Quest®

Quest® Recovery for Azure AD

User Guide

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

Quest Software Inc.

Attn: LEGAL Dept

4 Polaris Way

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.

Recovery for Azure AD User Guide
Updated - April, 2017

Contents

1

About Quest® Recovery for Azure Active Directory

Quest® Recovery for Azure Active Directory cloud application lets you perform the following operations:

- Back up Azure Active Directory and Office 365 users, groups and contacts
- Support for Azure Active Directory B2C tenants.
- Restore Azure Active Directory and Office 365 users and groups with their properties
  Now the application can process two types of Office 365 groups: Office 365 and Security groups.
- View differences between the selected backup and live Azure Active Directory or Office 365 and revert unwanted changes in the Differences report.
- Configure integration with Quest Recovery Manager for Active Directory to restore on-premises Active Directory objects.

The objects can be selected in a backup and then restored to Azure Active Directory or Office 365 without affecting other objects or attributes. Using the granular restore, objects that were accidentally deleted or modified can be recovered in a few minutes.
Recovery for Azure Active Directory can be started from Quest On Demand single SaaS command point. For more information about Quest On Demand, please see Quest On Demand product documentation.

To access Recovery for Azure Active Directory, you need to provide On Demand credentials or use your existing Quest Software account. For more details, please see Signing up for Quest On Demand.

The following sections describe how to configure and work with Recovery for Azure Active Directory:

- Before You Start
- Recovery for Azure Active Directory Console Overview
- Sign up for Quest On Demand
- Required Permissions
- Adding an Azure Active Directory Tenant
- Working with Recovery for Azure Active Directory
- Integration with Recovery Manager for Active Directory

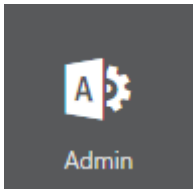
- Reporting
- Advanced Search

Before You Start

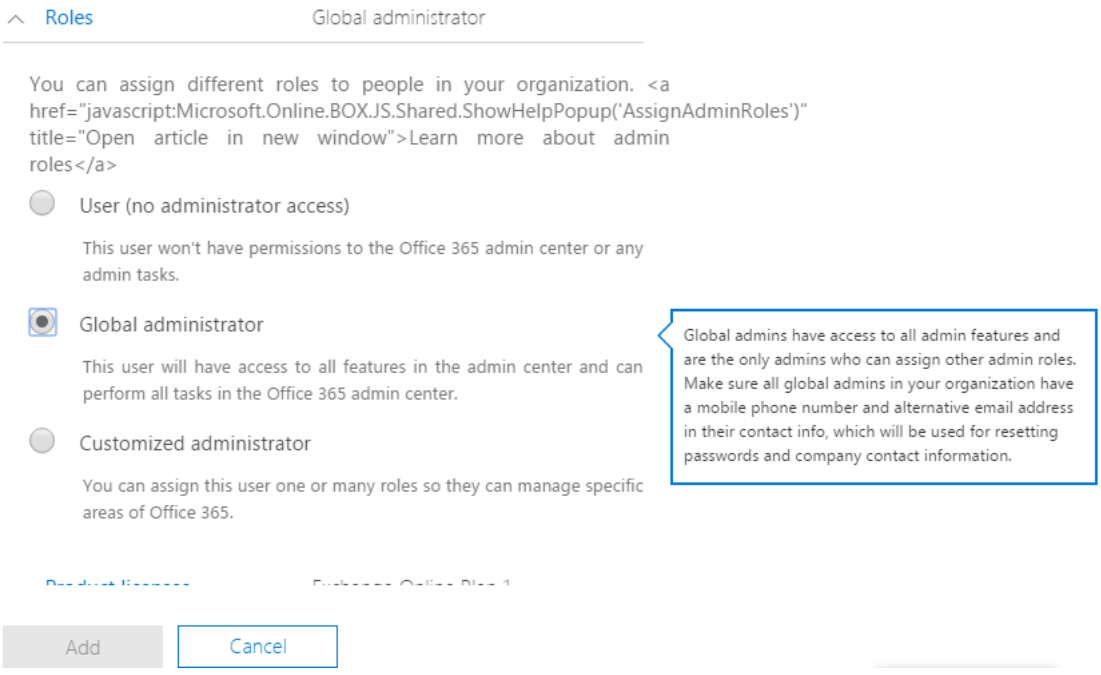
To access your Azure Active Directory or Office 365 tenant via Recovery for Azure Active Directory, use an Administrative account that has the **Global Administrator** role. If you do not have an account with the **Global Administrator** permissions, you should create the account by using one of the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

