNumber_Script.ps1"
```

If the command status is valid, the signed script has passed verification.

Microsoft Entra ID

Microsoft Entra ID data recovery only supports restoring the supported data types to the original location. After October 2023 release, the Microsoft Entra ID service now supports protecting the Device – BitLocker Recovery Keys. You can copy the BitLocker key from the backup. For details, refer to Copy BitLocker Recovery Keys.

Follow the instructions below to perform the restore and you can also refer to Microsoft Entra ID section for supported and unsupported components and attributes of the object types you can protect in the Microsoft Entra ID.

Copy BitLocker Recovery Keys

Procedure

To copy the BitLocker keys for the devices, follow the steps below:

1. Go to the **Restore** page and click the **Microsoft Entra ID** tile.
2. Click the **Recovery point** tile.
3. In the **Restore** wizard, a calendar displays all the data recovery points. You must switch the display of recovery points between the **Month** view and **Day** view and choose whether to display the finished with the exception in the calendar by selecting the **Include jobs with only partial backup data** option.
4. Hover over the data recovery point to view the job details, including the job status, job start time, scope name, scope ID, job ID, backup size, and the number of objects in a backup., and click the data recovery point that you want to use in the calendar.
5. Select **Device – BitLocker Recovery Keys** from the **Object Type** filter. You can manage the columns to adjust the view of bitlocker recovery keys.
6. Click the device name to find all the BitLocker keys that you can copy.
7. Click the **Copy BitLocker Recovery Key** button to copy the recovery key for the corresponding key ID.

Restore App Registrations

To restore app registrations, complete the steps in the below procedure.

Procedure

1. Go to the **Restore** page and click the **Microsoft Entra ID** tile.
2. Click the **Recovery point** tile.
3. In the restore wizard, a calendar displays all the data recovery points. You can choose whether to display the finished with the exception jobs in the calendar by selecting the **Include jobs with only partial backup data** option.
4. Hover over the data recovery point to view the job details, including the job status, job start time, scope name, scope ID, job ID, backup size, and the number of objects in a backup., and click the data recovery point that you want to use in the calendar.

5. Select **App registration** from the object type filter. You can manage the columns to adjust the view of app registrations.
6. Select the app registrations that you want to restore and then click the **Restore** button.
7. The **View properties** step displays the app registration information in a table. Click **Next** to continue the restore.
8. In the **Restore options** step, select **Merge**, **Overwrite**, or **Skip** as the conflict resolution.

   > **Note:** The restore job can restore the roles and administrators directly related to the selected app registrations.
   > If a conflict occurs, **Merge** is to add the backup data to the destination for the properties that support adding new items. The existing properties with unique values will be replaced with the backup data. **Overwrite** is to remove the conflicting object from the destination and restore the backup data. **Skip** is to skip the restore of the backup data and keep the destination object intact.

9. You can enter a description for this restore job for further reference.
10. Click **Next** to go to the **Overview** step. Review the restore settings. You can click **Back** to go back to the previous steps in the restore wizard to modify the settings.
11. Click **Restore** to run the restore job.

Restore Enterprise Applications

To restore enterprise applications, complete the following steps in the procedure.

Procedure

1. Go to the **Restore** page and click the **Microsoft Entra ID** tile.
2. Click the **Recovery point** tile.
3. In the restore wizard, a calendar displays all the data recovery points. You can choose whether to display the finished with the exception jobs in the calendar by selecting the **Include jobs with only partial backup data** option.
4. Hover over the data recovery point to view the job details, including the job status, job start time, scope name, scope ID, job ID, backup size, and the number of objects in a backup., and click the data recovery point that you want to use in the calendar.
5. Select **Enterprise application** from the object type filter. You can manage the columns to adjust the view of enterprise applications.
6. Select the enterprise applications that you want to restore and then click the **Restore** button.
7. The **View Property** step displays the enterprise application information in a table. Click **Next** to continue the restore.
8. In the **Restore Options** step, select **Merge**, **Overwrite**, or **Skip** as the conflict resolution.

   > **Note:** The restore job can restore the single sign-on (SSO) configuration for the enterprise application directly, if the enterprise application has not yet been permanently deleted. If the enterprise app has been permanently deleted, to restore the SSO configuration for this enterprise app, the **Restore Options** step will display the **Single Sign-On Configuration** field for you to choose to allow IBM® Storage Protect for Cloud to generate an SSO certificate during the restore or you can import the certificate manually. Note that if you choose to allow IBM® Storage Protect for Cloud to generate the certificate, you must download the certificate later from Job Monitor and then send it to your service provider of this enterprise application to update your certificate.

> **Note:** The **Attributes and Claims**, **Identifier (Entity ID)**, **currentSingleSignOnMode**, **ParentAppId**, or**IsCustomApp**of the SSO configuration can only be restored if you have configured a service account with the **Application Administrator** role. of the SSO configuration can only be restored if you have configured a service account with the **Application Administrator** role.
> The roles and administrators directly related to the selected enterprise applications can be restored as well.

9. If a conflict occurs, **Merge** is to add the backup data to the destination for the properties that support adding new items. The existing properties with unique values will be replaced with the backup data. **Overwrite** is to remove the conflicting object from the destination and restore the backup data. **Skip** is to skip the restore of the backup data and keep the destination object intact.
10. You can enter a description for this restore job for further reference.
11. Click **Next** to go to the **Overview** step. Review the restore settings. You can click **Back** to go back to the previous steps in the restore wizard to modify the settings.
12. Click **Restore** to run the restore job.

Restore Administrative Units

To restore administrative units, complete the following steps in the procedure.

Procedure

1. Go to the **Restore** page and click the **Microsoft Entra ID** tile.
2. Click the **Recovery point** tile.
3. In the restore wizard, a calendar displays all the data recovery points. You can choose whether to display the finished with the exception jobs in the calendar by selecting the **Include jobs with only partial backup data** option.
4. Hover over the data recovery point to view the job details, including the job status, job start time, scope name, scope ID, job ID, backup size, and the number of objects in a backup., and click the data recovery point that you want to use in the calendar.
5. Select **Administrative units** from the object type filter. You can manage the columns to adjust the view of administrative units.
6. You can also use the **Search** box to find the specific administrative units.
7. Select the administrative units that you want to restore and then click the **Restore** button.
8. The **View Properties** step will be displayed if you only selected one object to restore. You can view the properties backed up in the selected recovery points for the administrative unit. Click **Next** to continue.
9. In the **Restore Options** step, you can expand the list to view all the selected administrative units, and then select **Merge**, **Overwrite**, or **Skip** as the conflict resolution. Note that the restore job will not restore the groups that have been deleted from the selected administrative units.
   If a conflict occurs, **Merge** is to add the backup data to the destination. **Overwrite** is to remove the conflicting data from the destination and restore the backup data. **Skip** is to skip the restore of the backup data and keep the destination data intact.
10. You can enter a description for this restore job for further reference.
11. Click **Next** to review the restore settings in the **Overview** step.
12. Click **Restore** to run the restore job.

Restore Role and Administrator

Procedure

To restore roles and administrators, follow the steps below:

1. Go to the **Restore** page and click the **Microsoft Entra ID** tile.
2. Click the **Recovery point** tile.
3. In the restore wizard, a calendar displays all the data recovery points. You can choose whether to display the finished with the exception jobs in the calendar by selecting the **Include jobs with only partial backup data** option.
4. Hover over the data recovery point to view the job details, including the job status, job start time, scope name, scope ID, job ID, backup size, and the number of objects in a backup., and click the data recovery point that you want to use in the calendar.
5. Select **Role and administrator** from the object type filter. You can manage the columns to adjust the view of roles and administrators.
6. You can also use the **Search** box to find the specific roles and administrators.
7. Select the roles and administrators that you want to restore, and then click the **Restore** button.
8. The **View properties** step will be displayed if you only selected one object to restore. You can view the properties backed up in the selected recovery point. Click **Next** to continue.
9. In the **Restore options** step, you can expand the list to view all the selected roles and administrators, and then select **Merge**, **Overwrite**, or **Skip** as the conflict resolution.
10. If a conflict occurs, **Merge** is to add the backup data to the destination. **Overwrite** is to remove the conflicting data from the destination and restore the backup data. **Skip** is to skip the restore of the backup data and keep the destination data intact.
11. You can enter a description for this restore job for further reference.
12. Click **Next** to review the restore settings in the **Overview** step.
13. Click **Restore** to run the restore job.

Restore Groups

Before you begin

Before you restore a temporarily deleted group, ensure the IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID service app has the Global Administrator role.

Procedure

To restore groups, follow the steps below

1. Go to the **Restore** page and click the **Microsoft Entra ID** tile.
2. Click the **Recovery point** tile.
3. In the restore wizard, a calendar displays all the data recovery points. You can choose whether to display the finished with the exception jobs in the calendar by selecting the **Include jobs with only partial backup data** option.
4. Hover over the data recovery point to view the job details, including the job status, job start time, scope name, scope ID, job ID, backup size, and the number of objects in a backup., and click the data recovery point that you want to use in the calendar.
5. Select **Groups** from the object type filter. You can manage the columns to adjust the view of groups.
6. You can also use the **Group type** filter and the **Search** box to find the specific **Microsoft 365 Groups**, **Distribution lists**, **Security groups**, or **Mail-enabled security groups**.
7. Select the group that you want to restore, and then click the **Restore** button. You can view the group information in the **View properties** step.

   > **Note:** If you select multiple groups, you can directly configure restore options following the steps below in the **Restore groups** panel.

8. In the **Restore Options** step, you can expand the list to view all the selected groups, choose where you would like to restore the group, and then select **Merge**, **Overwrite**, or **Skip** as the conflict resolution.

If a conflict occurs, **Merge** is to add the backup data to the destination. If you select **Merge** as the restore option for groups, you must also select the **Keep Relationship** in the **Advanced Option** so that the properties in the relationship backed up at the recovery point can be added to the target group. **Overwrite** is to remove the conflicting group from the destination and restore the backup data. **Skip** is to skip the restore of the backup data and keep the destination group intact.

9. In the **Advanced** field, you can select the **Keep membership** option if you would like to restore the members, owners, or group membership. If you also want to restore the license, applications, roles and administrators, and administrative units for the selected groups, select the **Keep more relationships** option.
10. You can enter a description for this restore job for further reference.
11. Click **Next**.
12. If you have chosen to restore the backup data to its original location, you will go to the **Overview** page to review the restore settings and the group that you have selected for restore. Click **Restore** after you finish reviewing the settings; if you have chosen to restore the backup data to another location, you need to configure the destination where you would like to keep the recovered data. Continue with the steps below.
13. In the **Destination** step, select a destination app profile. Configure the **Advanced** options if you select **Merge** as the restore options for groups, to ensure that the properties in the relationship backed up at the recovery point can be added to the target group.
14. Click **Next**.
15. Review the restore settings in the Overview step and click Restore to run the restore job.

Restore Users

Before you begin

> **Note:** Before you restore a temporarily deleted user, ensure the IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID service app has the Global Administrator role.

Procedure

To restore users, follow the steps below:

1. Go to the **Restore** page and click the **Microsoft Entra ID** tile.
2. Click the **Recovery point** tile.
3. In the restore wizard, a calendar displays all the data recovery points. You can choose whether to display the finished with the exception jobs in the calendar by selecting the **Include jobs with only partial backup data** option.
4. Hover over the data recovery point to view the job details, including the job status, job start time, scope name, scope ID, job ID, backup size, and the number of objects in a backup, and click the data recovery point that you want to use in the calendar.
5. Select **User** from the object type filter. You can use **Name** or **User principal name** to find the user. You can also manage the columns to adjust the view of users.
6. Select the user that you want to restore and then click the **Restore** button. You can view the group information in the **View properties** step and then click **Next**. You can also choose to download the user properties and use the script in the downloaded package to automatically add the users to an on-premises active directory. For details, refer to Download User Properties.

   > **Note:** If you select multiple users, you can directly configure restore options following the steps below in the **Restore users** panel.

7. In the **Restore Options** step, you can expand the list to view all the selected users, choose where you would like to restore the user, and then select **Merge**, **Overwrite**, or **Skip** as the conflict resolution.

If a conflict occurs, **Merge** is to add the backup data to the destination for the properties that support adding new items. The existing properties with unique values will be replaced with the backup data. **Overwrite** is to remove the conflicting object from the destination and restore the backup data. **Skip** is to skip the restore of the backup data and keep the destination object intact.

8. If you have chosen to restore the backup data to its original location, you can enter a default password for the users being permanently deleted in the **Password** field and choose whether to force these users to change their password when they first sign in. Enter a description for this restore job for further reference, and then click **Next**to go to the **Overview** page to review the restore settings and the user that you have selected for restore. Click **Restore** after you finish reviewing the settings; if you have chosen to restore the backup data to another location, you need to configure the destination where you would like to keep the recovered data. Continue the steps below.
9. You can enter a description for this restore job for further reference.
10. Click **Next**.
11. In the **Destination** step, select a destination app profile. Configure **the Advanced** options if you select **Merge** as the restore options for groups, to ensure that the properties in the relationship backed up at the recovery point can be added to the target group.
12. In the **Password** field, you can enter a default password for the users being permanently deleted and choose whether to force these users to change their password when they first sign in.
13. Click **Next**.
14. Review the restore settings in the **Overview** step and click **Restore** to run the restore job.

Download User Properties

When restoring users (Restore Users), you can click **Download properties** to directly export the user information of the selected users to a local location. The downloaded ZIP file contains a PowerShell script to help you automatically add the users according to the exported user properties to an on-premises active directory. Follow the steps below:

Procedure

1. Extract the ZIP file and open the **BulkUserCreated.ps1** file.
2. Update the value for **$Domain**, **$UserOu**, and **$defaultPassword** attributes.
3. Save the changes and exit the file.
4. Right-click the **BulkUserCreated.ps1** file, and select **Run with PowerShell** from the drop-down list.
5. The result will be generated in the same folder, or you can check the users in your environment.

Azure Storage

Azure Storage service protects the Azure Blob Storage (including Data Lake Storage) and Azure Files. You can not only restore the backup data to its original location or to a different location but also export the backup data.

Follow the instructions below to perform the restore and you can also refer to Azure Storage section for the supported and unsupported status when restoring the backup data to its original location.

