



Quest® Identity Recovery for Microsoft Entra ID

User Guide



© 2026 Quest Software Inc. ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software Inc.

The information in this document is provided in connection with Quest Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST SOFTWARE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest Software does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.

Attn: LEGAL Dept
20 Enterprise, Suite 100

Aliso Viejo, CA 92656

Refer to our Web site (<https://www.quest.com>) for regional and international office information.

Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at <https://www.quest.com/legal>.

Trademarks

Quest, the Quest logo, and Join the Innovation are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit <https://www.quest.com/legal/trademark-information.aspx>. All other trademarks and registered trademarks are property of their respective owners.

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.

Identity Recovery for Microsoft Entra ID
User Guide
Updated - April 20, 2026

Contents

Getting Started with Quest Identity Recovery for Microsoft Entra ID	1
Accessing Quest Security Management Platform	2
Creating a Microsoft Entra Global Administrator Account	2
Access Control	4
Adding a Microsoft Entra Tenant	5
Working with Identity Recovery for Microsoft Entra ID	6
Consents and Permissions	6
Azure Account Used to Grant Consents	7
Basic Consent Permissions	8
Restore Consent Permissions	10
Exchange Online PowerShell for Backup Consent	13
Exchange Online PowerShell for Restore Consent	14
Trusted IP Settings	15
Identity Recovery for Microsoft Entra ID Interface	15
Tenant Selector	15
Dashboard	16
Backups	18
Unpacked Objects	18
Differences	18
Events	18
Tasks	18
Backup and Restore Workflow	18
Configuring and Creating Backups	19
Unpacking Backups	21
Restoring Objects	22
Which Objects Can Be Restored from the Recycle Bin?	26
Restoring Passwords	27
Differences Report	28
Restoring from Differences	28
Advanced Search	30
Using Operators in Keyword Queries	31
Search by Date Range	32
Using Query Strings	32
Email Notifications	34
Configuring Notification Templates	34
Restoring Directory Roles and Application Roles	36

Restoring Users	37
Restoring Groups	38
Restoring Service Principal Objects	39
Restoring Applications	43
Restoring Application Proxy Settings	44
Restoring Group Licenses	46
Restoring Devices	47
Restoring Conditional Access Policies	48
Restoring Claims Mapping Policy	50
Backup and Restore of Tenant Level Settings	51
Backup and Restore Administrative Units	53
Integration with Recovery Manager for Active Directory	54
Limitations When a Hybrid Connection is Not Configured	59
Hybrid Connection Widget	59
Working with Inactive Mailboxes	62
Restoring Mailboxes for Hybrid Users	62
Hybrid Connection Port and Protocol Requirements	64
Hybrid Connection Security	65
Restoring Email Address or Phone for Self-Service Password Reset	66
How does Identity Recovery for Microsoft Entra ID Handle Object Attributes?	72
Attributes Restored by Identity Recovery for Microsoft Entra ID	72
What is Not Protected by Microsoft Entra Connect but Can Be Restored by Identity Recovery for Microsoft Entra ID?	73
About Us	74
Technical Support Resources	74

Getting Started with Quest Identity Recovery for Microsoft Entra ID

Quest® Identity Recovery for Microsoft Entra ID lets you back up and restore Microsoft Entra ID and Microsoft 365 objects while providing granular recovery, difference reporting, and hybrid integration with Recovery Manager for Active Directory.

Key Features

- Back up Microsoft Entra ID and Microsoft 365 users, groups, service principals, devices, applications, administrative units, Conditional Access policies, Application Proxy settings, named locations, tenant level settings (such as directory settings, group lifecycle policies, external identity settings, user authentication settings, organization settings), and more.
- Support for Microsoft Entra B2C tenants.
- Restore Microsoft Entra ID and Microsoft 365 users, groups, service principals, devices, applications, administrative units, Conditional Access policies, Application Proxy settings, named locations, and tenant level settings.

i **NOTE:** Identity Recovery for Microsoft Entra ID can process two types of Microsoft 365 groups: Microsoft 365 groups and security groups. Group membership and ownership are restored for both types of groups. It does not restore any resources associated with Microsoft 365 groups and Microsoft Teams, such as conversations, Planner tasks and plans.

- View differences between backups and live Microsoft Entra ID or Microsoft 365 data and revert unwanted changes.
- Integrate with Quest Recovery Manager for Active Directory to restore on-premises Active Directory objects.

! **CAUTION:** Microsoft Entra is a dynamic and rapidly evolving platform, which means its APIs may be updated or changed with limited notice. These ongoing changes may occasionally impact features in Identity Recovery for Microsoft Entra ID. When possible, Quest aims to provide timely notification to customers in cases of such impact. For the latest updates on Entra ID APIs, refer to the [Microsoft Entra ID](#) documentation and [Microsoft Graph Changelog](#) .

Objects can be restored from any backup to Microsoft Entra ID or Microsoft 365 without affecting other objects or attributes. Granular restore lets you recover objects that were accidentally deleted or modified in minutes. For more information about the objects and attributes that can be restored, see the [Identity Recovery for Microsoft Entra ID Supported Attributes Guide](#).

Identity Recovery for Microsoft Entra ID is a part of Quest Security Management Platform – a unified cloud platform that provides access to multiple Quest Software tools for Microsoft product management. For information about the management tools and configuration settings that apply to all Security Management Platform modules, see the [Security Management Platform Global Settings User Guide](#).

The following sections describe the initial steps to get started with Identity Recovery for Microsoft Entra ID:

- [Accessing Quest Security Management Platform](#)
- [Creating a Microsoft Entra Global Administrator Account](#)
- [Access Control](#)
- [Adding a Microsoft Entra Tenant](#)

Accessing Quest Security Management Platform

Security Management Platform management is based on the concepts of organizations. When you sign up for the Security Management Platform service, you create an organization and you are granted the Platform Administrator role. The organization can then subscribe to products like Identity Recovery. For more information, see [Signing up for Security Management Platform Global Settings](#) in *Security Management Platform Global Settings User Guide*.

To access Quest Security Management Platform

1. Go to quest-on-demand.com.
2. On the Welcome to Security Management Platform page, select **Sign in with Microsoft**.
3. Sign in using your Microsoft MFA-enabled account.
4. As part of the login process with Microsoft Entra ID, users must consent to the set of minimal permissions required by the Quest Security Management Platform application.
5. Select **Create New Organization**.
6. Enter a name for your Security Management Platform organization.
7. Select the deployment region where you want your data to reside.
8. Select **Create New Organization**.

You are signed in as the Security Management Platform administrator for the new organization. You have the option to start a trial or purchase a commercial subscription to Identity Recovery.

Creating a Microsoft Entra Global Administrator Account

To access your Microsoft Entra or Microsoft 365 tenant through Identity Recovery for Microsoft Entra ID, an administrative account with the Global Administrator role is required. We recommend creating an account dedicated to Identity Recovery for Microsoft Entra ID for enhanced security. Once consent has been granted in Identity Recovery for Microsoft Entra ID, the account can be downgraded if necessary. For information on granting Identity Recovery for Microsoft Entra ID-specific consent, see [Consents and Permissions](#).

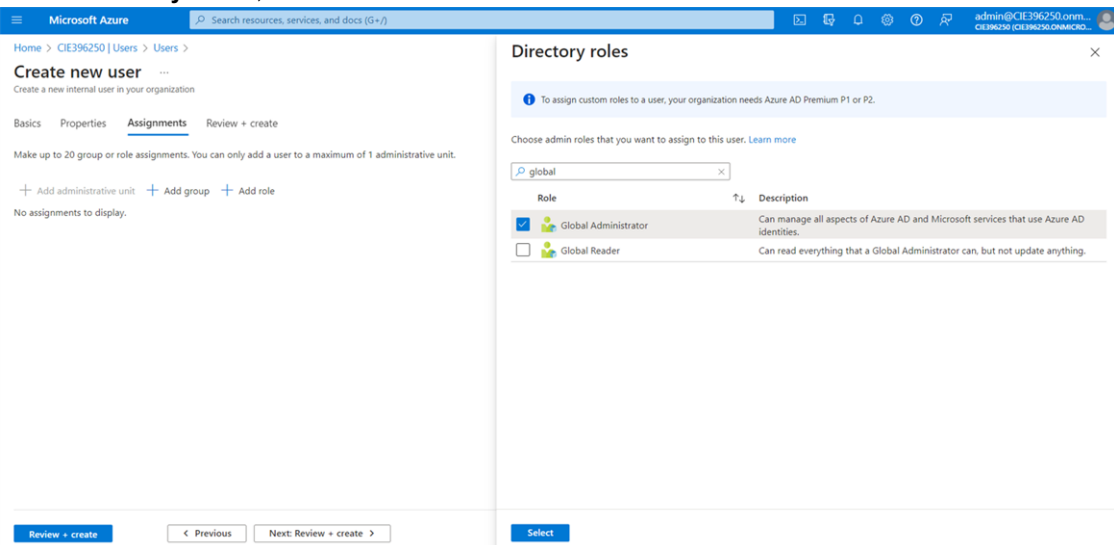
Prerequisites

You have an existing account with the Global Administrator role.

i | **NOTE:** If you do not have Global Administrator permissions, contact Microsoft support or your Microsoft 365 administrator.

To create a Global Administrator account in Azure portal

1. Sign in to [Azure portal](#) with an existing Global Administrator account.
2. Confirm your tenant by checking the tenant name next to your profile icon. To switch tenants, click your profile icon, select **Switch directories**, and then select the desired tenant from the **Directories + subscriptions** list.
3. Navigate to **Microsoft Entra ID**.
4. On the **Users** tab, select **New user**, then **Create new user**.
5. On the **Basics** tab, enter the required **Identity** details.
6. On the **Assignments** tab, select **Add role**.
7. Under **Directory roles**, choose **Global Administrator** and then select the **Select** button.



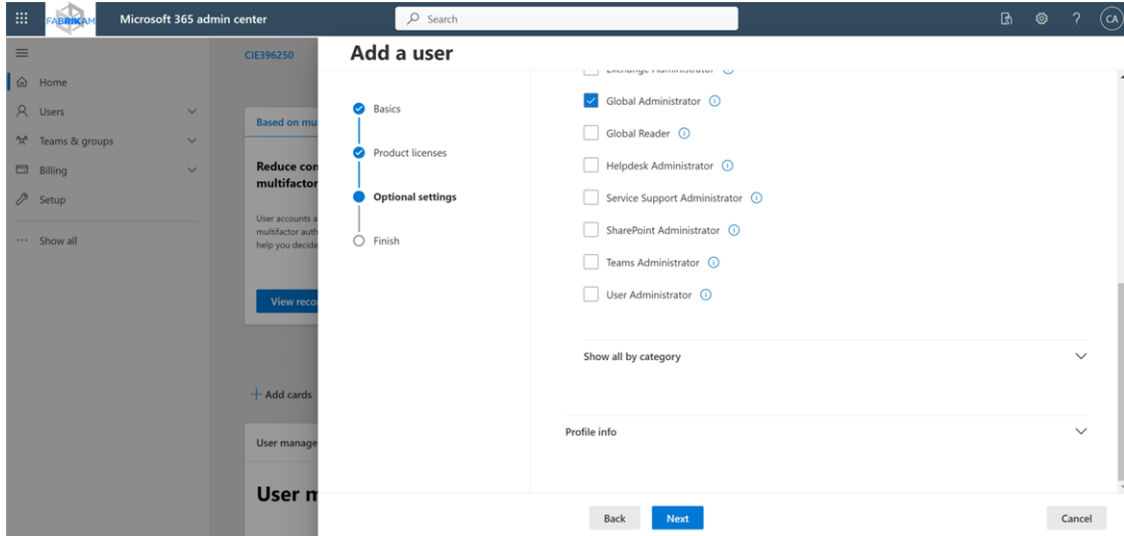
8. Select **Review + create**.
9. Select **Create**.

You can now use this account to access your Microsoft Entra ID tenant in Identity Recovery for Microsoft Entra ID.

To create a Global Administrator account in Microsoft 365 Admin Center

1. Sign in to [Microsoft 365 admin center](#) with an existing Global Administrator account.
2. Select **Users | Active users**, then select **Add a user**.
3. Enter basic user information and select **Next**.

4. In **Optional settings**, expand **Roles**, select **Admin center access**, then select **Global Administrator**.



5. Select **Next**.
6. Review and select **Finish adding**.

You can now use this account to access your Microsoft 365 tenant in Identity Recovery for Microsoft Entra ID.