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

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



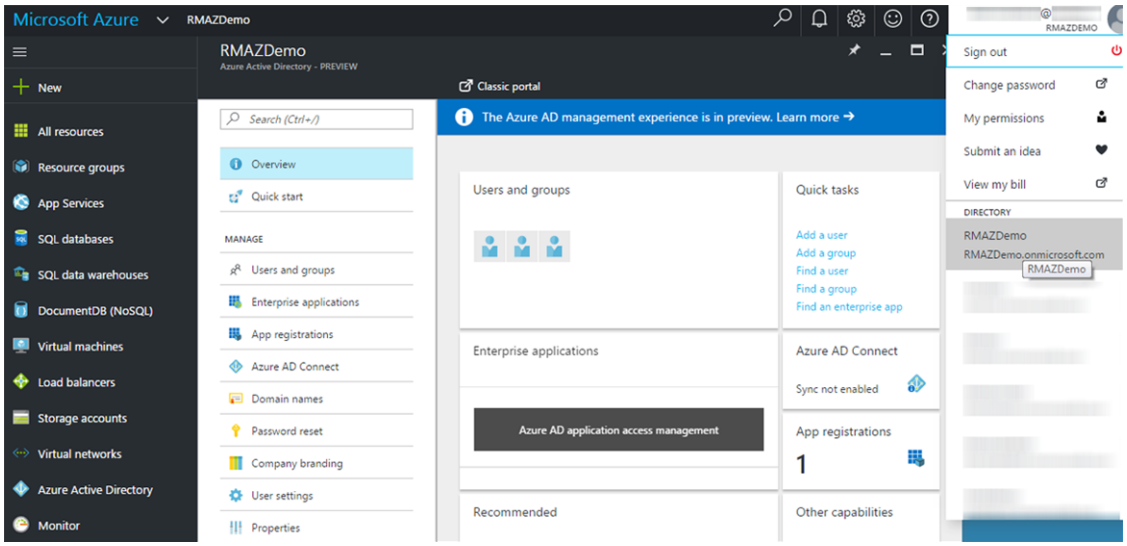
3. From the left pane, select **Users**, and then select **Add a user**.
4. Specify all necessary user information. In the **Roles** section, select the **Global administrator** radio button.



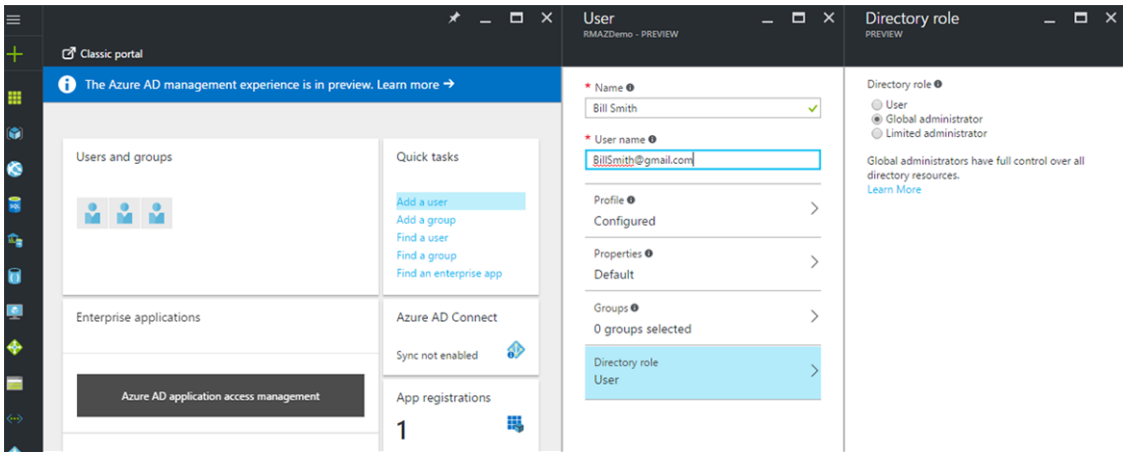
5. Click **Add**.
6. Now you can use this user account to access your Office 365 tenant in Recovery for Azure Active Directory.

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

1. Log into the Azure Management Portal (https://portal.azure.com/) with your individual account.
2. Select your tenant from the list of available tenants. To view the list of tenants, click on your profile icon in the upper-right corner of the screen.



3. Navigate to the **Azure Active Directory** section in the left pane.
4. Click **Add a user** on the **Quick tasks** tile and provide the required details in the "User" form. In the **Directory role** section, select the **Global administrator** radio button and click **OK**.



5. Click **Create**.

Recovery for Azure Active Directory Console Overview

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

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

Sign up for Quest On Demand

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

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

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

Required Permissions

This section lists the minimum user account permissions required to perform specific Recovery for Azure Active Directory tasks.

- To add a tenant and grant admin consent for the Recovery for Azure Active Directory module, the Azure **Global administrator** directory role is required. For more details, see Add an Azure AD tenant.
- After the tenant is added, you can change the permissions to **Limited administrator** directory role with the **User administrator** role enabled. Backup and restore operations will work. The **Global administrator** directory role is not required anymore.
- The **Limited administrator** directory role is used only for restore of users and Office 365 groups from Recycle Bin. Backup, unpack and restore of an attribute can work without **Limited administrator** and the directory role can be changed to **User**.