Restore Blob Storage

Procedure

To restore blob containers or blobs, follow the steps below:

1. Go to the **Restore** page and click the **Azure Storage** tile.
2. In the **Restore** wizard, the calendar displays the data recovery points of **Blob storage** by default. You choose whether to display the jobs finished with exceptions in the calendar by selecting the **Include jobs with only partial backup data** option.

3. Hover over the data recovery point to view the job details, including the job status, job start time, scope name, scope ID, job ID, backup size, and the number of objects in a backup.
4. Click the data recovery point that you want to use in the calendar. The objects backed up in the selected backup job are displayed in the table.
5. You can use the **Subscription** filter, **Resource group** filter, and the **Storage account** filter to find the blob containers of specific properties or use the **Search** box to search for blob containers via keywords in the name. You can also manage the columns to adjust the view of blob containers.
6. Find the blob containers that you want to restore or click the blob container to browse down to the blobs.
7. Select the blob container or blob that you want to restore and click **Restore**.
8. In the **Restore options** step, choose where you would like to restore the blob container or blobs, select **Skip** or **Overwrite** as the resolution if a conflict occurs during the restore, and then provide an optional description for further reference.
9. Click **Next**.
10. If you have chosen to restore the backup data to its original location, you will go to the **Overview** page to review the restore settings and the objects that you have selected for restore. Click **Restore** after you finish reviewing the settings; if you have chosen to restore the backup data to another location, you need to configure the destination where you would like to keep the recovered data. Continue with the steps below.
11. In the **Destination** step, select a destination subscription, resource group, region, storage account, and select a location in the storage account to store the restored data.
12. Click **Next**.
13. Review the restore settings in the **Overview** step and click **Restore** to run the restore job.

Restore File Shares

To restore the file shares or the folders or files in the file share, refer to the steps below:

Procedure

1. Go to the **Restore** page and click the **Azure Storage** tile.
2. In the **Restore** wizard, the calendar displays the data recovery points of **Blob storage** by default. Click the **File share** tab.
   You can choose whether to display the jobs finished with exceptions in the calendar by selecting the **Include jobs with only partial backup data** option.
3. Hover over the data recovery point to view the job details, including the job status, job start time, scope name, scope ID, job ID, backup size, and the number of objects in a backup.
4. Click the data recovery point that you want to use in the calendar. The objects backed up in the selected backup job are displayed in the table.
5. You can use the **Subscription** filter, **Resource group** filter, and the **Storage account** filter to find the file shares of specific properties or use the **Search** box to search for file shares via keywords in the name. You can also manage the columns to adjust the view of file shares.
6. Find the file shares that you want to restore or click the file share to browse down to the folders or files.
7. Select the file shares, folders, or files that you want to restore and click **Restore**.
8. In the **Restore Options** step, choose where you would like to restore the file shares, folders, or files, select **Skip** or **Overwrite** as the resolution if a conflict occurs during the restore, and then provide an optional description for further reference.
9. Click **Next**.
10. If you have chosen to restore the backup data to its original location, you will go to the **Overview** page to review the restore settings and the objects that you have selected for restore. Click **Restore** after you finish reviewing the settings; if you have chosen to restore the backup data to another location, you need to configure the destination where you would like to keep the recovered data. Continue with the steps below.

11. In the **Destination** step, select a destination subscription, resource group, region, storage account, and select a location in the storage account to store the recovered data.
12. Click **Next**.
13. Review the restore settings in the **Overview** step and click **Restore** to run the restore job.

Restore Admin Portal Settings

To restore the admin portal settings, note the following:

About this task

- For the settings that can be restored, refer to Admin Portal Settings
- If a setting includes encrypted data or files, the encrypted data and files cannot be restored. You can export the backup data to check the setting.
- If the state of a conditional access policy is On, the restore job will change it to Off, which will be alerted in the job report comment, as well as in Dry run report.

Procedure

Follow the steps below to restore the admin portal settings:

1. Go to the **Restore** page and click the **Admin Portal Settings** tile.
2. In the **Restore** wizard, a calendar displays all the data recovery points. You choose whether to display the finished with the exception jobs in the calendar by selecting the **Include jobs with only partial backup data** option.
3. Hover over the data recovery point to view the job details, including the job status, job start time, scope name, scope ID, job ID, backup size, and the number of objects in a backup.
4. Click the data recovery point that you want to use in the calendar.
5. You can use the following filters to update the view of the backup data:
   - Use the module filter to find the settings for **Microsoft Entra ID**, **Microsoft 365 Defender**, **Intune**, or **Exchange**,
   - Select the **Only show the settings that can be restored** option to filter the backup data for restore.
   - If you want to include the backup data for the PowerShell rules for restore or export, select the **Include rules created by PowerShell** option above the table.
   - Manage the columns to adjust the view of settings.
6. Select the settings that you want to restore and then click the **Restore** button.
7. In the **Restore Options** step, you can choose to run a restore directly or perform a **Dry run** first to review the affected settings in the report.
8. Select **Merge**, **Overwrite**, or **Skip** as the conflict resolution.

   > **Note:** If a conflict occurs, **Merge** is to add the backup data to the destination for the properties that support adding new items. The existing properties with unique values will be replaced with the backup data. For example, the protection settings of Safe links policy that are configured via checkbox field type will be overwritten by the backup data after being restored. **Overwrite** is to remove the conflicting object from the destination and restore the backup data. **Skip** is to skip the restore of the backup data and keep the destination object intact.

9. You can enter a description for this restore job for further reference.
10. Click **Restore** to run the restore job.

Restore Monitored Databases

Procedure

To restore the databases, follow the steps below:

1. Go to the **Restore** page and click the **Azure SQL** tile.
2. In the **Restore** wizard, a calendar displays all the monitoring points. Click **Native Azure SQL backup monitoring.**
   You can choose whether to display the finished with the exception jobs in the calendar by selecting the **Include jobs with only partial backup data** option.
3. Hover over the monitoring point to view the job details, including the job status, job start time, scope name, scope ID, job ID, and the number of objects in a backup.
4. Click a monitoring point in the calendar view the recovery points (PTR and LTR) retrieved for the protected databases.
5. By default, all the native Azure backups for PITR are displayed in the table. The **Earliest recovery point** column displays the earliest available backup, which indicates the retention period that you configured for the PITR backups. You can click the **Point-in-time restore** list to change the backups to **Long-term retention** (LTR) and use the Subscription filter and Resource group filter to find the databases that you want to restore. You can also manage the columns to adjust the view of databases.
6. Select a PITR/LTR recovery point that you want to restore.
7. Click the **Restore** button.
8. In the **Restore Options** step, select how to restore the database. You can choose to replace the existing database or create a new database. If you choose to create a new database, you need to provide a new database name in the **Destination** step.
9. You can enter a description for this restore job for further reference. Click **Next**.
10. If you choose to create a new database, enter a new database name in the **Destination** step. Otherwise, you will go to the **Overview** step.
11. Review the restore settings in the **Overview** step. You can click **Back** to go back to the previous steps in the restore wizard to modify the settings.
12. Click **Restore** to run the restore job.

Restore Backup Databases

About this task

To restore the databases, follow the steps below:

Procedure

1. Go to the **Restore** page and click the **Azure SQL** tile.
2. In the **Restore** wizard, a calendar displays all the data recovery points. Click **Azure SQL backup**.
   You can choose whether to display the finished with the exception jobs in the calendar by selecting the **Include jobs with only partial backup data** option.
3. Hover over the data recovery point to view the job details, including the job status, job start time, scope name, scope ID, job ID, and the number of objects in a backup.
4. Click a data recovery point in the calendar. The Azure SQL databases backed up in the selected backup job are displayed in the table.
5. You can use the **Subscription** filter and **Resource group** filter to find the databases or use the **Search** box to search for databases via keywords in the name. You can also manage the columns to adjust the view of databases.
6. Select the database that you want to restore and click **Restore**.
7. In the **Restore options** step, select how to restore the database. You can choose to replace the existing database or create a new database. If you choose to create a new database, you need to provide a new database name in the **Destination** step.

8. Review the restore settings in the **Overview** step. You can click **Back** to go back to the previous steps in the restore wizard to modify the settings.
9. Click **Restore** to run the restore job.

Restore Azure DevOps Organizations

Procedure

To restore the organizations, follow the steps below:

1. Go to the **Restore** page and click the **Azure DevOps** tile.
2. In the **Restore** wizard, a calendar displays all the data recovery points. You choose whether to display the finished with the exception or failed jobs in the calendar by selecting the **Include jobs with only partial backup data** option.
3. Hover over the data recovery point to view the job details, including the job status, job finished time, scope name, scope ID, job ID, backup size, and the number of objects in a backup.
4. Click the data recovery point that you want to use in the calendar. The organizations backed up in the selected backup job are displayed in the table.
5. Click the organizations to drill down to the items that you want to restore, select the items, and then click the **Restore** button.
6. In the **Restore options** step, you can select **Merge**, **Overwrite**, or **Skip** as the conflict resolution.
   Note the following:
   - If a conflict occurs, **Merge** is to add the backup data to the destination for the properties that support adding new items. The existing properties with unique values will be replaced with the backup data. For example, the protection settings of Safe links policy that are configured via checkbox field type will be overwritten by the backup data after being restored. **Overwrite** is to remove the conflicting object from the destination and restore the backup data. **Skip** is to skip the restore of the backup data and keep the destination object intact.
   - The deleted organizations cannot be restored.
7. You can enter a description for this restore job for further reference. Click **Next**.
8. Review the restore settings in the **Overview** step. You can click **Back** to go back to the previous steps in the restore wizard to modify the settings.
9. Click **Restore** to run the restore job.

Azure AD B2C

Azure AD B2C service protects app registrations, identity providers, user attributes, user flows, and users. You can restore the backup data to its original location.

Follow the instructions below to perform the restore and you can also refer to Azure AD B2C section for the supported and unsupported status when restoring the backup data to its original location.

Restore App Registrations

Procedure

To restore app registrations, follow the steps below:

1. Go to the **Restore** page and click the **Azure AD B2C** tile.
2. In the **Restore** wizard, a calendar displays all the data recovery points. You choose whether to display the finished with the exception jobs in the calendar by selecting the **Include jobs with only partial backup data** option.
3. Hover over the data recovery point to view the job details, including the job status, job start time, scope name, scope ID, job ID, backup size, and the number of objects in a backup, and click the data recovery point that you want to use in the calendar.
4. Select **App registration** from the object type filter. You can manage the columns to adjust the view of app registrations.
5. You can also use the **Search** box to find the specific app registrations.
6. Select the app registration that you want to restore and then click the **Restore** button.
7. In the **Restore app registrations** panel, select **Merge**, **Overwrite**, or **Skip** as the conflict resolution.

> **Note:** If a conflict occurs, **Merge** is to add the backup data to the destination for the properties that support adding new items. The existing properties with unique values will be replaced with the backup data. **Overwrite** is to remove the conflicting object from the destination and restore the backup data. **Skip** is to skip the restore of the backup data and keep the destination object intact.

8. You can enter a description for this restore job for further reference and click **Restore** to run the restore job.

Restore Identity Providers

Procedure

To restore identity providers, follow the steps below:

1. Go to the **Restore** page and click the **Azure AD B2C** tile.
2. In the **Restore** wizard, a calendar displays all the data recovery points. You choose whether to display the finished with the exception jobs in the calendar by selecting the **Include jobs with only partial backup data** option.
3. Hover over the data recovery point to view the job details, including the job status, job start time, scope name, scope ID, job ID, backup size, and the number of objects in a backup, and click the data recovery point that you want to use in the calendar.
4. Select **Identity provider** from the object type filter. You can manage the columns to adjust the view of identity providers.
5. You can also use the **Search** box to find the specific identity providers.
6. Select the identity provider that you want to restore and then click the **Restore** button.
7. In the **Restore identity provider** panel, select **Overwrite** or **Skip** as the conflict resolution.

> **Note:** If a conflict occurs, **Overwrite** is to remove the conflicting object from the destination and restore the backup data. **Skip** is to skip the restore of the backup data and keep the destination object intact.

8. You can enter a description for this restore job for further reference and click **Restore** to run the restore job.

Restore User Attributes

Procedure

To restore user attributes, follow the steps below:

1. Go to the **Restore** page and click the **Azure AD B2C** tile.
2. In the **Restore** wizard, a calendar displays all the data recovery points. You choose whether to display the finished with the exception jobs in the calendar by selecting the **Include jobs with only partial backup data** option.
3. Hover over the data recovery point to view the job details, including the job status, job start time, scope name, scope ID, job ID, backup size, and the number of objects in a backup, and click the data recovery point that you want to use in the calendar.
4. Select **User attribute** from the object type filter. You can manage the columns to adjust the view of user attributes.
5. You can also use the **Search** box to find the specific user attributes.
6. Select the user attribute that you want to restore and then click the **Restore** button.
7. In the **Restore user attribute** panel, select **Overwrite** or **Skip** as the conflict resolution.

> **Note:** If a conflict occurs, **Overwrite** is to remove the conflicting object from the destination and restore the backup data. **Skip** is to skip the restore of the backup data and keep the destination object intact.

8. You can enter a description for this restore job for further reference and click **Restore** to run the restore job.

Restore User Flows

Procedure

To restore user flows, follow the steps below:

2. In the **Restore** wizard, a calendar displays all the data recovery points. You choose whether to display the finished with the exception jobs in the calendar by selecting the **Include jobs with only partial backup data** option.
3. Hover over the data recovery point to view the job details, including the job status, job start time, scope name, scope ID, job ID, backup size, and the number of objects in a backup, and click the data recovery point that you want to use in the calendar.
4. Select **User flow** from the object type filter. You can manage the columns to adjust the view of user attributes.
5. You can also use the **Search** box to find the specific user attributes.
6. Select the user attribute that you want to restore and then click the **Restore** button.
7. In the **Restore user attribute** panel, select **Overwrite** or **Skip** as the conflict resolution.

> **Note:** If a conflict occurs, **Overwrite** is to remove the conflicting object from the destination and restore the backup data. **Skip** is to skip the restore of the backup data and keep the destination object intact.

8. You can enter a description for this restore job for further reference and click **Restore** to run the restore job.

Restore Users

Procedure

To restore users, follow the steps below:

1. Go to the **Restore** page and click the **Azure AD B2C** tile.
2. In the **Restore** wizard, a calendar displays all the data recovery points. You choose whether to display the finished with the exception jobs in the calendar by selecting the **Include jobs with only partial backup data** option.
