Quest

Quest® On Demand Recovery

User Guide

Legend

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

IMPORTANT, **NOTE**, **TIP**, **MOBILE**, or **VIDEO**: An information icon indicates supporting information.

On Demand Recovery User Guide
Updated - March 21, 2024

Contents

About Quest® On Demand Recovery

Quest® On Demand Recovery cloud application lets you perform the following operations:

- Backup Azure Active Directory and Office 365 users, groups, contacts, service principals, device information, Conditional Access policies, navigation properties, and Application Proxy settings.
- Support for Azure Active Directory B2C tenants.
- Restore Azure Active Directory and Office 365 users, groups, service principals, devices, Conditional Access policies, inactive mailboxes for permanently deleted users, and Application Proxy settings. The application can process two types of Office 365 groups: Office 365 groups and security groups. Group membership and ownership is restored for both types of groups.
- Backup and restore multifactor authentication settings.
- View differences between the selected backup and live Azure Active Directory or Office 365 and revert unwanted changes in the Differences report.
- Configure integration with Quest Recovery Manager for Active Directory to restore on-premises Active Directory objects.

The objects can be selected in a backup and then restored to Azure Active Directory or Office 365 without affecting other objects or attributes. Using the granular restore, objects that were accidentally deleted or modified can be recovered in a few minutes.

On Demand Recovery can be started from Quest On Demand single SaaS command point. For more information about Quest On Demand, see the Quest On Demand product documentation.

To access On Demand, you need to provide On Demand credentials or use your existing Quest Software account. For more details, see Signing up for Quest On Demand in the *On Demand Global Settings User Guide*.

The following sections describe how to configure and work with On Demand Recovery:

- On Demand Recovery Module Overview
- Before You Start
- Sign up for Quest On Demand
- Adding an Azure Active Directory Tenant
- Required Permissions
- Office 365 Tenant Requirements (Mailbox Data Protection)
- Access Control
- Working with On Demand Recovery
- Backup Unpacking
- Which Objects Can Be Restored from the Recycle Bin?
- Restoring Users

2

On Demand Recovery Module Overview

The main screen, called **Dashboard**, is opened after you connect to your Azure Active Directory tenant. The user interface of the administrative console consists of four main screens:

- **Dashboard**
  This is the main screen in the module. It is a source of all general information regarding current project status. You can view and open tasks from the **Dashboard**, view and manage available connections, view object charts and monitor recent errors. The toolbar provides links to most general tasks such as managing tenants, unpacking backups and browsing objects to restore.
- **Backups**
  This screen shows a list of backups that were created for the selected tenant.
- **Unpacked Objects**
  This screen contains all objects that were extracted from the selected backup and operations you can perform on them.
- **Differences**
  This screen allows you to compare the current state of objects in live Azure Active Directory or Office 365 with their state in a backup and roll back unwanted changes. This helps when troubleshooting problems that may result from the deletion or modification of critical objects.
- **Events**
  This screen provides you detailed information about errors and warnings that occur during backup creation and restore operations.
- **Tasks**
  This screen allows you to view task statuses and manage them.

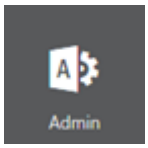
Before You Start

To access your Azure Active Directory or Office 365 tenant via On Demand Recovery, use an Administrative account that has the **Global Administrator** role. If you do not have an account with the **Global Administrator** permissions, you should create the account by using one of the procedures described below.

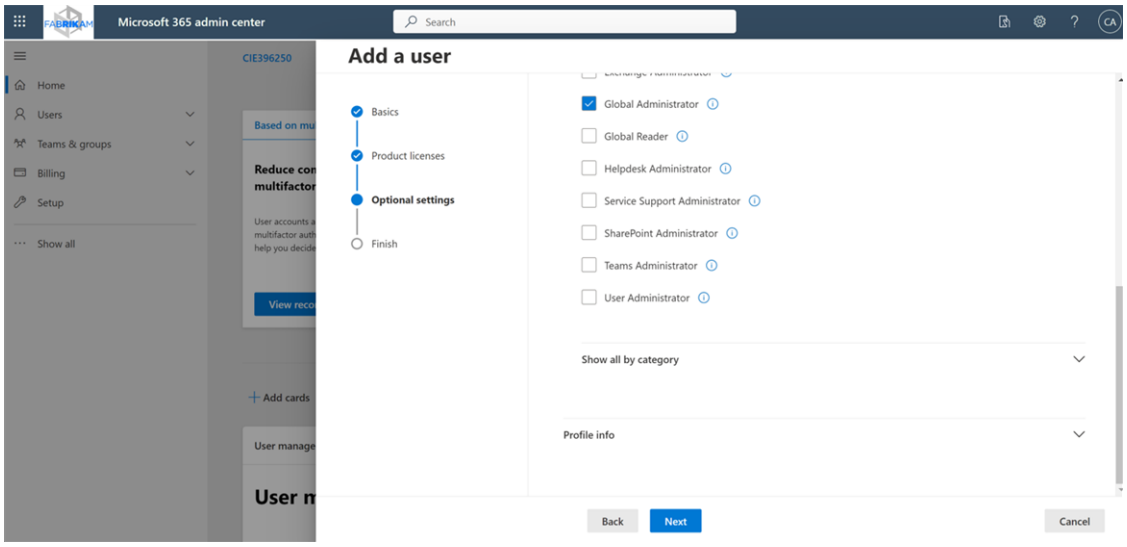
NOTE: Azure Active Directory is now Microsoft Entra ID.

To create an administrative user account with the Global Administrator role in Office 365 Admin Center

1. Sign in to Office 365 with your administrative account using this link https://login.microsoftonline.com.
2. Click the **Admin** tile.



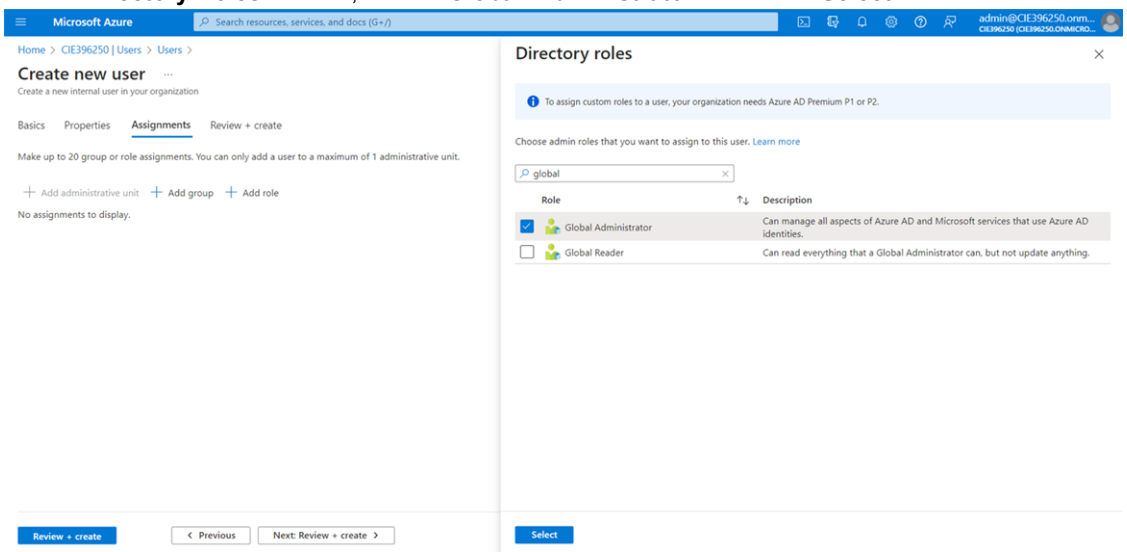
3. From the home screen, in the **User management** tile, click **Add user**.
4. Specify all necessary user information. In **Optional settings**, click **Roles**, then **Admin center access**, and check **Global Administrator**.



5. Click **Next**.
6. Once you have reviewed the information, click **Finish adding**.
7. Now you can use this user account to access your Office 365 tenant in On Demand Recovery.

To create an administrative user account with the Global Administrator role in Azure Management Portal

1. Log into the Azure Management Portal (https://portal.azure.com/) with your individual account.
2. Select your tenant from the list of available tenants. To view the list of tenants, click on your profile icon in the upper-right corner of the screen.
3. Navigate to the **Azure Active Directory** section in the left pane.
4. In the **Users** tab, click **New user**, then **Create new user**. Enter your basic details.
5. On the **Assignments** tab, click **Add role**.
6. In the **Directory roles** section, check **Global Administrator** and click **Select**.



7. Click **Review + create**.
8. Click **Create**.

4

Sign up for Quest On Demand

To get access to On Demand Recovery, you need to sign up for the Quest On Demand service and create an organization. For that, go to Quest On Demand and use one of the following options:

- Sign up using the existing Quest account
- Create a new Quest account and sign up for Quest On Demand
- Join an existing On Demand organization

For more details, refer to the Signing up for Quest On Demand section in *On Demand Global Settings User Guide*.

5

Adding an Azure Active Directory Tenant

For instructions on how to add or remove an Azure AD tenant, see the Tenant Management section in the *On Demand Global Settings User Guide*.

NOTE: Although GCC High tenants can be added on the **Tenants** page for use in other On Demand modules, On Demand Recovery does not support restoring objects from GCC High tenants. This type of tenant will not be available for selection in On Demand Recovery. GCC tenants are also not supported.

When a tenant is added, the creation of backups is disabled by default. You must enable the backup creation as described in Step 6 in Working with On Demand Recovery.

6

Required Permissions

This section lists the minimum user account permissions required to perform specific On Demand Recovery tasks.

Azure Account Used to Grant Consents

The ability for On Demand service principals to access and operate with tenant assets requires explicit permissions. The Tenant Administrator grants these permissions through consents.

Each tenant that is added has granted consent to the initial Core – Basic permission set to the On Demand service principal. Additional consents are required to work with different features of On Demand Recovery. There are two service principals for On Demand Recovery; **On Demand Recovery Basic** and **On Demand Recovery Restore**. For more information on explicit permission for each service principal, see Basic Consent Permissions and Restore Consent Permissions.

- On Demand Recovery requires Basic consent in the Recovery section. Basic consent is used for all read operations including backups.
    - For backup operations, the Global Reader role can be used.
- On Demand Recovery requires Restore consent in the Recovery section. Restore consent is used for all write operations including restore.
    - For restore operations, the Privileged Authentication Administrator, User Administrator, Windows 365 Administrator and Conditional Access Administrator roles must be used. In addition, if any Conditional Access policies use a custom security attribute, the Attribute Definition Reader role will also be required.

For some advanced features, a separate service account is required and you must specify this service account in the backup settings.

Role definitions for On Demand Recovery

- **User Administrator:** User Administrator role is required to check if user is soft-deleted. It checks if the user is in the Recycle Bin or not.
- **Privileged Authentication Administrator:** Privileged Authentication Administrator role is required to set the MFA setting of the user to enforced state from either enabled or disabled state.
- **Windows 365 Administrator:** Windows 365 Administrator role is required to restore devices and their owner or owned links.
- **Conditional Access Administrator:** Conditional Access Administrator role is required to restore Conditional Access policies.

- **Attribute Definition Reader:** Attribute Definition Reader is role is required only if Conditional Access policy uses filters for application on custom security attributes. If the filters are on default schema attributes, this role is not required while restoring or updating Conditional Access policies.

Basic Consent Permissions

In addition to the base consents required by On Demand, On Demand Recovery requires the following consents and permissions.

To view the list of Basic consent permissions in On Demand Recovery:

1. Click **Tenants** in the navigation panel on the left and click **Edit Consents** for the required tenant.
2. Go to the **Basic** tile, under **Recovery**.
3. Under **Status and Actions**, click **View Details**.

Application permissions are used in the app-only access scenario, without a signed-in user present. The application will be able to access any data that the permission is associated with. Only an administrator or owner of the service principal can consent to application permissions.

Delegated permissions are permissions that allow the application to act on a user's behalf. The application will never be able to access anything the signed in user themselves could not access.

For more information on application and delegated permissions, click here.

Type	Permissions	Application api name
Application	*Application.Read.All* Allows the app to read all applications and service principals without a signed-in user.	Microsoft Graph
Application	*DelegatedPermissionGrant.Read.All* Allows the app to read all delegated permission grants, without a signed-in user.	Microsoft Graph
Application	*Device.Read.All* Allows the app to read your organization's devices' configuration information without a signed-in user.	Microsoft Graph
Application	*Directory.Read.All* Allows the app to read data in your organization's directory, such as users, groups and apps, without a signed-in user.	Microsoft Graph
Application	*Group.Read.All* Allows the app to read group properties and memberships, and read the calendar and conversations for all groups, without a signed-in user.	Microsoft Graph
Application	*Policy.Read.All* Allows the app to read all your organization's policies without a signed in user.	Microsoft Graph

Type	Permissions	Application api name
Application	*RoleManagement.Read.Directory* Allows the app to read the role-based access control (RBAC) settings for your company's directory, without a signed-in user. This includes reading directory role templates, directory roles and memberships.	Microsoft Graph
Application	*User.Read.All* Allows the app to read the full set of profile properties, group membership, reports and managers of other users in your organization, without a signed-in user.	Microsoft Graph
Application	*UserAuthenticationMethod.Read.All* Allows the app to read authentication methods of all users in your organization, without a signed-in user. Authentication methods include things like a users 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.	Microsoft Graph
Delegated	*email* Allows the app to read your users' primary email address.	Microsoft Graph

Restore Consent Permissions

As well as the Basic consents required by On Demand Recovery, On Demand Recovery requires the following permissions to be granted consent for restore operations.

To view the list of Restore consent permissions in On Demand Recovery:

1. Click **Tenants** in the navigation panel on the left and click **Edit Consents** for the required tenant.
2. Go to the **Restore** tile, under **Recovery**.
3. Under **Status and Actions**, click **View Details**.

Application permissions are used in the app-only access scenario, without a signed-in user present. The application will be able to access any data that the permission is associated with. Only an administrator or owner of the service principal can consent to application permissions.

Delegated permissions are permissions that allow the application to act on a user's behalf. The application will never be able to access anything the signed in user themselves could not access.

For more information on application and delegated permissions, click here.

Type	Permissions	Application api name
Application	*Application.ReadWrite.All* Allows the app to create groups, read all group	Microsoft Graph

Type	Permissions	Application api name
	properties and memberships, update group properties and memberships, and delete groups. Also allows the app to read and write group calendar and conversations. All of these operations can be performed by the app without a signed-in user.	
Application	*AppRoleAssignment.ReadWrite.All* 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.	Microsoft Graph
Application	*Device.ReadWrite.All* Allows the app to read and write all device properties without a signed in user. Does not allow device creation or update of device alternative security identifiers.	Microsoft Graph
Application	*Directory.ReadWrite.All* Allows the app to read and write data in your organization's directory, such as other users, groups. It does not allow the app to delete users or groups, or reset user passwords.	Microsoft Graph
Application	*Group.ReadWrite.All* Allows the app to create groups, read all group properties and memberships, update group properties and memberships, and delete groups. Also allows the app to read and write group calendar and conversations. All of these operations can be performed by the app without a signed-in user.	Microsoft Graph
Application	*Policy.Read.All* Allows the app to read all your organization's policies without a signed in user.	Microsoft Graph
Application	*Policy.ReadWrite.ConditionalAccess* Allows the app to read and write your organization's conditional access policies on behalf of the signed-in user.	Microsoft Graph
Application	RoleManagement.ReadWrite.Directory 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.	Microsoft Graph

Type	Permissions	Application api name
Application	*UserAuthenticationMethod.ReadWrite.All* 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.	Microsoft Graph
Application	*User.ReadWrite.All* Allows the app to read and write the full set of profile properties, group membership, reports and managers of other users in your organization, without a signed-in user. Also allows the app to create and delete non-administrative users. Does not allow reset of user passwords.	Microsoft Graph
Delegated	*Directory.AccessAsUser.All* Allows the app to have the same access to information in your work or school directory as you do.	Microsoft Graph
Delegated	*Directory.ReadWrite.All* 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 Graph

Exchange Online PowerShell Consent

To perform Exchange tasks, you will need to grant consent to Exchange Online PowerShell, and assign the Exchange Admin Role. For details, please see the About admin consent status and the Granting and regranting admin consent sections in the *On Demand Global Settings User Guide*.

Service Credential Permissions

For some advanced features, a service account must be specified and are required in addition to consent permissions. A separate service account is used for backup operations for the following advanced features:

- Conditional Access policies
- Service Principal Default policies

Table 1: Backup Service Credential Permissions

For backup of advanced features, a service account must be specified in the backup settings. This service account is used to backup and read the following advanced features.

On Demand Recovery feature	Required Directory role
Backup of Conditional Access policies	Global Reader
Backup of Service Principal Default policies	Global Reader

Office 365 Tenant Requirements (Mailbox Data Protection)

Office 365 and on-premises Exchange offer some native means of protection against losing valuable data. To prevent the permanent deletion of mailbox data and to be able to restore a mailbox when it is deleted from the Recycle Bin, it is strongly recommended that you use Office 365 retention policy or Litigation Hold.