Adding an Azure Active Directory Tenant

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

NOTE: Creation of backups is disabled by default. After the tenant is added, you must enable the backup creation as described in Step 5 on the Working with Recovery for Azure Active Directory page.

Working with Recovery for Azure Active Directory

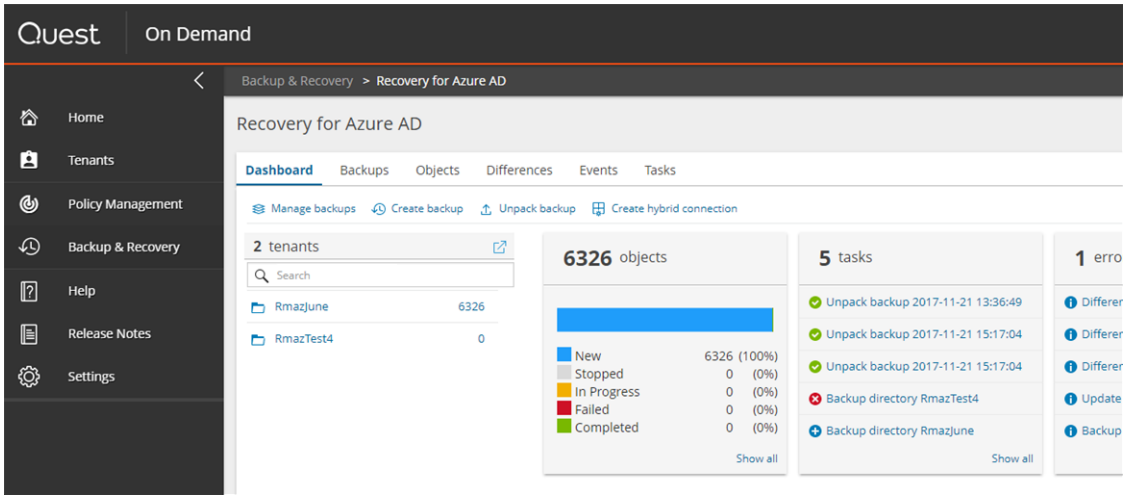
This section provides step-by-step instructions on how to use Recovery for Azure Active Directory.

NOTE: For Office 365 tenants: Recovery for Azure Active Directory can backup and restore Office 365 users, Office 365 groups and Security groups.

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

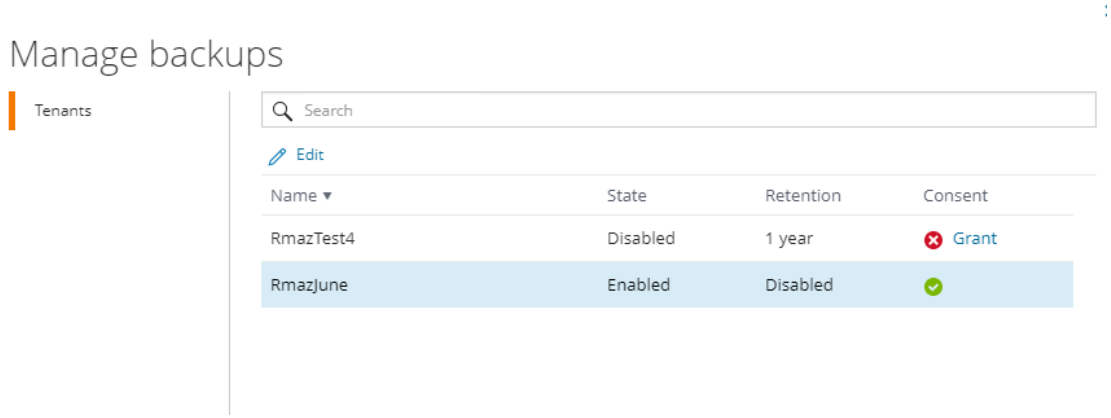
   NOTE: Microsoft admin consent status is "expired" after 90 days - status is changed to "Not Granted". Once expired, you must grant admin consent again to continue using the module.

4. To launch Recovery for Azure Active Directory, click **Backup & Recovery** on the left pane and press **Go** on the Recovery for Azure Active Directory tile. The **Dashboard** screen opens.