3. Hover over the data recovery point to view the job details, including the job status, job start time, scope name, scope ID, job ID, backup size, and the number of objects in a backup and click the data recovery point that you want to use in the calendar.
4. Select **User** from the object type filter. You can manage the columns to adjust the view of users.
5. You can also use the **Search** box to find the specific users.
6. Select the user that you want to restore and then click the **Restore** button.
7. In the **Restore users** panel, select **Merge**, **Overwrite**, or **Skip** as the conflict resolution.

> **Note:** If a conflict occurs, **Merge** is to add the backup data to the destination for the properties that support adding new items. The existing properties with unique values will be replaced with the backup data. **Overwrite** is to remove the conflicting object from the destination and restore the backup data. **Skip** is to skip the restore of the backup data and keep the destination object intact.

8. Enter a default password for the users being permanently deleted in the **Password** field and choose whether to force these users to change their password when they first sign in.
9. You can enter a description for this restore job for further reference and click **Restore** to run the restore job.

Export and Download Your Data

You can export and download your backup data of storage, folders, files, VM files, Microsoft Entra audit logs/ sign-in logs, or the Admin Portal Settings. After you perform the export job, go to the **Job monitor** to download the exported data to a local location. You must download the exported data in 7 days. Otherwise, the data will expire and cannot be downloaded.

About this task

A password is used to protect your exported data. After the data has been successfully exported, go to the Job Monitor to download the exported data in ZIP and get the password for extracting the exported data.

There is a monthly limitation of 500 GB of content that can be exported respectively for the Azure VM and Azure Storage. The **Export** button will be disabled if you've reached the limit.

Note the following:

- For Admin Portal Settings, you can export the backup data of the components to a JSON file.
- You can configure a set of email notification settings for the restore and export jobs, separate from the backup. For details, refer to Configure Notifications.
- The file-level export job for Azure VMs supports both VMs of Linux system and Windows system. If you would like to perform file-level data exportation of Azure VM backup data, you must have generated an index for the backup data. You can either enable the index generation during a backup when configuring the backup scope or generate the index directly from the Restore wizard before performing the export. Note that generating index for the disks with over 8 TB size is also supported
- The index generation for the following file systems is unsupported: **UFS – BSD default fs**, **ZFS – BSD alternative fs**, **BitLocker – Windows encrypted fs**, **LUKS – Linux encrypted fs**, **ReFS – Windows new fs**. Running index generation on these file systems will result in folders without indexes in restore recovery points.

To export the backup data, follow the steps below:

1. After you click the data recovery point in the calendar, the **Restore to recovery point** page appears. The objects backed up in the selected backup job are displayed in the table.
2. You can use the **Tenant** filter, **Subscription** filter, and **Resource group** filter to find the objects of specific properties or use the **Search** box to search for objects via keywords in the name.
3. Find the VM, blob container, file share where the data you want to export resides and drill down. Note the following:
   - The Audit log and Sign-in log of Microsoft Entra tenant support being exported after January 2023 release. You can go to the Microsoft Entra ID restore service and select the **Audit log** or **Sign-in log** from the filter to find the data you want to export and start an export job.
4. Select the storage, folders, files, log files, or Admin Portal Settings that you want to export.

   > **Note:** To perform the file-level export of Azure VM backup, you must have generated the index. If the backup scope has not enabled the index generation during a backup job, you can click the **Generate index** button in the Restore wizard to generate an index. Note that generating index for the Azure VM disks with over 8 TB size is also supported, but it is not supported for those with over 8 TB size. You can go to **Job monitor** to check the progress of the index job and download the job report. When the index generation is completed, you can go back to perform the file-level export.

5. Click **Export** to perform the export job. You must download the exported data in 7 days. Otherwise, the exported data will expire, and you cannot download it anymore.

Download the Exported Data

Follow the steps below to download the exported data:

1. Go to **Job monitor** and use the **Filters** or the Search box to find the export job record.
2. Click the **More actions** (•••) button next to the job record and click **Download content**.
3. In the **Download content** panel, click the Copy (⧉) button next to the password to copy it to your clipboard for decrypting your exported data
4. Click **Download** button in the Download content step.
5. Save the exported data to your desired location.

Generate and Download a Job Report

About this task

The **Job monitor** page displays the user activities of backup, restore, and export. You can use the **Filters** (such as, **Job type**, **Service type**, **Object type**, **Job status** and **Date range**) or the **Search** box to search for the backup, restore, and export jobs.

For the export jobs, you can download the exported content in a ZIP file after the job is completed and get the password from **Job monitor** to extract the ZIP file. For details, refer to Download the Exported Data.

Procedure

To generate and download a job report, follow the steps below:

1. Go to the **Job monitor** page.
2. You can use the search box or the **Filters** feature to find the job. You can also customize the view by adjusting the columns in display.
   - In the search box, enter the keyword in object name, job ID, or description (for restore jobs) to search for the jobs.
   - Click **Filters** and use the **Job type**, **Service type**, **Object type**, **Job status**, and **Date range** filters to find the jobs for which you want to generate report.
3. You can click the job ID to view the job details first or click the More actions (•••) button next to the job record directly to find the **Generate report** action.

   In the **Job details** panel, you can also click the More actions (•••) button to find the **Generate report** action.
4. After the job to generate report is completed, a blue dot will be displayed on the More actions (•••) button. Click the button and click **Download report** action from the list to download the generated report.
5. Save the job report to a local location.

Account Management

Example

Account Management is defined for permission management with security groups. To cater to the diverse administrative needs, administrators can create security groups with a custom permission scope, which can dive down to the specific functions of each service, such as Backup, Restore, and Export. The standard users added to a security group can inherit the group permissions automatically.

Administrators group is the built-in group that has all permissions in IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID. You cannot remove this group or update its permissions.

> **Note:** The users who have been designated as service administrators of IBM® Storage Protect for Cloud and the application administrators of IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID will be automatically synchronized to the **Administrators** group. If the user is demoted from the application administrator to a standard user, IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID will not automatically remove this user from the **Administrators** group. If you no longer want to grant this user the full control to the application, you must manually remove the user from the **Administrators** group.

Create a Security Group

To manage user permissions more efficiently, you can create a security group for a set of users and configure the group permissions. The users within this group will inherit the group permissions automatically.

Follow the steps below to create a security group:

1. Navigate to **Settings** > **Account management**.
2. Click **Create**.
3. In the **Create a security group** panel, complete the following settings:
   - **Name** – Enter a name for this security group.
   - **Description** – Enter a description for this security group for future reference. This field is optional.
   - **Invite users/groups** – Enter the email addresses of the users or groups that you want to add to this group. The users/groups you want to add to this group must have at least the Standard user permission to IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID. For details on adding a standard user through IBM® Storage Protect for Cloud, refer to Add Users.
   - **Grant permissions** – Turn on the switch next to the service that you want to allow this group to access and select the tenant and functionalities, such as **Backup**, **Restore**, **Export** to grant the specific permission.

     > **Note:** The region section is required for Azure VM, Azure storage, Azure SQL backup and native Azure SQL backup monitoring services.
4. Click **Save** to save this security group or click **Cancel** to exit this panel without saving.

Reports

IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID currently provides subscription consumption report and backup analysis report and system auditor report.

- **Subscription consumption** – Monitors the subscription details, status, and usage.
- **Backup analysis** – Displays the backup statistics and analysis on your enabled services.
- **System auditor** – Tracks the user activities in the application.

View Subscription Consumption Report

Click **Subscription** on the left navigation to view the subscription consumption report. The **Subscription consumption** report shows your subscription details, status, storage consumption statistics, and utilization of your enabled services. You can also click **Download PDF report** to download the PDF of the subscription consumption report.

You can check the following sections in the subscription consumption report:

- The **Subscription details** section displays the subscription information of enabled services and the amount of purchased capacity (TB)/user seats/instances/virtual machines/projects/databases.
- The **Storage consumption overview** section displays the total amount of purchased capacity and the consumed capacity of each service.

View Backup Analysis Report

Click **Backup analysis** on the left navigation to view the backup analysis report. On the **Backup analysis** page, you can view the backup statistics and analysis for the Microsoft Entra ID, Azure AD B2C, Azure VM, and Azure Storage, Azure DevOps, Azure SQL databases, and the used space in total and in each storage profile of the top 4

- The **Protected Microsoft Entra ID trend** section displays the trend of the objects in the Microsoft Entra tenant getting protected. You can hover over the dot in the chart to view the number of App Registrations, Enterprise Applications, Administrative Units, Roles and Administrators, Groups, and Users being protected on a specific backup date.
- The **Protected Azure AD B2C trends** section displays the trend of the objects in the Microsoft Entra tenant getting protected. You can hover over the dot in the chart to view the number of App Registrations, Identity Providers, User Attributes, User Flows, and Users being protected on a specific backup date.
- The **Protected virtual machines** section displays the total number of Azure VMs/Amazon EC2 instances that are available for protection, the number of Azure VMs/Amazon EC2 instances currently being protected or out of protection, and the number of accounts, tenants, subscriptions, and resource groups related to these protected or unprotected Azure VMs/Amazon EC2 instances.
- The **Protected Azure Storage** section displays the total number of the Blob containers and File shares available for protection, and the number of these storages and storage accounts currently being protected or out of protection.
- The **Protected Azure DevOps** section displays the total number of organizations and projects that are available for protection, the number of organizations and projects currently being protected or out of protection.
- The **Protected Azure SQL databases** section displays the following data of Native Azure SQL backup monitoring service and Azure SQL backup service: the total number of databases that are available for protection, the number of databases currently being protected or out of policy, and the number of tenants related to these protected or unprotected databases.

You can also click **Download PDF report** to download the PDF of the backup analysis report.

View System Auditor Report

Click **System auditor** on the left navigation to view the user activities in IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID.

You can perform the following actions on the records of user activities:

- Use the **Filters** (such as **Operation**, **Object type**, and **Date range**) to filter the records.
- Use the **Columns** (such as **Type**, **Username**, **IP address**, **Operation**, and **Event**) to customize the view of System auditor records.
- Use the **Search** box to search for the activities by username.

  > **Note:** Searching only supports entering the full username.

- Click the **View** link next to an event to go to the **View details** panel to view the changes. The changes will be highlighted for easy reference.
- Export the System auditor records. Follow the steps below:

  a. Click **Export**. The **Export** window appears.

  b. You can select the **Last 7 days** option or the **Last 30 Days** option as the time range for the export.

  c. Click **Export**. The audit report will be exported to your browser’s download location. Click **Cancel** to cancel the export.

View Notifications

Example

You can click the **Notification center** (🔔) button on the upper-right corner to view subscription expiration alerts, out of policy alerts, and BYOS alerts.

- **Subscription expiration alert**– If your backup service in the trial will expire in 7 days, a subscription expiration alert will be displayed in the notification center to inform you. If your backup service with enterprise subscription will expire in 30 days, a subscription expiration alert will be displayed in the notification center to inform you.
- **Out of policy alert** – When any backup service exceeds your subscription, an out of policy alert will be displayed in the notification center to inform you.
- **BYOS alert** – If you purchased a subscription for BYOS, a BYOS alert will be displayed in the notification center to inform you to update the BYOS storage configuration.

Troubleshooting Error Codes

CO-NoEnoughPermissionInCustomApp

Details:

Insufficient permissions of the app profile. Please verify the permissions of the app in the custom app profile that you created for IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID.

Solutions:

Check the API permissions that the custom Azure app has been consented with in the Microsoft Entra admin center. For the list of the required API permissions for the data that you want to protect, refer to the table in the Default Permissions Granted to the Service App section.

AS-NoPermission

Details:

IBM has no permission to access your storage account. Please check your firewall for whether the IBM reserved IP addresses or ARM virtual networks have been added as the trusted.

Solutions:

Verify whether the Delegated app that you use to protect this Azure storage has the required API permissions. For details, refer to Enable the Backup for Azure Virtual Machines, Azure Storage, and Azure SQL.

Check your firewall for whether the IBM reserved IP addresses or ARM virtual networks have been added as the trusted. For details, refer to Allow IBM Storage Protect for Cloud Agent Servers to Access Your Storage Account.

APS-NoServiceAccount

Details:

Some properties are not backed up or restored as there are no valid service accounts configured in IBM® Storage Protect for Cloud.

Solutions:

To protect the Group General Settings using the Admin Portal Settings service, a service account with the Cloud Application Administrator role is required. For detailed instructions, refer to Create a Service Account Profile.

APS-NoIntuneLicense

Details:

The Microsoft Intune license is invalid or expired. Please check your license in Microsoft 365 or exclude the related settings from backup.

Solutions:

To protect the Intune components using the Admin Portal Settings service, you must have active Microsoft Intune license. If you believe that you're getting this message in error, contact IBM Software Support for assistance.

APS-NoDefenderForOffice365

Details:

No Microsoft Defender for Office 365 subscription is active in your tenant. Please verify your subscription and try again.

Solutions:

To protect the Microsoft Defender components using the Admin Portal Settings service, you must have an active Microsoft Defender for Office 365 subscription. If there are no components in your Microsoft Defender, you can edit your backup scope to exclude the Defender objects.

APS-NoADMXFile

Details:

The object is not restored because the ADMX file on which it was based has been deleted.

Solutions:

Import the ADMX file to your Microsoft Intune and try to perform the restore job again.

AAD-NoEnoughPermissions

Details:

Insufficient permissions of the app profile. Please re-authorize the service app or verify the permissions of the app in the custom Azure app profile that you created for IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID.

Solutions:

The required app permissions have been updated. Please re-authorize the service app profile or manually update the app permissions of the custom Azure app that you are using. For details on re-authorizing an app, refer to Re-authorize an App Profile.

AAD-RestrictedAdminUnit

Details:

Insufficient permissions. This object is a member of a restricted management administrative unit and can only be managed by administrators scoped for that administrative unit. Please remove the object from the administrative unit and try again.

Solutions:

To protect the objects using the Microsoft Entra ID service, ensure they are removed from restricted management administrative units before restoring.