Office 365 Retention Policy

Retention policies do two basic things: they either protect data from deletion or delete unnecessary items.

- **Retain content** - content cannot be permanently deleted before the end of the retention period.
- **Delete content** - unnecessary content is permanently deleted at the end of the retention period.

You can create and manage retention policies on the:

- **Policies** page in the Microsoft 365 compliance center.
- **Retention** page under Data governance in the Office 365 Security & Compliance Center.

For details, see https://docs.microsoft.com/en-us/office365/securitycompliance/retention-policies.

Litigation Hold

As an alternative to retention policies, you can place a mailbox on Litigation Hold to preserve all mailbox content, including deleted items and original versions of modified items.

For more information, see https://docs.microsoft.com/en-us/exchange/policy-and-compliance/holds/litigation-holds?view=exchserver-2019.

8

Access Control

Quest On Demand provides permission-based roles to determine what permission level a user has and what tasks the user can perform.

For more details, see Adding users to an organization section in the *On Demand Global Settings User Guide.*

List of permissions that can be assigned to Recovery module users

- Can manage backup settings
- Can download hybrid credentials
- Can run backup manually
- Can unpack backups
- Can run difference report
- Can restore from objects
- Can restore from differences
- Can read backup history
- Can read unpacked objects
- Can read differences
- Can read task history
- Can read events
- Can read restore attributes
- Can read UI projects
- Can read UI collections
- Can manage events

NOTE: On Demand administrators have full access to global settings and all module permissions.

Working with On Demand Recovery

This section provides step-by-step instructions on how to use On Demand Recovery.

NOTE:

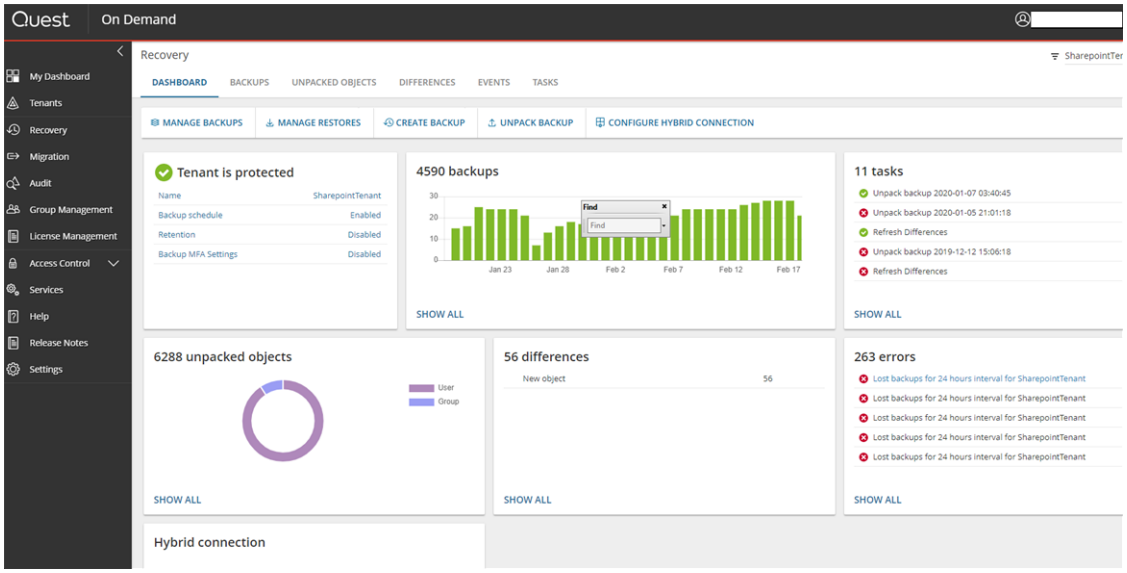
- **For Office 365 tenants**: On Demand Recovery can backup and restore Office 365 users, Office 365 groups and security groups. Group membership and ownership is restored for both types of groups. The product does not restore any resources associated with Office 365 groups and Microsoft Teams, such as conversations, Planner tasks and plans.
- Email notifications about failed backups can be enabled by request. For assistance, contact Quest Support.

1. Go to Quest On Demand and sign up for Quest On Demand. For more details, refer to Sign up for Quest On Demand.
2. Add your Azure Active Directory tenant as described in the Tenant Management section in the *On Demand Global Settings User Guide*.
3. After the tenant is added, make sure that the permissions required to work with Azure Active Directory tenant are granted. To grant the required permissions, click **Go** on the tenant tile and check that the Recovery module has the **Granted** status. For details, please see the Admin Consent Status section in the *On Demand Global Settings User Guide*. For a list of permissions that need to be granted consent for On Demand Recovery, refer to Consent permissions.

   NOTE: Microsoft admin consent status is "expired" after 90 days and the Recovery module status is changed to "Not Granted". Once expired, you must grant admin consent again to continue using the module.

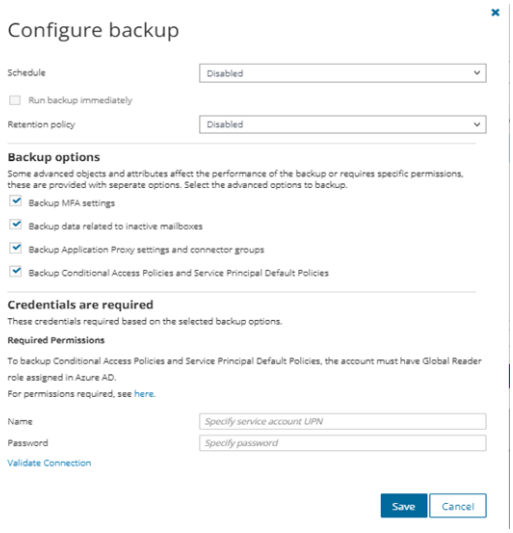
4. To perform Exchange tasks, you will need to grant consent to Exchange Online PowerShell, and assign the Exchange Admin Role. For details, please see the About admin consent status and the Granting and regranting admin consent sections in the *On Demand Global Settings User Guide*.

5. To launch On Demand Recovery, click **Recovery** on the left pane. The **Dashboard** screen opens.



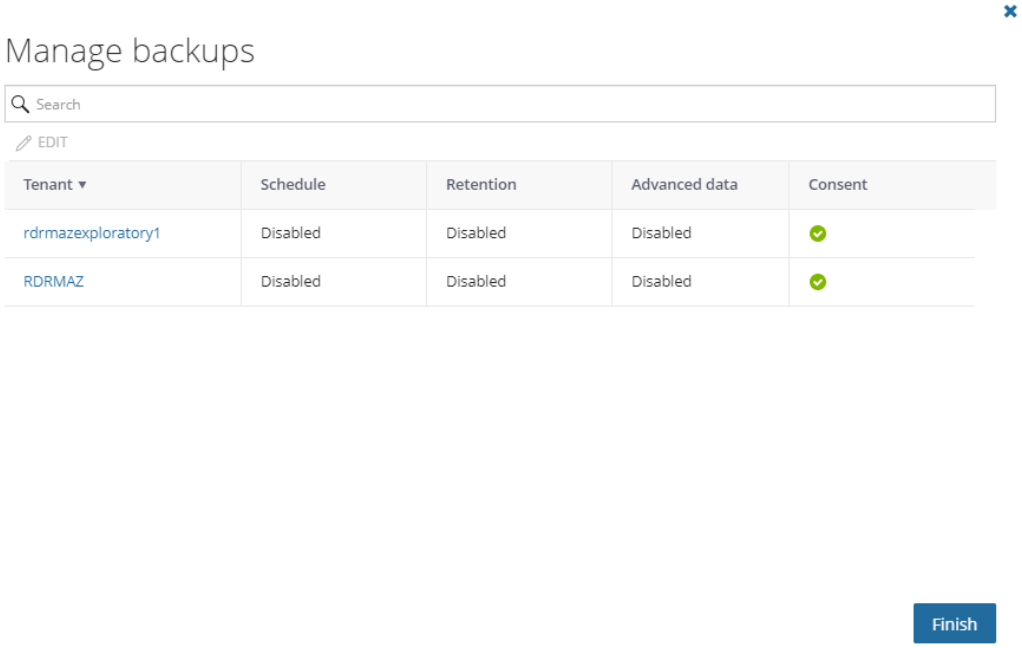
6. To configure a hybrid connection with on-premises Active Directory, see Integration with Recovery Manager for Active Directory.

7. To configure the backup settings, perform the following steps:
   a. Click **Manage backups** on the **Dashboard** screen.
   b. Select the tenant from the list and click **Edit**. The **Configure backup** dialog opens.



   - To enable the backup creation, select **Enabled** next to the **Schedule** option. On Demand Recovery will attempt up to 4 backups per day. Depending on the completion time required for each, the number of backups may be less.
   - Choose to immediately run the backup by selecting the **Run backup immediately** option. Deselecting this option will allow backups to only run when scheduled.
   - Specify the backup retention period using the **Retention policy** option in days. The backup retention policy is also applied to backups that are started manually. If no policy is set, the default retention policy is five years (1825 days). If the retention period is changed, the new policy will only affect new backups.
   - To backup multifactor authentication settings, select the **Backup MFA settings** option.
   - To backup data related to inactive mailboxes, select the **Backup data related to inactive mailboxes** option.
   - To backup Application Proxy settings, select the **Backup Application proxy settings and connector groups** option.
   - To backup service principal default policies and Conditional Access policies, select the **Backup Conditional Access Policies and Service Principal Default Policies** option.
     - By selecting this option, service principal default policies such as ClaimIssuancePolicy and TokenIssuancePolicy and their relation to service principals will be backed up.
     - You will need to specify service account credentials for the tenant if selecting this option. For details about required permissions, see Required permissions.
   c. Check the status of the module admin consent.

d. If you need to run the backup creation manually, go to the **Tasks** screen, select the Backup task and click **Start**.

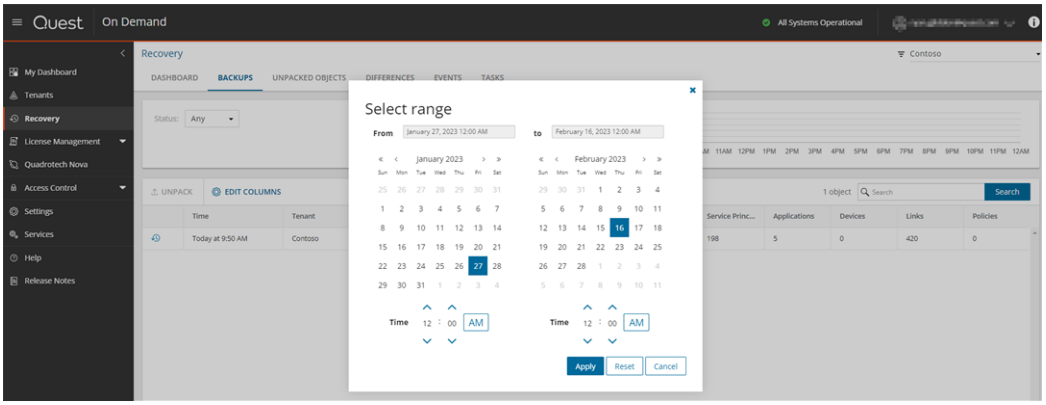


8. To start the backup creation manually, you can use the **Create Backup** option on the **Dashboard** screen.

9. To unpack a backup:

   a. Go to the **Backups** screen. Here, you will find each packed backup, and the properties associated with that backup.

   > **NOTE:** The Users column reflects the total number of users including guest accounts. The Guest column reflects only guest accounts.

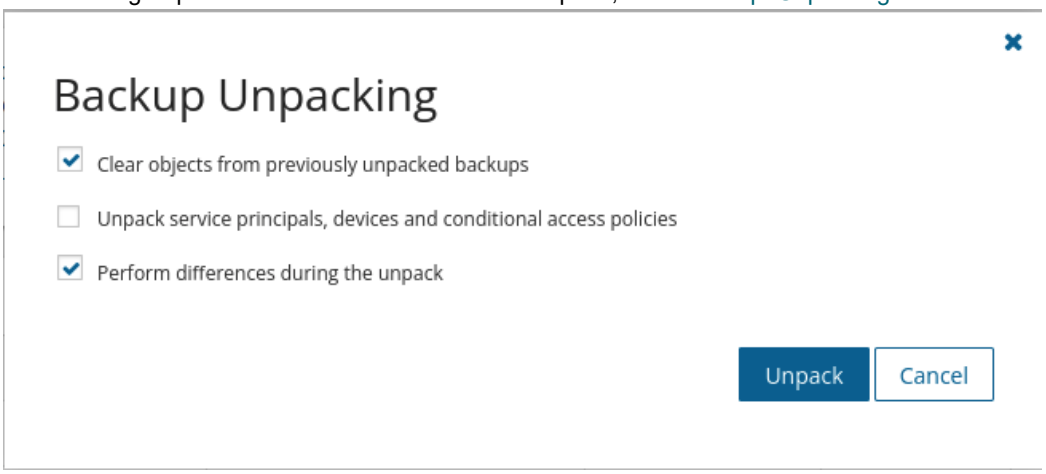


   b. From the **Tenant** drop-down list, select the tenant, then select the backup you want.

   c. You can specify predefined or custom date ranges to narrow the search results by selecting Custom range.

   d. Click **Unpack** in the actions menu.

   e. If the option **Unpack service principals and devices** is not selected, the unpack operation will work faster and the **Differences** report will contain only changes related to users and groups. For more details about this option, see Backup Unpacking.

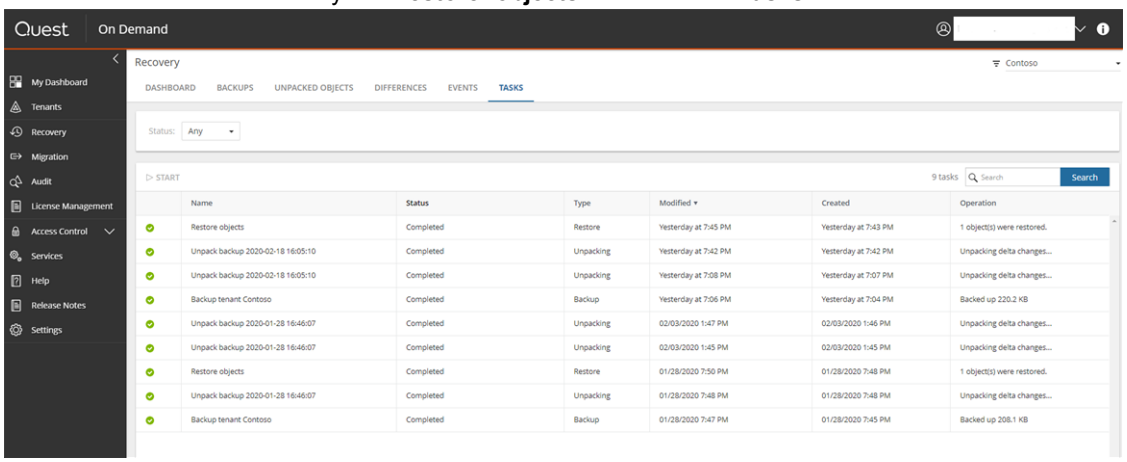


   f. In the **Backup Unpacking** dialog, click **Unpack**.

10. When the **Unpack backup** task is completed, go to the **Unpacked Objects** screen and select the users and groups that you want to restore and click **Restore**.

    > **NOTE:** If you do not unpack a backup, the **Unpacked Objects** screen will contain no objects or show a list of objects that were extracted from the previously unpacked backup.

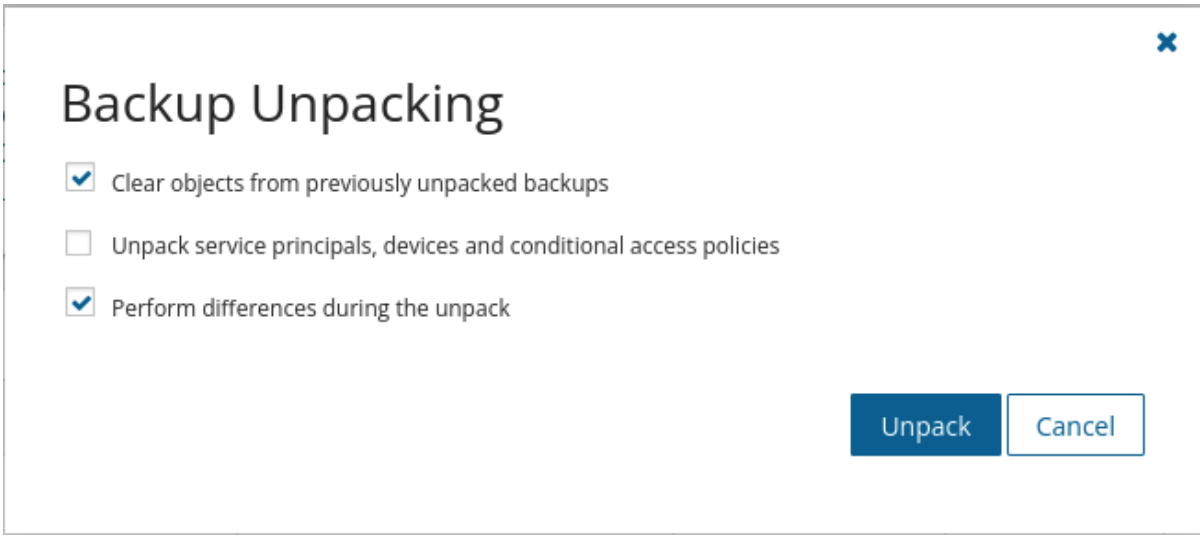
11. In the **Restore Objects** dialog, select the options for restore. See the **To restore objects** section in the Restoring Objects page for information on each option.
12. Also, you can view differences between the selected backup and live Azure Active Directory or Office 365 and revert the selected changes using the **Differences** report tool. For more details, see the Reporting section. You can export the selected report data to the CSV file.
13. You can view the status of your **Restore objects** task on the **Tasks** screen.