Access Control

Quest Security Management Platform uses the role-based access control (RBAC) security policy that restricts information system access to authorized users. Your Security Management Platform organization comes configured with a number of default roles which cannot be changed, but subscribers can create custom roles with the permissions to perform required tasks on the assets of the organization. For more information, see [Access Control: Roles](#) in the *Security Management Platform Global Settings User Guide*.

If you are the Security Management Platform Administrator or the owner of the subscription, you can add users to an existing organization and assign one or more roles. The role assignment determines what permission level a user has and ultimately, what tasks the user can perform. For more information, see [Adding users to an organization and assigning a role](#) in the *Security Management Platform Global Settings User Guide*.

The following permissions are available for Identity Recovery for Microsoft Entra ID:

- Can Manage Backup Settings
- Can Download Hybrid Credentials
- Can Manage Events
- Can Manage Project Settings
- Can Read Backup History
- Can Read Differences
- Can Read Events
- Can Read Restore Attributes
- Can Read Task History

- Can Read UI Collections
- Can Read UI Projects
- Can Read Unpacked Objects
- Can Restore from Differences
- Can Restore from Objects
- Can Run Backup Manually
- Can Run Difference Report
- Can Unpack Backups

The Identity Recovery for Entra ID Administrator role gives users full access to the Identity Recovery for Microsoft Entra ID permissions listed above, plus the following Security Management Platform organization permissions:

- Can Export Data (Identity Recovery)
- Can Read Access Control Roles
- Can Read Activity Trail (Identity Recovery)

The Identity Recovery Administrator role gives users full access to Identity Recovery permissions (Identity Recovery for AD and Identity Recovery for Entra ID), plus the following Security Management Platform organization permissions:

- Can Configure Agents
- Can Export Data (Identity Recovery)
- Can Read Access Control Roles
- Can Read Activity Trail (Identity Recovery)

Adding a Microsoft Entra Tenant

You must have a tenant in the organization before you can back up or restore data in Identity Recovery for Microsoft Entra ID. When you add a tenant, use an account with the Global Administrator role in Microsoft Entra ID.

Applications used to manage tenant properties participate in the consent flow provided by Microsoft Entra ID. This means a Global Administrator must provide admin consent when adding a tenant to Security Management Platform. Admin consent is granted on behalf of the Microsoft Entra ID organization.

For information on adding, removing, and managing a Microsoft Entra tenant, see [Managing your Microsoft Entra tenants and on-premise domains](#) in *Security Management Platform Global Settings User Guide*.

i **NOTE:** Although GCC High tenants can be added on the **Tenants** page for use in other Security Management Platform modules, Identity Recovery for Microsoft Entra ID does not support restoring objects from GCC High tenants.

Backups are disabled by default when a tenant is added. You must enable backups for new tenants as described in [Configuring and Creating Backups](#).

Working with Identity Recovery for Microsoft Entra ID

This chapter provides guidance on configuring and using Identity Recovery for Microsoft Entra ID to back up and restore Microsoft 365 and Microsoft Entra ID data across your tenants. It focuses on helping you understand and navigate the user interface and perform key tasks, such as creating backups, unpacking backups, and restoring objects. While later sections describe the considerations for restoring various objects types, this chapter provides the fundamental workflows and configuration steps essential for managing your recovery environment.

Consents and Permissions	Understand the minimum consents and permissions required for backup and restore operations within your tenant.
Identity Recovery for Microsoft Entra ID Interface	Gain familiarity with user interface components for manage tasks and monitoring statuses across your tenants.
Backup and Restore Workflow	Overview of the end-to-end standard process for backup and recovery using Identity Recovery for Microsoft Entra ID.
Configuring and Creating Backups	Set up automated backup schedules, define retention periods, and configure advanced options before creating backups.
Unpacking Backups	Extract objects from packed backups to make the objects available for restore and compare backups with live directory data.
Restoring Objects	Perform granular recovery of deleted or modified data, including options for restoring from the Recycle Bin.
Advanced Search	Use keyword operators and query strings to refine search results.
Email Notifications	Configure built-in templates to ensure recipients are promptly alerted by email about critical events, such as backup failures.

Consents and Permissions

This section describes the minimum service principal consents and administrative roles required for Identity Recovery for Microsoft Entra ID to back up and restore data in your tenant.

- [Azure Account Used to Grant Consents](#)
- [Basic Consent Permissions](#)
- [Restore Consent Permissions](#)
- [Exchange Online PowerShell for Backup Consent](#)
- [Exchange Online PowerShell for Restore Consent](#)
- [Trusted IP Settings](#)

Azure Account Used to Grant Consents

Security Management Platform service principals require explicit permissions to access and operate with tenant assets. A Microsoft Entra Global Administrator grants these permissions through consents. After consent is granted, the account can be downgraded if necessary. For information on granting admin consent and viewing consent status for a tenant, see [Managing admin consent permissions](#) in *Security Management Platform Global Settings User Guide*.

When a tenant is added, admin consent is granted to the initial Core – Basic permission set for the Security Management Platform service principal. Additional consents are required to work with specific Identity Recovery for Microsoft Entra ID features. Identity Recovery for Microsoft Entra ID uses two service principals: **Identity Recovery – Basic** and **Identity Recovery – Restore**. For more information on explicit permissions for each service principal, see [Basic Consent Permissions](#) and [Restore Consent Permissions](#).

i **NOTE:** Admin consent for each Recovery consent type expires after 90 days. When consent expires, the status on the Tenant Consents page changes to **Not Granted**, and you must grant admin consent again by selecting **Re-Grant Consent** to continue using that functionality.

Some consents also require a role to be assigned to the service principal in addition to the admin consent grant. These roles are needed to support specific functionality, such as managing Exchange.

The following table summarizes the consents and administrator roles required for backup and restore operations in Identity Recovery for Microsoft Entra ID.

Consent Type	Description	Required Roles
Basic	All read operations that support backup and restore, such as reading directory, user, group, application, and policy data.	<ul style="list-style-type: none">To grant this consent, use an account with the Global Administrator role (the account can be downgraded after consent is granted).
Restore	All write operations that support restore, such as updating users, groups, devices, applications, policies, authentication methods, and organization settings.	<ul style="list-style-type: none">For restore operations, the Authentication Administrator, User Administrator, Windows 365 Administrator and Conditional Access Administrator roles are required.If any Conditional Access policies use a custom security attribute, the Attribute Definition Reader role is also required.For restore operations on Organization settings, the Global Administrator role is also required.
Exchange Online PowerShell for Backup	Backs up the linkage between users and their Exchange mailboxes.	<ul style="list-style-type: none">To grant consent, use an account with the Global Administrator role (the account can be downgraded after consent is granted).In addition to granting consent, you must assign the Global Reader role to the service principal created in your tenant. For more information, see Exchange Online PowerShell for Backup Consent.

Exchange Online PowerShell for Restore

Manages Exchange and reads and writes information in the tenant to support restore operations.

- To grant consent, use an account with the Global Administrator role (the account can be downgraded after consent is granted).
- In addition to granting consent, you must assign the Exchange Administrator role. For more information, see [Exchange Online PowerShell for Restore Consent](#).

Basic Consent Permissions

The Basic consent type grants the permissions required for read operations in Identity Recovery for Microsoft Entra ID, including backup. A Global Administrator must grant this consent for the tenant.

To view permissions for Basic consent

1. Select **Tenants** in the navigation panel on the left.
2. On the required tenant tile, select **Edit Consents**.
3. Under **Identity Recovery**, go to the **Basic** consent type.
4. In the **Status and Actions** column, select **View Details**.

Application permissions are used in the app-only access scenario, without a signed-in user present. The application can access any data associated with those permissions, and only an administrator or owner of the service principal can consent to them.

Delegated permissions are permissions that allow the application to act on a user's behalf. The application cannot access anything the signed-in user could not access themselves.

For more information on application and delegated permissions, see [Permissions and consent overview](#) in the Microsoft Entra ID documentation.

Consent Version 2.2

Type	Permission	Application API Name
Application	<i>Application.Read.All</i> Allows the app to read all applications and service principals without a signed-in user.	Microsoft Graph
Application	<i>DelegatedPermissionGrant.Read.All</i> Allows the app to read all delegated permission grants, without a signed-in user.	Microsoft Graph
Application	<i>Device.Read.All</i> Allows the app to read your organization's devices' configuration information without a signed-in user.	Microsoft Graph
Application	<i>Directory.Read.All</i> Allows the app to read data in your organization's directory, such as users, groups and apps, without a	Microsoft Graph

Type	Permission	Application API Name
	signed-in user.	
Application	<i>Group.Read.All</i> 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	<i>RoleManagement.Read.Directory</i> 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	<i>User.Read.All</i> 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	<i>Policy.Read.All</i> Allows the app to read all your organization's policies without a signed-in user.	Microsoft Graph
Application	<i>UserAuthenticationMethod.Read.All</i> Allows the app to read 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	<i>Member.Read.Hidden</i> Read all hidden memberships.	Microsoft Graph
Application	<i>Organization.Read.All</i> Allows the app to read the organization and related resources, without a signed-in user. Related resources include things like subscribed SKUs and tenant branding information.	Microsoft Graph
Application	<i>PeopleSettings.Read.All</i> Allows the app to read tenant-wide people settings without a signed-in user.	Microsoft Graph
Delegated	<i>email</i> Allows the app to read your users' primary email address.	Microsoft Graph

i **NOTE:** When using application permissions to access CertificateBasedAuthConfiguration, the signed-in user must have the Global Reader role.

Restore Consent Permissions

The Restore consent type grants the permissions required for write operations in Identity Recovery for Microsoft Entra ID, including restore. A Global Administrator must grant this consent for the tenant.

To view permissions for Restore consent

1. Select **Tenants** in the navigation panel on the left.
2. On the required tenant tile, select **Edit Consents**.
3. Under **Identity Recovery**, go to the **Restore** consent type.
4. In the **Status and Actions** column, select **View Details**.

Application permissions are used in the app-only access scenario, without a signed-in user present. The application can access any data associated with those permissions, and only an administrator or owner of the service principal can consent to them.

Delegated permissions are permissions that allow the application to act on a user's behalf. The application cannot access anything the signed-in user could not access themselves.

For more information on application and delegated permissions, see [Permissions and consent overview](#) in the Microsoft Entra ID documentation.

Type	Permission	Application API Name
Application	<i>AdministrativeUnit.ReadWrite.All</i> Allows the app to create, read, update, and delete administrative units and manage administrative unit membership without a signed-in user.	Microsoft Graph
Application	<i>Application.ReadWrite.All</i> Allows the calling app to create and manage applications and service principals without a signed-in user. This includes read, update, update application secrets, and delete. Does not allow management of consent grants or application assignments to users or groups.	Microsoft Graph
Application	<i>AppRoleAssignment.ReadWrite.All</i> 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	<i>Device.ReadWrite.All</i> 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	<i>Directory.ReadWrite.All</i> Allows the app to read and write data in your organization's directory, such as other users, groups. It	Microsoft Graph

Type	Permission	Application API Name
	does not allow the app to delete users or groups, or reset user passwords.	
Application	<i>Group.ReadWrite.All</i> 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	<i>Policy.Read.All</i> Allows the app to read all your organization's policies without a signed in user.	Microsoft Graph
Application	<i>Policy.ReadWrite.Authorization</i> Allows the app to read and write your organization's authorization policy without a signed in user. For example, authorization policies can control some of the permissions that the out-of-the-box user role has by default.	Microsoft Graph
Application	<i>Policy.ReadWrite.ApplicationConfiguration</i> Allows the app to read and write your organization's application configuration policies without a signed-in user. This includes policies such as <i>activityBasedTimeoutPolicy</i> , <i>claimsMappingPolicy</i> , <i>homeRealmDiscoveryPolicy</i> , <i>tokenIssuancePolicy</i> , and <i>tokenLifetimePolicy</i> .	Microsoft Graph
Application	<i>Policy.ReadWrite.AuthenticationFlows</i> Allows the app to read and write all authentication flow policies for the tenant, without a signed-in user.	Microsoft Graph
Application	<i>Policy.ReadWrite.ConditionalAccess</i> Allows the app to read and write your organization's conditional access policies on behalf of the signed-in user.	Microsoft Graph
Application	<i>Policy.ReadWrite.ExternalIdentities</i> Allows the application to read and update the organization's external identities policy without a signed-in user. For example, external identities policy controls if users invited to access resources in your organization via B2B collaboration or B2B direct connect are allowed to self-service leave.	Microsoft Graph
Application	<i>RoleManagement.ReadWrite.Directory</i>	Microsoft Graph

Type	Permission	Application API Name
	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.	
Application	<i>UserAuthenticationMethod.ReadWrite.All</i> 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	<i>User.ManageIdentities.All</i> Allows the app to read, update and delete identities that are associated with a user's account that the signed-in user has access to. This controls the identities users can sign-in with.	Microsoft Graph
Application	<i>User.ReadWrite.All</i> 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	<i>Directory.AccessAsUser.All</i> Allows the app to have the same access to information in your work or school directory as you do.	Microsoft Graph
Delegated	<i>Directory.ReadWrite.All</i> 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
Delegated	<i>Organization.ReadWrite.All</i> Allows the app to read and write the organization and related resources, on behalf of the signed-in user. Related resources include things like subscribed SKUs and tenant branding information.	Microsoft Graph
Delegated	<i>PeopleSettings.ReadWrite.All</i> Allows the app to read and write all tenant-wide people settings on behalf of a signed-in user.	Microsoft Graph

i | **NOTE:** When using delegated permissions to update insights for contacts, items, or people, the signed-in user must have the Global Administrator role.