VM-ExtensionScriptExist

Details:

The custom script extension of type “CustomScriptExtension” or “CustomScript” already exists.

Solutions:

Remove the existing custom script extension of type “CustomScriptExtension” or “CustomScript” from Azure VMs before restoring.

Use Public APIs for Job Information

You can use the IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID Public APIs to retrieve the backup job information and monitor the performance of your enabled backup services.

Refer to the following for how to use Public APIs to get backup job information. To learn more, you can also refer to this SDK: SDK-SAMPLE

Note the following before you get started:

- To use the IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID Public APIs, you must at first go to the **IBM® Storage Protect for Cloud › Administration › App registrations** page to register an app with **PlatformBackup.ReadWrite.All** permission. For details, refer to Configure App Registrations.
- After you registered the app, get the access token to authenticate with IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID Public API. For details, refer to "Gets Access Token" on page 114.
- Use the *POST api/public/jobreport* API to retrieve the backup job information. For details, refer to "Gets Job Information" on page 115.
- You will also need the Web API URL to use the IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID Public APIs. The API URL varies with your data center. Refer to the list below for the API URL of your data center.

Data Center	Web API URL
Canada Central (Toronoto)	https://graph-ca.sp4c.storage-defender.ibm.com/backup/vm
Germany West Central (Frankfurt)	https://graph-de.sp4c.storage-defender.ibm.com/backup/vm
East US (Virginia)	https://graph-us.sp4c.storage-defender.ibm.com/backup/vm
UK South (London)	https://graph-uk.sp4c.storage-defender.ibm.com/backup/vm
Switzerland North (Zurich)	https://graph-ch.sp4c.storage-defender.ibm.com/backup/vm
Australia East (New South Wales)	https://auea-graph.sp4c.storage-defender.ibm.com/backup/vm

Gets Access Token

Gets the access token to authenticate with IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID Public API. To get the access token, specify the following attributes:

Element	Description
identityServiceUrl	For Commercial environment, use: • https://identity.sp4c.storage-defender.ibm.com
clientId	Specifies the application (client) ID of the app you registered through IBM® Storage Protect for Cloud > **Administration** > **App registrations**.
scope	Specifies the permission that has been granted to the app. For IBM® Storage Protect for Cloud Azure VMs, Storage, and Entra ID, the value is **platformbackup.readwrite.all**.
certificateThumbprint	The thumbprint of the corresponding .pfx certificate file of the .cer certificate you used when registering the app.

Element	Description
TokenLifetimeInMinutes	Specifies an expiration time for the retrieved token. The unit of time is Minute.

Example

```
Var identityServiceUrl = <"{https://identity.ibmstorageprotectforcloud.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)
},
Scope = "platformbackup.readwrite.all",
}
if (tokenResponse.IsError)
{
return;
}
return tokenResponse.Json
private static string CreateClientAuthJwt(DiscoveryDocumentResponse response)
{
var clientId = "{Client ID}";
var certificateThumbprint = "{Certificate Thumbprint}";

// Sets the token to expire in 5 minutes.
var tokenHandler = new JwtSecurityTokenHandler { TokenLifetimeInMinutes = 5 };

var securityToken = tokenHandler.CreateJwtSecurityToken(
issuer: clientId,
audience: response.TokenEndpoint,
subject: new ClaimsIdentity(
new List<Claim> { new Claim("sub", clientId),
new Claim("jti", Guid.NewGuid().ToString())}),
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;
}
```

Gets Job Information

Use the *POST api/public/jobreport* API to retrieve the backup job information.

Element	Description	Type	Required
StartTime	Sets a start time (UTC time) for the time range.	long	Yes
FinishTime	Sets a start time (UTC time) for the time range.	long	Yes

Element	Description	Type	Required
JobType	Sets a start time (UTC time) for the time range.	Enum Valid values: 1 (for Azure VM Backup) 128 (for Microsoft Entra ID Backup) 1024 (for Azure Storage Backup) 20003 (for Admin Portal Settings Backup) 20012, 20016 (for Azure SQL Backup) 20019 (for Azure AD B2C Backup)	Yes
ServiceType	Sets the service type of the jobs to get.	Enum Valid values: 1 (for Azure VM) 2 (for Microsoft Entra ID) 4 (for Azure Storage) 64 (for Admin Portal Settings) 512 (for Azure SQL) 4096 (for Azure AD B2C)	Yes
SearchText	Searches by job ID or description.	string	No
PageNumber	Sets the starting number of the page to get the jobs. The default value is 0.	int	Yes
PageSize	Sets the number of jobs to display on one page. The default value is 10.	int	Yes

Example

```
var apiRequestUrl= "{API URL}/api/public/jobreport";
var request = "{\"SearchText\":\"\",\"ServiceType\":0,\"JobType\":0,\"Pagination\":
{\"PageNumber\":0,\"PageSize\":0},\"StartTime\":0,\"FinishTime\":0}"
var requestBearerToken = "{Request Token}";
using (var client = new HttpClient())
{
client.DefaultRequestHeaders.Add("Authorization", "Bearer" + requestBearerToken);
var response = client.PostAsync(apiRequestUrl, new StringContent(request, Encoding.UTF8,
"application/json")).Result;
if (response.IsSuccessStatusCode)
{
var result = response.Content.ReadAsStringAsync().Result;
}
}
```

Supported and unsupported data types

Azure VM

Azure Virtual Machines restore service supports restoring the VMs, disks, or files to original locations, or to another location with different settings. The file-level export job for Azure VMs supports both VMs of Linux system and Windows system, and the file-level export/index generation is also supported for the disks with over 8 TB size. Refer to the following tables for the supported and unsupported properties or settings in the data recovery.

VM Compute

Table 13: VM Compute

VM Compute	Restore to original	Restore to another location or with different settings
VM Size	Supported	Supported
VMs in Availability Sets	Supported	Supported
VMs in Availability Zones	Supported	Supported
VMs that are deployed with Hybrid Use Benefit	Supported	Supported
VMs that are deployed from Azure Marketplace	Supported	Supported
VMs that are deployed from a custom image	Supported	Supported
VMs that are migrated to Azure	Supported	Supported
Diagnostic Settings	Unsupported	Unsupported
Gen2 VM	Supported	Supported
VMs with locks	Unsupported	Unsupported
Spot VMs	Unsupported	Unsupported
Scale Sets	Unsupported	Unsupported

VM Settings

Table 14: VM Settings

VM Settings		Restore to original	Restore to another location or with different settings
Basic	Subscription	Supported	Supported
	Resource Group	Supported	Supported
	Virtual Machine Name	Supported	Supported
	Region	Supported	Supported
	Image (Associated with OS disk)	Supported	Supported
	Azure Spot Instance	Unsupported	Unsupported
	Size	Supported	Supported

VM Settings			Restore to original	Restore to another location or with different settings
	Username		Supported	Supported
	Password		Supported	Supported
	Inbound port rules		Supported	Supported
	Licensing		Unsupported	Unsupported
	Scale Sets		Unsupported	Unsupported
Disks	VM disk encryption	Encryption at host	Supported	Supported
	OS disk type	Premium SSD	Supported	Supported
		Standard SSD	Supported	Supported
		Standard HDD	Supported	Supported
	Encryption type		Supported	Supported
	Managed/Unmanaged disks **Note:** The Unmanaged disk can be restored as an Unmanaged or Managed disk, but the Managed disk can only be restored as a Managed disk.		Supported	Supported
	Shared disk		Unsupported	Unsupported
	Temporary disk		Unsupported	Unsupported
Networking	Virtual network		Supported	Supported
	Subnet		Supported	Supported
	Public IP		Supported	Supported
	Network security group		Supported	Supported
	Accelerated networking		Unsupported	Unsupported
	Load balancing		Supported	Supported
Management	Boot diagnostics		Unsupported	Unsupported
	Enable OS guest diagnostics		Unsupported	Unsupported
	Diagnostics storage account		Unsupported	Unsupported
	System assigned managed identity		Unsupported	Unsupported
	Login with Azure AD		Unsupported	Unsupported
	Auto-shutdown		Unsupported	Unsupported
	Enable backup		Unsupported	Unsupported
	Guest OS updates		Unsupported	Unsupported
Advanced	Extensions		Unsupported	Unsupported
	Custom data		Unsupported	Unsupported
	User data		Unsupported	Unsupported
	Host group		Unsupported	Unsupported
	Proximity placement group		Unsupported	Unsupported
	VM generation		Supported	Supported
Tags			Unsupported	Unsupported

Microsoft Entra ID

The backup service for Microsoft Entra ID supports protecting the app registrations, enterprise applications, administrative units, roles and administrators, groups, users, device – bitLocker recovery keys, audit logs, and sign-in logs.

Microsoft Entra ID data recovery supports restoring the app registrations, enterprise applications, administrative units, and roles and administrators to the original location. It also supports restoring groups and users to the original location or to a new location. Refer to the tables below for supported and unsupported components and attributes of the object types you can protect in the Microsoft Entra ID.

Microsoft Entra ID service supports protecting the Device – BitLocker Recovery Keys. You can copy the BitLocker key from the backup. After December 2023 release, the Microsoft Entra ID service can also protect the extension attributes of the following objects: Users, Groups, Administrative Units, App Registrations, and Devices.

> **Note:** Due to the API limitation that some properties stored outside of the main data store for the resource are not supported as part of change tracking, the changes of some properties cannot be detected for incremental backup. Only a full backup can cover such changes. For more details on the limitation, refer to the Microsoft article: Change Tracking.

App Registration

Refer to the table below for the data recovery state for app registrations

- The **Photo** and **Secrets** cannot be kept. The restore job will generate new secrets and key IDs and will record the information in the job report..
- For certificates, the federated credentials cannot be restored.
- The **Created date** and the **Created on behalf of** cannot be restored.

Component	**Details**
Branding	Supported
Authentication	Supported
Certificates& Secrets	Unsupported
Token configuration	Supported
API permissions	Partially Supported **Note:** The API grant status is currently unsupported.
Expose an API	Supported
App roles	Supported
Owners	Supported
Roles and administrators	Unsupported
Manifest	Unsupported
Extension attributes	Supported

Object Attributes

Attributes	Status	Comment
publisherDomain	Supported	
requiredResourceAccess	Supported	
signInAudience	Supported	
spa	Supported	
tags	Supported	
tokenEncryptionKeyId	Supported	
verifiedPublisher	Supported	
web	Supported	
createdOnBehalfOf	Unsupported	
deletedDateTime	Supported	
publicClient	Supported	
passwordCredentials	Supported	
parentalControlSettings	Supported	
optionalClaims	Supported	
addIns	Supported	
api	Supported	
appId	Partially Supported	The appId can be kept if the app has not yet been permanently deleted from your Microsoft Entra tenant.
applicationTemplateId	Unsupported	
createdDateTime	Partially Supported	The createdDateTime can be kept if the app has not yet been permanently deleted from your Microsoft Entra tenant.
description	Supported	
disabledByMicrosoftStatus	Supported	
identifierUris	Supported	
info	Supported	
isDeviceOnlyAuthSupported	Supported	
isFallbackPublicClient	Supported	
keyCredentials	Supported	
notes	Supported	
groupMembershipClaims	Supported	
Name	Supported	
Logo	Unsupported	
Home page URL	Supported	
Terms of service URL	Supported	
Privacy statement URL	Supported	
Service management reference	Unsupported	
OAuth 2.0 authorization endpoint (v2)	Unsupported	
OAuth 2.0 token endpoint (v2)	Unsupported	

Attributes	Status	Comment
OAuth 2.0 authorization endpoint (v1)	Unsupported	
OAuth 2.0 token endpoint (v1)	Unsupported	
OpenID Connect metadata document	Unsupported	
Microsoft Graph API endpoint	Unsupported	
Federation metadata document	Unsupported	
WS-Federation sign-on endpoint	Unsupported	
SAML-P sign-on endpoint	Unsupported	
SAML-P sign-out endpoint	Unsupported	

Enterprise Application

Refer to the table below for the data recovery state for enterprise applications:

Note that the following properties cannot be restored:

- App owner organization ID
- Sign-in audience
- Key credentials
- Oauth2 permission scope

Component	Details
Properties	Supported
Owners	Supported
Roles and administrators	Unsupported
Users and groups	Supported
Single sign-on	Supported
Provisioning	Supported
Application proxy	Unsupported
Self-service	Unsupported

Object Attributes

Attribute	Status	Comment
accountEnabled	Supported	
addIns	Supported	
alternativeNames	Supported	
appDescription	Supported	
appId	Supported	
applicationTemplateId	Supported	
appOwnerOrganizationId	Supported	
appRoleAssignmentRequired	Supported	
description	Supported	
disabledByMicrosoftStatus	Supported	

Attribute	Status	Comment
homepage	Supported	
keyCredentials	Partially Supported	The attribute relates to the SSO configuration of the enterprise application. If the enterprise application has not yet been permanently deleted, the setting can be restored. Otherwise, you have to choose to allow IBM to generate a certificate for SSO configuration or import the certificate manually while configuring restore settings.
loginUrl	Supported	
logoutUrl	Supported	
notificationEmailAddresses	Supported	
oauth2PermissionScopes	Supported	
passwordCredentials	Partially Supported	The passwordCredentials can be kept if the app has not yet been permanently deleted from your Microsoft Entra tenant.
preferredSingleSignOnMode	Supported	
preferredTokenSigningKeyThumbprint	Supported	
replyUrls	Supported	
samlSingleSignOnSettings	Supported	
servicePrincipalNames	Supported	
servicePrincipalType	Supported	
signInAudience	Supported	
tags	Supported	
tokenEncryptionKeyId	Supported	
Name	Supported	
Object ID	Partially Supported	The object ID can be kept if the app has not yet been permanently deleted from your Microsoft Entra ID.
Enabled for users to sign-in	Supported	
Logo	Supported	
Assignment required	Supported	
Visible to users	Supported	
Notes	Supported	
Permission	Partially Supported	The admin consented permissions can be kept if the app has not yet been permanently deleted from your Microsoft Entra tenant.

Administrative Units

Table 19: Administrative Units

Data Type	Status
Properties	Supported
Users	Supported
Groups	Supported
Devices	Supported
Roles and administrators	Unsupported
Extension attributes	Supported
membershipRule	Supported
membershipType	Supported
membershipRuleProcessingState	Supported

Object Attributes

Table 20: Object Attributes

Attribute	Status
Description	Supported
Visibility	Supported

Roles and Administrators

Table 21: Roles and Administrators

Object Type	Status
Assignment	Supported **Note:** Currently, only the eligible assignments and active assignments are supported. The expired assignments are unsupported.