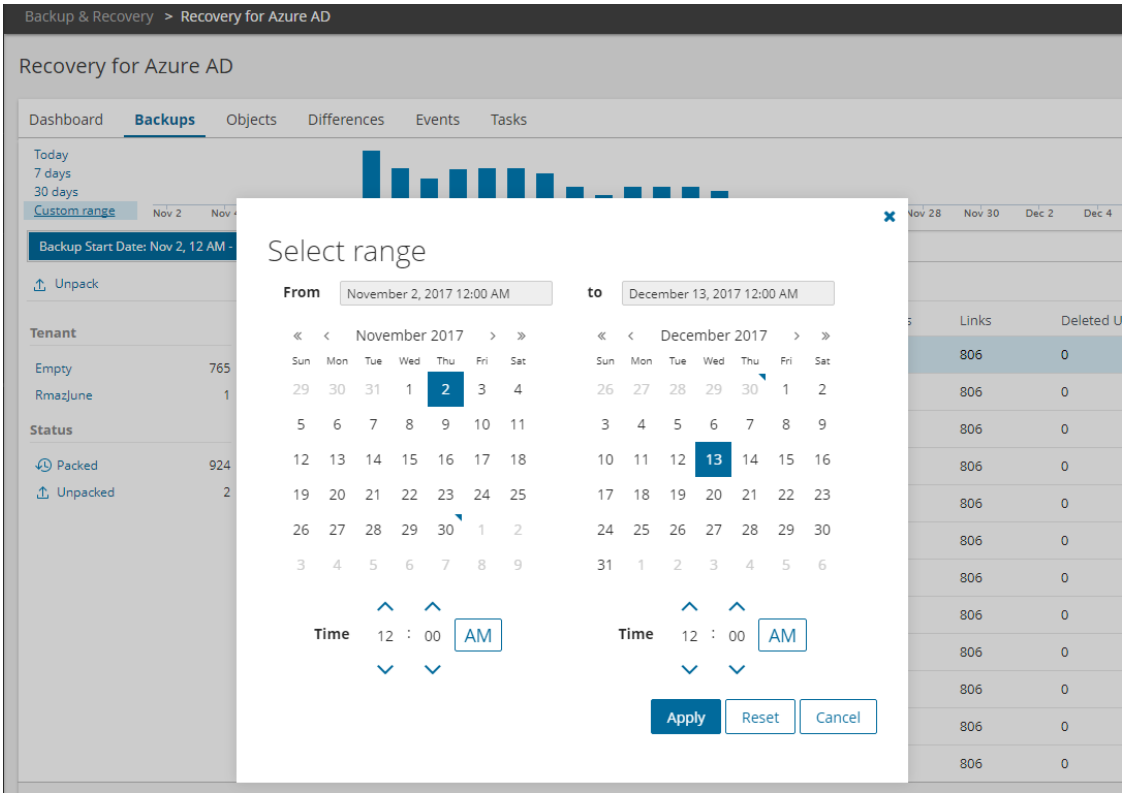


5. To configure a hybrid connection with on-premises Active Directory, see here.

6. To enable the automatic creation of backups for a tenant and set the backup retention policy, perform the following:
    a. Press **Manage backups** on the **Dashboard** screen.
    b. Select the tenant from the list and press **Edit**.
        - To enable the backup creation, in the **Configure backup** dialog, select **Enabled** next to the **Automatic backup every hour** option.
        - Specify the backup retention period using the **Backup retention policy** option. The backup retention policy is also applied to backups that are started manually.
        - Check the status of the module admin consent.
    c. Click **Save**.
    d. If you need to run the backup creation manually, go to the **Tasks** screen, select the Backup task and press **Start**.