14. Open the **Events** screen to view errors or warnings, if they occur during the restore operation.
    - Use the **Export** option to export the selected log data to the CSV format.
    - Use the **Acknowledge** option to hide events that are not actual anymore. The status of acknowledged events is changed from 'Current' to 'Obsolete'. To view the list of obsolete events, click **Obsolete** on the left side of the screen.

Backup Unpacking

In the **Backup Unpacking** dialog, you have the option to **Unpack service principals, devices, and conditional access policies**. If this option is not selected, the unpack operation will work faster and the **Differences** report will contain only changes related to users and groups. Otherwise, you will see changes related to users, groups, service principals, devices, and Conditional Access policies. The table below provides the full list of objects and changes that will be shown on the corresponding screens.



If the **Unpack service principals, devices, and conditional access policies** option is **NOT** selected, the following items will be shown:

Unpacked Objects view

- User
- Group

Differences view

- User
- Group
- DirectoryLinkChange
- DirectoryRoleLinkChange

If the **Unpack service principals, devices, and conditional access policies** option is selected, the following items will be shown:

Unpacked Objects view

- User
- Group
- Service Principal
- Device

Differences view

- User
- Group
- Service Principal
- Device
- OAuth2PermissionGrant
- AppRoleAssignment
- OwnerLinkChange
- GroupOwnerLinkChange
- DirectoryRoleLinkChange
- RegisteredOwnerDeviceLinkChange
- RegisteredUserDeviceLinkChange

Perform differences during the unpack is selected by default. The differences operation will automatically begin during unpack operation. If this is not selected, then only the unpack operation will be performed.

11

Restoring Objects

After you complete an **Unpack backup** task, go to the **Unpacked Objects** tab to select the objects that you want to restore.

> **NOTE:** If you do not unpack a backup, the **Unpacked Objects** tab does not display any objects or shows a list of objects that were extracted from the previously unpacked backup.

You can choose one of the following views to see the unpacked objects:

- **List View** - This view lists the unpacked objects from your backup. You can select objects to export to a CSV file or select objects to restore.
- **Objects** - This view displays the number of unpacked objects by category in graph form. You can use the filters to display specific types of objects.

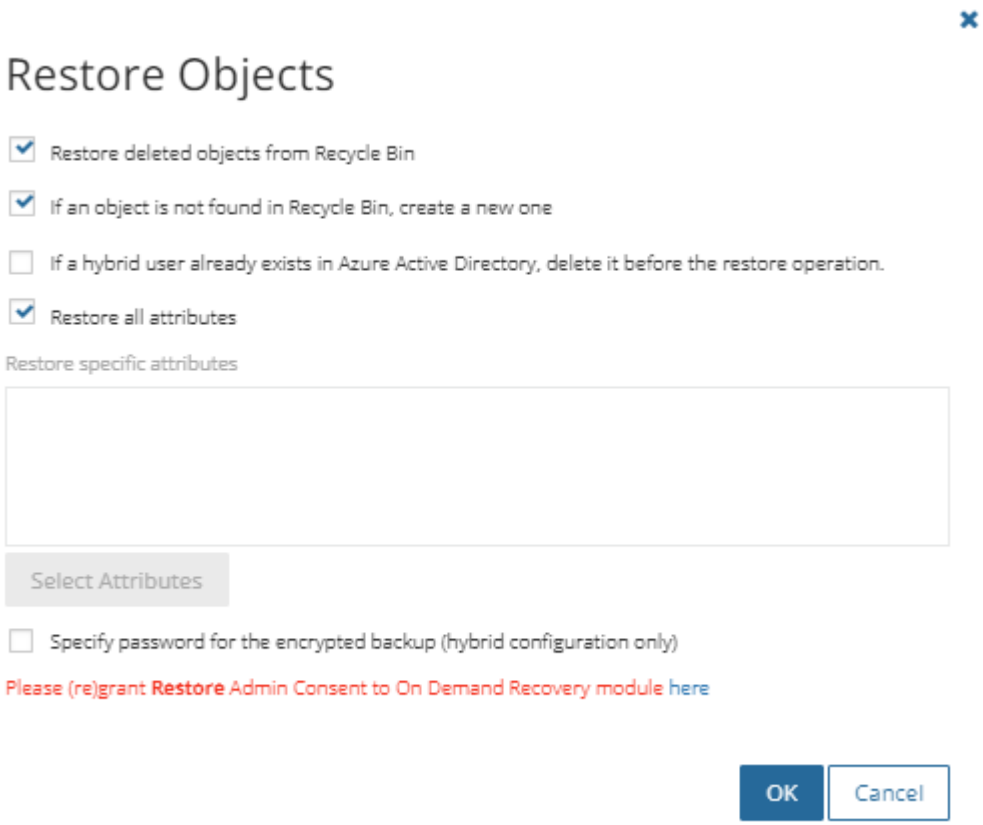
To restore objects

1. On the **Unpacked Objects** tab, **in List View**, click the check boxes next to the objects that you want to restore.
   a. You can use the **Search** field to search for specific objects to restore.
   b. You can use the filters to display specific objects that you want to restore. The following filters are available:
      - **Tenant** - allows you to filter objects by a specified tenant.
      - **Backup** - allows you to filter objects by a specified backup.
      - **Type** - allows you to filter objects by type.
      - **User Type** - allows you to filter objects by type of user.
      - **AAD Connect** - allows you to filter by objects synced from a hybrid environment.
      - **MFA** - allows you to filter objects by multifactor authentication setting.
      - **Mail Enabled** - allows you to filter by objects that have a mailbox (enabled) or do not have a mailbox (disabled).

> **CAUTION:** The Restore button will be disabled when objects from multiple tenants are selected. To display the Restore button, please select a single tenant.

2. Click **Restore**.

3. In the **Restore Objects** dialog, you can select the following options:
    - **Restore deleted objects from Recycle Bin** - This restores accidentally deleted objects from the Recycle Bin. On Demand Recovery preserves original object identifiers (GUID).
    - **If a user or group is not found in Recycle Bin, create a new one** - This recreates permanently deleted users, groups, and subgroups. This option recreates users and groups with attributes that are required for object identification. If you need to restore all attributes for the object including membership information (links), use this option together with the **Restore all attributes** option.
    - **If a hybrid user already exists in Azure Active Directory, delete it before the restore operation** - This action lets you preserve the original cloud mailbox of a hybrid user after restore in the following scenario:
        a. There is a hybrid user. This user is deactivated by the administrator for some reason.
        b. Then the user returns, and the account is enabled again by the administrator. After the activation, the user is recreated in the cloud with the new mailbox.
        c. We want to use the original cloud mailbox for the user. The only one way to do this is to restore the user from a backup. But before the restore, the newly created cloud user must be removed from Azure AD using this option.
    - **Restore all attributes** - This restores all object attributes including membership information (links). If this option is not selected, you can specify specific attributes that you want to restore by clicking **Browse**. .
    - **Restore specific attributes** - see below
    - **Specify password for the encrypted backup** - This allows you to type a password that is used to decrypt the encrypted backup. This is strongly recommended only for hybrid users.
    - You may also need to grant/regrant Restore Admin Consent for the On Demand Recovery module. Ensure this has been completed before progressing.



4. Click **OK**.

To restore selected attributes

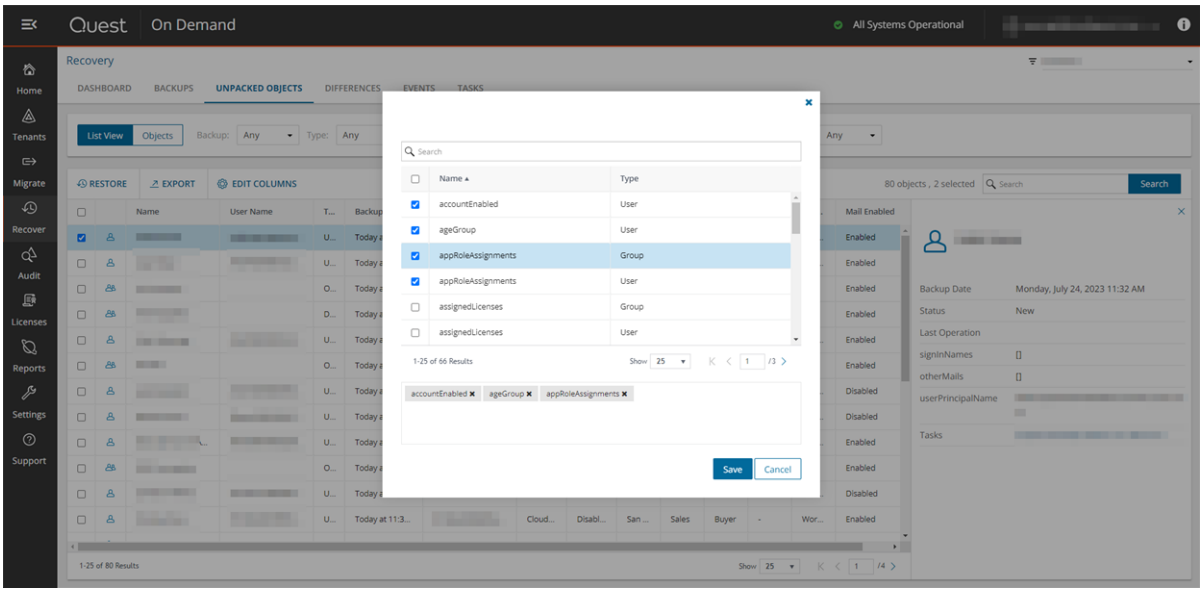
On Demand Recovery allows you to restore specific attributes for each object, with each object type displaying its own list of attributes to restore. To do this:

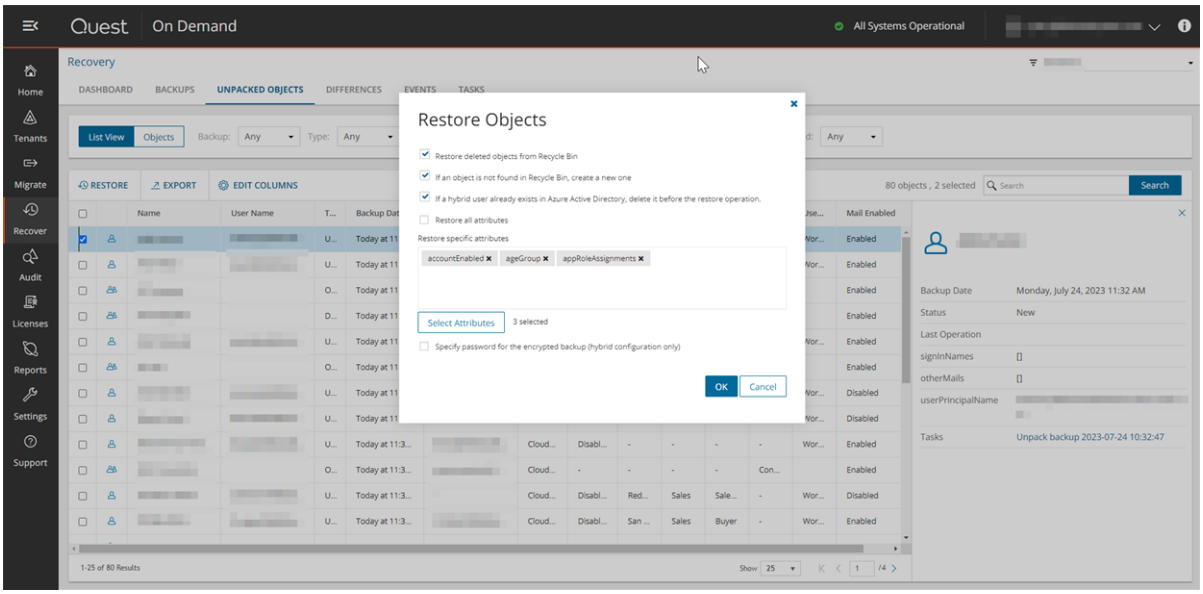
1. Uncheck the **Restore all attributes** option, and click **Select Attributes**.

NOTE: Only the attributes for the selected object type will be displayed.

NOTE: Any application extension attributes found for an object will also be displayed and can be selected for restore.

2. Select the required attributes to restore for the object by checking the box(es). and click **Save**. Your selected attributes will appear in the Restore specific attributes box.
3. Click **OK** when all required options have been selected.





Which Objects Can Be Restored from the Recycle Bin?

On Demand Recovery can restore the following objects from the Recycle Bin:

- Users (all types of users including B2B, B2C, guests, hybrid)
- Office 365 Groups
- Applications

NOTE: Links, permissions, and roles cannot be restored from the Recycle Bin. But if an object from the above list is soft deleted and then recovered from the Recycle Bin, all attributes and links including group membership and app role assignments are preserved by Microsoft.

Objects that cannot be restored from the Recycle Bin:

- Distribution groups
- Security groups
- Mail-enabled security groups
- All groups synchronized by Azure AD Connect from on-premises Exchange server (hybrid configuration)
- Service principals
- Devices

Restoring Passwords

On Demand Recovery does not backup passwords. During the restore of permanently deleted users, the application sets a random password that can be changed by the administrator at the next login.

12

Restoring Directory Roles and Application Roles

On Demand Recovery backs up and restores the assigned roles in Azure AD.

Supported scenarios

The following scenarios are supported in On Demand Recovery:

- Restoring eligible/active assigned roles that are associated with applications integrated with Azure AD. For more information, see Restoring Service Principal bjects.
- Restoring directory roles and their members including users and group members.
- Restoring role assignments for users, groups and service principals.

Limitations

The following roles are not restored by On Demand Recovery:

- Custom Azure AD roles are not restored.
- Custom Office 365 roles are not restored.

Restoring Users

Users that were accidentally deleted can be restored using On Demand Recovery. Users who have been moved to the Deleted users page (soft deleted) can be restored along with users who have been permanently deleted (hard deleted) from Azure AD.

Supported scenarios

The following scenarios are supported by On Demand Recovery:

- Restoring a soft or hard deleted user as a group owner if they were previously an owner of a security group or Microsoft 365 group.

Restored user attributes

For a list of user attributes restored by On Demand Recovery, visit the On Demand Recovery Supported Attributes guide.

13

Restoring Groups

In Azure AD, there are two types of groups; Security and Microsoft 365. When a Microsoft 365 group is deleted in Azure AD, it is soft deleted. That is, the Microsoft 365 group is moved to the Deleted groups page where it can be restored or permanently deleted. When a security group is deleted in Azure AD, it is hard deleted. That is, the security group is permanently deleted and not moved to the Deleted groups page. The Differences report in On Demand Recovery identifies groups as being either hard deleted or soft deleted in Azure AD. Both types of groups can be restored from the Differences report.

Supported scenarios

The following scenarios are supported in On Demand Recovery:

- Restoring group owners associated with a security group.
- Restoring group owners associated with a Microsoft 365 group.

Restored group attributes

For a list of group attributes restored by On Demand Recovery,visit the On Demand Recovery Supported Attributes guide.

Limitations

The following groups are not restored by On Demand Recovery:

- Distribution groups

Restoring Service Principal Objects

On Demand Recovery supports backing up and restoring service principal objects with the following properties:

- **oAuth2PermissionGrants** - the OAuth 2.0 scopes (delegated permissions) that have been granted to an application (represented by a service principal) as part of the user or admin consent process.
- **appRoleAssignments** - link between a service principal and a directory object.
- **roles** - administrator roles in Azure Active Directory. Refer to this article for details.
- **appRoles** - the collection of application roles that an application may declare.
- **Service principal owners** - the owners are a set of users who are allowed to modify service principal objects.

For the full list of service principal attributes that are restored and not restored by On Demand Recovery, see How does On Demand Recovery Handle Object Attributes?

What is the difference between a service principal object and an application object?

When you register an Azure AD application in the Azure portal, two objects are created in your Azure AD tenant; an application object and a service principal object.