Exchange Online PowerShell for Backup Consent

This application is required to back up the linkage between users and their Exchange mailboxes. You need to grant consent to Exchange Online PowerShell for Backup and assign the Global Reader role to the service principal created in your tenant. This role is required to access Exchange and retrieve the mailbox properties linked to the user accounts.

To view permissions for Exchange Online PowerShell for Backup consent

1. Select **Tenants** in the navigation panel on the left.
2. On the required tenant tile, select **Edit Consents**.
3. Under **Identity Recovery**, go to the **Exchange Online PowerShell for Backup** consent type.
4. In the **Status and Actions** column, select **View Details**.

The following permissions must be granted for Identity Recovery for Microsoft Entra ID to perform Exchange backup operations:

Type	Permission	Application API Name
Application	<i>Exchange.ManageAsApp</i> Allows the app to manage the organization's Exchange environment without any user interaction. This includes mailboxes, groups, and other configuration objects. To enable management actions, an admin must assign the appropriate roles directly to the app.	Office 365 Exchange Online
Application	<i>RoleManagement.ReadWrite.Directory</i> 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

To assign the Global Reader role to the service principal:

1. Select **Tenants** in the navigation panel on the left.
2. On the required tenant tile, select **Edit Consents**.
3. Under **Identity Recovery**, go to **Exchange Online PowerShell for Backup**.
4. In the **Status and Actions** column, select **Assign Role**.

i | **NOTE:** After the Global Reader role is assigned, the permission *RoleManagement.ReadWrite.Directory* can be manually removed for your tenant application.

Exchange Online PowerShell for Restore Consent

This application is required to manage Exchange Online and to read and write information in the tenant. To perform Exchange tasks, you need to grant consent to Exchange Online PowerShell for Restore and assign the Exchange Administrator role to the service principal created in your tenant. This role is required to perform Exchange task such as linking mailboxes to users, restoring inactive mailboxes, and deleting mail-enabled groups.

To view permissions for Exchange Online PowerShell for Restore consent

1. Select **Tenants** in the navigation panel on the left.
2. On the required tenant tile, select **Edit Consents**.
3. Under **Identity Recovery**, go to the **Exchange Online PowerShell for Restore** consent type.
4. In the **Status and Actions** column, select **View Details**.

The following permissions must be granted for Identity Recovery for Microsoft Entra ID to perform Exchange restore operations:

Type	Permission	Application API Name
Application	<i>Exchange.ManageAsApp</i> Allows the app to manage the organization's Exchange environment without any user interaction. This includes mailboxes, groups, and other configuration objects. To enable management actions, an admin must assign the appropriate roles directly to the app.	Office 365 Exchange Online
Application	<i>RoleManagement.ReadWrite.Directory</i> 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

To assign the Exchange Administrator role to the service principal:

1. Select **Tenants** in the navigation panel on the left.
2. On the required tenant tile, select **Edit Consents**.
3. Under **Identity Recovery**, go to **Exchange Online PowerShell for Restore**.
4. In the **Status and Actions** column, select **Assign Role**.

i **NOTE:** After the Exchange Administrator role is assigned, the permission `RoleManagement.ReadWrite.Directory` can be manually removed for your tenant application.

Trusted IP Settings

To strengthen access control for your tenant, we recommend configuring an IP allowlist using the ranges below. Identity Recovery for Microsoft Entra ID will access your tenant only from these addresses, so any traffic outside these ranges can be safely blocked.

Region	IP Prefixes
US	52.233.76.96/29, 20.230.254.72/29
EU	13.69.216.192/29, 13.69.214.48/29
Canada	20.104.81.8/29, 4.205.3.248/29
UK	51.145.35.32/29, 20.254.44.208/29
Australia	20.191.252.152/29, 68.218.80.112/29

Identity Recovery for Microsoft Entra ID Interface

The interface consists of the following components:

- [Tenant Selector](#)
- [Dashboard](#)
- [Backups](#)
- [Unpacked Objects](#)
- [Differences](#)
- [Events](#)
- [Tasks](#)

Tenant Selector

On the dashboard, the tenant selector determines which tenant data is displayed on the tiles. You can choose to display data for a single tenant or for all tenants.

i **NOTE:** If you select **Show All**, certain tiles and options that apply to a specific tenant are not available. The tile descriptions in [Dashboard](#) apply when one tenant is selected.

The tenant selector is also available at the top-right of each page. Use the tenant selector to choose which tenant data you are working with.

Dashboard

When you launch Identity Recovery for Microsoft Entra ID (**Recover | Microsoft Entra ID**), the **Dashboard** is the first page displayed.

The dashboard interface includes a top navigation bar with the Quest logo, 'Security Management Platform', and system status 'All Systems Operational'. Below this is a breadcrumb trail for 'Identity Recovery for Microsoft Entra ID' and a tenant selector set to 'Demo Tenant'. The main dashboard area features a menu with 'MANAGE BACKUPS', 'MANAGE RESTORES', 'CREATE BACKUP', 'UNPACK BACKUP', and 'CONFIGURE HYBRID CONNECTION'. The content is organized into several panels: a 'Tenant is protected' overview for WZ6DB, a '2 backups' bar chart, a '7 tasks' list, a '1810 unpacked objects' donut chart, a '4 differences' table, a '1 error' list, and a 'Hybrid connection' warning panel with a 'CONFIGURE CONNECTION' button.

Dashboard Menu

The action buttons on the dashboard menu offer quick access to the following key tasks:

- **Manage Backups** – Allows you to open the **Configure backup** dialog, where you can enable scheduled backups and configure backup settings.
- **Manage Restores** – Displays the admin consent status for each tenant for restore operations. If a tenant has not been granted consent, you can open the Tenant Consents page from here to grant the required consent.
- **Create Backup** – Starts a backup for the selected tenant.
- **Unpack Backup** – Opens the **Backup Unpacking** dialog, where you choose unpacking options and unpack a backup so that objects are available on the **Unpacked Objects** page.

- **Configure Hybrid Connection** – Allows you to download hybrid credentials to work with on-premises Recovery Manager for Active Directory.

Dashboard Tiles

The tiles on the dashboard give you an overview of recent activity and quick access to the tasks you run most often:

Tenant is protected/Not protected

If backups are not scheduled for the tenant, this tile displays **Not protected**. Use the **Configure backups** option to enable a backup schedule and configure backup settings.

If backups are scheduled for the tenant, this tile displays **Tenant is protected** and shows a summary of the backup configuration.

Backups

If no backups are available for the tenant, use the **Create backup** option to create a backup.

If backups are available for the tenant, this tile displays the number of backups and a chart showing the number of backups by date. To go to the **Backups** page, select **Show All**.

Tasks

This tile displays recent tasks that have been initiated or completed by users. To go to the **Tasks** page, select **Show All**.

Unpacked objects

If there are no backups to unpack, use the **Unpack Backup** option to unpack a backup.

If unpacked objects are available, this tile displays the number of unpacked objects and a chart showing the number of unpacked objects by object type. To go to the **Unpacked Objects** page, select **Show All**.

Differences

To compare data from an unpacked backup with live directory data, use the **Refresh Report** option on this tile to refresh the differences report.

If a differences report is available, this tile displays the overall number of differences and a list of the occurrences of each type of change (for example, new object, link added, and hard deleted object). To go to the **Differences** page, select **Show All**.

Errors

This tile displays a summary of any errors, warnings, or informational events that occurred during recent operations. To go to the **Events** page, select **Show All**.

Hybrid connection

If a hybrid connection is not configured, use the **Configure Connection** option on this tile to set up a hybrid connection with Recovery Manager for Active Directory for protecting cloud and on-premises objects and attributes.

If a hybrid connection is configured, this tile shows its status, including any warnings.

Backups

The **Backups** tab displays the backups created for the selected tenant. For each backup, you can see counts for each object type. From here, you can review backup history and unpack backups for restore. For more information, see [Unpacking Backups](#).

Unpacked Objects

Use the **Unpacked Objects** tab to view, search, and filter the objects from unpacked backups. You can then select the items you want to restore and start the restore. For more information, see [Restoring Objects](#).

Differences

Use the **Differences** tab to compare a backup with your live Microsoft Entra ID or Microsoft 365 tenant. From here, you can also restore selected differences or roll back unwanted changes, such as deleted or modified critical objects. For more information, see [Differences Report](#).

Events

Use the **Events** tab to review events, including errors and warnings, that occur during Identity Recovery for Microsoft Entra ID operations.

Tasks

Use the **Tasks** tab to view and manage tasks initiated by users, such as creating, unpacking, and restoring backups, and refreshing differences.

Backup and Restore Workflow

This topic provides an overview of the end-to-end flow of working with Identity Recovery for Microsoft Entra ID. Use this workflow to familiarize yourself with the user interface and understand the overall process of backup and recovery; refer to the linked topics for comprehensive details.

i **NOTE:** Before you configure backups or perform restore operations, ensure that the required consents and permissions for Identity Recovery for Microsoft Entra ID are granted for each Microsoft Entra tenant. For more information, see [Consents and Permissions](#).

1. To launch the Identity Recovery for Microsoft Entra ID **Dashboard**, select **Recover** in the navigation panel on the left, then select **Microsoft Entra ID** in the menu bar.
2. If you plan to perform hybrid restores with on-premises Active Directory, configure a hybrid connection with Recovery Manager for Active Directory. For more information, see [Integration with Recovery Manager for Active Directory](#).

3. To enable and configure backups, select, **Manage Backups** in the dashboard menu. For more information, see [Configuring and Creating Backups](#).
4. To create a backup manually, select **Create Backup** in the dashboard menu.
5. On the **Backups** page, select unpack options and unpack the backup. For more information, see [Unpacking Backups](#).

i | **NOTE:** After a backup is unpacked, you can either continue with the restore workflow on the **Unpacked Objects** page (Step 6) or use the **Differences** page (Step 7) to compare the backup with the live tenant and restore selected changes.

6. On the **Unpacked Objects** page, configure restore options and restore objects from the unpacked backup. For information, see [Restoring Objects](#).
7. Use the **Differences** page to view the differences between a selected backup and live Microsoft Entra ID or Microsoft 365 data, and, if needed, restore selected differences to roll back unwanted changes. For more information, see [Differences Report](#).
8. On the **Tasks** page, view the status and history of user-initiated tasks, such as backup, unpack, differences, and restore operations.
9. On the **Events** page, view any errors or warnings that may have occurred.

Configuring and Creating Backups

To configure backups

1. Select **Manage Backups** from the dashboard menu, then select the name of the tenant you want to configure backups for. If backups are not enabled for the tenant, you can also select the tenant from the tenant selector, then select **Configure backups** on the **Not protected** tile.
2. To enable scheduled backups, in the **Configure backup** dialog, select the **Enabled** option next to **Schedule**. The solution attempts up to 4 backups a day. Depending on how long each backup takes, the number may be fewer.

✕

Configure backup

Schedule Disabled ▾

Run backup immediately

Specify the backup retention period using the retention policy option. The backup retention policy is also applied to backups started manually. Specify the retention policy in the number of days. If no policy is set, the default is 5 years (1825 days). Warning: When changing the retention period, the new policy will only affect new backups.

Retention policy 1825

Backup options

Some advanced objects and attributes affect the performance of the backup or requires specific permissions, these are provided with separate options. Select the advanced options to backup.

- Back up linkage between users and inactive mailboxes
- Back up Application Proxy settings and connector groups
- Back up Custom Claims Policy settings
- Back up Organization settings

Save
Cancel

3. To start the backup immediately after you save and finish the configuration, select the **Run backup immediately** option.
4. Specify the retention policy as the number of days (1 to 1825) to retain backups. The default retention period is 1825 days (5 years).

i | **NOTES:**

- The retention policy applies to both scheduled and manually run backups.
- If you change the retention policy, the new retention period applies only to future backups.