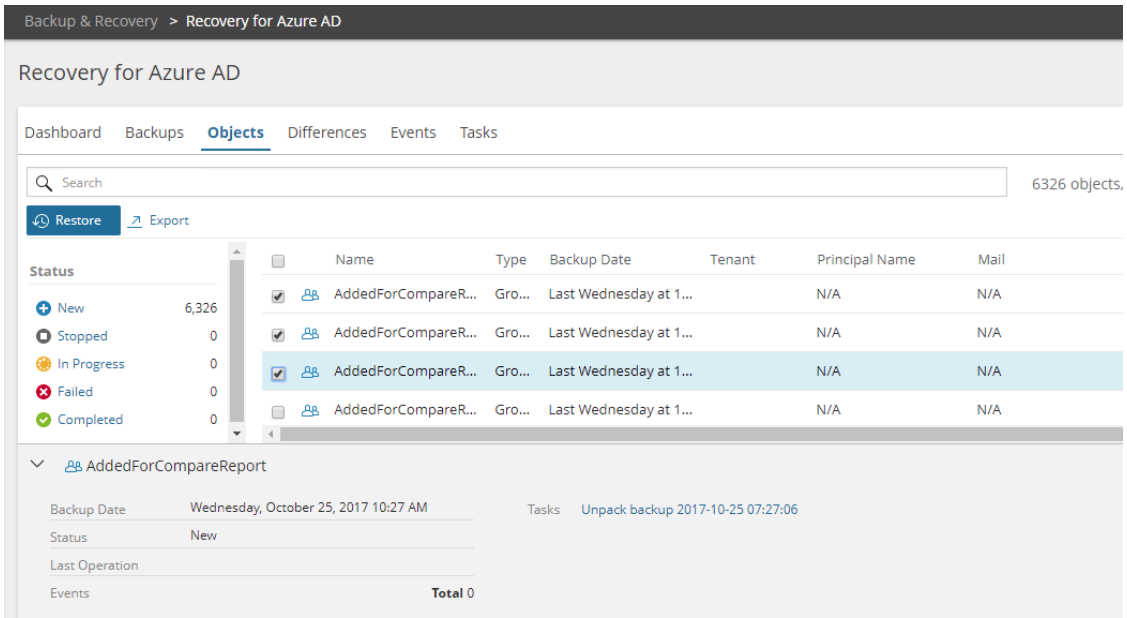


7. To start the backup creation manually, you can use the **Create backup** option on the **Dashboard** screen.
8. To unpack a backup:
    a. Go to the **Backups** view.
    b. Select the tenant from the left side of the screen, then select the backup you want. You can specify predefined or custom date range to narrow the search results.
    c. Press **Unpack** in the actions menu.
    d. In the **Backup Unpacking** dialog, click **Unpack**.



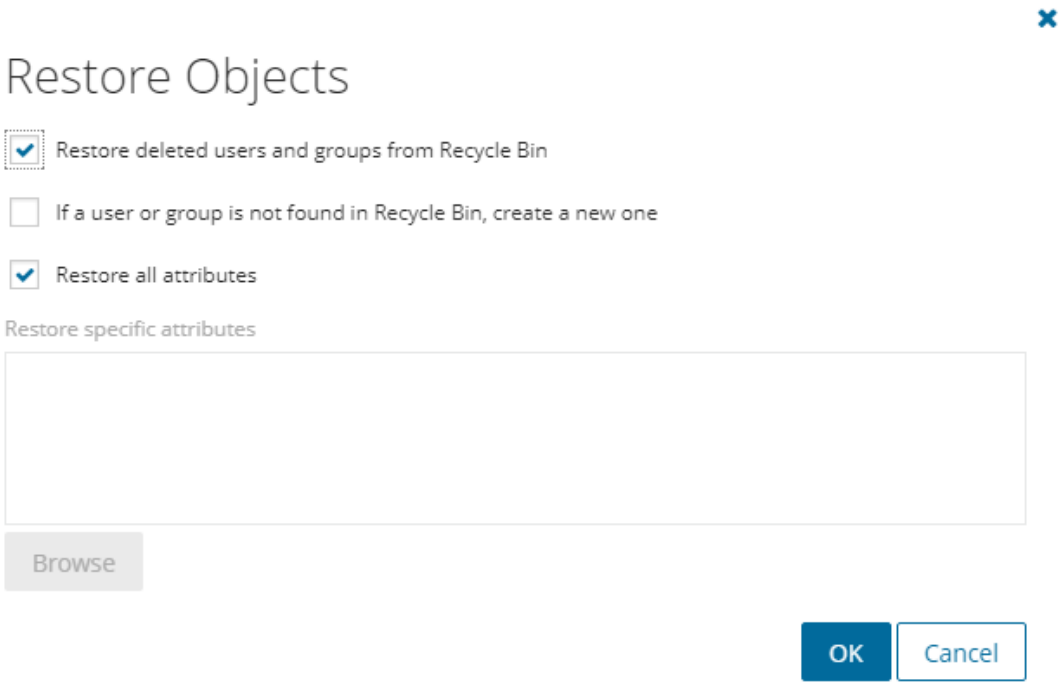
9. When the **Unpack backup** task is completed, go to the **Objects** view and select users and groups that you want to restore and click **Restore**.

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



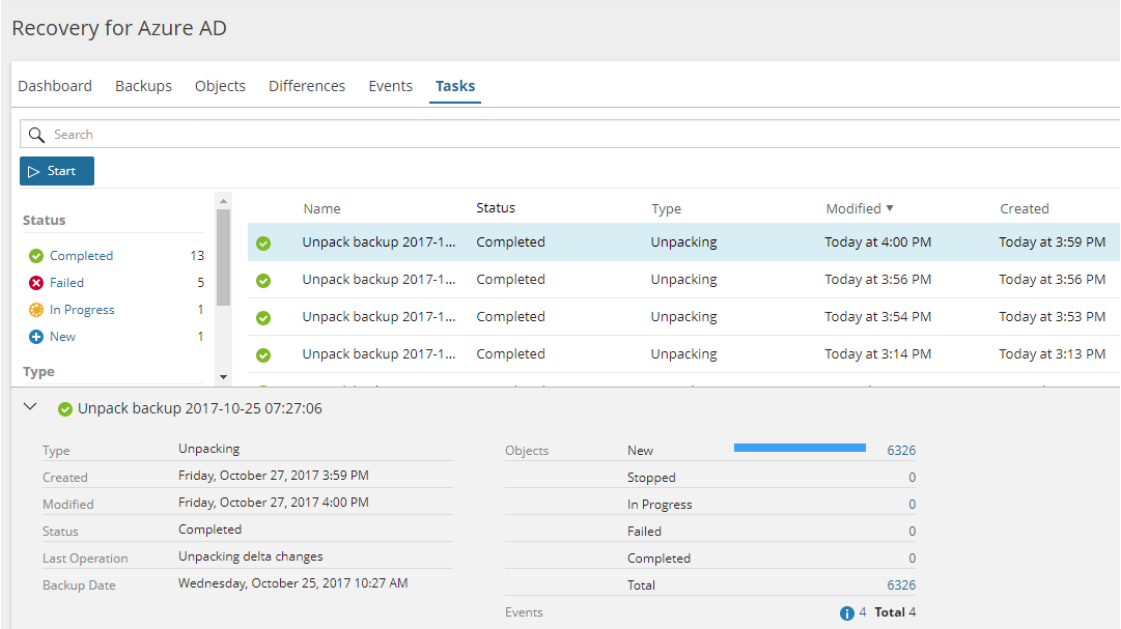
10. In the **Restore Objects** dialog, you can select the following options:

    - **Restore deleted users and groups from Recycle Bin** - Restores accidentally deleted users and Office 365 groups from Recycle Bin. Recovery for Azure Active Directory preserves original object identifiers (GUID).
    - **If a user or group is not found in Recycle Bin, create a new one** - Recreates permanently deleted users, groups and subgroups. This option recreates users and groups with attributes that are required for object identification. If you need to restore all attributes for the object including membership information (links), use this option together with the **Restore all attributes** option.
    - **Restore all attributes** - Restores all object attributes including membership information (links). If this option is not selected, you can specify specific attributes that you want to restore. For that, click **Browse** and specify the attributes you need.



11. Also, you can view differences between the selected backup and live Azure Active Directory or Office 365 and revert the selected changes using the Differences report tool. For more details, please see the Reporting section. You can export the selected report data to the CSV file.

12. You can view the status of your **Restore objects** task on the **Tasks** screen.



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

Integration with Recovery Manager for Active Directory

Recovery for Azure Active Directory can be integrated with Recovery Manager for Active Directory 9.0 or higher to restore and undelete on-premises objects that are synchronized with cloud by Azure AD Connect.

Prerequisites

- Azure AD tenant that is synchronized with on-premises Active Directory by Azure AD Connect
- Recovery Manager Portal 9.0
  The portal can be run in any machine in your environment. It is not required to install all Recovery Manager for Active Directory components. To get the latest version of Recovery Manager Portal, please go to https://www.quest.com/products/recovery-manager-for-active-directory-forest-edition/.

How to configure Recovery Manager Portal to enable integration with cloud

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** and click **On Demand integration…**
4. In the On Demand integration dialog, select **Enable integration** check box and specify Relay URL and credentials. To get these parameters, please go to Recovery for Azure Active Directory and perform the following steps:
   a. On the **Dashboard** screen, click **Create hybrid connection**.
   b. In the Create hybrid connection dialog, click **Download hybrid credentials** to download a configuration file with Relay credentials.
   c. Save the file to the folder of your choice.
   d. 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 Recovery Manager Portal.

> **NOTE:** Azure AD Connect synchronization occurs automatically after the restore operation. But Recovery for Azure Active Directory has the ability to force synchronization cycle and requires credentials for the machine where Azure AD Connect is installed.

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

What can be restored in hybrid configuration

- On-premises object attributes that were synchronized with the cloud
- On-premises groups
- Office 365 licenses (assignedLicenses property for cloud users) and cloud group membership
- Deleted on-premises users and groups

Important Considerations

- To restore on-premises objects, Recovery for Azure Active Directory uses attribute values from the RMAD backup that is closest in time but older than the cloud backup unpacked in the RMAZ 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 Recovery Manager Portal – in this case, the on-premises backup will be unpacked automatically during the restore operation.
- Recovery for Azure Active Directory shows only on-premises attributes synchronized with the cloud and cloud-only attributes for the selected object when you click **Browse** in the Restore Objects dialog. On-premises only attributes are not included in this list. To restore on-premises only attributes, you must select the **Restore all attributes** option in the Restore Objects dialog.
- After the hybrid restore operation, Recovery for Azure Active Directory forces Azure AD Connect synchronization to push on-premises changes to the cloud and wait until it completes the synchronization. Restore events can be used to track steps of Azure AD Connect synchronization, such as export and import.
- Restore of group membership from the Difference report is not supported for hybrid environments. Please use the **Objects** view, to restore 'member' or 'memberOf' attribute of an object.
- Hybrid restore from the Differences report uses attribute values from the on-premises backup. These values may be different from the corresponding values shown in the Differences report.
- Recovery for Azure Active Directory supports one hybrid connection per the On Demand organization. If you need to manage multiple hybrid tenants, create a separate On Demand organization for each Hybrid Azure AD tenant.
- One instance of Recovery Manager Portal can be used with one Azure AD tenant and one Azure AD Connect server. Install multiple RMAD web portals if you need to work with multiple Azure AD tenants and Azure AD connect servers.
- Recovery for Azure Active Directory restores Back Link attributes: 'memberOf' (the back link for the 'member' attribute) and 'directReports' (the back link for the 'manager' attribute). These attributes can be selected along with all other attributes when you click **Browse** in the Restore Objects dialog.
- Separate Microsoft Azure Relay service is used for each hybrid connection (one per On Demand organization). Recovery for Azure Active Directory creates WCF Relay per On Demand organization. No changes to On-Premises Firewall settings are required.
- Delegation settings specified in Recovery Manager Portal are not applied in the hybrid configuration, so Recovery for Azure AD users can restore objects from all on-premises domains and forests that are synchronized with the Azure AD tenant. Also, in Recovery Manager Portal, you need to add domain controllers for every domains that will be restored and specify account under which the restore operation will be performed. For more details, see the *Administering Recovery Manager Portal* section of *Recovery Manager for Active Directory User Guide*.