- **Application object**
  An Azure AD application is defined by its one and only application object, which resides in the Azure AD tenant where the application was registered, known as the application's "home" tenant. The Azure AD Graph Application entity defines the schema for an application object's properties.
- **Service principal object**
  In order to access resources that are secured by an Azure AD tenant, the entity that requires access must be represented by a security principal. This is true for both users (user principal) and applications (service principal). The security principal defines the access policy and permissions for the user/application in that tenant. This enables core features such as authentication of the user/application during sign-in, and authorization during resource access.
  When an application is given permission to access resources in a tenant (upon registration or consent), a service principal object is created. The Azure AD Graph ServicePrincipal entity defines the schema for a service principal object's properties.

For more details, see https://www.microsoftpressstore.com/articles/article.aspx?p=2473127.

Service principals provisioned from Azure Gallery

On Demand Recovery supports restoring service principals provisioned from Azure Gallery for users that have the service account for the tenant. This account must have at least the **User Administrator** role in the Azure portal.

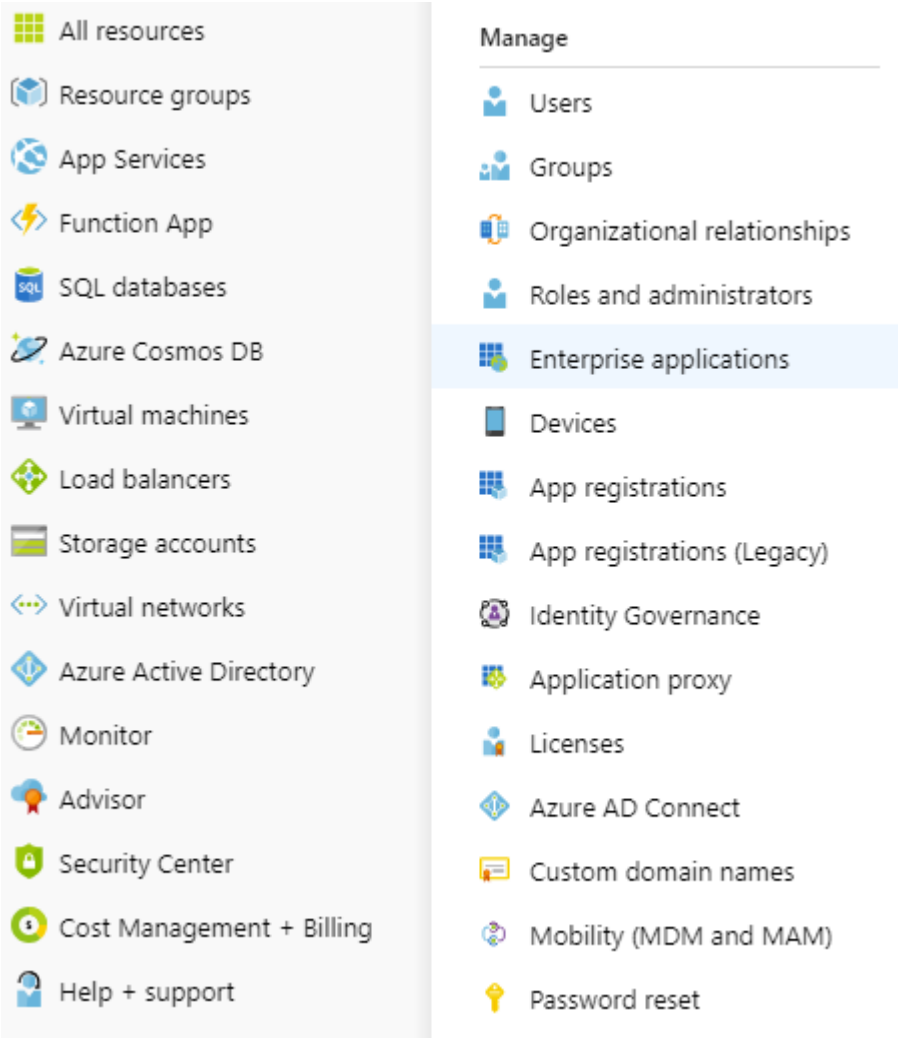
Limitations: On Demand Recovery does not backup certificate settings for applications.

To make SAML SSO work after the restore of a service principal provisioned from Azure Gallery, you must install the new certificate for the corresponding application. For details on how to provide the certificate for a particular

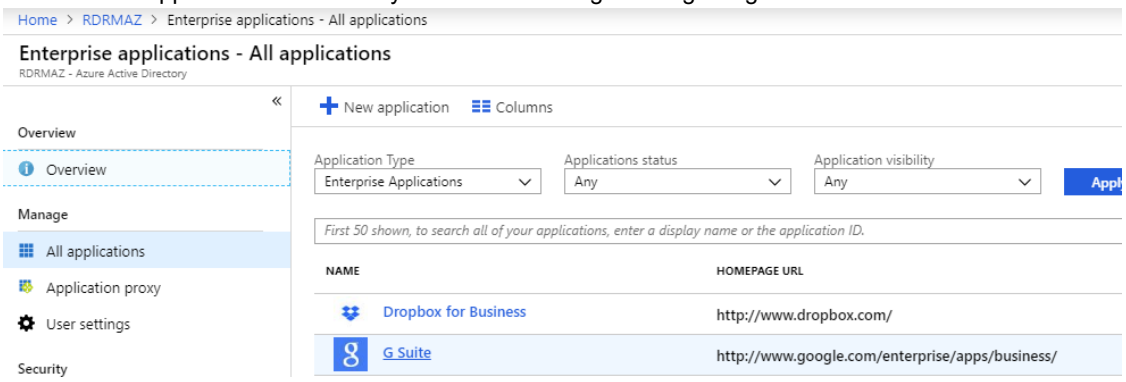
application, refer to the application configuration guide.

To access the application configuration guide

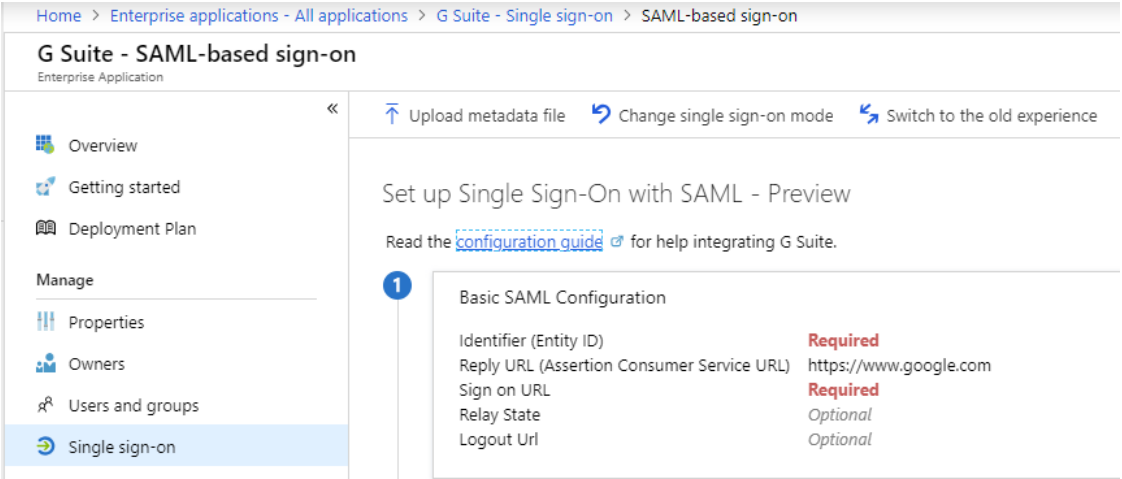
1. In Azure Management Portal, navigate to the **Azure Active Directory** section in the left pane and click **Enterprise applications**.



2. Choose the application for which you want to configure single sign-on.



3. Under the **Manage** section, select **Single sign-on**.



4. Click the **configuration guide** link.

Which actions are shown in the Differences report for a service principal?

- Deletion of a service principal object
- Changes to the accountEnabled attribute
- Add/remove roles assigned to service principals (custom roles are not monitored)
- Add/remove owners from service principals
- Add/remove owners from application

Names of administrator roles in the Azure portal are slightly different from the names of the corresponding roles that are shown in the **Differences** report. For information, see the following comparison table:

Table 2: Names of administrator roles in the Azure portal and the corresponding role in the Differences report

Azure portal	Differences report
Global Administrator	Company Administrator
Billing Administrator	Billing Administrator
Compliance Administrator	Compliance Administrator
Conditional Access Administrator	Conditional Access Administrator
Dynamics 365 Administrator	CRM Service Administrator
Exchange Administrator	Exchange Service Administrator
Guest Inviter	Guest Inviter
Password Administrator	Helpdesk Administrator
Azure Information Protection administrator	Information Protection Administrator
Intune Administrator	Intune Service Administrator
Skype for Business Administrator	Lync Service Administrator

Azure portal	Differences report
Power BI Administrator	Power BI Service Administrator
Privileged role Administrator	Privileged Role Administrator
Reports Reader	Reports Reader
Security Administrator	Security Administrator
Security Reader	Security Reader
Service Administrator	Service Support Administrator
User Administrator	User Account Administrator

15

Restoring Applications

You can restore applications from the Recycle Bin as well as hard deleted applications. On Demand Recovery performs the following actions when restoring applications:

- If there is an application in the Recycle Bin, it is restored. After the application is restored, On Demand Recovery restores application attributes that are in the backup.
- If there is no application in the Recycle Bin, On Demand Recovery attempts to restore it from the backup.

Supported scenarios

The following scenarios are supported by On Demand Recovery:

- Restoring hard deleted applications.
- Restoring soft deleted applications.
- Restoring applications from the Recycle Bin.

16

Restoring Application Proxy Settings

On Demand Recovery supports the recovery of Application Proxy settings, Connector groups, and Connector group membership.

Supported scenarios

The following scenarios are supported in On Demand Recovery:

- Restoring changes to Application Proxy configuration.
- Restoring connector group membership if an Application Proxy is moved into another connector group.
- If an Application Proxy is moved into another connector group and the previous connector group was deleted, On Demand Recovery puts the Application Proxy back to the connector group with the same name.
- If an Application Proxy is put into another connector group and the previous connector group is deleted and there is no connector group with the same name, the new connector group with this name will be automatically recreated and the Application Proxy will be put into it.

Limitations

All of the Application Proxy settings can only be restored at once, granular restore of Application Proxy settings is not supported.

Configuration data restored for an Application Proxy item

On Demand Recovery restores the following configuration data for an Application Proxy item:

Connector Groups

For deleted connector groups, On Demand Recovery restores the following attributes:

- name
- region

Other connector group data is currently backed up but cannot be restored.

OnPremisesPublishing Settings

An onPremisesPublishing object represents the set of properties for configuring Application Proxy for an on-premises application.

- externalUrl
- internalUrl
- externalAuthenticationType

- isTranslateHostHeaderEnabled
- isTranslateLinksInBodyEnabled
- isOnPremPublishingEnabled
- isHttpOnlyCookieEnabled
- isSecureCookieEnabled
- isPersistentCookieEnabled
- applicationServerTimeout
- useAlternateUrlForTranslationAndRedirect

For details, see https://docs.microsoft.com/en-us/graph/api/resources/onpremisespublishing?view=graph-rest-beta.

Connectors

Connector data is currently backed up but cannot be restored.

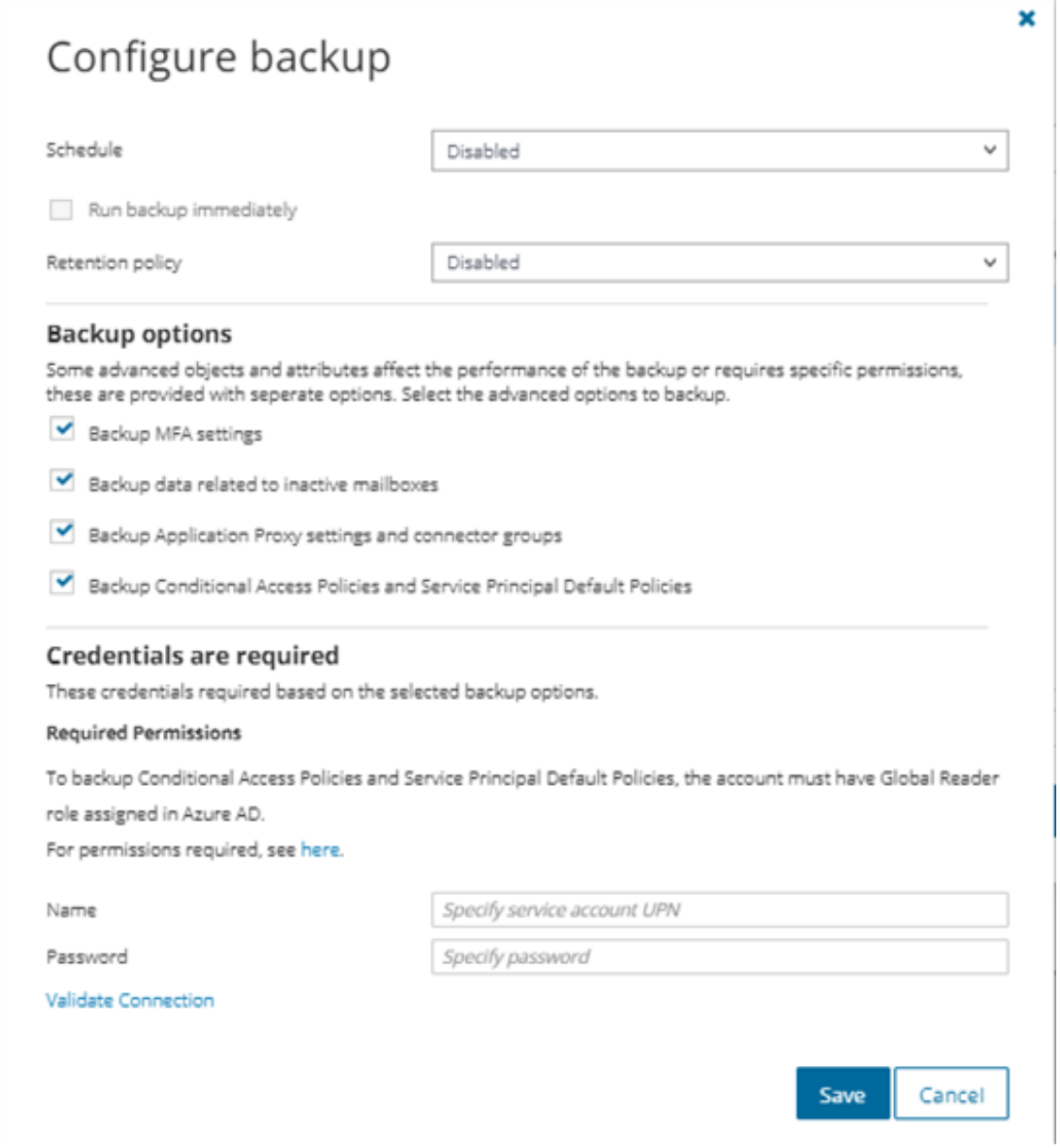
- id
- machineName
- externalIP
- status
- connectorGroupId

Prerequisites

Backing up Application Proxy settings is not enabled by default. You must select this option when configuring backup options.

To backup Application Proxy settings and connector groups

1. Click **Manage backups** on the **Dashboard** screen.
2. Select the tenant from the list and click **Edit**.
   The **Configure backup** dialog opens.



3. Select the **Backup Application Proxy settings and connector groups** option.
4. Click **Save**.

For details, see How does On Demand Recovery Handle Object Attributes?

17

Restoring Multifactor Authentication Settings

On Demand Recovery supports backing up and restoring the following multifactor authentication (MFA) settings:

- Authentication Requirement State
- Authentication Methods. Possible values:
  - One Way SMS
  - Two Way Voice Mobile
  - Two Way Voice Office
  - Phone App Notification
  - Phone App One Time Password
- Default Authentication Method
- Authentication Phone
- Authentication Email
- Alternate Authentication Phone
- Alternate Authentication Email

For more details, see the How does On Demand Recovery Handle Object Attributes? section.