Description	Supported
Role settings	Supported

Object Attributes

Table 22: Object Attributes

Attributes	Status
description	Supported
isBuiltIn	Supported

Attributes	Status
isEnabled	Supported
rolePermissions	Supported
templateId	Partially Supported **Note:** The templateId can be kept if the roles and administrators have not yet been permanently deleted from your Microsoft Entra tenant.
version	Supported
visibility	Supported

Groups

Refer to the table below for the data recovery state for groups:

- The backup service for Microsoft Entra ID can protect the following types of Microsoft Entra groups: **Microsoft 365 Group**, **Distribution List**, **Security Group**, and **Mail-Enabled Security Group**.
- The Microsoft 365 Groups with dynamic users are supported, but the **Dynamic distribution** group type is not supported.
- The Phone, Mail, and Sensitivity Label cannot be restored.
- The assigned labels cannot be restored.
- The created time and expiration time cannot be kept.
- If the group is synchronized from the on-premises active directory, the synchronization information cannot be restored. It will be restored as the cloud only group.
- The assigned licenses can be restored if there are enough available licenses.

Data Type	Status
Properties	Supported
Photo	Supported
Members	Supported
Owners	Supported
Roles and administrators	Unsupported
Administrative units	Supported
Group memberships	Supported
Applications	Supported
Azure role assignments	Supported **Note:** Note: To protect the Azure role assignments, you must grant the service app the User Access Administrator role in the corresponding subscription.
Extension attributes	Supported

Object Attributes

Table 24: Object Attributes

Attribute	**Status**	**Comment**
classification	Supported	
deletedDateTime	Supported	
description	Supported	
groupTypes	Supported	
deducedGroupType	Unsupported	
mailEnabled	Supported	
mailNickname	Supported	
mail	Supported	
membershipRule	Supported	
membershipRuleProcessingState	Supported	
preferredDataLocation	Supported	
preferredLanguage	Supported	
resourceBehaviorOptions	Supported	
resourceProvisioningOptions	Supported	
securityEnabled	Supported	
securityIdentifier	Supported	
theme	Supported	
visibility	Supported	
isAssignableToRole	Supported	
Membership type	Supported	
Source	Supported	
Type	Supported	
Object ID	Partially Supported	The object ID can be kept if the group has not yet been permanently deleted from your Microsoft Entra ID.
Created at	Unsupported	Read-only property in Microsoft Entra ID.
Email	Supported	
Direct members	Supported	
Group memberships	Supported	
Group name	Supported	
Group description	Supported	
Group writeback state	Supported	

Users

Refer to the table below for the data recovery state for users:

- The guest users can also be protected in the Microsoft Entra ID Users category.
- The creation time of the user profile and the creation type cannot be kept.

- If the user is synchronized from the on-premises active directory, the synchronization information cannot be restored. It will be restored as the cloud only user.
- For the users who have not yet been permanently deleted, the restore job will fail if any role assignments are not supported for restore.

Component	Status
Profiles	Supported
Photo	Supported **Note:** Due to an API limitation, the photo cannot be reverted to empty. Therefore, the restore job will skip the photo if the photo in the backup is empty.
Assigned roles	Supported **Note:** Currently, only the eligible assignments and active assignments are supported. The expired assignments are unsupported.
Administrative units	Supported
Groups	Supported
Applications	Supported
License	Supported
Devices	Unsupported
Azure role assignments	Supported **Note:** To protect the Azure role assignments, you must grant the service app the **User Access Administrator** role in the corresponding subscription.
Authentication methods	Partially Supported **Note:** The Alternative Phone belongs to MFA. The backup and restore of MFA properties are not supported.
Extension attributes	Supported

Object Attributes

Attributes	Status	Comment
accountEnabled	Supported	
ageGroup	Supported	

Attributes	Status	Comment
businessPhones	Supported	
city	Supported	
companyName	Supported	
consentProvidedForMinor	Supported	
country	Supported	
createdDateTime	Unsupported	Read-only property in Microsoft Entra ID.
creationType	Unsupported	Read-only property in Microsoft Entra ID. If the user account was created as a local account for an Azure Active Directory B2C tenant, the value is LocalAccount or nameCoexistence.
deletedDateTime	Unsupported	
department	Supported	
employeeHireDate	Unsupported	Read-only property in Microsoft Entra ID.
employeeId	Supported	
employeeOrgData	Supported	
employeeType	Supported	
externalUserState	Unsupported	Read-only property in Microsoft Entra ID.
externalUserStateChangeDateTime	Unsupported	Read-only property in Microsoft Entra ID.
faxNumber	Supported	
givenName	Supported	
identities	Supported	
jobTitle	Supported	
lastPasswordChangeDateTime	Unsupported	Read-only property in Microsoft Entra ID.
mail	Supported	
mailNickname	Supported	
mobilephone	Supported	
officeLocation	Supported	
onPremisesImmutableId	Supported	
onPremisesProvisioningErrors	Unsupported	
otherMails	Supported	
passwordPolicies	Supported	
postalCode	Supported	
preferredDataLocation	Supported	
preferredLanguage	Supported	
showInAddressList	Unsupported	
state	Supported	
streetAddress	Supported	

Attributes	Status	Comment
surname	Supported	
usageLocation	Supported	
userPrincipalName	Supported	
userType	Supported	
Manager	Supported	Read-only property in Microsoft Entra ID.
Display name	Supported	
Object ID	Partially Supported	The object ID can be kept if the user has not yet been permanently deleted from your Microsoft Entra ID.
Sign in sessions valid from date time	Unsupported	Read-only property in Microsoft Entra ID.
Authorization info	Supported	
Legal age group classification	Supported	

Admin Portal Settings

Admin Portal Settings data recovery service supports exporting the settings in Microsoft Entra ID, Microsoft 365 Defender admin center, Exchange admin center, and Intune admin center. Admin Portal Settings restore service can also restore some components to its original location. Refer to the table below for the settings that are protected by the Admin Portal Settings service:

Portal	Components/Policies			Export	Restore
Microsoft Entra ID	Security	Named locations	Named Locations and Trusted IP Addresses **Note:** MFA-named locations are unsupported	Supported	MFA Named Locations and Trusted IP Addresses are supported
		Authentication methods	Security Settings/ Policies > Auth Methods	Supported	Unsupported
		Conditional Access	Conditional Access Policies	Supported	Supported
	Company branding	Company branding settings		Supported	Unsupported
	Groups	General		Supported	Supported
		Expiration		Supported	Supported

Portal	Components/Policies			Export	Restore
		Naming policy **Note:** When you restore the group naming policy, the conflict resolution “Merge” will go with the overwrite approach.		Supported	Supported
Microsoft 365 Defender	Email collaboration	Threat policies	Anti-spam	Supported	Supported
			Anti-phishing	Supported	Supported
			Anti-malware	Supported	Supported
			Safe Attachments	Supported	Supported
			Safe Links	Supported	Supported
Exchange	Permission	Exchange Management Scope		Supported	Unsupported
Intune	Devices	Compliance policies		Supported	Unsupported
		Conditional access	Supported	Unsupported	
		Configuration profiles	Supported	Unsupported	
		Scripts	Supported	Unsupported	
	Apps	App protection policies **Note:** The app protection policies configured for **Windows Information Protection** (WIP) using the **Without enrollment** management type are not supported. **Note:** The restore of Data Recovery Agent certificate in **Windows Information Protection** (WIP) is unsupported.		Supported	Unsupported
		App configuration policies		Supported	Unsupported
	Endpoint Security	Security baselines		Supported	Unsupported
		Endpoint detection and response		Supported	Unsupported

Microsoft Entra ID (Named Location)

Please note that the tables exclusively list high-level settings and do not encompass specific object details. For comprehensive information or additional support, kindly contact our Support team.

Object Name	Object Type	Export	Restore
CountryNamedLocationModel	CountriesAndRegions	Supported	Supported
	CountryLookupMethod	Supported	Supported
	IncludeUnknownCountriesAndRegions	Supported	Supported
IpNamedLocationModel	IpRanges	Supported	Supported
	IsTrusted	Supported	Supported

Object Attributes

Attributes	Export	Restore
CreatedDateTime	Supported	Unsupported
ModifiedDateTime	Supported	Unsupported

Microsoft Entra ID (Authentication Configuration)

Please note that the tables exclusively list high-level settings and do not encompass specific object details. For comprehensive information or additional support, kindly contact our Support team.

Object Name	Object Type	Export	Restore
Fido2AuthenticationMethodConfigurationModel	IsAttestationEnforced	Supported	Unsupported
	IsAttestationEnforced	Supported	Unsupported
	KeyRestrictions	Supported	Unsupported
AdditionalFeatureDataOfMSAuthenticatorMethodModel	Key	Supported	Unsupported
	State	Supported	Unsupported
	IncludeTarget	Supported	Unsupported
	ExcludeTarget	Supported	Unsupported
EmailAuthenticationMethodConfigurationModel	AllowExternalIdToUseEmailOtp	Supported	Unsupported
TemporaryAccessPassAuthenticationMethodConfigurationModel	DefaultLength	Supported	Unsupported
	DefaultLifetimeInMinute	Supported	Unsupported
	IsUsableOnce	Supported	Unsupported
	MaximumLifetimeInMinutes	Supported	Unsupported
	MinimumLifetimeInMinutes	Supported	Unsupported

Object Attributes

Attributes	Export	Restore
State	Supported	Unsupported
IncludeTargets	Supported	Unsupported
ExcludeTargets	Supported	Unsupported

Microsoft Entra ID (Conditional Access)

Please note that the tables exclusively list high-level settings and do not encompass specific object details. For comprehensive information or additional support, kindly contact our Support team.

Date Type	Export	Restore
TemplateId	Supported	Unsupported
Conditions	Supported	Supported
CreatedDateTime	Supported	Unsupported
Description	Supported	Unsupported
GrantControls	Supported	Supported
ModifiedDateTime	Supported	Unsupported
SessionControls	Supported	Supported
State	Supported	Supported

Microsoft Entra ID (Company Branding)

Please note that the tables exclusively list high-level settings and do not encompass specific object details. For comprehensive information or additional support, kindly contact our Support team.

Data Type	Export	Restore
BackgroundColor	Supported	Unsupported
BackgroundImage	Supported	Unsupported
BackgroundImageRelativeUrl	Supported	Unsupported
BannerLogo	Supported	Unsupported
BannerLogoRelativeUrl	Supported	Unsupported
CdnList	Supported	Unsupported
SignInPageText	Supported	Unsupported
SquareLogo	Supported	Unsupported
SquareLogoRelativeUrl	Supported	Unsupported
UsernameHintText	Supported	Unsupported
BackgroundImageStr	Supported	Unsupported
BannerLogoStr	Supported	Unsupported
SquareLogoStr	Supported	Unsupported
BackgroundImageExtension	Supported	Unsupported
BannerLogoExtention	Supported	Unsupported
SquareLogoExtension	Supported	Unsupported

Microsoft Entra ID (Group General)

Please note that the tables exclusively list high-level settings and do not encompass specific object details. For comprehensive information or additional support, kindly contact our Support team.

Data Type	Export	Restore
TemplateId	Supported	Unsupported
Value	Supported	Supported

Object Attributes

Attributes	Status	Note

Self Service Group Management	Supported	To protect this property, you must have a service account profile configured in IBM® Storage Protect for Cloud interface and the service account you use must have the **Cloud Application Administrator** role.
Security Group	Supported	
Microsoft 365 Group	Supported	

Microsoft Entra ID (Group Naming Policy)

Please note that the tables exclusively list high-level settings and do not encompass specific object details. For comprehensive information or additional support, kindly contact our Support team.

Data Type	Export	Restore
TemplateId	Supported	Unsupported
Value	Supported	Supported

Object Attributes

Attributes	Export	Restore
Name	Supported	Supported
Value	Supported	Supported
AdditionalData	Supported	Unsupported
ODataType	Supported	Unsupported

Microsoft Entra ID (Group Expiration)

Please note that the tables exclusively list high-level settings and do not encompass specific object details. For comprehensive information or additional support, kindly contact our Support team.

Data Type	Export	Restore
TemplateId	Supported	Unsupported
Value	Supported	Supported

Object Attributes

Attributes	Export	Restore
AlternateNotificationEmails	Supported	Supported
GroupLifetimeInDays	Supported	Supported
AdditionalData	Supported	Unsupported
ManagedGroupTypes	Supported	Supported
GroupsId	Supported	Supported
GroupNames	Supported	Supported

Exchange Management

Please note that the tables exclusively list high-level settings and do not encompass specific object details. For comprehensive information or additional support, kindly contact our Support team.

Attributes	Export	Restore
RecipientRoot	Supported	Unsupported
Filter	Supported	Unsupported
RecipientFilter	Supported	Unsupported
ServerFilter	Supported	Unsupported
DatabaseFilter	Supported	Unsupported
TenantOrganizationFilter	Supported	Unsupported
ScopeRestrictionType	Supported	Unsupported
Exclusive	Supported	Unsupported
QueryFilter	Supported	Unsupported
AdminDisplayName	Supported	Unsupported

Microsoft 365 Defender

Refer to the lists below for the policies in Microsoft 365 Defender protected by Admin Portal Settings service.

Please note that the tables exclusively list high-level settings and do not encompass specific object details. For comprehensive information or additional support, kindly contact our Support team.

