Quest® On Demand Recovery

Supported Attributes

Version: 1.6
Deployment Date: January 30, 2024

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

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.**

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

On Demand Recovery User Guide
Updated - February 16, 2024

Contents

3

About Supported Attributes

On Demand Recovery allows the restoration of Azure Active Directory and Office 365 users, groups, applications, service principals, devices, Conditional Access policies and Application Proxy settings. The application can process two types of Office 365 groups: Office 365 groups and security groups. Group membership and ownership is restored for both types of groups.

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.

The following guide provides attributes for each object type that can be restored by On Demand Recovery, as of version 1.6, deployed on January 30, 2024. These object types include:

- Azure Users
- Azure Groups
- Service Principals (Enterprise Applications)
- Devices
- Applications (Application Registrations)
- Conditional Access Policy
- Application Proxy
- Country Named Location
- IP Named Location

For more information on restoring objects, visit the On Demand Recovery documentation.

4

Azure Users

Users are the representation of an Azure Active Directory (Azure AD) work or school user account.
The lists below include all supported Azure user attributes that can be restored by On Demand Recovery.

General

Attribute Name	Description
accountEnabled	*True* if the account is enabled; otherwise, *False*.
ageGroup	The age group of the user.
appRoleAssignments	Represents the app roles a user has been granted for an application.
assignedLicenses	The licenses that are assigned to the user, including inherited (group-based) licenses. This property doesn't differentiate directly-assigned and inherited licenses. **NOTE:** see Assigned Licenses and Plans list below for detailed information on complex attribute.
businessPhones	The telephone numbers for the user.
city	The city in which the user is located.
companyName	The company name which the user is associated. This property can be useful for describing the company that an external user comes from.
consentProvidedForMinor	Sets whether consent has been obtained for minors.
country	The country/region in which the user is located.
department	The name of the department in which the user works.
directReports	The users and contacts that report to the user. (The users and contacts that have their manager property set to this user.)
displayName	The name displayed in the address book for the user. This value is usually the combination of the user's first name, middle initial, and last name.
employeeId	The employee identifier assigned to the user by the organization.
faxNumber	The fax number of the user.

Attribute Name	Description
givenName	The given name (first name) of the user.
identities (B2C only)	Represents the identities that can be used to sign in to this user account.
jobTitle	The user’s job title.
mail	The SMTP address for the user.
mailNickname	The mail alias for the user.
manager	The user or contact that is this user's manager.
memberOf	The groups, directory roles and administrative units that the user is a member of.
mfaState	Identifies multifactor authentication state for the user. **NOTE:** see Multifactor Authentication list below for detailed information on this complex attribute.
mobilePhone	The primary cellular telephone number for the user.
officeLocation	The office location in the user's place of business.
otherMails	A list of additional email addresses for the user.
ownedDevices	Devices that are owned by the user.
ownedObjects	Get the list of directory objects that are owned by the user.
passwordPolicies	Specifies password policies for the user.
postalCode	The postal code for the user's postal address. The postal code is specific to the user's country/region.
registeredDevices	Devices that are registered for the user.
roles	Specifies administrator roles assigned to a 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).
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”.

Assigned Licenses and Plans

In Azure AD licenses and plans are assigned to users to give them access. Licenses and plans can be assigned and unassigned.

When the complex attribute 'assignedLicenses' is selected for restore, the following attributes will also be restored. Individual attributes cannot be selected and are all restored together.

Attribute Name	Description
assignedDateTime (Assigned Plans)	The date and time at which the plan was assigned.
capabilityStatus (Assigned Plans)	Condition of the capability assignment.
disabledPlans	A collection of the unique identifiers for plans that have been disabled.
licenseAssignmentStates	State of license assignments for this user.
service (Assigned Plans)	The name of the service to activate.
servicePlanId (Assigned Plans)	The plan identifier of the service plan to activate.
skuId	The unique identifier for the SKU.
state	Indicate the current state of this assignment.