NOTE:

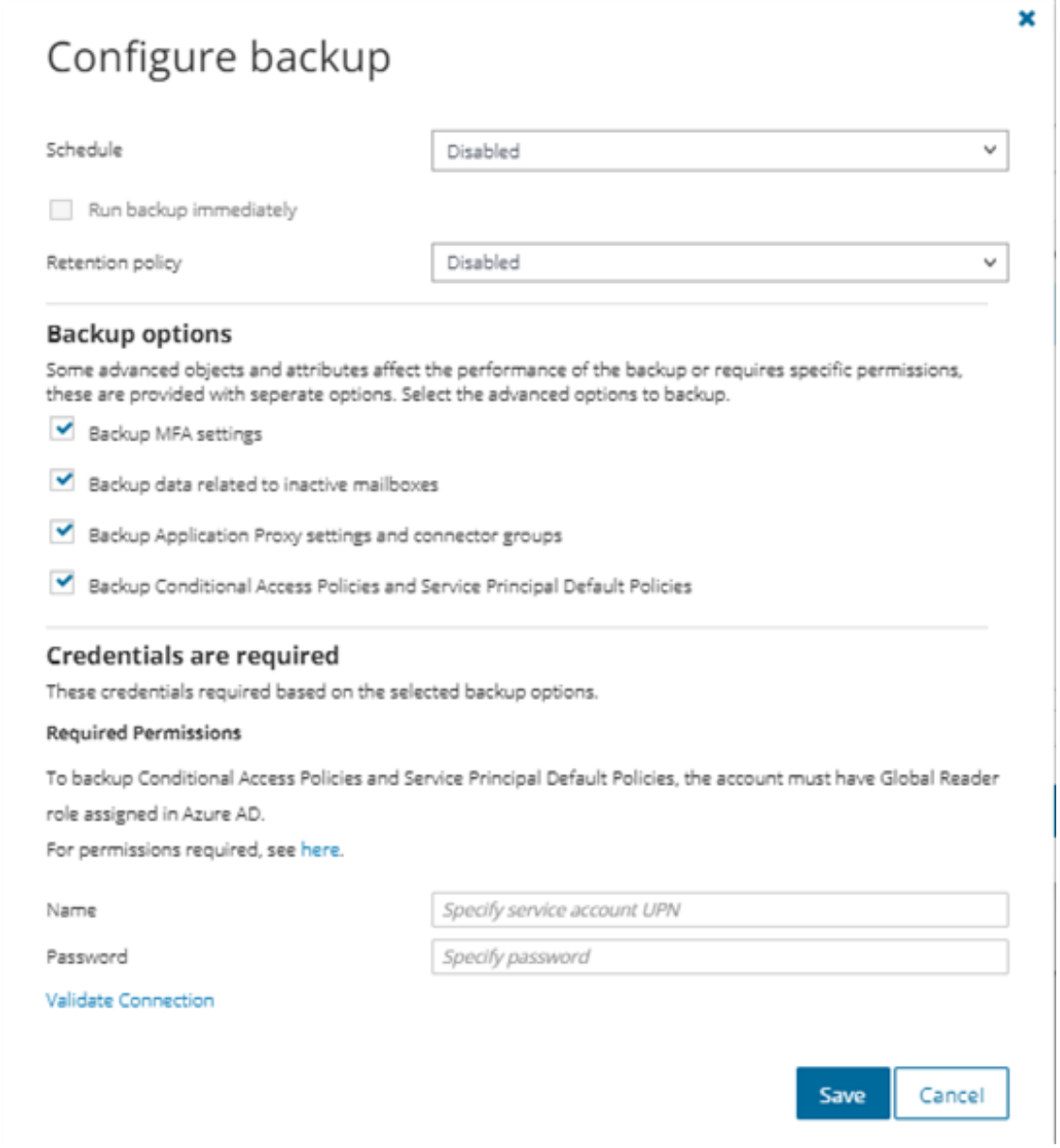
- If a user that uses Microsoft Authenticator as an additional authentication method is permanently deleted, then all authentication methods for this user cannot be restored. On Demand Recovery does not restore binding of the application to the user.
- On Demand Recovery does not restore user passwords.

Prerequisites

Backing up multifactor authentication settings is not enabled by default. You must select this option when configuring backup options.

To backup multifactor authentication settings

1. Click **Manage backups** on the **Dashboard** screen.
2. Select the tenant from the list and click **Edit**.
   The **Configure backup** dialog opens.



3. Select the **Backup MFA settings** option.
4. Click **Save**.

NOTE:

- It is possible to determine the scope of customer IP Prefixes that can access the customer Azure AD tenant using Azure Active Directory (Azure AD) Conditional Access. This option significantly reduces security risks and can be recommended for customers who want to backup multifactor authentication settings. For further information, contact Quest Support.
- Multifactor authentication must be disabled for the On Demand Recovery service account or you should add On Demand Recovery IP prefixes to the list of 'Trusted IPs'.

To configure Trusted IP settings, use this table to allow the following subnets for relevant region:

Region	IP Prefixes
US	52.233.76.96/29
EU	13.69.216.192/29
Canada	20.104.81.8/29
UK	51.145.35.32/29
Australia	20.191.252.152/29

For more details, see Configure Azure Multi-Factor Authentication settings.

18

Restoring Group Licenses

On Demand Recovery restores group licenses, which means reassignment of a license to a group after its recreation or restore from the Recycle Bin. Granular restore of the assignedLicenses attribute is supported as well.

Supported scenarios

The following scenarios are supported by On Demand Recovery:

- If a group is moved to the Recycle Bin, group licenses are restored simultaneously with the group object.
- Direct and inherited licenses for users are now distinguished.
- Inherited licenses are reassigned automatically by restoring membership.
- If the **licenseAssignmentStates** attribute is not present in old backups, user object assignments in Azure AD are used to distinguish inherited and direct licenses.
- The same logic is applied to the **Differences** report to show only one change if a group which is giving licenses was changed or deleted. In this case, the report will contain only the "Group change" or "Group deletion" action.

NOTE: If you are restoring a permanently deleted user from an old backup, the user license may be assigned twice; by group and directly.

19

Restoring Devices

On Demand Recovery can restore Azure AD device objects that were removed from the Azure Portal. For registered or joined devices, single sign-on (SSO) data (if any) is also restored.

Limitations

The following limitation exist when restoring devices in On Demand Recovery:

- Automatically restoring SSO data for a device that was permanently deleted together with the device owner. In this case, the device owner should join the device once again.
- If a device was unjoined by the device owner, it will be restored in the Azure Portal but SSO will not work.

Not supported

The following scenarios are not supported in On Demand Recovery:

- Windows Hello for joined devices
- Microsoft Intune is not supported
- Restricted access for devices
- Restoring of devices in hybrid configuration

Restored devices attributes

For a list of group attributes restored by On Demand Recovery, visit the On Demand Recovery Supported Attributes guide.

20

Restoring Conditional Access Policies

On Demand Recovery supports backing up and restoring Conditional Access policies and Named Location policies in cloud-only environments.

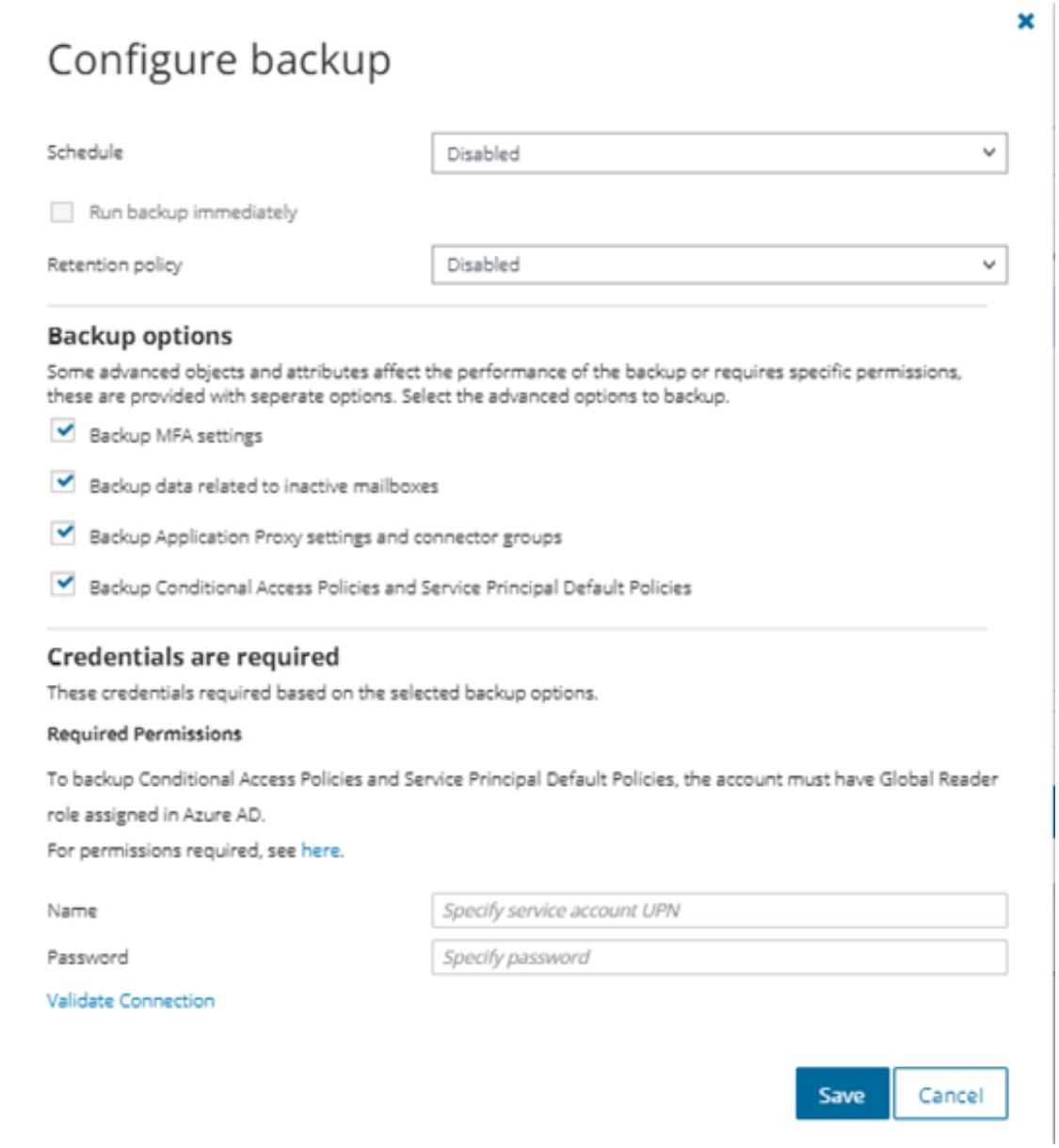
> **NOTE:** When policies are created using a predefined template in Azure and then restored after being hard deleted, the "templateId" attribute is not restored as it is read-only.

Prerequisites

Backing up Conditional Access Policies and Named Location Policies is not enabled by default. You must select this option when configuring backup options.

To backup Conditional Access policies and Named Location policies

1. Click **Manage backups** on the **Dashboard** screen.
2. Select the tenant from the list and click **Edit**.
   The **Configure backup** dialog opens.



3. Select the **Backup Conditional Access Policies and Service Principal Default Policies** option and specify service account credentials for the tenant. The specified account must have the following permissions:
   - The specified account must have at least one of the following roles in the Azure portal for backup operations; **Global Reader** or **Global Administrator**.
4. Click **Save**.

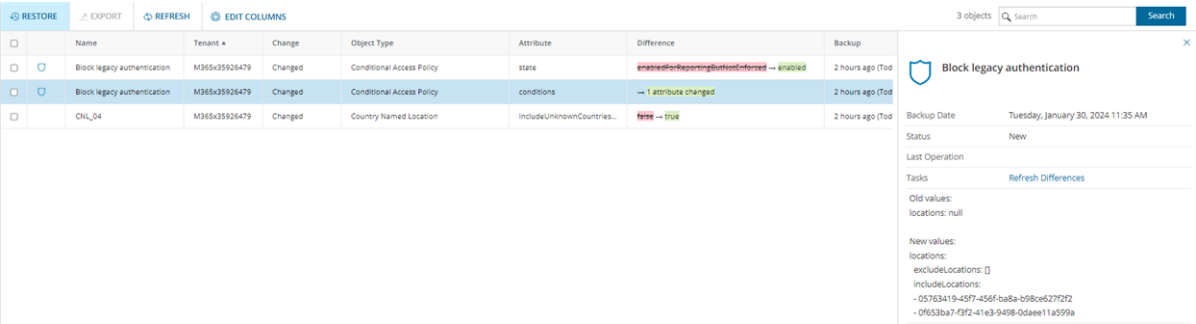
Supported Scenarios

If a backup contains Conditional Access policies or Named Location policies, the **Objects** view will show the type of policy.

The following policy types are supported by On Demand Recovery:

- Conditional Access Policy
- Country Named Location
- IP Named Location

On Demand Recovery restores the whole policy object and what has changed is displayed in the Differences report. On Demand Recovery checks whether objects (users, groups, named locations) assigned to the policy exist in Azure Active Directory. If any objects are missing, the policy is restored but a warning is shown.



A user can select attributes to be restored for Conditional Access policies and Named Location policies. For the full list of policy attributes that are restored and not restored by On Demand Recovery, see How does On Demand Recovery Handle Object Attributes?

Limitations

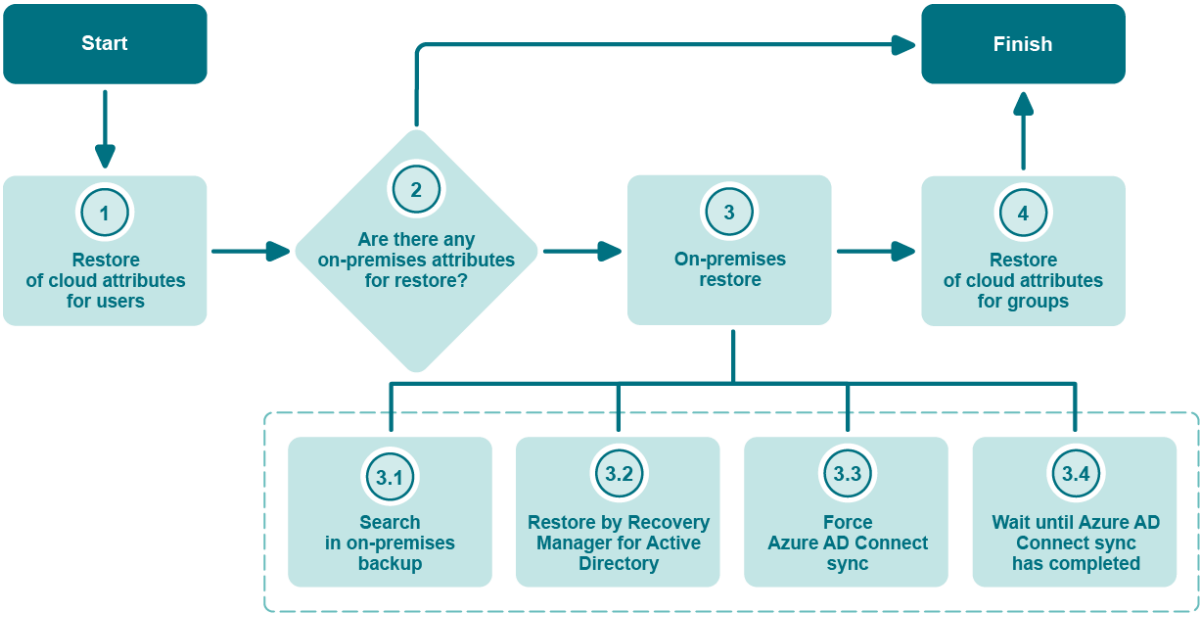
Other policy types such as claims mapping policy, token issuance policy, token lifetime policy and many others are currently not supported by On Demand Recovery. See the *Known issues* list in the On Demand Recovery release notes.

- If the "AuthenticationStrength" attribute in "grantControl" is not present in the tenant while restoring, the restore of the Conditional Access policy will fail. "AuthenticationStrength" is a relational attribute and On Demand Recovery does not backup this attribute, so if it is deleted from the tenant, we will not restore the Conditional Access policy and error will be shown.
- The "TermsOfUse" attribute in "grantControl" will not be restored. A warning will be shown: "Terms of Use for the policy are not set."
- The restore of a relational attribute does not have any special attributes that can be selected from the user interface. In each instance that a user, group, application and/or named location is restored, the restore of the relational attribute is also run even if the minimum attributes to restore were selected.
- If On Demand Recovery has "All", "None" or "AllTrusted" selected in live policies, no relational attribute will be restored and the policy in Microsoft Entra ID will remain as is.
- If "All", "None" or "AllTrusted" is selected in a backup for On Demand Recovery, and a link is subsequently added to a user in live polices, restoring that user will result in the link being removed. In this case, the policy will be updated with default value ("None" or null or []).
- Links removed or added are not visible in the Differences report.

Integration with Recovery Manager for Active Directory

On Demand Recovery can be integrated with Recovery Manager for Active Directory 9.0 or higher to restore and undelete on-premises objects that are synchronized with cloud by Azure AD Connect. The following figure illustrates the hybrid restore process.

Figure 1: Hybrid Restore Operation Flow Diagram



NOTE:

- All attributes that can be modified by Azure AD Graph API are considered as cloud attributes and restored on the first step. For example: **assignedLicense**, **usageLocation**, **membership** in cloud groups.
- On Demand Recovery also restores users from the Recycle Bin or recreates them before the on-premises restore with the **Undelete** option. Azure AD Connect matches these objects after the cloud restore by the Security Identifier as well as the **immutableID** attribute which is restored from the On Demand Recovery backup.
- On-premises restore is always performed for **member**, **memberOf**, **accountEnabled**, **manager** and **directReports** attributes.
- Groups are restored after the on-premises restore, because in case of permanent deletion, On Demand Recovery needs to wait until a group is recreated by Azure AD Connect.