5. Under **Backup options**, select the checkboxes for any advanced options you want to include in the backup:
 - **Back up linkage between users and inactive mailboxes** – Backs up the data that links users to inactive mailboxes.
 - **Backup Application Proxy settings and connector groups** – Backs up Application Proxy settings and connector groups.
 - **Back up Custom Claims Policy settings** – Backs up Custom Claims Policy settings for service principals.
 - **Back up Organization settings** – Backs up tenant-level organization settings.
6. Select **Save** and then **Finish**.

To manually create backups

To start a backup manually at any time, select **Create Backup** from the dashboard menu.

Unpacking Backups

On the **Backups** page, each packed backup and its associated properties are displayed in a separate row. Each backup row shows the backup start time, duration, and counts for each object type.

i **NOTE:** The **Users** column reflects the total number of users, including guest accounts. The **Guests** column reflects only guest accounts.

In the header, you can narrow the list of backup records using predefined or custom filters:

- **Status** – Select **Packed** or **Unpacked** to view only packed or unpacked records. By default, **Any** is selected.
- **Date Range** – Select **Today**, **7 days**, **30 days**, or **Custom range** to show records for the specific date range. For **Custom range**, select the start and end date from the calendar, then select **Apply**.

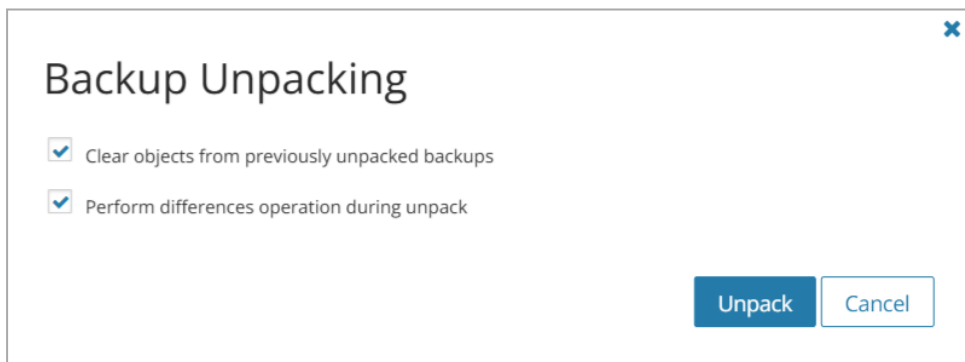
i **NOTE:** Results show records matching both the status and date range filters. Remove any filter by selecting the x icon on the corresponding badge, or select **Clear All** to remove all filters.

You can also use the search box to find specific backup records. For information about using advanced search operators, see [Advanced Search](#).

To unpack a backup

After creating a backup, you need to unpack the backup to make the backed up objects available for restore operations.

1. On the **Backups** page, select the row for the backup you want to unpack, then select **Unpack**.
2. In the **Backup Unpacking** dialog, review the default unpack options and deselect the checkboxes if required.



- **Clear objects from previously unpacked backups** – Removes the objects created by previous unpack tasks before unpacking the selected backup.
- **Perform differences during the unpack** – Compares the selected backup with the live data and displays the changes on the **Differences** page. If you deselect this option, then only the unpack operation will be performed.

3. Select **Unpack**.

Restoring Objects

After unpacking a backup, the unpacked objects available for restore are displayed on the **Unpacked Objects** tab. You can choose one of the following views to display the unpacked objects:

- **List View** – Lists the unpacked objects from your backup in a table. You can select objects to restore, or export the list to a CSV file.
- **Objects** – Displays the number of unpacked objects by category in summary charts.

Filters

In the header of the List view or Objects view, you can narrow the list of object records using the following filters:

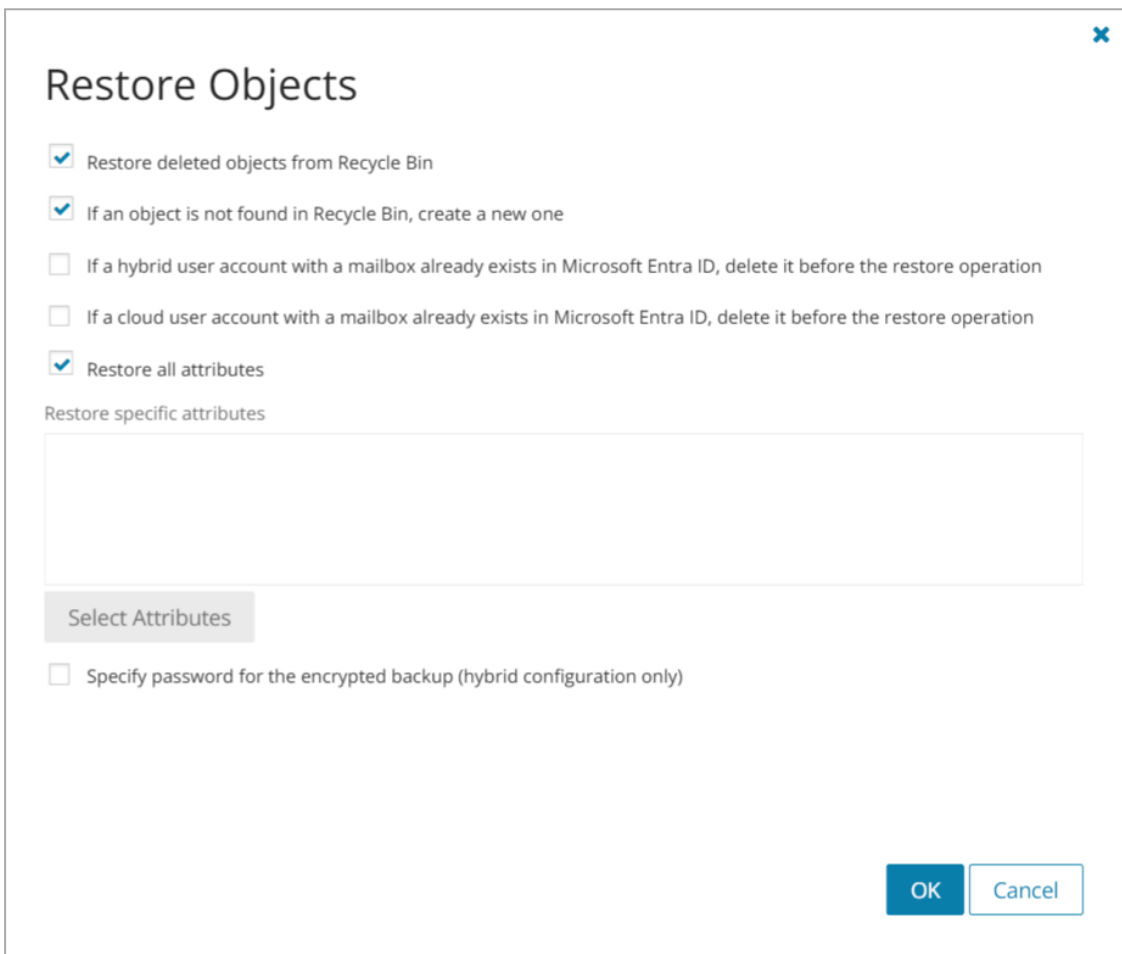
- **Tenant** – Filter objects by a specific tenant.
- **Backup** – Filter objects by backup date and time.
- **Type** – Filter objects by type. The following object types are available:
 - Administrative Unit
 - Claims Mapping Policy
 - Conditional Access Policy
 - Country Named Location
 - Device
 - Directory Setting
 - External Identities Settings
 - Group Lifecycle Policy
 - IP Named Location
 - Microsoft 365 Group
 - Organization
 - Security Defaults
 - Security Group
 - Service Principal
 - User
 - User Authentication Settings
 - User Authorization Settings
- **User Type** – Filter objects by user type (for example, **Work or school**, **B2B Guest**).
- **Microsoft Entra Connect** – Filter by objects synced from a hybrid environment (**Enabled**) or cloud-native objects (**Cloud Only**).
- **MFA** – Filter objects by whether multifactor authentication is mandatory for sign-ins (**Enforced**), available but not required (**Enabled**), turned off (**Disabled**), or by verification method (for example, **OneWaySMS**, **TwoWayVoiceMobile**).
- **Mail Enabled** – Filter objects that have a mailbox (**Enabled**) or do not have a mailbox (**Disabled**).

Prerequisites

Before restoring objects, ensure the selected tenant has been granted consent to perform restore operations. To check the consent status, on the dashboard, select **Manage Restores** from the menu. If you see a green icon for the tenant, you have granted the necessary consents. If the tenant has not been granted consent, select **Grant** next to the tenant to be navigated to the Tenant Consents page. Under **Identity Recovery**, for the **Restore** consent type, select **Grant Consent** or **Re-Grant Consent**. For more information, see [Consents and Permissions](#).

To restore objects

1. On the **Unpacked Objects** tab, in **List View**, select the checkboxes for the objects you want to restore.
2. Select **Restore**.
3. In the **Restore Objects** dialog, review the available restore options and adjust as needed:



Restore Objects

- Restore deleted objects from Recycle Bin
- If an object is not found in Recycle Bin, create a new one
- If a hybrid user account with a mailbox already exists in Microsoft Entra ID, delete it before the restore operation
- If a cloud user account with a mailbox already exists in Microsoft Entra ID, delete it before the restore operation
- Restore all attributes

Restore specific attributes

Select Attributes

Specify password for the encrypted backup (hybrid configuration only)

OK Cancel

- **Restore deleted objects from Recycle Bin** – Restores soft-deleted objects currently available in the Recycle Bin. The original object identifiers (GUID) are preserved.

- **If an object is not found in Recycle Bin, create a new one** – Recreates permanently deleted objects or soft-deleted objects that expired or were removed from the Recycle Bin. This option restores 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 Microsoft Entra ID, delete it before the restore operation** – Deletes existing hybrid user records before the restore to preserve the original cloud mailbox. For more information, see [Restoring Mailboxes for Hybrid Users](#).
- **If a cloud user account with a mailbox already exists in Microsoft Entra ID, delete it before the restore operation** – Deletes existing cloud user records before the restore to preserve the original cloud mailbox.
- **Restore all attributes** – Restores all object attributes including membership information (links). To restore only specific attributes, deselect this option and follow the steps in [To restore selected attributes](#).
- **Specify password for the encrypted backup** – If you are using a hybrid configuration, this option allows you to enter a password during restore to decrypt an encrypted backup.

4. Select **OK**.

i | **NOTE:** By Microsoft policy, hard-deleted objects receive a new Object ID (GUID) after restore. This breaks direct references like permissions, app assignments, and group memberships that relied on the original ID.

To restore selected attributes

Identity Recovery for Microsoft Entra ID allows you to restore specific attributes for each object.

1. In the **Restore Objects** dialog, deselect the **Restore all attributes** option, and select **Select Attributes**.

i | **NOTE:** Only the attributes for the selected object types will be displayed.