Multifactor Authentication

To secure user sign-in events in Azure AD, multifactor authentication can be enabled on user accounts.

When the complex attribute 'MFAState' is selected for restore, the following attributes will also be restored. Individual attributes cannot be selected and are all restored together.

Attribute Name
Default MFA method
Email authentication methods
Phone authentication methods
SMS sign-on status
User state of MFA settings

Hybrid User

Attribute Name	Description
onPremisesDistinguishedName	Contains the on-premises Active Directory distinguished name or DN.
onPremisesDomainName	Contains the on-premises domainFQDN, also called dnsDomainName synchronized from the on-premises directory.
onPremisesExtensionAttributes	Contains extensionAttributes 1-15 for the user.
onPremisesImmutableId	This property is used to associate an on-premises Active Directory user account to their Azure AD user object.

Attribute Name	Description
onPremisesSamAccountName	Contains the on-premises samAccountName synchronized from the on-premises directory.
onPremisesSecurityIdentifier	Contains the on-premises security identifier (SID) for the user that was synchronized from on-premises to the cloud.

5

Azure Groups

The lists below include all supported Azure group attributes that can be restored by On Demand Recovery.

General

Attribute Name	Description
appRoleAssignments	Represents the app roles a group has been granted for an application.
assignedLicenses	The licenses that are assigned to the group. **NOTE:** see Assigned Licenses and Plans list below for detailed information on complex attribute.
description	An optional description for the group.
displayName	The display name for the group.
groupTypes	Specifies the group type and its membership. If the collection contains Unified, the group is a Microsoft 365 group; otherwise, it's either a security group or distribution group. **NOTE:** distribution groups are not supported by On Demand Recovery.
isAssignableToRole	Indicates whether this group can be assigned to an Azure Active Directory role.
mail	The SMTP address for the group.
mailEnabled	Specifies whether the group is mail-enabled.
mailNickname	The mail alias for the group.
memberOf	Groups and administrative units that this group is a member of.
members (Enterprise Applications/Service Prinicpals)	
members (Groups and Directory Roles)	
members (Users)	
membershipRule	The rule that determines members for this group if the group is a dynamic group.
membershipRuleProcessingState	Indicates whether the dynamic membership processing is on or

Attribute Name	Description
	paused.
owners	The owners of the group.
preferredDataLocation	The preferred data location for the Microsoft 365 group. By default, the group inherits the group creator's preferred data location.
roles	
securityEnabled	Specifies whether the group is a security group.
theme	Specifies a Microsoft 365 group's color theme.
visibility	Specifies the group join policy and group content visibility for groups. Possible values are: Private, Public, or HiddenMembership.

Assigned Licenses and Plans

Groups can be used in Azure AD to assign licenses and plans to large numbers of users or to assign user access to deployed enterprise applications. When a user becomes a member of a group they are automatically assigned the appropriate licenses.

When the complex attribute "AssignedLicenses" is selected to be restored, the following attributes will also be restored. Individual attributes cannot be selected and are all restored together.

Attribute Name	Description
disabledPlans	A collection of the unique identifiers for plans that have been disabled.
skuId	The unique identifier for the SKU.

Hybrid Group

Attribute Name
onPremisesDomainName
onPremisesImmutableId
onPremisesSamAccountName
onPremisesSecurityIdentifier

6

Devices

The list below includes all supported device attributes that can be restored by On Demand Recovery.

General

Attribute Name	Description
accountEnabled	*True* if the account is enabled; otherwise, *False*.
alternativeSecurityIds	
approximateLastSignInDateTime	The approximate date and time of the previous sign in of the device.
complianceExpirationDateTime	The timestamp when the device is no longer deemed compliant.
deviceId	Unique Identifier set by Azure Device Registration Service at the time of registration. This is an alternate key that can be used to reference the device object.
deviceMetadata	Metadata information of the device.
deviceVersion	Version of the device.
displayName	The display name for the device.
isManaged	*True* if the device is managed by a Mobile Device Management (MDM) app; otherwise, *false*.
operatingSystem	The type of operating system on the device.
operatingSystemVersion	The version of the operating system on the device.
physicalIds	Physical IDs for the device.
registeredOwners	The user that cloud joined the device or registered their personal device.
registeredUsers	Collection of registered users of the device. For cloud joined devices and registered personal devices, registered users are set to the same value as registered owners at the time of registration.
systemLabels	List of labels applied to the device by the system.