To perform a restore operation in Recovery for Azure Active Directory

1. Unpack a backup.
2. Go to the **Objects** screen and select on-premises objects to restore.
3. Click **Restore**.
4. In the Restore Objects dialog, if you select the **Restore all attributes** option, Recovery for Azure Active

Directory 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.

Reporting

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

The report shows the following changes:

- Creation of new users or groups
- Changes to Azure AD B2C "local accounts", "guest accounts", "social accounts"
- Changes to object attributes, including Office 365 licenses
- Group membership and manager property changes (**DirectoryLinkChange** object type)
- Objects moved to Recycle Bin
- Permanently deleted objects

NOTE: Restore of group membership from the Difference report is not supported for hybrid environments. Please use the **Objects** view, to restore 'member' or 'memberOf' attribute of an object.

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

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

1. Create a backup of your directory.
2. Change any object attributes in your live Azure Active Directory or Office 365.
3. Unpack the backup to compare with the current version of your directory. For that, click **Unpack backup** on the **Dashboard** view. In the Backup Unpacking dialog, click **Browse** and select the backup.
4. After the backup is unpacked, go to the **Differences** view.
5. To refine the data, use the **Search** field or facets on the left side of the screen.
   For more information about the search syntax, see Advanced Search.
6. Select the changes you want to roll back and click **Restore**.
7. To update the report data, use the **Refresh** option.
8. The **Export** feature allows you to export the selected report data to the CSV format. Note that the CSV file contains internal column names, for example: the **Attribute** column in the **Difference** greed has the "changedAttribute" internal name. You can use internal column names to create search queries. For more information, refer to Advanced Search.

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 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.

To search for	Operator	Example	Result
Specify part of a word NOTE: Asterisk matches zero or more non-space characters.	*	serv*	Include terms beginning with "serv".
Exclude specified content	-	-mail*	Excludes content with values that match the exclusion.
	NOT (case-sensitive)	NOT mail*	
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'.
	OR (case-sensitive)	mail OR user	
	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".

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 the list of internal column names and string examples, see below:

Objects screen

Column Display Name	Column Internal Name	To search for	Query Example
Name	displayName	An object by object name	displayName:JackJones
Type	objectType	An object by object type	objectType:user
Backup Date	backupDate	An object by the specified backup data/time	backupDate:[2017-06-27]
Directory	tenant	An object by directory name	tenant:demo365
Principal Name	userPrincipalName	An object by principal name	userPrincipalName:
Mail	mail	An object by mail address	mail:Jack.Jones@contoso.com
City	city	An object by city	city:London
Department	department	An object by department	department:Sales
Job Title	jobTitle	An object by job title	jobTitle:manger

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*

Differences screen

Column Display Name	Internal Column Name	To search for	Query Example
Name	objectName	Changes related to a specified object name	objectName:NormanThomas*
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:JackJones@contoso.com
	newValue	Search by new attribute value (value after the change)	newValue:JackJones@gmail.com
Backup time	backupDate	Search by the specified backup data/time	backupDate:[2017-06-27]

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"

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*

How does Recovery for Azure Active Directory handle object attributes?

- Recovery for Azure Active Directory restores all attributes based on data provided by Azure AD Graph API including schema extension attributes with some exceptions listed in the *Skipped attributes* section below.
- Recovery for Azure Active Directory restores custom properties. For more details, see https://azure.microsoft.com/en-us/resources/samples/active-directory-dotnet-graphapi-directoryextensions-web/.
- For more information about known issues and limitations, refer http://support.quest.com/technical-documents/on-demand-recovery-for-azure-active-directory/release-notes/about-quest-recovery-for-azure-active-directory/known-issues.

Attributes restored by Recovery for Azure AD

For more information, see https://msdn.microsoft.com/en-us/library/azure/ad/graph/api/entity-and-complex-type-reference. This list of attributes is actual for December 2017 and may be different from the customer's attribute list depending on the scenario of using Azure Active Directory.