2. Select the checkboxes for the attributes you want to restore for each object.

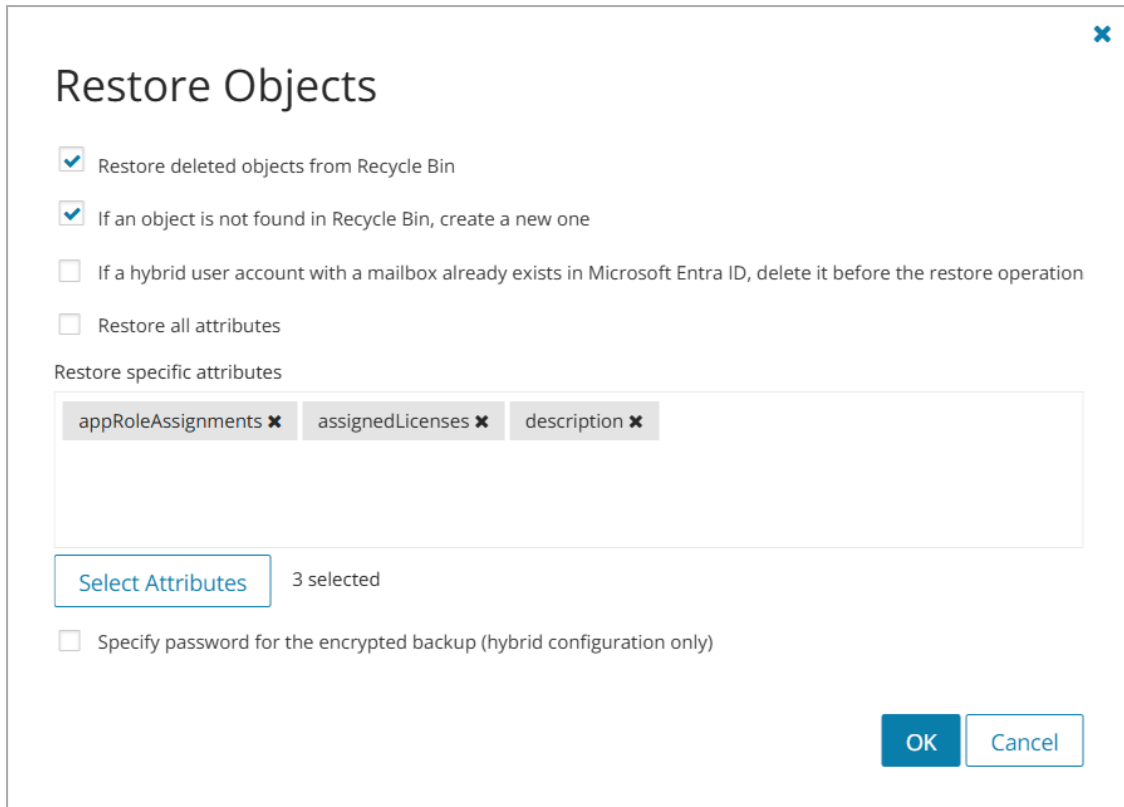
✕

<input type="checkbox"/>	Name ▲	Type
<input checked="" type="checkbox"/>	appRoleAssignments	Group
<input checked="" type="checkbox"/>	assignedLicenses	Group
<input checked="" type="checkbox"/>	description	Group
<input checked="" type="checkbox"/>	description	Administrative Unit
<input type="checkbox"/>	displayName	Group
<input type="checkbox"/>	displayName	Administrative Unit

1-25 of 33 ResultsShow < 1 / 2 >

appRoleAssignments ✕assignedLicenses ✕description ✕

3. Select **Save**. Your selected attributes will be displayed in the **Restore specific attributes** box.



4. Select **OK**.

Which Objects Can Be Restored from the Recycle Bin?

Identity Recovery for Microsoft Entra ID can restore the following objects from the Recycle Bin:

- Users (all types including B2B, B2C, guests, and hybrid)
- Microsoft 365 groups
- Service principals (enterprise applications)
- Applications (application registrations)
- Application proxy
- Administrative units

i **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:

- Security groups
- Distribution groups

- Mail-enabled groups
- All groups synchronized by Microsoft Entra Connect from on-premises
- Devices
- Conditional Access policies
- Country named locations
- IP named locations
- Tenant level settings

Restoring Passwords

Identity Recovery for Microsoft Entra ID does not back up passwords. During the restore of permanently deleted users, a random password is set that can be changed by the administrator at the next login.

Differences Report

The differences report allows you to compare a selected backup with live Microsoft Entra ID or Microsoft 365 directory data. It highlights modifications or deletions since the backup was created, enabling granular restores or rollbacks of specific attributes, entire objects, or unwanted changes without affecting unchanged items. This report helps you troubleshoot and resolve issues 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 Microsoft Entra 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, including deletion of a service principal, addition or removal of roles (custom roles are not monitored), and changes to the 'accountEnabled' property.
- Objects moved to the Recycle Bin.
- Permanently deleted objects.
- Links affected by the deletion of groups, such as Microsoft Entra group membership, group owners, and application assignments (shown only in the differences report).

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

Restoring from Differences

On the **Differences** page, choose one of the following views to compare the differences between the unpacked backup and live directory data:

- **List View** – Lists each difference in a table. You can select specific changes to restore or rollback, or export the list to a CSV file.
- **Differences** – Displays the differences categorized by change type or object type in summary charts.

Filters

In the header of the List view or Differences view, you can narrow the list of differences records using the following filters:

- **Tenant** – Filter differences by a specific tenant.
- **Backup** – Filter differences by backup date and time.
- **Type** – Filter differences by object type and change category. The following types are available:
 - Administrative Unit
 - Administrative Unit Link Change
 - Application Owner Link Change
 - App Role Assignment
 - Conditional Access Policy
 - Country Named Location
 - Device
 - Director Link Change
 - Directory Role Link Change
 - Directory Setting
 - External Identities Settings
 - Group
 - Group Lifecycle Policy
 - Group Lifecycle Policy Link Change
 - Group Owner Link Change
 - IP Named Location
 - Microsoft 365 Group
 - OAuth2PermissionGrant
 - Owner Link Change
 - Registered Owner Device Link Change
 - Registered User Device Link Change
 - Scoped Role Membership
 - Security Group
 - Service Principal
 - User
 - User Authentication Settings
 - User Authorization Settings

- **Change Type** – Filter differences by the type of change:
 - **Changed** – Attribute-level modifications.
 - **Link added** – Newly added relationships (links).
 - **Link removed** – Removed relationships (links).
 - **New object** – Objects created after the backup.
 - **Object hard deleted** – Permanently deleted objects.
 - **Object soft deleted** – Objects marked as deleted but not physically removed.
- **Top 5 attributes** – Filter by one of five attributes with the highest number of changes.

You can also use the search box to find specific object records. For information about using advanced search operators, see [Advanced Search](#).

Prerequisites

- You have created a backup of your directory.
- Changes exist in your live Microsoft Entra ID or Microsoft 365 since the backup was created.
- While unpacking the backup, you selected the **Perform differences during the unpack** option in the **Backup Unpacking** dialog.

To view differences and restore changes

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

1. Go to the **Differences** tab.
2. Select the changes you want to restore or roll back, then select **Restore**.
3. In the **Restore Differences** dialog, select the relevant options:
 - **Specify password for the encrypted backup (hybrid configuration only)** – Allows you to enter a password during restore to decrypt an encrypted backup.
 - **If a hybrid user already exists in Microsoft Entra ID, delete it before the restore operation** – Deletes existing hybrid user records before the restore to preserve the original cloud mailbox. For more information, see [Restoring Mailboxes for Hybrid Users](#).
 - **If a cloud user already exists in Microsoft Entra ID, delete it before the restore operation** – Deletes existing cloud user records before the restore to preserve the original cloud mailbox.
4. To update the report with current live data, select **Refresh**.
5. Review the results of the restore and repeat if necessary.

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 1: 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'.
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".

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

Search by Date Range

Table 2: 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 3: 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:Sam.Jones@mycompany.com

Column display name	Column internal name	To search for	Query example
		mail address	
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 4: 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 specific attribute	changedAttribute:link
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 5: 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 6: 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*

Email Notifications

Email notifications in Security Management Platform alert designated recipients when specific events occur. For example, after a Backup Failure event, the configured recipients receive an email notification. Identity Recovery for Microsoft Entra ID includes built-in notification templates to ensure that you are kept up to date on critical activity within your organization. For information on how to configure who will receive the notification, see [Configuring Notification Templates](#).

The following built-in notification template is currently available:

- Backup Failures

Configuring Notification Templates

Notification templates allow you to configure who will receive notifications so that they can take the appropriate action to address the outlined risks to your environment. Notification templates are managed through Security Management Platform Global Settings.

To edit a notification template

1. In the side navigation panel of Security Management Platform, select **Settings**.
2. In the main panel, select **Notification | Email Notifications** in the menu bar.
3. Expand **Identity Recovery for Microsoft Entra ID**.
4. Select the notification template name of the template you want to edit.
5. To add recipients, enter the required email addresses and select **Add Recipients**.
6. To remove recipients, select the checkboxes for the relevant recipients listed under **Selected Recipients**, and select **Remove**.
7. Optionally, send a test email by selecting the checkboxes for one or more recipients and selecting **Send Test Email**.
8. Select **Save**.

The next time an event that is associated with this notification template occurs, all listed recipients receive a notification email.

Restoring Directory Roles and Application Roles

Identity Recovery for Microsoft Entra ID backs up and restores the assigned roles in Microsoft Entra ID.

Supported scenarios

The following scenarios are supported in Identity Recovery for Microsoft Entra ID:

- Restoring eligible/active assigned roles that are associated with applications integrated with Microsoft Entra ID. For more information, see [Restoring Service Principal Objects](#).
- 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 Identity Recovery for Microsoft Entra ID:

- Custom Microsoft Entra roles are not restored.
- Custom Microsoft 365 roles are not restored.

Restoring Users

Users that were accidentally deleted can be restored using Identity Recovery for Microsoft Entra ID. 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 Microsoft Entra ID.

Supported scenarios

The following scenarios are supported by Identity Recovery for Microsoft Entra ID:

- 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.

i **NOTE:** Because of Microsoft requirements, hard deleted objects will receive a new Object ID upon restore of these objects. Please consider the implications of having a new Object ID after restoring these objects.

Restored user attributes

For a list of user attributes restored by Identity Recovery for Microsoft Entra ID, see the [Identity Recovery for Microsoft Entra ID Supported Attributes Guide](#).

Restoring Groups

In Microsoft Entra ID, there are two types of groups: security and Microsoft 365. If either type is deleted in Microsoft Entra ID, it is soft deleted and moved to the **Deleted groups** page where it can be restored or permanently deleted. The differences report in Identity Recovery for Microsoft Entra ID identifies groups as being soft deleted or hard deleted in Microsoft Entra ID. Both soft deleted or hard deleted Microsoft 365 groups can be restored from the differences report. For security groups, only hard-deleted groups are currently supported.

Supported scenarios

The following scenarios are supported in Identity Recovery for Microsoft Entra ID:

- Restoring security groups and group membership
- Restoring Microsoft 365 groups and group membership
- Restoring dynamic groups
- Restoring group owners associated with a security group
- Restoring group owners associated with a Microsoft 365 group

i **NOTE:** Because of Microsoft requirements, hard-deleted objects will receive a new Object ID upon restore of these objects. Please consider the implications of having a new Object ID after restoring these objects.

Restored group attributes

For a list of group attributes restored by Identity Recovery for Microsoft Entra ID, see the [Identity Recovery for Microsoft Entra ID Supported Attributes Guide](#).

Limitations

The following groups are not restored by Identity Recovery for Microsoft Entra ID:

- Distribution groups

Restoring Service Principal Objects

Identity Recovery for Microsoft Entra ID 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 Microsoft Entra ID. 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 the solution, see [How does Identity Recovery for Microsoft Entra ID Handle Object Attributes?](#)

i **NOTE:** Due to the design specifications set by Microsoft, the default App Role can only be assigned to a principal if the corresponding resource application has not declared any App Roles. This limitation prevents Identity Recovery for Microsoft Entra ID from restoring default application role assignments for such principals. See [Microsoft documentation](#) for more information.

i **NOTE:** Because of Microsoft requirements, hard deleted objects will receive a new Object ID upon restore of these objects. Please consider the implications of having a new Object ID after restoring these objects.