7

Service Principals (Enterprise Applications)

The lists below include all supported Enterprise application attributes that can be restored by On Demand Recovery.

General

Attribute Name	Description
accountEnabled	*True* if the service principal account is enabled; otherwise, *False*.
alternativeNames	Used to retrieve service principals by subscription, identify resource group and full resource ids for managed identities.
appId	The unique identifier for the associated application (its appId property).
applicationProxy	
applicationTemplateId (Gallery App only)	Unique identifier of the applicationTemplate that the servicePrincipal was created from.
appRoleAssignedTo	App role assignments for this app or service, granted to users, groups, and other service principals.
appRoleAssignmentRequired	Specifies whether users or other service principals need to be granted an app role assignment for this service principal before users can sign in or apps can get tokens.
appRoleAssignments	App role assignment for another app or service, granted to this service principal.
appRoles	The roles exposed by the application which this service principal represents.
displayName	The display name of the service principal.
homepage	Home page or landing page of the application.
loginUrl	Specifies the URL where the service provider redirects the user to Azure AD to authenticate.
logoutUrl	Specifies the URL that will be used by Microsoft's authorization service to logout an user using OpenId Connect front-channel, back-channel or SAML logout protocols.
memberOf	Roles that this service principal is a member of.

Attribute Name	Description
notificationEmailAddresses	Specifies the list of email addresses where Azure AD sends a notification when the active certificate is near the expiration date.
oauth2PermissionGrants	Delegated permission grants authorizing this service principal to access an API on behalf of a signed-in user.
owners	Directory objects that are owners of this servicePrincipal. The owners are a set of non-admin users or servicePrincipals who are allowed to modify this object.
preferredSingleSignOnMode	Specifies the single sign-on mode configured for this application.
roles	
samlSingleSignOnSettings	The collection for settings related to saml single sign-on. **NOTE:** see SAML Single Sign-On (SSO) (Service Principals) attributes list below for detailed information on complex attribute.
servicePrincipalNames	Contains the list of identifiersUris, copied over from the associated application.
servicePrincipalType	Identifies if the service principal represents an application or a managed identity. This is set by Azure AD internally. For a service principal that represents an application this is set as Application. For a service principal that represent a managed identity this is set as ManagedIdentity.
signinAudience	Specifies the Microsoft accounts that are supported for the current application.
ssoSettings	
tags	Custom strings that can be used to categorize and identify the service principal.
userAttributesAndClaims	The attribute value shows how many attributes/claims were changed. This attribute can be restored if the User Attributes & Claims section was changed or a service principal was permanently deleted.

SAML Single Sign-On (SSO)

SAML Single Sign-On is a mechanism that leverages SAML allowing users to log on to multiple applications after logging into the identity provider. As the user must log in once, SAML SSO provides a faster, seamless user experience.

Attribute Name
relayState

App Role Assignments

Azure App Role assignments are used to assign application permissions to users. After a customer signs up to an application an admin for the Azure AD directory assigns users to the roles, thus giving the user permission to the application. When a user signs in, the user's assigned roles are sent as claims.

Attribute Name	Description
appRoleAssignmentRequired	Specifies whether users or other service principals need to be granted an app role assignment for this service principal before users can sign in or apps can get tokens.
displayName (App Role)	Display name for the permission that appears in the app role assignment and consent experiences.
memberOf (Directory Role)	The directory roles that the user is a member of.
memberOf (Groups)	The groups that the user is a member of.

Applications (Application Registrations)

The lists below include all supported application registration attributes that can be restored by On Demand Recovery.