Prerequisites

- Azure AD tenant that is synchronized with on-premises Active Directory by Azure AD Connect
- Recovery Manager Portal 9.0. If you have Azure AD Connect version 1.4.32.0 or higher, the Recovery Manager Portal 10.1 is required. (Recovery Manager for Active Directory version 10.2.1 or earlier)
- Hybrid Recovery node (Recovery Manager for Active Directory version 10.2.2 or later)

The portal can be run in any machine in your environment. It is not required to install all Recovery Manager for Active Directory components. To get the latest version of Recovery Manager Portal, go to https://www.quest.com/products/recovery-manager-for-active-directory-forest-edition/.

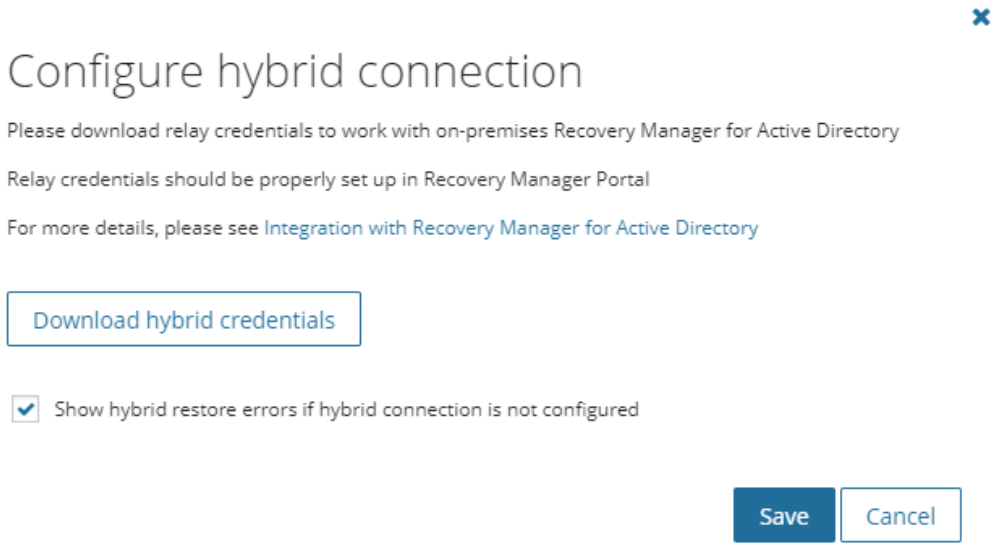
To configure Recovery Manager Portal to enable integration with cloud - v.10.2.1 or earlier

NOTE: The following instructions are for users operating Recovery Manager for Active Directory version 10.2.1 or earlier. For users operating Recovery Manager for Active Directory version 10.2.2 or later, see *To configure Hybrid Recovery node to enable integration with cloud - v.10.2.2 or later* below.

1. Connect to the Recovery Manager Portal with your Web browser.
2. In the Recovery Manager Portal, open the **Configuration** tab.
3. Expand **Portal Settings**
4. **Recommended:** Select the **Automatically unpack backups for restore operations** option to automatically unpack the required backup. If the option is not selected, the restore operation may fail because the backup was not unpacked or was removed due to retention policies for the unpack operation. For more details, see the *Recovery Manager for Active Directory User Guide*.

5. Click **On Demand integration**. In the On Demand integration dialog, select the **Enable integration** check box and specify the Relay URL and credentials. To get these parameters, go to On Demand Recovery and perform the following steps:

   a. On the **Dashboard** screen, click **Configure hybrid connection**.



   b. In the Configure hybrid connection dialog, click **Download hybrid credentials** to download a configuration file with Relay credentials.

   c. When a customer does not want to configure a hybrid connection with Quest Recovery Manager for Active Directory, the corresponding connection error events can be deactivated by changing their severity from Error to Info. To do this, clear the **Show hybrid restore errors if hybrid connection is not configured** check box.

   d. Save the file to the folder of your choice.

   e. Go back to the On Demand integration dialog, click **Choose file** and select the configuration file. For security reasons, you should remove this file from your computer after the credentials will be specified in the Recovery Manager Portal.

   NOTE: Azure AD Connect synchronization occurs automatically after the restore operation. But On Demand Recovery forces synchronization cycles and requires credentials for the machine where Azure AD Connect is installed.

6. Specify Azure AD Connect host name and credentials. If Azure AD Connect and Recovery Manager Portal are installed on the same machine, leave the fields blank.

NOTE: You may get an error related to the proxy settings while configuring integration with On Demand Recovery. To resolve this issue, perform the following actions:

1. Open the Recovery Manager Portal configuration file **%Program Files%\Quest\Recovery Manager Portal\EnterprisePortalSettings.xml**.
2. Set the *UseDefaultSystemProxy* parameter to *False* and check that *ProxyAddress* has the correct value.
   - If *UseDefaultSystemProxy* is set to *False* and *ProxyAddress* is specified, the value of *ProxyAddress* will be used as a proxy server address.
   - If *UseDefaultSystemProxy* is set to *False* and *ProxyAddress* is not specified, the direct connection will be used.
   - If *UseDefaultSystemProxy* is set to *True* and *ProxyAddress* is specified or has no value, the proxy server specified for your browser will be used.
3. Make sure that URI contains the protocol prefix and the port number, e.g. http:/localhost:8080/.
4. Restart the Recovery Manager Portal service.

For more information about integration with Recovery Manager for Active Directory, see Integration with On Demand Recovery.

To configure Hybrid Recovery node to enable integration with cloud - v.10.2.2 or later

For Recovery Manager for Azure Directory 10.2.2 and later versions, you will need to disable the Recovery Manager Portal (if previously enabled), and configure and integrate the Hybrid Recovery node from On Demand Recovery into the Recovery Manager for Azure Directory console. For more information on this, go to Hybrid Recovery with On Demand Recovery.

What can be restored in hybrid configuration

- On-premises groups
- User licenses (e.g. Office 365 licenses and assignedLicenses property for cloud users) and cloud group membership
- Deleted on-premises users and groups
- Service principals' appRoleAssignments to on-premises users
- appRoleAssignments to non-Office groups (used for SSO and App Roles)
- Directory roles: Global Administrator, Exchange Administrator, Compliance Administrator
- Other cloud-only properties: such as Block sign in, Authentication contact information, Minors and Consent
- Multifactor authentication (MFA) settings if a customer uses cloud multifactor authentication
- Conditional Access policies
- Inactive mailboxes of permanently deleted users

Important Considerations

- To restore on-premises objects, On Demand Recovery uses attribute values from the RMAD backup that is closest in time but older than the cloud backup unpacked in the On Demand Recovery user interface. If the closest on-premises backup is 24 hours older than the cloud backup, you will receive the warning message. By default, the search of the closest in time on-premises backup is performed among the backups that were unpacked in Recovery Manager Portal. You can use the **Automatically unpack backups for restore operations** option on **Portal Settings** of the **Configuration** tab in the Recovery Manager Portal – in this case, the on-premises backup will be unpacked automatically during the restore operation (RMAD v10.2.1 or earlier).
- On Demand Recovery displays only cloud-synchronized on-premises attributes and cloud-only attributes for the selected object when you click **Browse** in the Restore Objects dialog. This does not include on-premises only attributes. To restore on-premises only attributes, you must select the **Restore all attributes** option in the Restore Objects dialog.
- After the hybrid restore operation, On Demand Recovery forces Azure AD Connect synchronization to push on-premises changes to the cloud and wait until it completes the synchronization. Restore events can be used to track steps of Azure AD Connect synchronization, such as export and import.
- To restore 'member' or 'memberOf' attributes for an object, restore the group from the **Unpacked Objects** view. Restoring of group memberships from the **Differences** report is not supported in hybrid environments.
- On Demand Recovery supports one hybrid connection per On Demand organization. If you need to manage multiple hybrid tenants, create a separate On Demand organization for each Hybrid Azure AD tenant.
- One instance of Recovery Manager Portal can be used with one Azure AD tenant and one Azure AD Connect server. Install multiple RMAD web portals if you need to work with multiple Azure AD tenants and Azure AD connect servers.
- On Demand Recovery restores Back Link attributes: 'memberOf' (the back link for the 'member' attribute) and 'directReports' (the back link for the 'manager' attribute). These attributes can be selected along with all other attributes when you click **Browse** in the Restore Objects dialog.
- Separate Microsoft Azure Relay service is used for each hybrid connection (one per On Demand organization). On Demand Recovery creates WCF Relay per On Demand organization. No changes to On-Premises Firewall settings are required.

To perform a restore operation in On Demand Recovery

1. Unpack a backup.
2. Go to the **Objects** screen and select on-premises objects to restore.
3. Click **Restore**.
4. In the Restore Objects dialog, if you select the **Restore all attributes** option, On Demand Recovery will restore all on-premises attributes and cloud-only attributes from the backup.
5. You can perform the restore of on-premises objects from the **Differences** report as well.

NOTE: You can restore a hybrid user using only On Demand Recovery without configuring a hybrid connection. In this case, do not forget to clear the **Show hybrid restore errors if hybrid connection is not configured** check box in the Configure hybrid connection dialog. If the hybrid connection is not configured, On Demand Recovery restores a cloud user and their cloud attributes without an on-premises user. For more information, see How does On Demand Recovery Handle Object Attributes? This scenario does not work for Federated Domains. For details, see Working with Inactive Mailboxes.

Limitations When a Hybrid Connection is Not Configured

On Demand Recovery can restore cloud-only users and groups without a configured Recovery Manager for Active Directory hybrid connection. If a hybrid connection is not configured intentionally or Recovery Manager for Active Directory is not installed yet, recovery features for hybrid users and groups are limited. As a result, the following errors will occur: "Cloud restore was interrupted due to failed restore of the on-premise object" and "A hybrid connection is required to complete the restore of the on-premises attributes with RMAD".

- If a hybrid user is permanently deleted, On Demand Recovery will create a cloud object with cloud properties, including on-premises values, but actual values will be taken from the cloud backup, such as user surname, office, etc. If a hybrid user is recreated in the on-premises Active Directory by Recovery Manager for Active Directory or by any other on-premises recovery solution, this user object will be automatically synchronized by Azure AD Connect resulting in the full recovery of the hybrid user. If a hybrid user is not recreated, on-premises attributes will be missing, for example, on-premises groups membership, etc.
- If On Demand Recovery tries to restore a hybrid user that has not been deleted but has modified on-premises attributes, the task will fail with the following error: "Cannot restore attribute". This error occurs due to the "Unable to update the specified properties for on-premises mastered Directory Sync objects or objects currently undergoing a migration" error. In this case, On Demand Recovery will show changes in the Difference report correctly, but will not be able to restore them.
- For a non-deleted hybrid group (modified in the cloud), cloud attributes such as licenses or assigned Enterprise applications can be restored. On Demand Recovery cannot restore a permanently deleted hybrid group that was synchronized by Azure AD Connect, so the error that Recovery Manager for Active Directory configuration is needed will be shown in the case of restoring of the permanently deleted group.

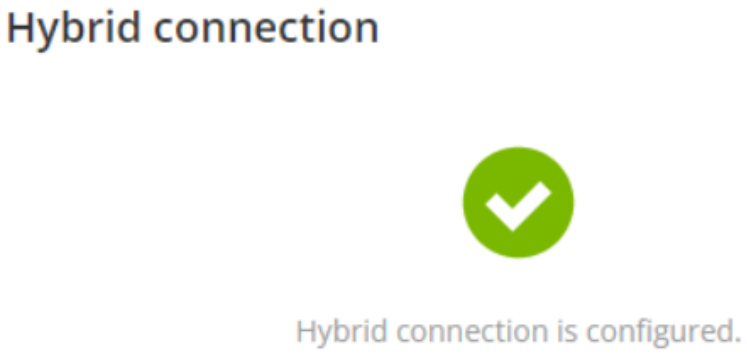
Hybrid Connection Widget

The **Hybrid connection** widget on the **Dashboard** screen shows issues with the hybrid connection. The widget state is synchronized automatically every time the page is refreshed.

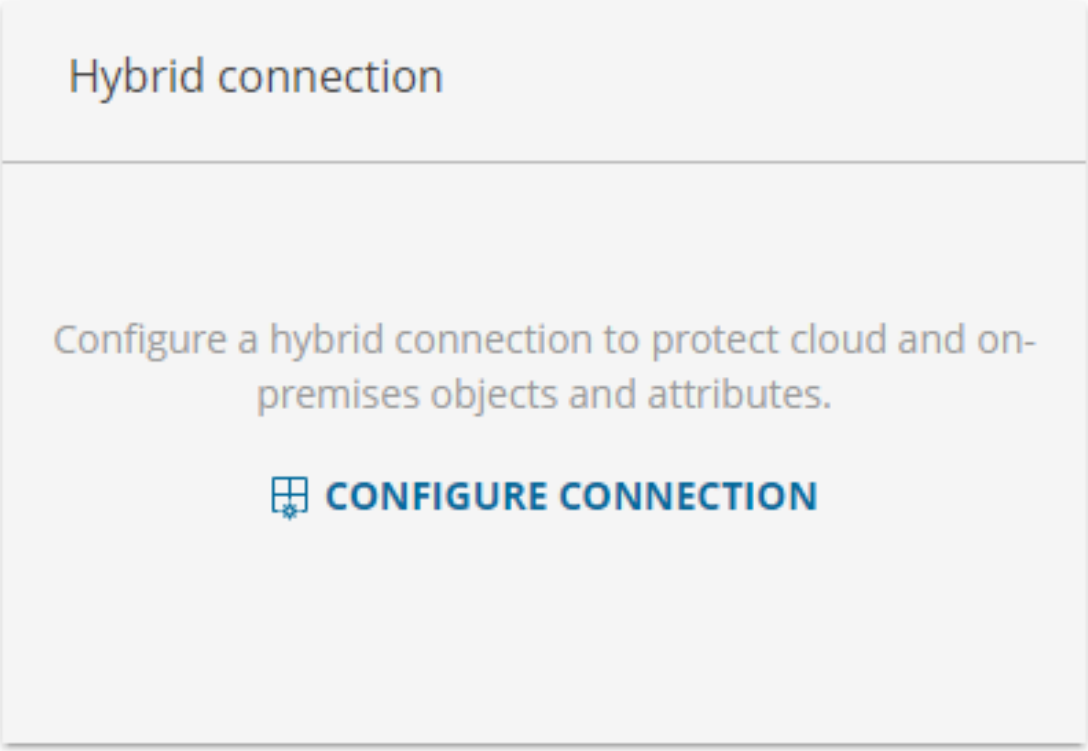
When a customer does not want to configure a hybrid connection with Quest Recovery Manager for Active Directory, the corresponding connection error events can be deactivated by changing their severity from Error to Info. To do this, clear the **Show hybrid restore errors if hybrid connection is not configured** check box in the **Configure hybrid connection** dialog. For details, see Integration with Recovery Manager for Active Directory.

The widget has the following states:

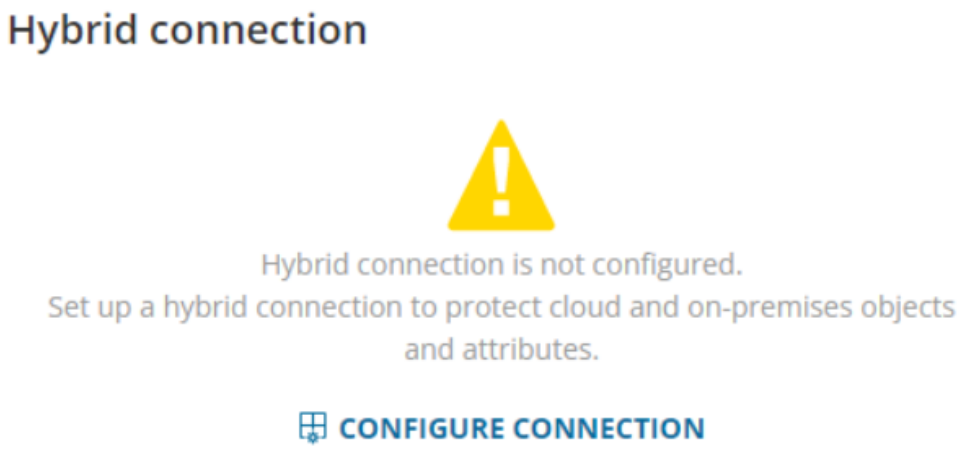
- If the hybrid connection is properly configured and works fine, the widget is green.