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

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

- **Application object**
A Microsoft Entra application is defined by its one and only application object, which resides in the Microsoft Entra tenant where the application was registered, known as the application's "home" tenant. The Microsoft Graph Application entity defines the schema for an application object's properties.
- **Service principal object**
In order to access resources that are secured by a Microsoft Entra 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 Microsoft Entra 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 Microsoft Entra Gallery

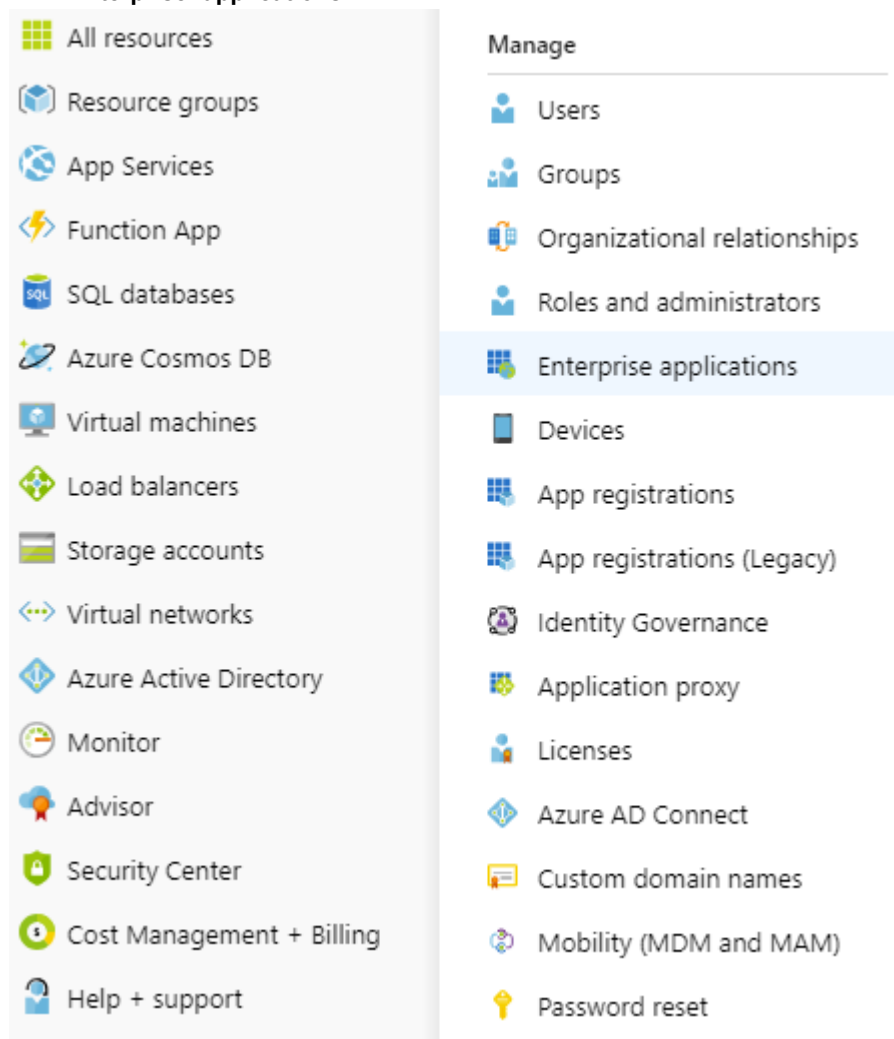
Identity Recovery for Microsoft Entra ID supports restoring service principals provisioned from Microsoft Entra Gallery.

Limitations: Identity Recovery for Microsoft Entra ID does not backup certificate settings for applications.

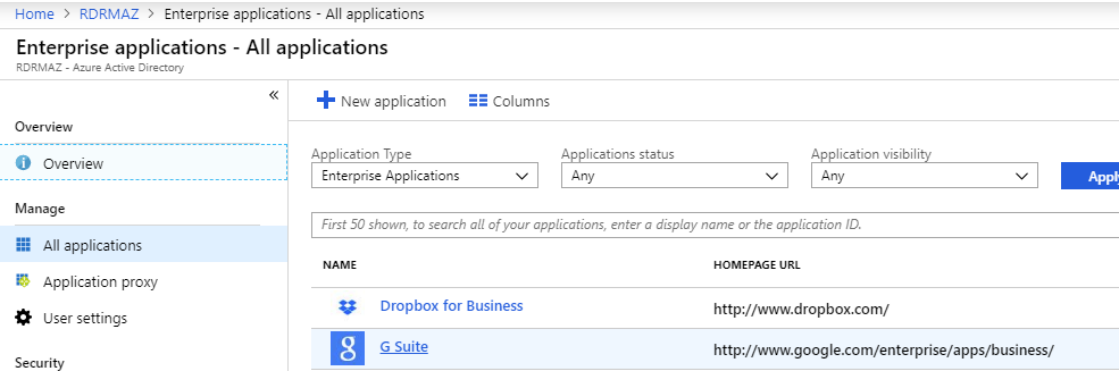
To make SAML SSO work after the restore of a service principal provisioned from Microsoft Entra Gallery, you must install the new certificate for the corresponding application. For details on how to provide the certificate for a particular application, refer to the application configuration guide.

To access the application configuration guide

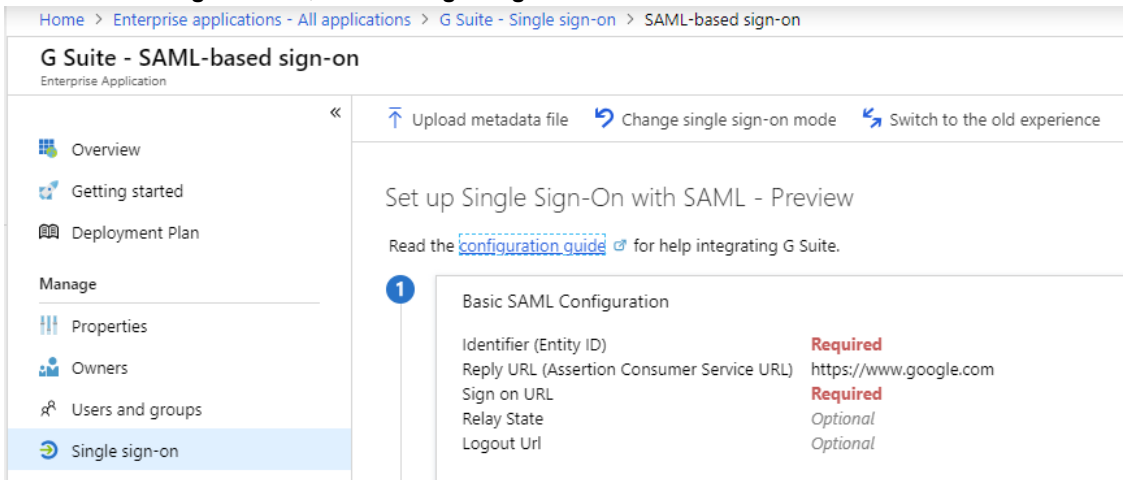
1. In Azure Management Portal, navigate to the **Microsoft Entra ID** section in the left pane and click **Enterprise applications**.



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



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



- Click the **configuration guide** link.

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 7: 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 portal	Differences report
Azure Information Protection administrator	Information Protection Administrator
Intune Administrator	Intune Service Administrator
Skype for Business Administrator	Lync Service Administrator
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

Restoring Applications

You can restore applications from the Recycle Bin as well as hard deleted applications. Identity Recovery for Microsoft Entra ID performs the following actions when restoring applications:

- If there is an application in the Recycle Bin, it is restored. After the application is restored, Identity Recovery for Microsoft Entra ID restores application attributes that are in the backup.
- If there is no application in the Recycle Bin, Identity Recovery for Microsoft Entra ID attempts to restore it from the backup.

Supported scenarios

The following scenarios are supported by Identity Recovery for Microsoft Entra ID:

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

i **NOTE:** Because of Microsoft requirements, hard deleted objects will receive a new Object ID upon restore of these objects. Please consider the implications of having a new Object ID after restoring these objects.

Restoring Application Proxy Settings

Identity Recovery for Microsoft Entra ID supports the recovery of Application Proxy settings, Connector groups, and Connector group membership.

Supported scenarios

The following scenarios are supported in Identity Recovery for Microsoft Entra ID:

- 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, Identity Recovery for Microsoft Entra ID 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

Identity Recovery for Microsoft Entra ID restores the following configuration data for an Application Proxy item:

Connector Groups

For deleted connector groups, Identity Recovery for Microsoft Entra ID 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 back up Application Proxy settings and connector groups

1. On the **Dashboard**, select **Manage backups**.
2. Select the tenant from the list.
3. In the **Configure backup** dialog, under **Backup options**, select **Back up Application Proxy settings and connector groups**.
4. Select **Save**.

For more information, see [How does Identity Recovery for Microsoft Entra ID Handle Object Attributes?](#)

Restoring Group Licenses

Identity Recovery for Microsoft Entra ID 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 Identity Recovery for Microsoft Entra ID:

- 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 Microsoft Entra ID 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.

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

Restoring Devices

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

i **NOTE:** Because of Microsoft requirements, hard deleted objects will receive a new Object ID upon restore of these objects. Please consider the implications of having a new Object ID after restoring these objects.

Limitations

The following limitations exist when restoring devices in Identity Recovery for Microsoft Entra ID:

- 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 Identity Recovery for Microsoft Entra ID:

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

Restored device attributes

For a list of device attributes restored by Identity Recovery for Microsoft Entra ID, see the [Identity Recovery for Microsoft Entra ID Supported Attributes Guide](#).

Restoring Conditional Access Policies

Identity Recovery for Microsoft Entra ID supports backing up and restoring Conditional Access policies and Named Location policies in cloud-only environments.

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

To backup Conditional Access policies

Backing up Conditional Access policies and Named Location policies is enabled by default.

Supported Scenarios

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

The following policy types are supported by Identity Recovery for Microsoft Entra ID:

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

Identity Recovery for Microsoft Entra ID restores the whole policy object and displays the changes in the differences report. The solution checks whether objects (users, groups, named locations) assigned to the policy exist in Microsoft Entra ID. 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 the solution, see the [Identity Recovery for Microsoft Entra ID Supported Attributes Guide](#).

i **NOTE:** Because of Microsoft requirements, hard deleted objects will receive a new Object ID upon restore of these objects. Please consider the implications of having a new Object ID after restoring these objects.

Limitations

Other policy types such as token issuance policy, token lifetime policy, and many others are currently not supported by Identity Recovery for Microsoft Entra ID. For more information, see the [Known issues](#) in the 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 Identity Recovery for Microsoft Entra ID 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 Identity Recovery for Microsoft Entra ID 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 Identity Recovery for Microsoft Entra ID, and a link is subsequently added to a user in live policies, 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.

Restoring Claims Mapping Policy

Identity Recovery for Microsoft Entra ID supports backing up and restoring Claims Mapping Policy.

Claims Mapping Policy is used to customize the claims emitted in tokens for specific applications within a tenant. With claims-mapping policies, you can select which claims are included in tokens, create new claim types, and change the source of data emitted in specific claims.

Supported Scenarios

Identity Recovery for Microsoft Entra ID restores the entire Claims Mapping Policy object and displays any changes in the differences report. The product checks whether the service principals to which the policy is applied exist in Microsoft Entra ID. If any service principals are missing, the policy is restored but a warning is displayed.

Restored Claims Mapping Policy attributes

For a list of Claims Mapping Policy attributes restored by Identity Recovery for Microsoft Entra ID, see the [Identity Recovery for Microsoft Entra ID Supported Attributes Guide](#).

Backup and Restore of Tenant Level Settings

Identity Recovery for Microsoft Entra ID supports the ability to backup and restore many types of tenant level settings.

Object Types

The backup and restore of the following tenant level settings are supported by Identity Recovery for Microsoft Entra ID. The corresponding object type for each tenant level setting will appear in the Unpacked Objects list view.

Tenant Level Setting	Object Type
Backup and restore of user settings	User Authorization Settings User Authentication Settings External Identities Settings
Backup and restore of group settings (Naming policy)	Directory Settings
Backup and restore of group settings (Expiration policy)	Group Lifecycle Policy
Backup and restore of security settings (Security defaults policy)	Security Defaults
Backup and restore of Organization settings	Organization

i NOTE:

- Backing up Organization settings is not enabled by default. You need to select this option when configuring backup options. For more information, see [Backup and Restore Workflow](#).
- For restore operations on Organization settings, the signed-in user must have the Global Administrator role.

Limitations

The following tenant level settings cannot be currently restored by Identity Recovery for Microsoft Entra ID:

- Password reset
- Domains

Tenant level settings attributes

For a list of attributes restored by Identity Recovery for Microsoft Entra ID, see the [Identity Recovery for Microsoft Entra ID Supported Attributes Guide](#). Each attribute can be restored individually. For information about the steps, see *To restore selected attributes* in [Restoring Objects](#).

Backup and Restore Administrative Units

Identity Recovery for Microsoft Entra ID can backup and restore Microsoft Entra administrative units from the Recycle Bin.

i **NOTE:** An additional permission *AdministrativeUnit.ReadWrite.All* is required to restore administrative units. For more information, go to the [Restore Consent Permissions](#) section.

Object Types

The corresponding object type for administrative units will appear in the Unpacked Objects list view:

Setting	Object Type
Backup and restore of administrative units	Administrative Unit Link to scopedRoleMember will be displayed in Differences report with type "ScopedRoleMembership".