General

Attribute Name	Description
api	Specifies settings for an application that implements a web API. ℹ **NOTE:** see API attributes list below for detailed information on complex attribute.
applicationTemplateId	Unique identifier of the applicationTemplate.
appRoles	The collection of roles defined for the application.
defaultRedirectUri	The default redirect URI.
displayName	The display name of the application.
groupMembershipClaims	Configures the groups claim issued in a user or OAuth 2.0 access token that the application expects.
identifierUris	The URIs that identify the application within its Azure AD tenant, or within a verified custom domain if the application is multi-tenant.
info	Basic profile information of the application, such as it's marketing, support, terms of service, and privacy statement URLs. ℹ **NOTE:** see Info attributes list below for detailed information on complex attribute.
isFallbackPublicClient	Specifies the fallback application type as public client, such as an installed application running on a mobile device.
optionalClaims	Application developers can configure optional claims in their Azure AD applications to specify the claims that are sent to their application by the Microsoft security token service. ℹ **NOTE:** see Optional Claims attributes list below for detailed information on complex attribute.

Attribute Name	Description
owners	Directory objects that are owners of the application
publisherDomain	The verified publisher domain for the application.
requiredResourceAccess	Specifies the resources that the application needs to access. This property also specifies the set of delegated permissions and application roles that it needs for each of those resources. This configuration of access to the required resources drives the consent experience. **NOTE:** see Required Resource Access attributes list below for detailed information on complex attribute.
samlMetadataUrl	The URL where the service exposes SAML metadata for federation.
signInAudience	Specifies the Microsoft accounts that are supported for the current application.
spa	Specifies settings for a single-page application, including sign out URLs and redirect URIs for authorization codes and access tokens. **NOTE:** see Spa attributes list below for detailed information on complex attribute.
tags	Custom strings that can be used to categorize and identify the application.
web	Specifies settings for a web application. **NOTE:** see Web attributes list below for detailed information on complex attribute.

API

Attribute Name	Description
acceptMappedClaims	When *true*, allows an application to use claims mapping without specifying a custom signing key.
knownClientApplications	Used for bundling consent if you have a solution that contains two parts: a client app and a custom web API app.
oauth2PermissionScopes	The definition of the delegated permissions exposed by the web API represented by this application registration.
preAuthorizedApplications	Lists the client applications that are pre-authorized with the specified delegated permissions to access this application's APIs.
requestAccessTokenVersion	Specifies the access token version expected by this resource. This changes the version and format of the JWT produced independent of the endpoint or client used to request the access token.

App Roles

Azure Application Roles are used to assign application permissions to users. Application roles are defined by adding them to the application manifest. After a customer signs up to an application an admin for the Azure AD directory assigns users to the roles, thus giving the user permission to the application. When a user signs in, the user's assigned roles are sent as claims.

Attribute Name	Description
allowedMemberTypes	Specifies whether this app role can be assigned to users and groups, to other applications, or both.
appRoles	The collection of roles the application declares.
description	The description for the app role.
displayName	Display name for the permission that appears in the app role assignment and consent experiences.
id	Unique role identifier inside the appRoles collection.
isEnabled	When creating or updating an app role, this must be set to *true* (which is the default).
value	Specifies the value to include in the roles claim in ID tokens and access tokens authenticating an assigned user or service principal.

Info

Attribute Name	Description
logoUrl	CDN URL to the application's logo. Read-only.
marketingUrl	Link to the application's marketing page.
privacyStatementUrl	Link to the application's privacy statement.
supportUrl	Link to the application's support page.
termsOfServiceUrl	Link to the application's terms of service statement.

Optional Claims

Attribute Name	Description
accessToken	The optional claims returned in the JWT access token.
idToken	The optional claims returned in the JWT ID token.
saml2Token	The optional claims returned in the SAML token.

Required Resource Access

Attribute Name	Sub-Attribute Name	
resourceAppId		The unique identifier for the resource that the application requires access to. This should be equal to the appId declared on the target resource application.
resourceAccess	id type	The list of OAuth2.0 permission scopes and app roles that the application requires from the specified resource.