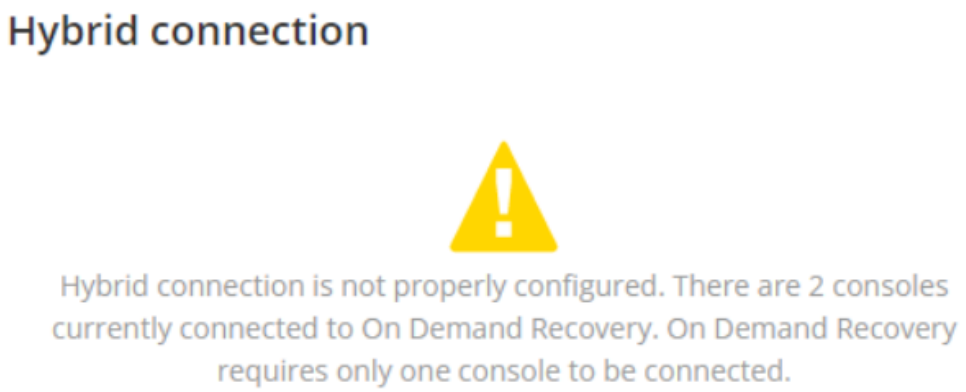
- If the hybrid connection is not configured because you do not need it, the widget is gray and advises you to configure the connection. In this case, the **Show hybrid restore errors if hybrid connection is not configured** check box is not selected in the **Configure hybrid connection** dialog.



- If the hybrid connection is not configured and the **Show hybrid restore errors if hybrid connection is not configured** check box is selected in the **Configure hybrid connection** dialog, the widget is yellow and has a warning sign.



- If one or more console is connected to On Demand Recovery and the **Show hybrid restore errors if hybrid connection** check box is selected in the **Configure hybrid connection** dialog, the widget is yellow and has a warning sign. For more information, go to the *Configure Hybrid Recovery* section in Hybrid Recovery with On Demand Recovery.



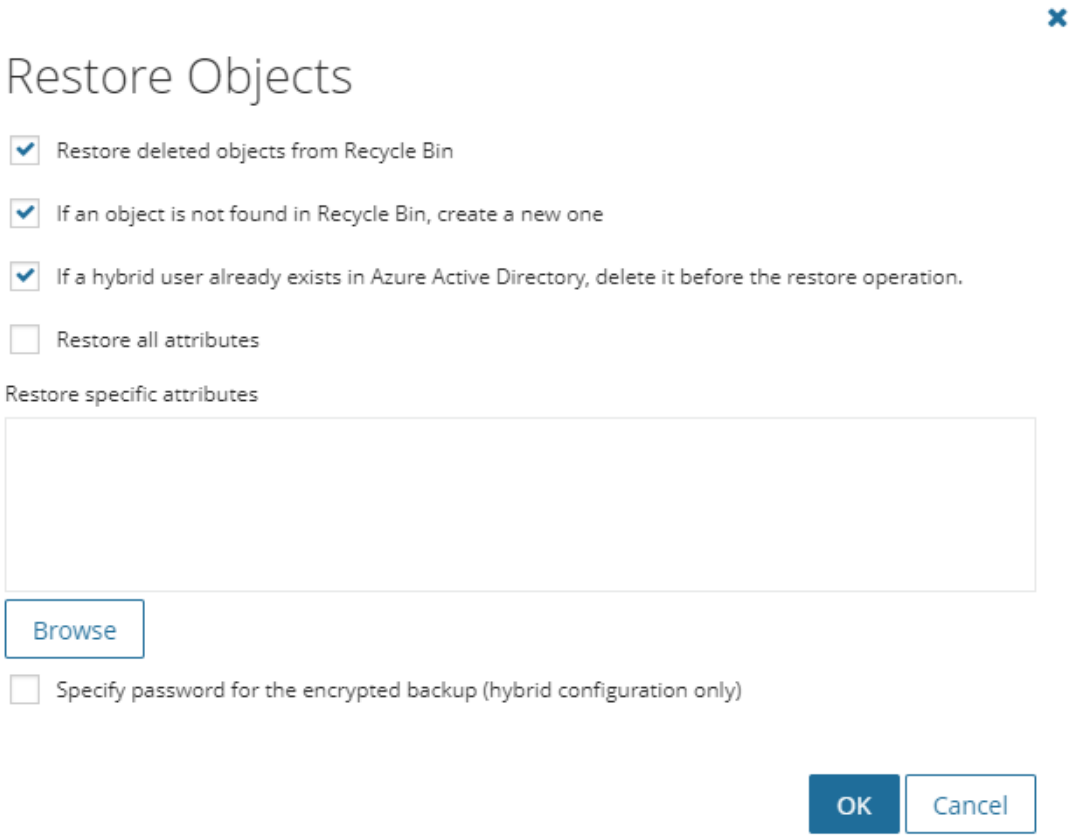
Working with Inactive Mailboxes

On Demand Recovery supports restore of inactive mailboxes of hard-deleted users. The Federated Domain scenario is also supported. This feature requires Recovery Manager for Active Directory 9.0 or higher.

To preserve the original cloud mailbox of a hybrid user after restore, you have to select the **If a hybrid user already exists in Azure Active Directory, delete it before the restore operation** option in the **Restore Object** dialog.

User scenario

1. There is a hybrid user. This user is deactivated by the administrator for some reason. This means that the user account goes to the Recycle Bin. After 30 days, Azure AD cleans this account from the Recycle Bin.
2. Then, the user returns and the account is enabled again by the administrator. After the activation, the user is recreated in the cloud with the new mailbox.
3. We want to use the original cloud mailbox for the user. The only one way to do this is to restore the user from the backup. But before the restore, the newly created cloud user must be removed from Azure AD using this new option.



If you restore a hybrid user and their mailbox with On Demand Recovery

- For Non-Federated Domains, On Demand Recovery restores a cloud user and its mailbox without an on-premises user.
- For Federated Domains, restore of hybrid users requires Recovery Manager for Active Directory. In this scenario, On Demand Recovery restores a hybrid user and its mailbox in the cloud. Recovery Manager for Active Directory restores this hybrid user on premises, then it calls Azure AD Connect to synchronize the user back to the cloud and make the cloud user previously restored by On Demand Recovery be in the Federated Domain. Without Recovery Manager for Active Directory, the cloud user will be non-federated after restore and you will not log in with this user.

Hybrid Connection Port and Protocol Requirements

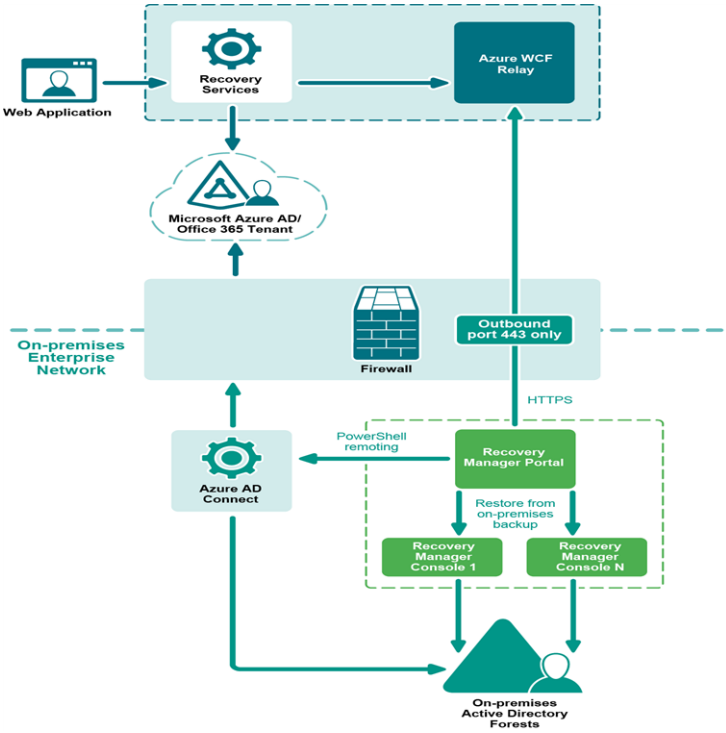
Hybrid configuration with Recovery Manager for Active Directory requires only outbound TCP/UDP port 443 to be opened on the Recovery Manager Portal server to access the internet. If the Recovery Manager Portal server already has access to the internet, you do not need to change the Firewall configuration.

NOTE: If you do not want to open all outbound IP Prefixes and your firewall or proxy allows DNS allow lists, you can add connections to <your name space>.servicebus.windows.net to your allow list.

Table 3: Hybrid connection port and protocol requirements

Protocol	Ports	Direction
HTTPS	443 (TCP/UDP)	Outbound

Figure 2: Hybrid Restore Components Diagram



Hybrid Connection Security

FIPS 140-2 compliant TLS protocol is used for traffic encryption. HTTPS certificate is validated on our client side (Recovery Manager Portal).

Server side is Azure WCF Relay that is created and configured in Quest Azure Subscription.

Shared Access Signature (SAS) is used for authentication. A SAS token is based on an access key generated by On Demand Recovery cloud. This key is downloaded to the on-premises server with Recovery Manager Portal and used in the portal configuration to establish the Hybrid connection (from on-premises to the cloud). The SAS token is sent to the cloud and verified on each connection request. For details about Shared Access Signature algorithm, click the following link: https://docs.microsoft.com/en-us/azure/service-bus-relay/relay-authentication-and-authorization.

24

Restoring Email Address or Phone for Self-Service Password Reset

On Demand Recovery restores an email address or phone that was specified as an authentication method for the self-service password reset user option in the Azure portal. So users can reset their passwords without help of the tenant administrator.

Supported scenarios

The following scenarios are supported by On Demand Recovery:

- Restoring email, mobile phone number, and office phone number for the self-service password reset option.

Limitations

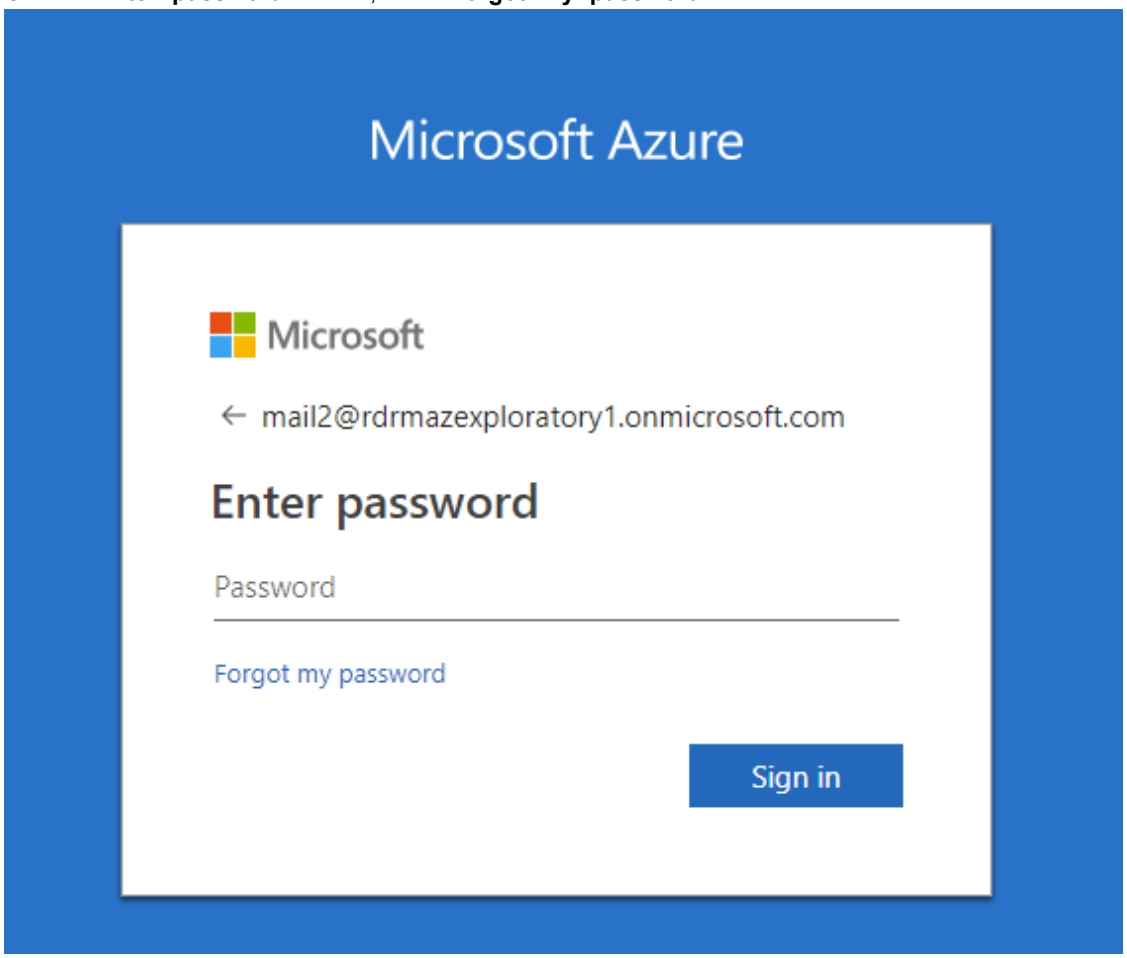
The following scenarios are not supported by On Demand Recovery:

- Restoring user passwords and the password reset is the only option to log in to the Azure portal after the restore of a permanently deleted user.
- The following authentication methods are not restored; security questions, mobile app notification, and mobile app code.

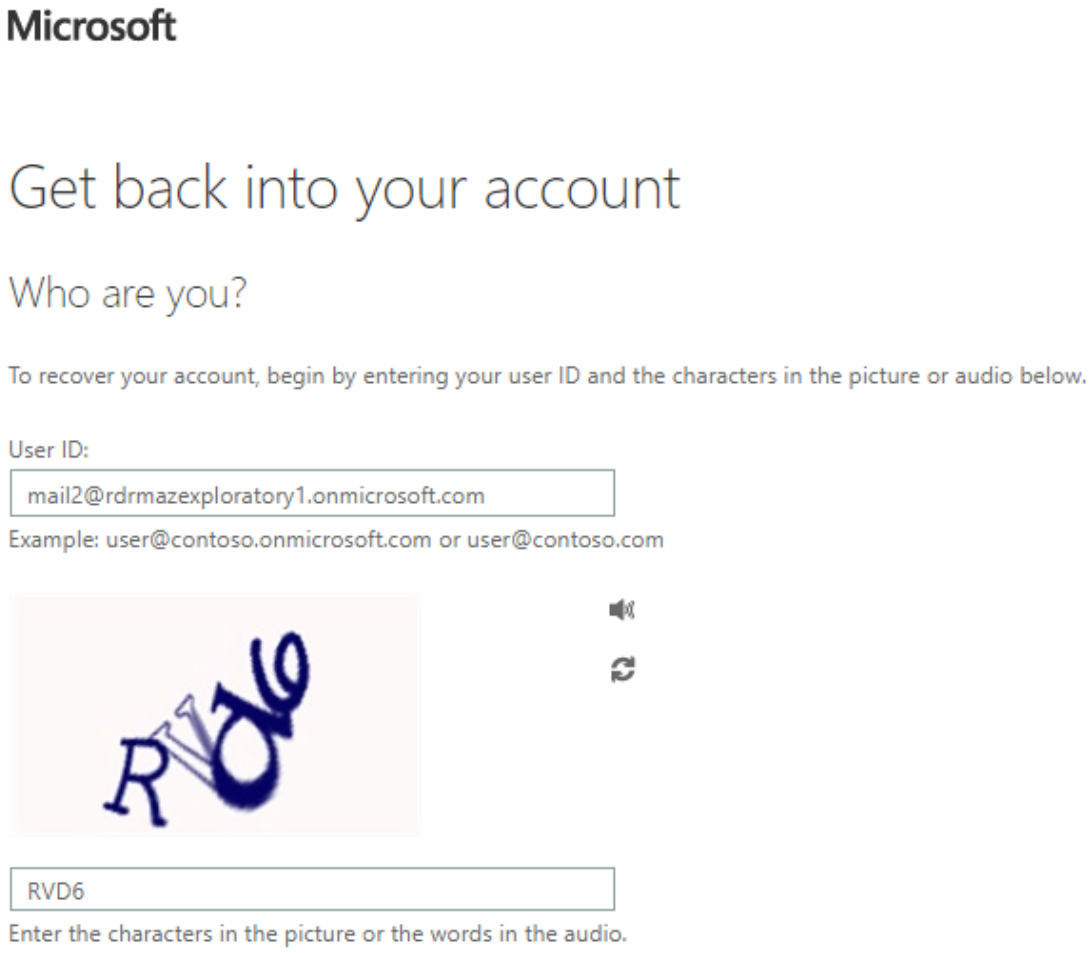
For details on how to enable self-service password reset in your Azure AD tenant, click here.