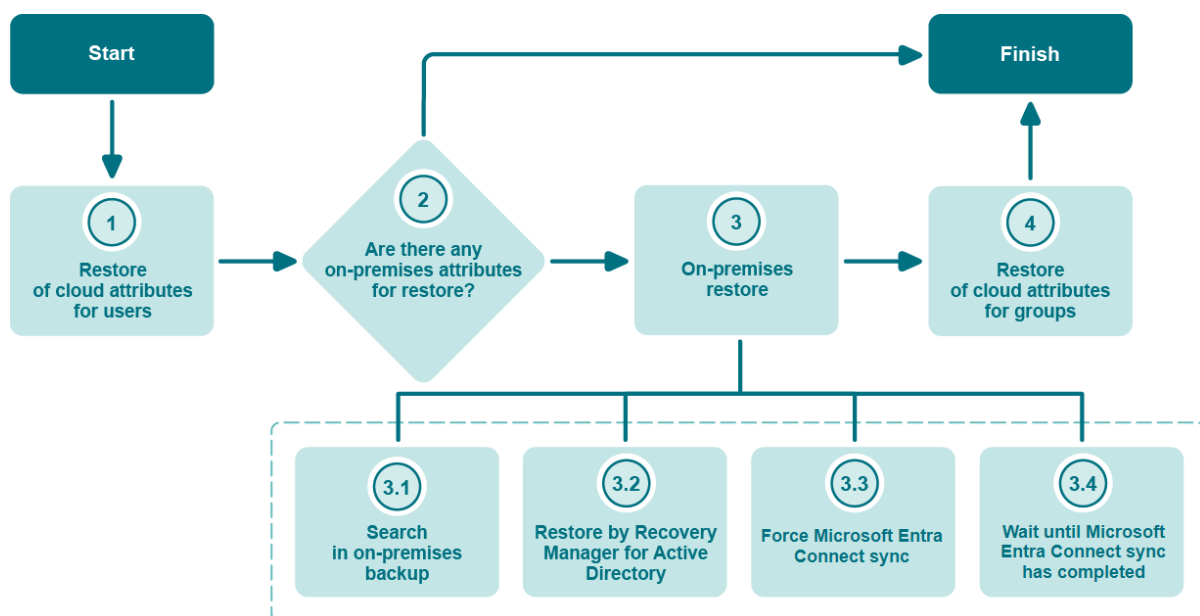
Administrative units attributes

For a list of attributes restored by Identity Recovery for Microsoft Entra ID, see the [Identity Recovery for Microsoft Entra ID Supported Attributes Guide](#). Each attribute can be restored individually. For information about the steps, see *To restore selected attributes* in [Restoring Objects](#).

Integration with Recovery Manager for Active Directory

Identity Recovery for Microsoft Entra ID 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 Microsoft Entra Connect. The following figure illustrates the hybrid restore process.

Figure 1: Hybrid Restore Operation Flow Diagram



i NOTE:

- All attributes that can be modified by Microsoft Graph API are considered as cloud attributes and restored on the first step. For example: **assignedLicense**, **usageLocation**, **membership** in cloud groups.
- Identity Recovery for Microsoft Entra ID also restores users from the Recycle Bin or recreates them before the on-premises restore with the **Undelete** option. Microsoft Entra Connect matches these objects after the cloud restore by the Security Identifier as well as the **immutableID** attribute which is restored from the Identity Recovery for Microsoft Entra ID 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, Identity Recovery for Microsoft Entra ID needs to wait until a group is recreated by Microsoft Entra Connect.

Prerequisites

- Microsoft Entra tenant that is synchronized with on-premises Active Directory by Microsoft Entra Connect.
- For Recovery Manager for Active Directory (RMAD) version 10.2.2 or later, the Hybrid Connector service must be enabled and configured in the RMAD console. To get the latest version of Recovery Manager for Active Directory, click [here](#).
 - For Recovery Manager for Active Directory 10.2.1 or earlier, the Recovery Manager Portal is required. If you have Microsoft Entra Connect version 1.4.32.0 or higher, the Recovery Manager Portal 10.1 is required.
 - The portal can be run on any machine in your environment. It is not required to install all Recovery Manager for Active Directory components.

To configure Hybrid Connector service with Recovery Manager for Active Directory - v.10.2.2 or later

For Recovery Manager for Active Directory 10.2.2 and later versions, you will need to disable the Recovery Manager Portal (if previously enabled), and enable and configure the Hybrid Connector service in the Recovery Manager for Active Directory (RMAD) console.

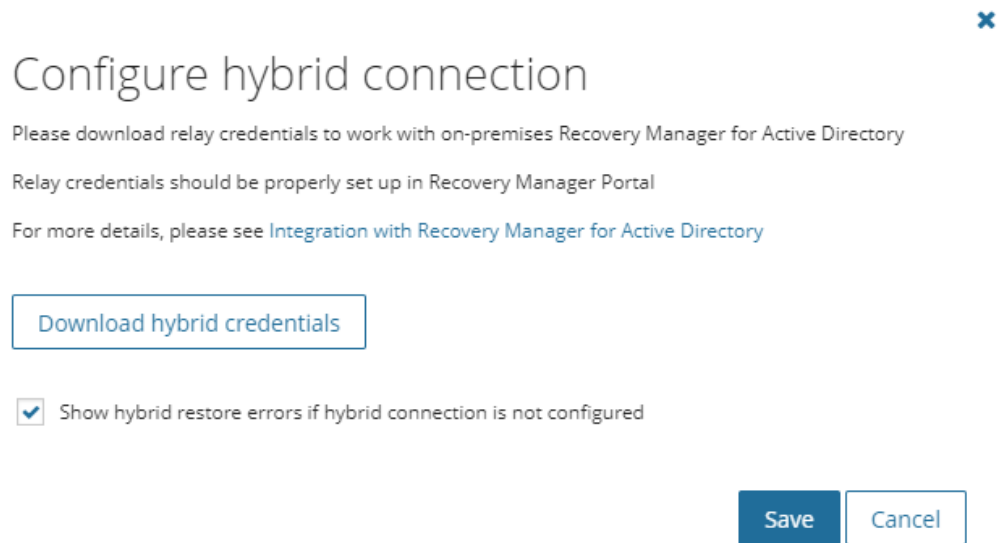
1. In the RMAD console, select the **Hybrid Recovery** node from the tree and select **Enable Integration with On Demand Recovery**.
2. In Identity Recovery for Microsoft Entra ID, select **CONFIGURE CONNECTION** under the **Hybrid Connection** tile.
3. Download the credentials.
4. In the RMAD console, open the hybrid credential file saved from step 3. This will automatically populate all the required fields.
5. Provide Microsoft Entra Connect host settings.
6. Enter the domain username, password and primary computer for each domain discovered in the backup.

For more information on this, see [Hybrid Recovery with On Demand Recovery](#).

To configure Recovery Manager Portal to enable integration with Recovery Manager for Active Directory - v.10.2.1 or earlier

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. Select **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 Identity Recovery for Microsoft Entra ID and perform the following steps:
 - a. On the **Dashboard**, select **Configure Hybrid Connection**.



- b. In the Configure hybrid connection dialog, select **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, deselect the **Show hybrid restore errors if hybrid connection is not configured** checkbox.
 - 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.
- i** **NOTE:** Microsoft Entra Connect synchronization occurs automatically after the restore operation. But Identity Recovery for Microsoft Entra ID forces synchronization cycles and requires credentials for the machine where Microsoft Entra Connect is installed.
6. Specify Microsoft Entra Connect host name and credentials. If Microsoft Entra Connect and Recovery Manager Portal are installed on the same machine, leave the fields blank.

i **NOTE:** You may get an error related to the proxy settings while configuring integration with Identity Recovery for Microsoft Entra ID. 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 [Hybrid Recovery with On Demand Recovery](#).

What can be restored in hybrid configuration?

- On-premises groups
- User licenses (e.g. Microsoft 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-Microsoft 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
- Conditional Access policies

i **NOTE:** Because of Microsoft requirements, hard deleted objects will receive a new Object ID upon restore of these objects. Please consider the implications of having a new Object ID after restoring these objects.

Important Considerations

- To restore on-premises objects, Identity Recovery for Microsoft Entra ID uses attribute values from the RMAD backup that is closest in time but older than the cloud backup unpacked in the Identity Recovery for Microsoft Entra ID 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)

- Identity Recovery for Microsoft Entra ID 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.

i **NOTE:** Hybrid recovery uses the default recovery method defined in Recovery Manager for Active Directory (**Settings | General** tab). The default recovery method does not allow for the recovery of passwords from backups. As Identity Recovery for Microsoft Entra ID does not provide an option to set a password for recovered users, hybrid users are restored without a password and are disabled.

- After the hybrid restore operation, Identity Recovery for Microsoft Entra ID forces Microsoft Entra 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 Microsoft Entra 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.
- Identity Recovery for Microsoft Entra ID supports one hybrid connection per Security Management Platform organization. If you need to manage multiple hybrid tenants, create a separate Security Management Platform organization for each Hybrid Microsoft Entra tenant.
- One instance of Recovery Manager Portal can be used with one Microsoft Entra tenant and one Microsoft Entra Connect server. Install multiple RMAD web portals if you need to work with multiple Microsoft Entra tenants and Microsoft Entra connect servers.
- Identity Recovery for Microsoft Entra ID 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 Security Management Platform organization). Identity Recovery for Microsoft Entra ID creates WCF Relay per organization. No changes to On-Premises Firewall settings are required.

To perform a restore operation in Identity Recovery for Microsoft Entra ID

1. Unpack a backup.
2. Go to the **Unpacked Objects** page and select on-premises objects to restore.
3. Select **Restore**.
4. In the **Restore Objects** dialog, if you select the **Restore all attributes** option, Identity Recovery for Microsoft Entra ID 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.

i **NOTE:** You can restore a hybrid user using only Identity Recovery for Microsoft Entra ID without configuring a hybrid connection. In this case, do not forget to deselect the **Show hybrid restore errors if hybrid connection is not configured** checkbox in the Configure hybrid connection dialog. If the hybrid connection is not configured, Identity Recovery for Microsoft Entra ID restores a cloud user and their cloud attributes without an on-premises user. For more information, see [How does Identity Recovery for Microsoft Entra ID Handle Object Attributes?](#) This scenario does not work for Federated Domains.

Limitations When a Hybrid Connection is Not Configured

Identity Recovery for Microsoft Entra ID 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, Identity Recovery for Microsoft Entra ID 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 Microsoft Entra 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 Identity Recovery for Microsoft Entra ID 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, Identity Recovery for Microsoft Entra ID 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. Identity Recovery for Microsoft Entra ID cannot restore a permanently deleted hybrid group that was synchronized by Microsoft Entra 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** 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** checkbox in the **Configure hybrid connection** dialog. For details, see [Integration with Recovery Manager for Active Directory](#).

The widget has the following states:

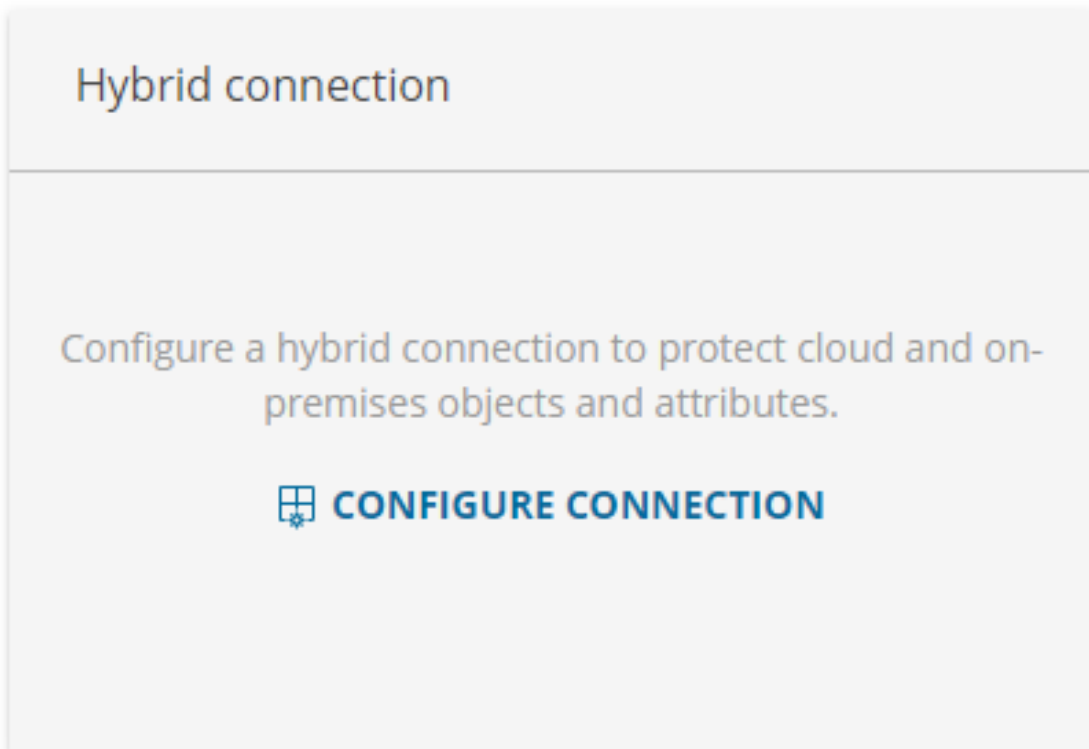
- If the hybrid connection is properly configured and works fine, the widget is green.