Spa

Attribute Name	Description
redirectUris	Specifies the URLs where user tokens are sent for sign-in, or the redirect URIs where OAuth 2.0 authorization codes and access tokens are sent.

Web

Attribute Name	Sub-Attribute Name	Description
homePageUrl		Home page or landing page of the application.
implicitGrantSettings	enabledAccessTokenIssuance enabledIdTokenIssuance	Specifies whether this web application can request tokens using the OAuth 2.0 implicit flow.
logoutUrl		Specifies the URL that will be used by Microsoft's authorization service to logout an user using front-channel, back-channel or SAML logout protocols.
redirectUris		Specifies the URLs where user tokens are sent for sign-in, or the redirect URIs where OAuth 2.0 authorization codes and access tokens are sent.
redirectUriSettings		Specifies the index of the URLs where user tokens are sent for sign-in. This is only valid for applications using SAML.

9

Application Proxy

The list below includes all supported Application Proxy attributes that can be restored by On Demand Recovery.

General

Attribute Name	Description
alternateUrl	A user-friendly URL that will point to the traffic manager.
applicationServerTimeout	The duration the connector will wait for a response from the backend application before closing the connection.
externalAuthenticationType	Details the pre-authentication setting for the application. Pre-authentication enforces that users must authenticate before accessing the app.
externalUrl	The address your users will go to in order to access the app from outside your network.
internalUrl	The URL that you use to access the application from inside your private network.
isBackendCertificateValidationEnabled	Indicates whether backend SSL certificate validation is enabled for the application.
isHttpOnlyCookieEnabled	Indicates if the HTTPOnly cookie flag should be set in the HTTP response headers.
isOnPremPublishingEnabled	Indicates if the application is currently being published via Application Proxy or not.
isPersistentCookieEnabled	Indicates if the Persistent cookie flag should be set in the HTTP response headers.
isSecureCookieEnabled	Indicates if the Secure cookie flag should be set in the HTTP response headers.
isTranslateHostHeaderEnabled	If set to true, translates URLs in headers.
isTranslateLinksInBodyEnabled	If set to true, translates URLs in body.
singleSignOnSettings	Represents the single sign-on configuration for the on-premises application.
useAlternateUrlForTranslationAndRedirect	

Connector Group

Attribute Name
name
region

State: Enabled or Disabled

Assignments:

- Users and groups for which the policy is applied
- Cloud applications for which the policy is enabled
- Included/excluded locations
- Device platforms

Access controls:

- Block access
- Grant access (require multifactor authentication, compliant device or domain joined device)

10

Conditional Access Policy

The list below includes all supported Conditional Access Policy attributes that can be restored by On Demand Recovery.

General

Attribute Name	Description
conditions	Specifies the rules that must be met for the policy to apply.
displayName	Specifies a display name for the conditionalAccessPolicy object.
grantControls	Specifies the grant controls that must be fulfilled to pass the policy.
sessionControls	Specifies the session controls that are enforced after sign-in.
state	Specifies the state of the conditionalAccessPolicy object.

Country Named Location

The list below includes all supported Country Named Location attributes that can be restored by On Demand Recovery.

Attribute Name	Description
countriesAndRegions	List of countries and/or regions in two-letter format specified by ISO 3166-2.
countryLookupMethod	Determines what method is used to decide which country the user is located in.
displayName	Human-readable name of the location.
includeUnknownCountriesAndRegions	*true* if IP addresses that don't map to a country or region should be included in the named location.

IP Named Location

The list below includes all supported IP Named Location attributes that can be restored by On Demand Recovery.

Attribute Name	Description
displayName	Human-readable name of the location.
ipRanges	List of IP address ranges in IPv4 CIDR format (for example, 1.2.3.4/32) or any allowable IPv6 format from IETF RFC5969.
isTrusted	*true* if this location is explicitly trusted.

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

Technical Support Resources

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

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

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