To log in to the Azure portal after the user restore if an email address was specified as authentication method for the password reset option

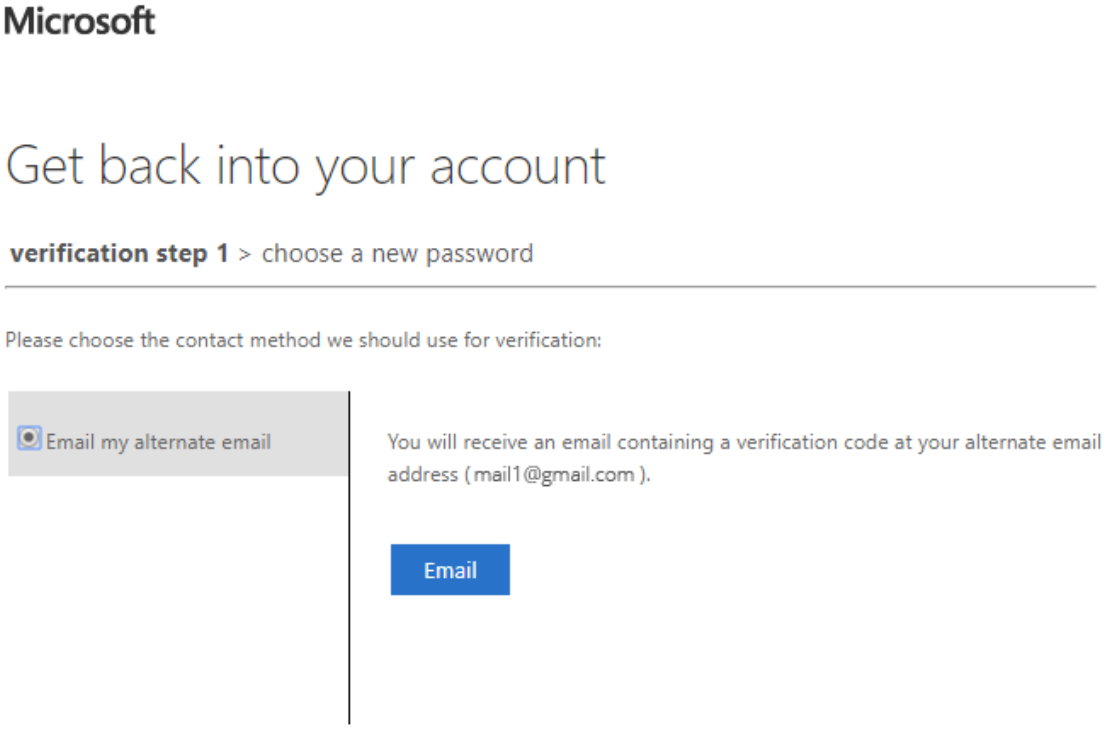
1. Go to the Azure portal and enter the user name.
2. On the **Enter password** screen, click **Forgot my password**.



3. On the **Get back into your account** screen, type the user name and prove that you are not a robot by entering the characters you see on the screen, and then select **Next**.

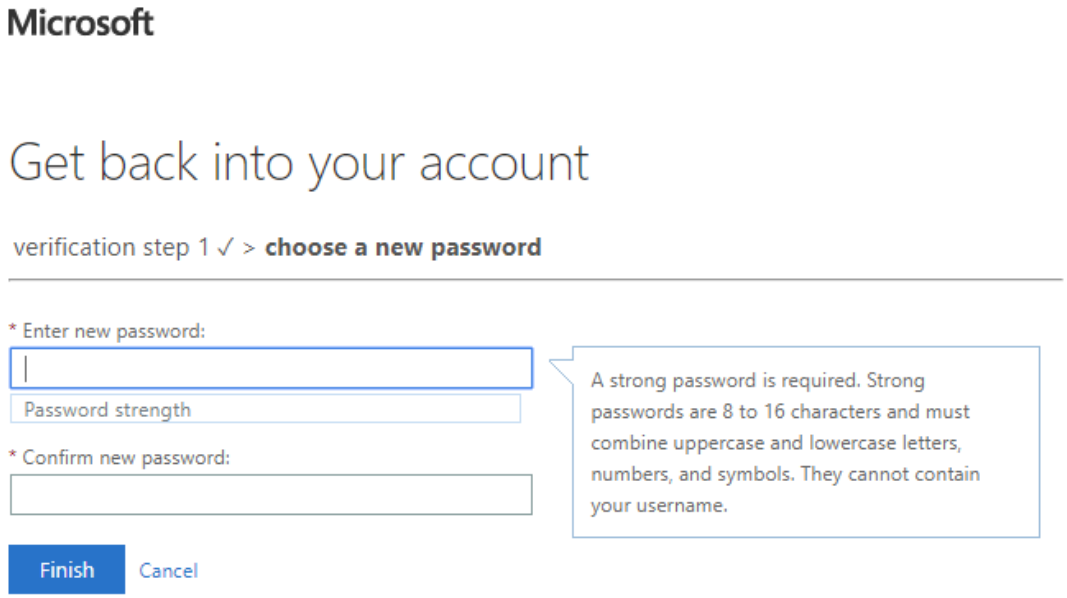


4. On the next screen, select **Email my alternate email**, and then select **Email**.

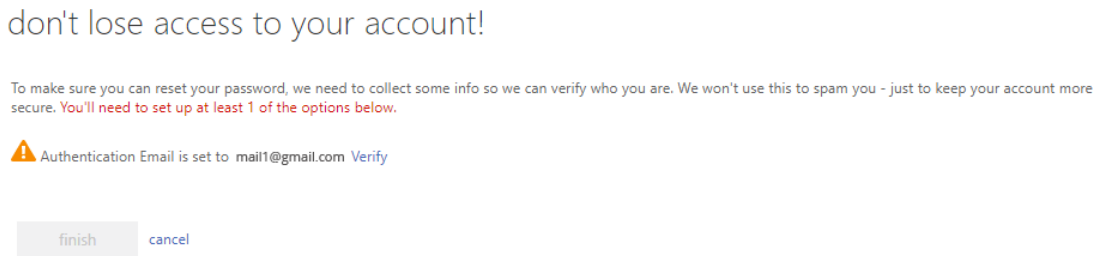


5. Type the verification code from the email into the box, and then select **Next**.

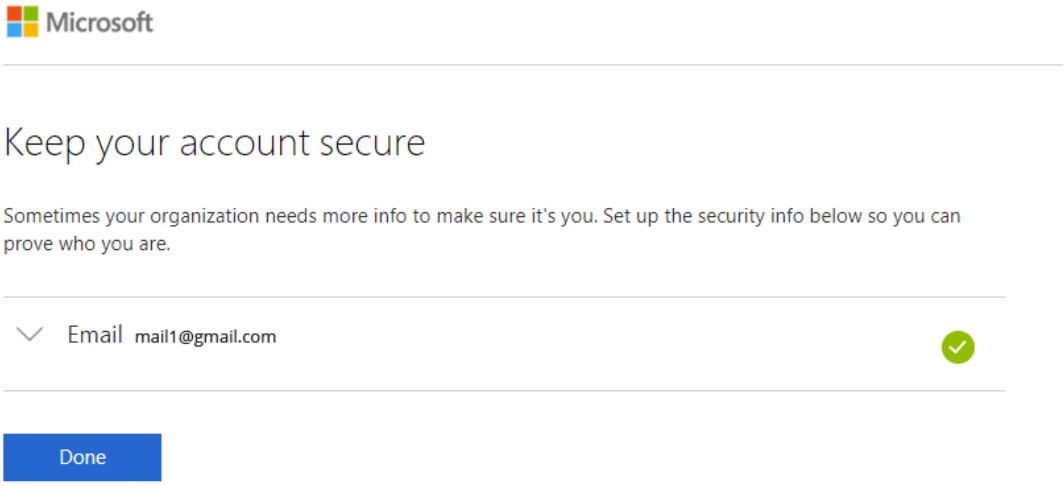
6. Type and confirm your new password, and then select **Finish**. Your password has been reset and can be used to log in to the Azure portal.



7. Log in with the new password.
8. Then you may see the screen where you will be asked to verify your email address if the Converged service is not enabled in your environment. You can click **Cancel** and verify the email address later.



9. If the Converged service is enabled, you will get the screen like below. In this case, no further action is required.



25

Reporting

On Demand Recovery includes the comparison report feature that is used to monitor and roll back changes occurred in live Azure Active Directory or Office 365 since the backup was created. The report assists you with troubleshooting and resolving problems that may result from the deletion of critical objects or parameter changes.

The report shows the following changes:

- Creation of new users or groups
- Changes to Azure AD B2C "local accounts", "guest accounts", and "social accounts"
- Changes to object attributes, including licenses
- Group membership and manager property changes (**DirectoryLinkChange** object type)
- Changes to service principal objects: deletion of a service principal, add/remove roles (custom roles are not monitored), changes to the **accountEnabled** property
- Objects moved to the Recycle Bin
- Permanently deleted objects
- When deleting a group, all links that were affected by this action are shown in the Differences report, such as Azure AD group membership, Conditional Access policies, group owners, and application assignments.

> **NOTE:** To restore 'member' or 'memberOf' attributes for an object, restore the group from the **Unpacked Objects** view. Restoring of group memberships from the **Differences** report is not supported in hybrid environments.

To view and roll back changes in Azure Active Directory or Office 365

> **NOTE:** Objects added to the directory after the backup was created cannot be deleted using the **Restore** option in the comparison report. This option removes only membership information for the selected object and logs an event.

1. Create a backup of your directory.
2. Change any object attributes in your live Azure Active Directory or Office 365.
3. Unpack the backup to compare with the current version of your directory. For that, click **Unpack backup** on the **Dashboard** view. In the Backup Unpacking dialog, click **Browse** and select the backup.
4. After the backup is unpacked, go to the **Differences** view.
5. To refine the data, use the **Search** field or facets on the left side of the screen.
   For more information about the search syntax, see Advanced Search.
6. Select the changes you want to roll back and click **Restore**.
7. To update the report data, use the **Refresh** option.

8. The **Export** feature allows you to export the selected report data to the CSV format. Note that the CSV file contains internal column names, for example: the **Attribute** column in the **Difference** report has the "changedAttribute" internal name. You can use internal column names to create search queries. For more information, refer to Advanced Search.

26

Advanced Search

You can use words, symbols, and query strings in your search to make your search results more precise.

Consider the following:

- It is recommended to add an asterisk to the end of your search term. The asterisk will replace a character in your search string to indicate that any number of characters can be substituted in place of the asterisk.
- Do not put spaces between the symbol or word. For example, a search for `changedAttribute:link*` will work, but will not work for `changedAttribute: link*`
- Press **Enter** to get the search results.
- Keywords are not case-sensitive.
- You can export selected search results to the CSV file.

Using Operators in Keyword Queries

You can use special punctuation marks to refine your search.

Table 4: Operators that can be used in keyword queries

To search for	Operator	Example	Result
Specify part of a word	*	serv*	Include terms beginning with "serv".
Exclude specified content	-	-mail*	Excludes content with values that match the exclusion.
Exclude specified content	**NOT** (case-sensitive)	NOT mail*	Excludes content with values that match the exclusion
Include specified content	+	+mail*	Includes content with values that match the inclusion.
Multiple keywords	space	mail user	Returns content that includes either 'mail' or 'user'.
Multiple keywords	**OR** (case-sensitive)	mail OR user	Returns content that includes either 'mail' or 'user'.

To search for	Operator	Example	Result
Multiple keywords	**AND** (case-sensitive)	mail AND user	Returns content that includes both these keywords.
Exact phrase	Quotation marks	"Object hard deleted"	Finds items that contain the exact phrase "Object hard deleted".

NOTE: Asterisk matches zero or more non-space characters.

Search by Date Range

Table 5: Query examples to search by date range

Time stamp	Query example
Search for the backup created on September 18, 2017 Eastern Time (UTC-5) in the **Select backups to unpack** dialog	when:[2017-09-18T00:00:00-05 TO 2017-09-19T00:00:00-05]
All events after June 27	timestamp:[2017-06-27 TO *]
All events up to June 27 9:03:27	timestamp:[* TO 2017-06-28T09:03:27]
January 27-28 interval	timestamp:[2017-01-27 TO 2017-01-28]
53 second interval on January 27 9:13 UTC	timestamp:[2017-01-27T09:13:00Z TO 2017-01-27T09:13:53Z]
The same time interval as previous but with time zone specified	timestamp:[2017-01-27T12:13:00+03 TO 2017-01-27T12:13:53+03]
1 – 3 weeks of 2017 year	timestamp:[2017-W1 TO 2017-W3]
First 50 days of 2017 year	timestamp:[2017-001 TO 2017-050]

Using Query Strings

You can refine your search for the report data by using search expressions. To perform a keyword search in a specified column, you need to use the internal name of the column instead of the column display name. For example, `<internal column name>:<search term or expression>`. For a list of internal column names and string examples, see the tables below.

Table 6: Unpacked Objects screen

Column display name	Column internal name	To search for	Query example
Name	displayName	An object by object name	displayName:SamJones
Type	objectType	An object by object type	objectType:user
Backup Date	backupDate	An object by the specified backup date/time	backupDate:[2017-06-27]
Directory	tenant	An object by directory name	tenant:demo365
Principal Name	userPrincipalName	An object by principal name	userPrincipalName:Sam.Jones@mycompany.com
Mail	mail	An object by mail address	mail:Sam.Jones@mycompany.com
City	city	An object by city	city:London
Department	department	An object by department	department:Sales
Job Title	jobTitle	An object by job title	jobTitle:manager
Description	description	An object using keywords in the object descriptions	description:Sales
User Type	userType	An object by user type	userType:new
Telephone Number	telephoneNumber	An object by telephone number	telephoneNumber:44658

Table 7: Differences screen

Column display name	Internal column name	To search for	Query example
Name	objectName	Changes related to a specified object name	objectName:SamThomas*
Change	changeType	Objects by change type	changeType:"Object hard deleted"
Object Type	objectType	Objects by object type	objectType:User
Attribute	changedAttribute	Changes related to a	changedAttribute:link

Column display name	Internal column name	To search for	Query example
		specific attribute	
Difference	oldValue	Search by old attribute value (value before the change)	oldValue:User1@mycompany.com
Difference	newValue	Search by new attribute value (value after the change)	newValue:User1@gmail.com
Backup time	backupDate	Search by the specified backup date/time	backupDate:[2017-06-27]

Table 8: Events screen

Column display name	Internal column name	To search for	Query example
Time	timestamp	Specified timestamp	timestamp:NormanThomas*
Description	message	Keywords in event descriptions	message:"Object attributes were restored"
Object Name	object.name	Objects by an object name	object.name:User
Task Name	task.name	Specified task	task.name:"Restore objects"

Table 9: Tasks screen

Column display name	Column internal name	To search for	Query example
Title	name	A task by task name	name:"restore objects"
State	status	A task by task status	status:completed
Type	type	A task by task type	type:restore
Modified	modified	A task by the date when the task was modified	modified:[2017-06-26]
Created	created	A task by the date when the task was created	created:[2017-06-27]
Operation	lastResultDescription	Keywords in the operation description	lastResultDescription:unpack*

27

How does On Demand Recovery Handle Object Attributes?

- On Demand Recovery restores supported attributes based on data provided by Microsoft Graph API including schema extension attributes for Users.
- For more information about known issues and limitations, see http://support.quest.com/technical-documents/on-demand-recovery-for-azure-active-directory/release-notes/about-quest-recovery-for-azure-active-directory/known-issues.
- For more details about Azure Active Directory MSOnline module, see https://learn.microsoft.com/en-us/powershell/module/msonline/?view=azureadps-1.0.

NOTE: On Demand Recovery does not support the restore of objects in restricted management administrative units.

Attributes Restored by On Demand Recovery

For a full list of attributes restored by On Demand Recovery, visit the On Demand Recovery Supported Attributes guide.

What is Not Protected by Azure AD Connect but Can Be Restored by On Demand Recovery?

Azure Active Directory Connect synchronizes many attributes for users and groups from on-premises Active Directory but there are also cloud objects, properties, and links to Office 365 resources which are not protected by Azure AD Connect and restored only with On Demand Recovery.

Table 10: Types of cloud-only objects restored by On Demand Recovery

Object Type	Description	Azure Recycle Bin
Guest users	An Azure AD business-to-business (B2B) collaboration user that typically resides in a partner organization and has limited privileges in the inviting directory.	30 days
Office 365 Groups	Groups that are used for collaboration between users, both inside and outside the company.	30 days
Cloud only Security Groups	Groups that are used for granting access to Office and Azure resources.	No
Dynamic Security Groups	Groups with dynamic rule-based membership.	No
Dynamic Office 365 Groups	Office 365 Groups with dynamic rule-based membership.	30 days
Devices	Device registration records in Azure Active Directory.	No
Application Registration	Stores application manifest (non-Gallery application manifests are not supported), logo, sign in, up URLS and other information.	30 days
Conditional Access Policies	Azure Active Directory policies that are used to control user access to cloud applications and resources.	No
Named Locations	Named lists of IP prefixes that are used in Conditional Access Policies.	No

About Us

Quest creates software solutions that make the benefits of new technology real in an increasingly complex IT landscape. From database and systems management, to Active Directory and Office 365 management, and cyber security resilience, Quest helps customers solve their next IT challenge now. Around the globe, more than 130,000 companies and 95% of the Fortune 500 count on Quest to deliver proactive management and monitoring for the next enterprise initiative, find the next solution for complex Microsoft challenges and stay ahead of the next threat. Quest Software. Where next meets now. For more information, visit www.quest.com.

Technical Support Resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at https://support.quest.com.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to-videos
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product