Anti-Phishing

Data Type	Status
FilterRule	Supported

Object Attributes

Attribute	Export	Restore
TargetedUsersToProtect	Supported	Supported
AdminDisplayName	Supported	Supported
AuthenticationFailAction	Supported	Supported
Conditions	Supported	Supported
DmarcQuarantineAction	Supported	Supported
DmarcRejectAction	Supported	Supported
Enabled	Supported	Supported
EnableFirstContactSafetyTips	Supported	Supported
EnableMailboxIntelligence	Supported	Supported
EnableMailboxIntelligenceProtection	Supported	Supported
EnableOrganizationDomainsProtection	Supported	Supported
EnableSimilarDomainsSafetyTips	Supported	Supported
EnableSimilarUsersSafetyTips	Supported	Supported
EnableSpoofIntelligence	Supported	Supported
EnableSuspiciousSafetyTip	Supported	Supported
EnableTargetedDomainsProtection	Supported	Supported
EnableTargetedUserProtection	Supported	Supported

Attribute	Export	Restore
EnableUnauthenticatedSender	Supported	Supported
EnableUnusualCharactersSafetyTips	Supported	Supported
EnableViaTag	Supported	Supported
ExceptIfRecipientDomainIs	Supported	Supported
ExceptIfSentTo	Supported	Supported
ExceptIfSentToMemberOf	Supported	Supported
Exceptions	Supported	Supported
ExcludedDomains	Supported	Supported
ExcludedSenders	Supported	Supported
HonorDmarcPolicy	Supported	Supported
ImmutableId	Supported	Unsupported
ImpersonationProtectionState	Supported	Supported
IsDefault	Supported	Unsupported
MailboxIntelligenceProtectionAction	Supported	Supported
MailboxIntelligenceProtectionActionRecipients	Supported	Supported
MailboxIntelligenceQuarantineTag	Supported	Supported
PhishThresholdLevel	Supported	Supported
PolicyTag	Supported	Supported
RecipientDomainIs	Supported	Supported
RecommendedPolicyType	Supported	
SentTo	Supported	Supported
SentToMemberOf	Supported	Supported
SpoofQuarantineTag	Supported	Supported
TargetedDomainActionRecipients	Supported	Supported
TargetedDomainProtectionAction	Supported	Supported
TargetedDomainQuarantineTag	Supported	Supported
TargetedDomainsToProtect	Supported	Supported
TargetedUserActionRecipients	Supported	Supported
TargetedUserProtectionAction	Supported	Supported
TargetedUserQuarantineTag	Supported	Supported

Anti-Spam

Data Type	Status
FilterRule	Supported

Object Attributes

Attributes	Export	Restore
EnableSafeList	Supported	Supported
ActionWhenThresholdReached	Supported	Supported

Attributes	Export	Restore
AddXHeaderValue	Supported	Supported
AllowedSenderDomains	Supported	Supported
AllowedSenders	Supported	Supported
ApplyPhishActionToIntraOrg	Supported	Supported
AutoForwardingMode	Supported	Supported
BccSuspiciousOutboundAdditionalRecipients	Supported	Supported
BccSuspiciousOutboundMail	Supported	Supported
BlockedSenderDomains	Supported	Supported
BlockedSenders	Supported	Supported
BulkQuarantineTag	Supported	Supported
BulkSpamAction	Supported	Supported
ConfigurationType	Supported	Supported
DirectoryBasedEdgeBlockModel	Supported	Supported
DownloadLink	Supported	Supported
EnableEndUserSpamNotifications	Supported	Supported
EnableLanguageBlockList	Supported	Supported
EnableRegionBlockList	Supported	Supported
EndUserSpamNotificationCustomFromAddress	Supported	Supported
EndUserSpamNotificationCustomSubject	Supported	Supported
EndUserSpamNotificationFrequency	Supported	Supported
EndUserSpamNotificationLanguage	Supported	Supported
EndUserSpamNotificationLimit	Supported	Supported
ExceptIfFrom	Supported	Supported
ExceptIfFromMemberOf	Supported	Supported
ExceptIfRecipientDomainIs	Supported	Supported
ExceptIfSenderDomainIs	Supported	Supported
ExceptIfSentTo	Supported	Supported
ExceptIfSentToMemberOf	Supported	Supported
FalsePositiveAdditionalRecipients	Supported	Supported
FromMemberOf	Supported	Supported
HighConfidencePhishAction	Supported	Supported
HighConfidencePhishQuarantineTag	Supported	Supported
HighConfidenceSpamAction	Supported	Supported
HighConfidenceSpamQuarantineTag	Supported	Supported
HostedContentFilterPolicy	Supported	Supported
IncreaseScoreWithBizOrInfoUrls	Supported	Supported
IncreaseScoreWithImageLinks	Supported	Supported

Attributes	Export	Restore
IncreaseScoreWithNumericIps	Supported	Supported
IncreaseScoreWithRedirectToOtherPort	Supported	Supported
InlineSafetyTipsEnabled	Supported	Supported
IPAllowList	Supported	Supported
IPBlockList	Supported	Supported
IsDefault	Supported	Unsupported
MarkAsSpamBulkMail	Supported	Supported
MarkAsSpamEmbedTagsInHtml	Supported	Supported
MarkAsSpamEmptyMessages	Supported	Supported
MarkAsSpamFormTagsInHtml	Supported	Supported
MarkAsSpamFramesInHtml	Supported	Supported
MarkAsSpamFromAddressAuthFail	Supported	Supported
MarkAsSpamJavaScriptInHtml	Supported	Supported
MarkAsSpamNdrBackscatter	Supported	Supported
MarkAsSpamObjectTagsInHtml	Supported	Supported
MarkAsSpamSensitiveWordList	Supported	Supported
MarkAsSpamSpfRecordHardFail	Supported	Supported
MarkAsSpamWebBugsInHtml	Supported	Supported
ModifySubjectValue	Supported	Supported
NotifyOutboundSpam	Supported	Supported
NotifyOutboundSpamRecipients	Supported	Supported
PhishQuarantineTag	Supported	Supported
PhishSpamAction	Supported	Supported
PhishZapEnabled	Supported	Supported
Priority	Supported	Supported
QuarantineRetentionPeriod	Supported	Supported
RecipientDomainIs	Supported	Supported
RecipientLimitExternalPerHour	Supported	Supported
RecipientLimitInternalPerHour	Supported	Supported
RecipientLimitPerDay	Supported	Supported
RecommendedPolicyType	Supported	Unsupported
RedirectToRecipients	Supported	Supported
RegionBlockList	Supported	Supported
SenderDomainIs	Supported	Supported
SentTo	Supported	Supported
SentToMemberOf	Supported	Supported
SpamAction	Supported	Supported
SpamQuarantineTag	Supported	Supported
SpamZapEnabled	Supported	Supported
TestModeAction	Supported	Supported
TestModeBccToRecipients	Supported	Supported

Attributes	Export	Restore
ZapEnabled	Supported	Supported

Anti-Malware

Data Type	Status
FilterRule	Supported

Object Attributes

Attribute	Export	Restore
AdminDisplayName	Supported	Supported
CustomExternalBody	Supported	Supported
CustomExternalSubject	Supported	Supported
CustomInternalBody	Supported	Supported
CustomInternalSubject	Supported	Supported
CustomFromAddress	Supported	Supported
CustomFromName	Supported	Supported
CustomNotifications	Supported	Supported
EnableExternalSenderAdminNotifications	Supported	Supported
EnableFileFilter	Supported	Supported
EnableInternalSenderAdminNotifications	Supported	Supported
ExternalSenderAdminAddress	Supported	Supported
FileTypeAction	Supported	Supported
FileTypes	Supported	Supported
InternalSenderAdminAddress	Supported	Supported
IsDefault	Supported	Unsupported
QuarantineTag	Supported	Supported
RecommendedPolicyType	Supported	Unsupported
ZapEnabled	Supported	Supported
MalwareFilterPolicy	Supported	Supported
State	Supported	Unsupported
Priority	Supported	Supported
Comments	Supported	Unsupported
Description	Supported	Supported
RuleVersion	Supported	Unsupported
SentTo	Supported	Supported
SentToMemberOf	Supported	Supported
RecipientDomainIs	Supported	Supported
ExceptIfSentTo	Supported	Supported
ExceptIfSentToMemberOf	Supported	Supported
ExceptIfRecipientDomainIs	Supported	Supported

Attribute	Export	Restore
Conditions	Supported	Unsupported
Exceptions	Supported	Unsupported
ImmutableId	Supported	Unsupported

Safe Links

Data Type	Status
FilterRule	Supported

Object Attributes

Attributes	Export	Restore
AdminDisplayName	Supported	Supported
AllowClickThrough	Supported	Supported
Comments	Supported	Supported
Conditions	Supported	Unsupported
CustomNotificationText	Supported	Supported
DeliverMessageAfterScan	Supported	Supported
Description	Supported	Supported
DisableUrlRewrite	Supported	Supported
DoNotRewriteUrls	Supported	Supported
EnableOrganizationBranding	Supported	Supported
EnableSafeLinksForEmail	Supported	Supported
EnableSafeLinksForOffice	Supported	Supported
EnableSafeLinksForTeams	Supported	Supported
ExceptIfRecipientDomainIs	Supported	Supported
ExceptIfSentTo	Supported	Supported
ExceptIfSentToMemberOf	Supported	Supported
Exceptions	Supported	Unsupported
ImmutableId	Supported	Unsupported
IsBuiltInProtection	Supported	Unsupported
LocalizedNotificationTextList	Supported	Supported
RecipientDomainIs	Supported	Supported
RecommendedPolicyType	Supported	Unsupported
RuleVersion	Supported	Unsupported
ScanUrls	Supported	Supported
SentTo	Supported	Supported
SentToMemberOf	Supported	Supported
TrackClicks	Supported	Supported
UseTranslatedNotificationText	Supported	Supported

Safe Attachments

Data Type	Status
FilterRule	Supported

Object Attributes

Attributes	Export	Restore
Action	Supported	Supported
ActionOnError	Supported	Supported
AdminDisplayName	Supported	Supported
Comments	Supported	Unsupported
Conditions	Supported	Unsupported
ConfidenceLevelThreshold	Supported	Supported
Description	Supported	Supported
Enable	Supported	Supported
EnableFileFilter	Supported	Supported
EnableOrganizationBranding	Supported	Supported
ExceptIfRecipientDomainIs	Supported	Supported
ExceptIfSentToMemberOf	Supported	Supported
Exceptions	Supported	Unsupported
ImmutableId	Supported	Unsupported
IsBuiltInProtection	Supported	Unsupported
IsDefault	Supported	Unsupported
OperationMode	Supported	Supported
Priority	Supported	Supported
QuarantineTag	Supported	Supported
RecipientDomainIs	Supported	Supported
RecommendedPolicyType	Supported	Unsupported
Redirect	Supported	Supported
RedirectAddress	Supported	Supported
RuleVersion	Supported	Unsupported
ScanTimeout	Supported	Supported
SentTo	Supported	Supported
SentToMemberOf	Supported	Supported
State	Supported	Supported

Intune

Refer to the lists below for the settings in Microsoft Intune admin center protected by Admin Portal Settings.

Please note that the tables exclusively list high-level settings and do not encompass specific object details. For comprehensive information or additional support, kindly contact our Support team.