Hybrid connection



Hybrid connection is configured.

- 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** checkbox 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** checkbox is selected in the **Configure hybrid connection** dialog, the widget is yellow and has a warning sign.

Hybrid connection



Hybrid connection is not configured.
Set up a hybrid connection to protect cloud and on-premises objects and attributes.

 **CONFIGURE CONNECTION**

- If one or more console is connected to Identity Recovery for Microsoft Entra ID and the **Show hybrid restore errors if hybrid connection** checkbox 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 Identity Recovery for Microsoft Entra ID](#).

Hybrid connection



There are 2 connections with RMAD consoles.
Ensure only one console is configured to connect to Identity Recovery for Microsoft Entra ID.

Working with Inactive Mailboxes

Identity Recovery for Microsoft Entra ID supports the backup and restore of inactive mailboxes of hard-deleted users.

i NOTE: This feature requires the following consent permissions and roles:

- Consent granted to Exchange Online PowerShell for Backup and the Global Reader role assigned. For more information, see [Exchange Online PowerShell for Backup Consent](#).
- Consent granted to Exchange Online PowerShell for Restore and the Exchange Administrator role assigned. For more information, see [Exchange Online PowerShell for Restore Consent](#).

i NOTE: If you need to restore the inactive mailbox of a hybrid user, see [Restoring Mailboxes for Hybrid Users](#).

To back up and restore inactive mailboxes, you need to back up the mailbox properties associated with the user account.

To back up the linkage between users and inactive mailboxes:

1. On the **Dashboard**, select **Manage Backups**.
2. In the **Manage backups** dialog, select the tenant from the list and select **Edit**.
3. In the **Configure backup** dialog, under **Backup options**, select the checkbox **Back up linkage between users and inactive mailboxes**.
4. Select **Save**.

Restoring Mailboxes for Hybrid Users

To preserve the original cloud mailbox of hybrid users, you need to remove the newly created cloud user from Microsoft Entra ID before the restore.

To do so, in the **Restore objects** dialog, select the checkbox **If a hybrid user account already exists in Microsoft Entra ID, delete it before the restore operation**.

Hybrid user scenario

1. A hybrid user is deactivated by the administrator. The user account goes to the Recycle Bin. After 30 days, Microsoft Entra ID cleans this account from the Recycle Bin.
2. The user returns to the organization and the user account is enabled by the administrator. After the activation, the user is recreated in the cloud with the new mailbox.
3. To use the original cloud mailbox for the user, the user needs to be restored from the backup. Before restoring the user, the newly created cloud user is removed from Microsoft Entra ID.

If you restore a hybrid user and their mailbox with Identity Recovery for Microsoft Entra ID:

- For Non-Federated Domains, Identity Recovery for Microsoft Entra ID 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, Identity Recovery for Microsoft Entra ID restores a hybrid user and its mailbox in the cloud. Recovery Manager for Active Directory restores this hybrid user on-premises, then it calls Microsoft Entra Connect to synchronize the user back to the cloud and make the cloud user previously restored by Identity Recovery for Microsoft Entra ID 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

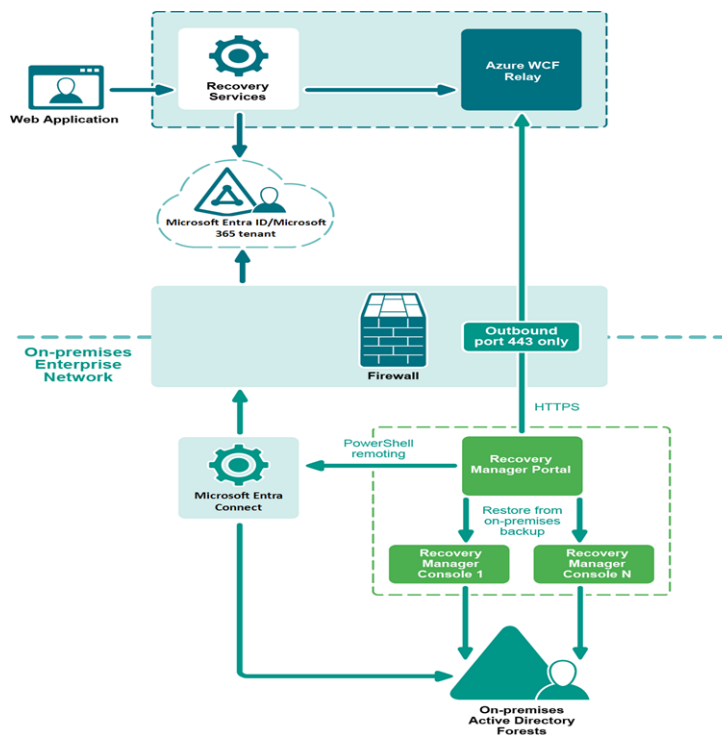
Hybrid configuration with Recovery Manager for Active Directory requires only outbound TCP/UDP port 443 to be opened on the Recovery Manager Portal server to access the internet. If the Recovery Manager Portal server already has access to the internet, you do not need to change the Firewall configuration.

i **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 8: 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 Identity Recovery for Microsoft Entra ID 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>.

Restoring Email Address or Phone for Self-Service Password Reset

Identity Recovery for Microsoft Entra ID 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 global administrator.

Supported scenarios

The following scenarios are supported by Identity Recovery for Microsoft Entra ID:

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

i **NOTE:** Because of Microsoft requirements, hard deleted objects will receive a new Object ID upon restore of these objects. Please consider the implications of having a new Object ID after restoring these objects.

Limitations

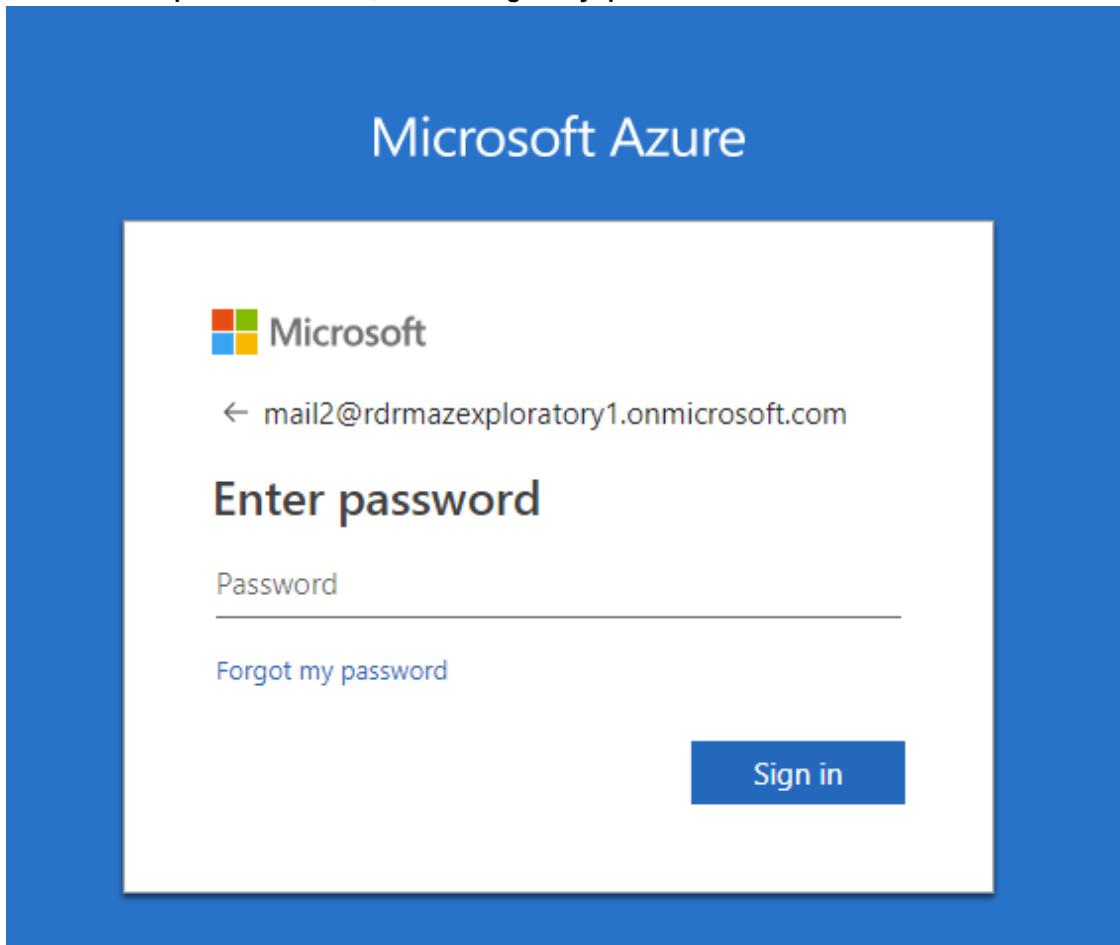
The following scenarios are not supported by Identity Recovery for Microsoft Entra ID:

- 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 Microsoft Entra 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, select **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**.

Microsoft

Get back into your account

Who are you?

To recover your account, begin by entering your user ID and the characters in the picture or audio below.

User ID:

Example: user@contoso.onmicrosoft.com or user@contoso.com



Enter the characters in the picture or the words in the audio.

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

Microsoft

Get back into your account

verification step 1 > choose a new password

Please choose the contact method we should use for verification:

<input checked="" type="radio"/> Email my alternate email	You will receive an email containing a verification code at your alternate email address (mail1@gmail.com).
	<input type="button" value="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.

Microsoft

Get back into your account

verification step 1 ✓ > **choose a new password**

* Enter new password:

Password strength

* Confirm new password:

Finish Cancel

A strong password is required. Strong passwords are 8 to 16 characters and must combine uppercase and lowercase letters, numbers, and symbols. They cannot contain your username.

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 select **Cancel** and verify the email address later.

don't lose access to your account!

To make sure you can reset your password, we need to collect some info so we can verify who you are. We won't use this to spam you - just to keep your account more secure. **You'll need to set up at least 1 of the options below.**

⚠ Authentication Email is set to mail1@gmail.com [Verify](#)

finish cancel

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



Keep your account secure

Sometimes your organization needs more info to make sure it's you. Set up the security info below so you can prove who you are.

∨ Email mail1@gmail.com



Done

How does Identity Recovery for Microsoft Entra ID Handle Object Attributes?

- For more information about known issues and limitations in Identity Recovery for Microsoft Entra ID, see [Known issues](#) in the Release Notes.
- For more details about MSONline module, see <https://learn.microsoft.com/en-us/powershell/module/msonline/?view=azureadps-1.0>.

i | **NOTE:** Identity Recovery for Microsoft Entra ID does not support the restore of objects in restricted management administrative units.

Attributes Restored by Identity Recovery for Microsoft Entra ID

For a full list of attributes restored by Identity Recovery for Microsoft Entra ID, see the [Identity Recovery for Microsoft Entra ID Supported Attributes Guide](#). Each attribute can be restored individually. For information about the steps, see *To restore selected attributes* in [Restoring Objects](#).

What is Not Protected by Microsoft Entra Connect but Can Be Restored by Identity Recovery for Microsoft Entra ID?

Microsoft Entra Connect synchronizes many attributes for users and groups from on-premises Active Directory but there are also cloud objects, properties, and links to Microsoft 365 resources which are not protected by Microsoft Entra Connect and restored only with Identity Recovery for Microsoft Entra ID.

Table 9: Types of cloud-only objects restored by Identity Recovery for Microsoft Entra ID

Object Type	Description	Azure Recycle Bin
Guest users	A Microsoft Entra business-to-business (B2B) collaboration user that typically resides in a partner organization and has limited privileges in the inviting directory.	30 days
Microsoft 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 Microsoft 365 and Microsoft Entra ID resources.	No
Dynamic Security Groups	Groups with dynamic rule-based membership.	No
Dynamic Microsoft 365 Groups	Microsoft 365 Groups with dynamic rule-based membership.	30 days
Devices	Device registration records in Microsoft Entra ID.	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	Microsoft Entra 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 Software creates technology and solutions that build the foundation for enterprise AI. Focused on data management and governance, cybersecurity and platform modernization, Quest helps organizations address their most pressing challenges and make the promise of AI a reality. Around the globe, more than 45,000 companies including over 90% of the Fortune 500 count on Quest Software. For more information, visit www.quest.com or follow Quest Software on [X \(formerly Twitter\)](#) and [LinkedIn](#).

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