User attributes

Attribute Name	Description
accountEnabled	*True* if the account is enabled; otherwise, *False*.
assignedLicenses	The licenses that are assigned to the user.
city	The city in which the user is located.
country	The country/region in which the user is located.
department	The name for the department in which the user works.
displayName	The name displayed in the address book for the user.
employeeId	The employee identifier assigned to the user by the organization.
memberOf	The groups that the user is a member of.
manager	The user or contact that is this user's manager.
directReports	This attribute contains the list of users that directly report to the user.
facsimileTelephoneNumber	The primary facsimile telephone number for the user.
givenName	The given name (first name) of the user.
isCompromised	Indicates whether this user is compromised.
jobTitle	The user's job title.
mailNickname	The mail alias for the user.
mobile	The primary cellular telephone number for the user.
objectType	Identifies the object type.

otherMails	Specifies other email addresses for the user.
passwordPolicies	Specifies password policies for the user.
physicalDeliveryOfficeName	This attribute is for storing a description for the office, for example the office building/number.
postalCode	The postal code for the user's postal address.
preferredLanguage	The preferred language for the user.
showInAddressList	*True* if the Outlook global address list should contain this user, otherwise, *False*. If not set, this will be treated as *True*.
signInNames	The list of sign in names for the user.
state	The state or province in the user's address.
streetAddress	The street address of the user's place of business.
surname	The user's surname (family name or last name).
telephoneNumber	Specifies the user's telephone number.
usageLocation	A two letter country code (ISO standard 3166).
userPrincipalName	The user principal name (UPN) of the user.
userType	A string value that can be used to classify user types in your directory, such as “Member” and “Guest”.

Group attributes

Attribute Name	Description
description	An optional description for the group.
displayName	The display name for the group.
members	Members of this group.
memberOf	The groups that the group is a member of.
mailEnabled	Specifies whether the group is mail-enabled.
securityEnabled	Specifies whether the group is a security group.
mailNickname	The mail alias for the group.
objectType	Identifies the object type.

Restoring passwords

Recovery for Azure Active Directory does not back up passwords. During the restore of permanently deleted users, the application sets a random password that can be changed by the administrator at the next login.

Skipped attributes

These attributes are backed up but are not restored by Recovery for Azure Active Directory.

Attribute Name	Description
immutableId	This property is used to associate an on-premises Active Directory user account to their Azure AD user object.
mail	The SMTP address for the user.
assignedPlans	The plans that are assigned to the user.
companyName	The company name which the user is associated.

deletionTimestamp	The time at which the directory object was deleted.
dirSyncEnabled	*True* if this object is synced from an on-premises directory; *False* if this object was originally synced from an on-premises directory but is no longer synced.
lastDirSyncTime	Indicates the last time at which the object was synced with the on-premises directory.
objectId	The unique identifier for the object.
onPremisesSecurityIdentifier	Contains the on-premises security identifier (SID) for the user that was synchronized from on-premises to the cloud.
onPremisesDomainName	Contains the on-premises domainFQDN, also called dnsDomainName synchronized from the on-premises directory.
onPremisesNetBiosName	Contains the on-premises NetBiosName synchronized from the on-premises directory.
onPremisesSamAccountName	Contains the on-premises sAMAccountName synchronized from the on-premises directory.
onPremisesDistinguishedName	Contains the on-premises DistinguishedName synchronized from the on-premises directory.
passwordProfile	Specifies the password for the user.
provisionedPlans	The plans that are provisioned for the user.
provisioningErrors	A collection of error details that are preventing this group from being provisioned successfully.
proxyAddresses	Contains various known address entries.
refreshTokensValidFromDateTime	Any refresh tokens or sessions tokens (session cookies) issued before this time are invalid.
sipProxyAddress	Specifies the voice over IP (VOIP) session initiation protocol (SIP) address for the object.
thumbnailPhoto	A thumbnail photo to be displayed for the user.
legalAgeGroupClassification	Age group classification based on user's interest.

About us

We are more than just a name

We are on a quest to make your information technology work harder for you. That is why we build community-driven software solutions that help you spend less time on IT administration and more time on business innovation. We help you modernize your data center, get you to the cloud quicker and provide the expertise, security and accessibility you need to grow your data-driven business. Combined with Quest's invitation to the global community to be a part of its innovation, and our firm commitment to ensuring customer satisfaction, we continue to deliver solutions that have a real impact on our customers today and leave a legacy we are proud of. We are challenging the status quo by transforming into a new software company. And as your partner, we work tirelessly to make sure your information technology is designed for you and by you. This is our mission, and we are in this together. Welcome to a new Quest. You are invited to Join the Innovation™.

Our brand, our vision. Together.

Our logo reflects our story: innovation, community and support. An important part of this story begins with the letter Q. It is a perfect circle, representing our commitment to technological precision and strength. The space in the Q itself symbolizes our need to add the missing piece – you – to the community, to the new Quest.

Contacting Quest

For sales or other inquiries, visit www.quest.com/contact.

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