Apps (Protection Policies)

Object Name	Object Type	Export	Restore
AndroidManagedAppProtectionModel	CustomBrowserDisplayName	Supported	Supported
	CustomBrowserPackageId	Supported	Supported
	DeployedAppCount	Supported	Unsupported
	DisableAppEncryptionIfDeviceEncryptionIsEnabled	Supported	Supported
	EncryptAppData	Supported	Supported
	MinimumRequiredPatchVersion	Supported	Supported
	MinimumWarningPatchVersion	Supported	Supported
	ScreenCaptureBlocked	Supported	Supported
	Apps	Supported	Supported
	AppsNextLink	Supported	Unsupported
	DeploymentSummary	Supported	Unsupported
IosManagedAppProtectionModel	AppDataEncryptionType	Supported	Supported
	CustomBrowserProtocol	Supported	Supported
	DeployedAppCount	Supported	Unsupported
	FaceIdBlocked	Supported	Supported
	MinimumRequiredSdkVersion	Supported	Supported
	Apps	Supported	Supported
	AppsNextLink	Supported	Unsupported
	DeploymentSummary	Supported	Unsupported
WindowsInformationProtectionModel	AzureRightsManagementServicesAllowed	Supported	Supported
	DataRecoveryCertificate	Supported	Supported
	EnforcementLevel	Supported	Supported
	EnterpriseDomain	Supported	Supported
	EnterpriseInternalProxyServers	Supported	Supported
	EnterpriseIPRanges	Supported	Supported
	EnterpriseIPRangesAreAuthoritative	Supported	Supported
	EnterpriseNetworkDomainNames	Supported	Supported
	EnterpriseProtectedDomainNames	Supported	Supported
	EnterpriseProxiedDomains	Supported	Supported
	EnterpriseProxyServers	Supported	Supported
	EnterpriseProxyServersAreAuthoritative	Supported	Supported
	ExemptApps	Supported	Supported
	IconsVisible	Supported	Supported

Object Name	Object Type	Export	Restore
	IndexingEncryptedStoresOrItemsBlocked	Supported	Supported
	IsAssigned	Supported	Supported
	NeutralDomainResources	Supported	Supported
	ProtectedApps	Supported	Supported
	ProtectionUnderLockConfigRequired	Supported	Supported
	RevokeOnUnenrollDisabled	Supported	Supported
	RightsManagementServicesTemplateId	Supported	Supported
	SmbAutoEncryptedFileExtensions	Supported	Supported
	Assignments	Supported	Supported
	ExemptAppLockerFiles	Supported	Unsupported
	ProtectedAppLockerFiles	Supported	Unsupported
	ProtectedAppLockerFilesNextLink	Supported	Unsupported
ManagedAppProtectionModel	IsAssigned	Supported	Supported
	Assignments	Supported	Supported
	AssignmentsNextLink	Supported	Unsupported

Apps (Configuration Policies)

Object Name	Object Type	Export	Restore
ManagedApp	appGroupType	Supported	Supported
	apps	Supported	Supported
	assignments	Supported	Supported
	customSettings	Supported	Supported
	deployedAppCount	Supported	Unsupported
	description	Supported	Supported
	displayName	Supported	Supported
	isAssigned	Supported	Supported
	roleScopeTagIds	Supported	Supported
	settings	Supported	Supported
	targetedAppManagementLevels	Supported	Supported
Managed Device (IOS)	targetedMobileApps	Supported	Supported
	roleScopeTagIds	Supported	Supported
	description	Supported	Supported
	displayName	Supported	Supported
	encodedSettingXml	Supported	Supported
	settings	Supported	Supported

Devices (Compliance Policies)

Object Name	Object Type	Export	Restore
DeviceCompliancePolicyModel	UserStatuses	Supported	Unsupported
	ScheduledActionsForRule	Supported	Supported
	DeviceStatusOverview	Supported	Unsupported
	DeviceStatuses	Supported	Unsupported
	DeviceSettingStateSummaries	Supported	Unsupported
	Assignments	Supported	Supported
	Version	Supported	Unsupported
	LastModifiedDateTime	Supported	Unsupported
	Description	Supported	Supported
	CreatedDateTime	Supported	Unsupported
	UserStatusOverview	Supported	Unsupported
AndroidCompliancePolicyModel	SecurityRequireUpToDateSecurityProviders	Supported	Supported
	SecurityRequireSafetyNetAttestationCertifiedDevice	Supported	Supported
	SecurityRequireSafetyNetAttestationBasicIntegrity	Supported	Supported
	SecurityRequireGooglePlayServices	Supported	Supported
	SecurityRequireCompanyPortalAppIntegrity	Supported	Supported
	SecurityPreventInstallAppsFromUnknownSources	Supported	Supported
	SecurityDisableUsbDebugging	Supported	Supported
	SecurityBlockJailbrokenDevices	Supported	Supported
	PasswordRequiredType	Supported	Supported
	PasswordRequired	Supported	Supported
	PasswordPreviousPasswordBlockCount	Supported	Supported
	PasswordMinutesOfInactivityBeforeLock	Supported	Supported
	PasswordMinimumLength	Supported	Supported
	PasswordExpirationDays	Supported	Supported
	OsMinimumVersion	Supported	Supported
	OsMaximumVersion	Supported	Supported
	DeviceThreatProtectionRequiredSecurityLevel	Supported	Supported
	DeviceThreatProtectionEnabled	Supported	Supported

Object Name	Object Type	Export	Restore
	SecurityRequireVerifyApps	Supported	Supported
	StorageRequireEncryption	Supported	Supported
AndroidWorkProfileCompliancePolicyModel	SecurityRequireUpToDateSecurityProviders	Supported	Supported
	SecurityRequireSafetyNetAttestationCertifiedDevice	Supported	Supported
	SecurityRequireSafetyNetAttestationBasicIntegrity	Supported	Supported
	SecurityRequireGooglePlayServices	Supported	Supported
	SecurityRequireCompanyPortalAppIntegrity	Supported	Supported
	SecurityPreventInstallAppsFromUnknownSources	Supported	Supported
	SecurityDisableUsbDebugging	Supported	Supported
	SecurityBlockJailbrokenDevices	Supported	Supported
	PasswordRequiredType	Supported	Supported
	PasswordRequired	Supported	Supported
	PasswordPreviousPasswordBlockCount	Supported	Supported
	PasswordMinutesOfInactivityBeforeLock	Supported	Supported
	PasswordMinimumLength	Supported	Supported
	PasswordExpirationDays	Supported	Supported
	OsMinimumVersion	Supported	Supported
	OsMaximumVersion	Supported	Supported
	MinAndroidSecurityPatchLevel	Supported	Supported
	DeviceThreatProtectionRequiredSecurityLevel	Supported	Supported
	DeviceThreatProtectionEnabled	Supported	Supported
	SecurityRequireVerifyApps	Supported	Supported
	StorageRequireEncryption	Supported	Supported
IosCompliancePolicyMode	DeviceThreatProtectionEnabled	Supported	Supported
	DeviceThreatProtectionRequiredSecurityLevel	Supported	Supported
	ManagedEmailProfileRequired	Supported	Supported

Object Name	Object Type	Export	Restore
	OsMaximumVersion	Supported	Supported
	OsMinimumVersion	Supported	Supported
	PasscodeBlockSimple	Supported	Supported
	PasscodeExpirationDay	Supported	Supported
	PasscodeMinimumCharacterSetCount	Supported	Supported
	PasscodeMinimumLength	Supported	Supported
	PasscodeMinutesOfInactivityBeforeLock	Supported	Supported
	PasscodePreviousPasscodeBlockCount	Supported	Supported
	PasscodeRequired	Supported	Supported
	PasscodeRequiredType	Supported	Supported
MacOSCompliancePolicyModel	PasswordRequiredType	Supported	Supported
	PasswordRequired	Supported	Supported
	PasswordPreviousPasswordBlockCount	Supported	Supported
	PasswordMinutesOfInactivityBeforeLock	Supported	Supported
	PasswordMinimumLength	Supported	Supported
	PasswordMinimumCharacterSetCount	Supported	Supported
	PasswordExpirationDays	Supported	Supported
	PasswordBlockSimple	Supported	Supported
	OsMinimumVersion	Supported	Supported
	OsMaximumVersion	Supported	Supported
	FirewallEnableStealthMode	Supported	Supported
	FirewallEnabled	Supported	Supported
	FirewallBlockAllIncoming	Supported	Supported
	DeviceThreatProtectionRequiredSecurityLevel	Supported	Supported
	DeviceThreatProtectionEnabled	Supported	Supported
	StorageRequireEncryption	Supported	Supported
	SystemIntegrityProtectionEnabled	Supported	Supported
Windows10CompliancePolicyModel	RequireHealthyDeviceReport	Supported	Supported
	PasswordRequiredType	Supported	Supported
	PasswordRequiredToUnlockFromIdle	Supported	Supported
	PasswordMinutesOfInactivityBeforeLock	Supported	Supported

Object Name	Object Type	Export	Restore
	PasswordMinimumLength	Supported	Supported
	PasswordMinimumCharacterSetCount	Supported	Supported
	PasswordExpirationDays	Supported	Supported
	PasswordBlockSimple	Supported	Supported
	OsMinimumVersion	Supported	Supported
	OsMaximumVersion	Supported	Supported
	MobileOsMinimumVersion	Supported	Supported
	MobileOsMaximumVersion	Supported	Supported
	EarlyLaunchAntiMalwareDriverEnabled	Supported	Supported
	CodeIntegrityEnabled	Supported	Supported
	BitLockerEnabled	Supported	Supported
	SecureBootEnabled	Supported	Supported
	StorageRequireEncryption	Supported	Supported
Windows81CompliancePolicyModel	OsMaximumVersion	Supported	Supported
	OsMinimumVersion	Supported	Supported
	PasswordBlockSimple	Supported	Supported
	PasswordExpirationDay	Supported	Supported
	PasswordMinimumCharacterSetCount	Supported	Supported
	PasswordMinimumLength	Supported	Supported
	PasswordMinutesOfInactivityBeforeLock	Supported	Supported
	PasswordPreviousPasswordBlockCount	Supported	Supported
	PasswordRequired	Supported	Supported
	PasswordRequiredType	Supported	Supported
	StorageRequireEncryption	Supported	Supported

Devices (Conditional Access)

ObjectName	ObjectType	Export	Restore
ConditionalAccessPolicyModel	TemplateId	Supported	Unsupported
	Conditions	Supported	Supported
	Description	Supported	Unsupported
	GrantControls	Supported	Supported
	SessionControls	Supported	Supported
	State	Supported	Supported

Devices (Configuration Profiles)

Object Name	Object Type	Export	Restore
AndroidCustomConfigurationModel	OmaSettings	Supported	Supported
AndroidGeneralDeviceConfigurationModel	PasswordBlockTrustAgents	Supported	Supported
	PasswordExpirationDays	Supported	Supported
	PasswordMinimumLength	Supported	Supported
	PasswordMinutesOfInactivityBeforeScreenTimeout	Supported	Supported
	PasswordPreviousPasswordBlockCount	Supported	Supported
	PasswordRequired	Supported	Supported
	PasswordRequiredType	Supported	Supported
	PasswordSignInFailureCountBeforeFactoryReset	Supported	Supported
	PowerOffBlocked	Supported	Supported
	ScreenCaptureBlocked	Supported	Supported
	SecurityRequireVerifyApps	Supported	Supported
	StorageBlockGoogleBackup	Supported	Supported
	StorageBlockRemovableStorage	Supported	Supported
	StorageRequireDeviceEncryption	Supported	Supported
	StorageRequireRemovableStorageEncryption	Supported	Supported
	VoiceAssistantBlocked	Supported	Supported
	VoiceDialingBlocked	Supported	Supported
	WebBrowserBlockAutofill	Supported	Supported
	WebBrowserBlocked	Supported	Supported
	WebBrowserBlockJavaScript	Supported	Supported
	WebBrowserBlockPopups	Supported	Supported
	PasswordBlockFingerprintUnlock	Supported	Supported
	WebBrowserCookieSettings	Supported	Supported
	NfcBlocked	Supported	Supported
	KioskModeBlockVolumeButtons	Supported	Supported

Object Name	Object Type	Export	Restore
	AppsBlockClipboardSharing	Supported	Supported
	AppsBlockCopyPaste	Supported	Supported
	AppsBlockYouTube	Supported	Supported
	AppsHideList	Supported	Supported
	AppsInstallAllowList	Supported	Supported
	AppsLaunchBlockList	Supported	Supported
	BluetoothBlocked	Supported	Supported
	CameraBlocked	Supported	Supported
	CellularBlockDataRoaming	Supported	Supported
	CellularBlockMessaging	Supported	Supported
AndroidWorkProfileCustomConfigurationModel	OmaSettings	Supported	Supported
Windows81GeneralConfigurationModel	UpdatesRequireAutomaticUpdates	Supported	Supported
	StorageRequireDeviceEncryption	Supported	Supported
	PasswordSignInFailureCountBeforeFactoryReset	Supported	Supported
	PasswordRequiredType	Supported	Supported
	PasswordPreviousPasswordBlockCount	Supported	Supported
	PasswordMinutesOfInactivityBeforeScreenTimeout	Supported	Supported
	PasswordMinimumLength	Supported	Supported
	PasswordMinimumCharacterSetCount	Supported	Supported
	PasswordExpirationDays	Supported	Supported
	PasswordBlockPicturePasswordAndPin	Supported	Supported
	DiagnosticsBlockDataSubmission	Supported	Supported
	CellularBlockDataRoaming	Supported	Supported
	BrowserTrustedSitesSecurityLevel	Supported	Supported
	BrowserRequireSmartScreen	Supported	Supported
	BrowserRequireHighSecurityForRestrictedSites	Supported	Supported

Object Name	Object Type	Export	Restore
	BrowserRequireFraudWarning	Supported	Supported
	BrowserRequireFirewall	Supported	Supported
	AccountsBlockAddingNonMicrosoftAccountEmail	Supported	Supported
	ApplyOnlyToWindows81	Supported	Unsupported
	BrowserBlockAutofill	Supported	Supported
	BrowserBlockAutomaticDetectionOfIntranetSites	Supported	Supported
	BrowserBlockEnterpriseModeAccess	Supported	Supported
	BrowserBlockJavaScript	Supported	Supported
	UserAccountControlSettings	Supported	Supported
	BrowserBlockPlugins	Supported	Supported
	BrowserBlockSendingDoNotTrackHeader	Supported	Supported
	BrowserBlockSingleWordEntryOnIntranetSites	Supported	Supported
	BrowserEnterpriseModeSiteListLocation	Supported	Supported
	BrowserInternetSecurityLevel	Supported	Supported
	BrowserBlockPopups	Supported	Supported
	BrowserLoggingReportLocation	Supported	Supported
	WorkFoldersUrl	Supported	Supported
DeviceConfigurationModel	CreatedDateTime	Supported	Unsupported
	Description	Supported	Supported
	LastModifiedDateTime	Supported	Unsupported
	Version	Supported	Unsupported
	Assignments	Supported	Supported
	AssignmentsNextLink	Supported	Supported
	DeviceSettingStateSummaries	Supported	Supported
	DeviceSettingStateSummariesNextLink	Supported	Supported
	DeviceStatuses	Supported	Supported
	DeviceStatusesNextLink	Supported	Supported
	DeviceStatusOverview	Supported	Supported
	UserStatuses	Supported	Supported
	UserStatusesNextLink	Supported	Supported

Object Name	Object Type	Export	Restore
	UserStatusOverview	Supported	Supported

Devices (Scripts and remediations)

Object Name	Object Type	Export	Restore
DeviceScriptWindowsRecordModel	EnforceSignatureCheck	Supported	Supported
	RunAs32Bit	Supported	Supported
	Description	Supported	Supported
	ScriptContent	Supported	Supported
	CreatedDateTime	Supported	Unsupported
	LastModifiedDateTime	Supported	Unsupported
	RunAsAccount	Supported	Supported
	FileName	Supported	Supported
	RoleScopeTagIds	Supported	Supported
	Assignments	Supported	Supported
	RunState	Supported	Supported
	ResultMessage	Supported	Supported
	LastStateUpdateDateTime	Supported	Unsupported
	ErrorCode	Supported	Supported
	ErrorDescription	Supported	Supported
	SuccessDeviceCount	Supported	Supported
	ErrorDeviceCount	Supported	Supported
	UserPrincipalName	Supported	Supported
DeviceScriptMacOsRecordModel	EnforceSignatureCheck	Supported	Supported
	RunAs32Bit	Supported	Supported
	Description	Supported	Supported
	ScriptContent	Supported	Supported
	CreatedDateTime	Supported	Unsupported
	LastModifiedDateTime	Supported	Unsupported
	RunAsAccount	Supported	Supported
	FileName	Supported	Supported
	RoleScopeTagIds	Supported	Supported
	Assignments	Supported	Supported
	RunState	Supported	Supported
	ResultMessage	Supported	Supported
	LastStateUpdateDateTime	Supported	Unsupported
	ErroCode	Supported	Supported
	ErrorDescription	Supported	Supported
	SuccessDeviceCount	Supported	Supported
	ErrorDeviceCount	Supported	Supported
	UserPrincipleName	Supported	Supported

Object Name	Object Type	Export	Restore
ConfigurationPolicyModelRecord	EnforceSignatureCheck	Supported	Supported
	RunAs32Bit	Supported	Supported
	Description	Supported	Supported
	ScriptContent	Supported	Supported
	CreateDateTime	Supported	Unsupported
	LastModifiedDateTime	Supported	Unsupported
	RunAsAccount	Supported	Supported
	FileName	Supported	Supported
	RoleScopeTagIds	Supported	Supported
	Assignments	Supported	Supported
	RunState	Supported	Supported
	ResultMessage	Supported	Supported
	LastStateUpdateDateTime	Supported	Unsupported
	ErrorCode	Supported	Supported
	ErrorDescription	Supported	Supported
	SuccessDeviceCount	Supported	Supported
	ErrorDeviceCount	Supported	Supported
	UserPrincipleName	Supported	Supported

Endpoint Security (Security baseline)

Object Type	Export	Restore
IsAssigned	Supported	Supported
TemplateId	Supported	Unsupported
Description	Supported	Supported
LastModifiedDateTime	Supported	Unsupported
RoleScopeTagIds	Supported	Supported
Assignments	Supported	Supported
IsBuiltIn	Supported	Unsupported
Setting	Supported	Supported
ConflictCount	Supported	Supported
ErrorCount	Supported	Supported
FailedCount	Supported	Supported
NotApplicableCount	Supported	Supported
NotApplicablePlatformCount	Supported	Supported
SuccessCount	Supported	Supported

Endpoint Security (Endpoint detection and response)

Object Name	Object Type	Export	Restore
EndpointSecurityBaseline	IsAssigned	Supported	Supported

Object Name	Object Type	Export	Restore
	TemplateId	Supported	Unsupported
	Description	Supported	Supported
	LastModifiedDateTime	Supported	Unsupported
	RoleScopeTagIds	Supported	Supported
	Assignments	Supported	Supported
DeviceConfigurationProfileConfigurationPolicy	Description	Supported	Supported
	CreationSource	Supported	Supported
	CreatedDateTime	Supported	Unsupported
	LastModifiedDateTime	Supported	Unsupported
	Platforms	Supported	Unsupported
	PriorityMetaData	Supported	Supported
	RoleScopeTagIds	Supported	Supported
	Name	Supported	Supported
	SettingCount	Supported	Supported
	Technologies	Supported	Supported
	TemplateReference	Supported	Supported
	Assignments	Supported	Supported
	Settings	Supported	Supported

Azure SQL

Refer to the following table for the supported object types you can protect in Azure SQL.

Attributes	Properties	Status	Note
Essentials	Tags	Supported	
	Pricing tier	Supported	
	Earliest restore point	Unsupoprted	The property is supported only when it is in both the General Purpose service tier and the Serverless compute tier simultaneously.
	Auto-pause delay	Supported	
Compute + storage	Service tier	Supported	
	DTUs	Supported	
	Max storage	Supported	
Backups	Differential backup frequency	Supported	
	PITR retention	Supported	
	Weekly LTR	Supported	
	Monthly LTR	Supported	
	Yearly LTR	Supported	
	Storage redundancy	Supported	

Attributes	Properties	Status	Note
Security	Ledger database	Supported	The ledger database is unsupported in the Native Azure SQL backup monitoring service.
	Ledger automatic digest storage	Supported	The Ledger automatic digest storage is unsupported in the Native Azure SQL backup monitoring service.
	Always encrypted with secure enclaves	Unsupported	

Azure Storage

Azure storage service protects the Azure Blob Storage (including Data Lake Store and Date Lake Storage Gen2) and Azure Files. You can not only restore the backup data to its original location or to a different location, but also export the backup data. Refer to the following tables for the supported and unsupported status when restoring the backup data to its original location.

Object Metadata or Components

Summary for complex table

Object Type	Components	Status
Container	Access Level	Supported
	Access policy	Partially Supported
	Properties	Supported
	Metadata	Supported
	Content	Supported
Folder	Properties	Supported
	Content	Supported
Blob	Properties	Supported
	Metadata	Partially supported
	Blob index tags	Partially supported
	Versions	Not supported
	Snapshots	Not supported
	Content	Supported
File Share	Properties	Supported
	Metadata	Supported
	Content	Supported
File Share Directory	Properties	Supported
	Metadata	Supported
	Content	Supported
File Share File	Properties	Supported
	Metadata	Supported
	Content	Supported

Objects Attributes/Properties

Summary for complex table

Object Type	Attributes	Status
Container	Name	Supported
	URL	Supported
	Last modified	Unsupported
	eTag	Unsupported
	Lease status	Unsupported
	Lease state	Unsupported **Note:** The restore job will set the Lease state to **Available**.
	Lease duration	Unsupported
	Encryption scope	Unsupported
	Version-level immutability support	Unsupported
Folder	Name	Supported
	URL	Supported
Blob	Name	Supported
	URL	Supported
	Last modified	Unsupported
	Creation time	Unsupported
	Version ID	Unsupported
	Type	Supported
	Size	Supported
	Access tier	Supported
	Access tier last modified	Unsupported
	Archive status	Unsupported
	Rehydrate priority	Unsupported
	Server encrypted	Supported
	eTag	Unsupported
	Version-level immutability policy	Unsupported
	Cache-control	Unsupported
	Content-type	Unsupported
	Content-MD5	Unsupported
	Content-Encoding	Unsupported
	Content-Language	Unsupported
	Content-Disposition	Unsupported
	Lease status	Unsupported
	Lease state	Unsupported
	Lease duration	Unsupported
	Copy status	Unsupported
	Copy completion time	Unsupported
	Copy source	Unsupported

Object Type	Attributes	Status
File Share	Name	Supported
	URL	Supported
	Last modified	Unsupported
	eTag	Unsupported
	Quota	Supported
	Usage	Supported
	Tier	Supported
Share Directory	Name	Supported
	URL	Supported
	Last modified	Unsupported
	eTag	Unsupported
Share File	Name	Supported
	URL	Supported
	Last modified	Unsupported
	Size	Supported
	eTag	Unsupported
	Content-MD5	Unsupported

Azure DevOps

Refer to the following table for the supported object types you can protect in Azure DevOps.

Object Types					Backup	Restore
Organization **Note:** The deleted organizations cannot be restored.	Organization settings	General	Overview	Name	Supported	Supported
				Use the new URL		
				Privacy URL		
				Description		
				Time Zone		
				Geography		
				Region		
			Users **Note:** Group rules are currently unsupported.		Supported	Supported
		Security	Groups		Supported	Supported
			Users			
	Project	Overview	Wiki	Wiki	Supported	Supported
				Comment	Supported	Supported
		Repositories	Branches	File	Supported	Supported
				History	Supported	Supported
			Tags		Supported	Supported

Object Types						Backup	Restore
		Project settings	General	Overview	Name	Supported	Unsupported
					Description	Supported	Supported
					Process	Supported	Unsupported
					Visibility	Supported	Supported
					Azure DevOps services-Boards	Supported	Supported
					Azure DevOps services-Repos	Supported	Supported
					Azure DevOps services-Pipelines	Supported	Supported
					Azure DevOps services-Test Plans	Supported	Supported
					Azure DevOps services-Artifacts	Supported	Supported
				Permissions	Groups	Supported	Supported
			Boards	Project configuration	Iterations	Supported	Supported
					Areas	Supported	Supported
			Repos	Repositories settings	Settings	Supported	Supported

Object Types						**Backup**	**Restore**
					Policies	Supported	Partially Supported **Note:** The **Build validation** policy, **Status check** policy, and **Automatically include reviews** policy are currently unsupported.
					Security	Supported	Supported
					Approvals and checks	Supported	Supported
				Repository type	Git	Supported	Supported
					Team Foundation Version Control (TFVC)	Unsupported	Unsupported
		Pipelines	Pipelines	Pipelines	Azure Repos Git	Supported	Supported
			Library	Library item	Variable groups	Supported	Supported
					Approvals and checks	Partially supported ***Note**: The disable approvals and checks are currently unsupported.	Partially supported ***Note**: The disable approvals and checks are currently unsupported.

Object Types						Backup	Restore
		Boards	Work items	Epics	Global ID	Supported	Supported
					Subject	Supported	Supported
					Owner	Supported	Supported
					Comment	Supported	Supported
					Add Tag	Supported	Supported
					State	Supported	Supported
					Area	Supported	Supported
					Iteration	Supported	Supported
					Description	Supported	Supported
					Priority	Supported	Supported
					Discussion	Supported	Supported
					Add link	Supported	Supported
					Add attachments	Supported	Supported
				Issue	Global ID	Supported	Supported
					Subject	Supported	Supported
					Owner	Supported	Supported
					Comment	Supported	Supported
					Add Tag	Supported	Supported
					State	Supported	Supported
					Area	Supported	Supported
					Iteration	Supported	Supported
					Description	Supported	Supported
					Priority	Supported	Supported
					Discussion	Supported	Supported
					Add Link	Supported	Supported
					Add Attachments	Supported	Supported
				Tasks	Global ID	Supported	Supported
					Subject	Supported	Supported
					Owner	Supported	Supported
					Comment	Supported	Supported
					Add Tag	Supported	Supported
					State	Supported	Supported
					Area	Supported	Supported
					Ieration	Supported	Supported
					Description	Supported	Supported
					Priority	Supported	Supported
					Activity	Supported	Supported
					Discussion	Supported	Supported
					Add Link	Supported	Supported

Object Types						Backup	Restore
					Add Attachments	Supported	Supported

Azure AD B2C

The backup service for Azure AD B2C supports protecting the app registrations, identity providers, user attributes, user flows, and users. Azure AD B2C data recovery only supports restoring the supported data types to the original location.

Example

Refer to the tables below for supported and unsupported object types you can protect in the Azure AD B2C service.

App Registration

The data recovery state for app registrations is the same as that of the Microsoft Entra ID service. For details, refer to App Registration.

Identity Provider

Refer to the list below for the data recovery state for identity providers.

Social Identity Provider

Refer to the list below for the social identity providers protected in the Azure AD B2C service:

Amazon

Attributes	Backup	Restore
Origin URL	Supported	Supported
Callback URL	Supported	Supported
Name	Supported	Supported
Client ID	Supported	Supported
Client secret	Unsupported	Unsupported

Facebook

Attributes	Backup	Restore
Origin URL	Supported	Supported
Callback URL	Supported	Supported
Name	Supported	Supported
Client ID	Supported	Supported
Client secret	Unsupported	Unsupported

Google

Attributes	Backup	Restore
Origin URL	Supported	Supported
Callback URL	Supported	Supported

Attributes	Backup	Restore
Name	Supported	Supported
Client ID	Supported	Supported
Client secret	Unsupported	Unsupported

Linkedln

Attributes	Backup	Restore
Origin URL	Supported	Supported
Callback URL	Supported	Supported
Name	Supported	Supported
Client ID	Supported	Supported
Client secret	Unsupported	Unsupported

Twitter

Attributes	Backup	Restore
Origin URL	Supported	Supported
Callback URL	Supported	Supported
Name	Supported	Supported
Client ID	Supported	Supported
Client secret	Unsupported	Unsupported

OpenID Identity Provider

Attributes	Backup	Restore
Name	Supported	Supported
Metadata URL	Supported	Supported
Client ID	Supported	Supported
Client secret	Unsupported	Unsupported
Scope	Supported	Supported
Response type	Supported	Supported
Response mode	Supported	Supported
Domain hint	Supported	Supported
User ID	Supported	Supported
Display name	Supported	Supported
Given name	Supported	Supported
Surname	Supported	Supported
Email	Supported	Supported

User Attribute

Refer to the table below for the data recovery state for user attributes:

Object types		Backup	Restore
Build-In Attribute		Unsupported	Unsupported
Custom Attribute	Name	Supported	Supported

Object types		Backup	Restore
	Data Type	Supported	Supported
	Description	Supported	Supported

User Flow

Refer to the table below for the data recovery state for user flows:

Property	Backup	Restore
Enable JavaScript enforcing page layout	Unsupported	Unsupported
Multifactor authentication	Supported	Supported **Note:** The multifactor authentication of SMS or phone call is unsupported.
Conditional access	Supported	Supported
Token lifetime	Supported	Supported
Token compatibility settings	Unsupported	Unsupported
Session behavior	Supported	Supported
Password configuration	Supported	Supported
Captcha	Unsupported	Unsupported
Identity providers	Supported	Supported
User attributes	Supported	Supported
Application claims	Unsupported	Unsupported
API connectors	Supported	Supported

Object Attributes

Attributes	Backup	Restore
Type of method	Supported	Supported
MFA enforcement	Supported	Supported
Enforce conditional access policies	Supported	Supported
Access & id token lifetime	Supported	Supported
refresh token lifetime	Supported	Supported
refresh token sliding window lifetime	Supported	Supported
lifetime length	Supported	Supported
Issuer (iss) claim	Supported	Supported
Subject (sub) claim	Unsupported	Unsupported
Claim representing user flow	Unsupported	Unsupported
Web app session lifetime	Supported	Supported
Web app session timeout	Supported	Supported
Single sign-on configuration	Supported	Supported

Attributes	Backup	Restore
Require ID Token in logout requests	Supported	Supported
Enforce SSO logout validation	Unsupported	Unsupported
Enable keep me signed in session	Supported	Supported
Keep me signed in session	Supported	Supported
Self-service password reset	Supported	Supported
Forced password reset	Supported	Supported
Password complexity	Supported	Supported
Local accounts	Supported	Supported
Social identity providers	Supported	Supported
Custom identity providers	Supported	Supported

User

Refer to the table below for the data recovery state for users:

Object Types		Backup	Restore
Overview	Display name	Supported	Supported
	Last name	Supported	Supported
	First name	Supported	Supported
	User principal name	Supported	Supported
	User type	Supported	Supported
	Authorization info	Supported	Supported
	Job title	Supported	Supported
	Company name	Supported	Supported
	Department	Supported	Supported
	Employee ID	Supported	Supported
	Employee type	Supported	Supported
	Employee hire date	Supported	Supported
	Office location	Supported	Supported
	Manager	Supported	Supported
	Sponsors	Supported	Supported
	Street address	Supported	Supported
	City	Supported	Supported
	State or province	Supported	Supported
	ZIP or postal code	Supported	Supported
	Country or region	Supported	Supported
	Business phone	Supported	Supported
	Mobile phone	Supported	Supported
	Email	Supported	Supported
	Other emails	Supported	Supported
	Fax number	Supported	Supported
	Mail nickname	Supported	Supported
	Age group	Supported	Supported

Object Types		Backup	Restore
	Consent provided for minor	Supported	Supported
	Account enabled	Supported	Supported
	Usage location	Supported	Supported
	preferredLanguage	Supported	Supported
	preferredDataLocation	Supported	Supported
	passwordPolicies	Supported	Supported
Assigned roles		Supported	Supported
Group		Supported	Supported
Application		Supported	Supported
License		Unsupported	Unsupported
Device		Unsupported	Unsupported
Azure role assignment		Unsupported	Unsupported
Authentication method	phoneAuthenticationMethod	Supported	Supported
	emailAuthenticationMethod	Supported	Supported

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.