Quest

On Demand Recovery

Security Guide

© 2023 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

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.

On Demand Recovery Security Guide
Updated - September 2023

Contents

1

Introduction

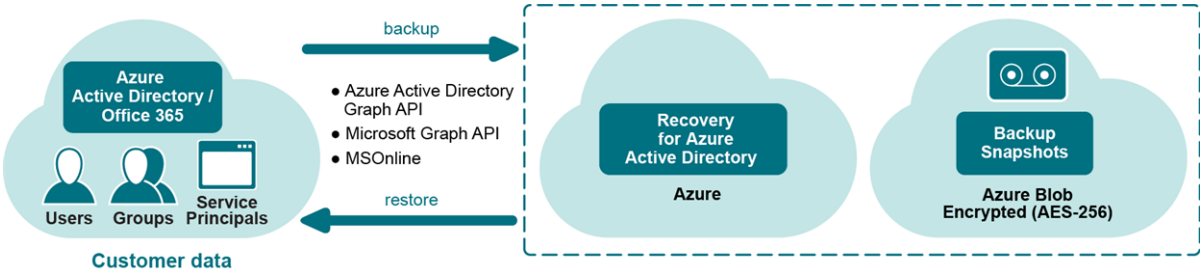
Managing information system security is a priority for every organization. In fact, the level of security provided by software vendors has become a differentiating factor for IT purchase decisions. Quest Software strives to meet standards designed to provide its customers with their desired level of security, whether it relates to privacy, authenticity and integrity of data, availability, or protection against malicious users and attacks.

This document describes the security features of On Demand Recovery. This includes access control, protection of customer data, secure network communication, and more.

About On Demand Recovery

On Demand Recovery cloud application automatically backs up Azure Active Directory and Office 365 users, groups, service principals, device information, conditional access policies and navigation properties and lets you restore deleted or damaged data selectively.

Figure 1: On Demand Recovery overview



On Demand Recovery offers:

- **Back up Azure Active Directory and Office 365 users, groups, service principals, device information, conditional access policies, and navigation properties** - On Demand Recovery automatically backs up a directory on a regular basis.
- **Granular, selective restore** – Objects can be selected in a backup and then restored to Azure Active Directory or Office 365 without affecting other objects or attributes.
- **Restore users from the Recycle Bin** - Restore or recreate users that were inadvertently moved to the Recycle Bin.
- **Cloud solution** - On Demand Recovery does not require that you install or maintain any additional software. Backup snapshots are stored in the cloud.

Architecture overview

The following scheme shows the key components of the On Demand Recovery configuration.

Figure 2: Main architecture diagram

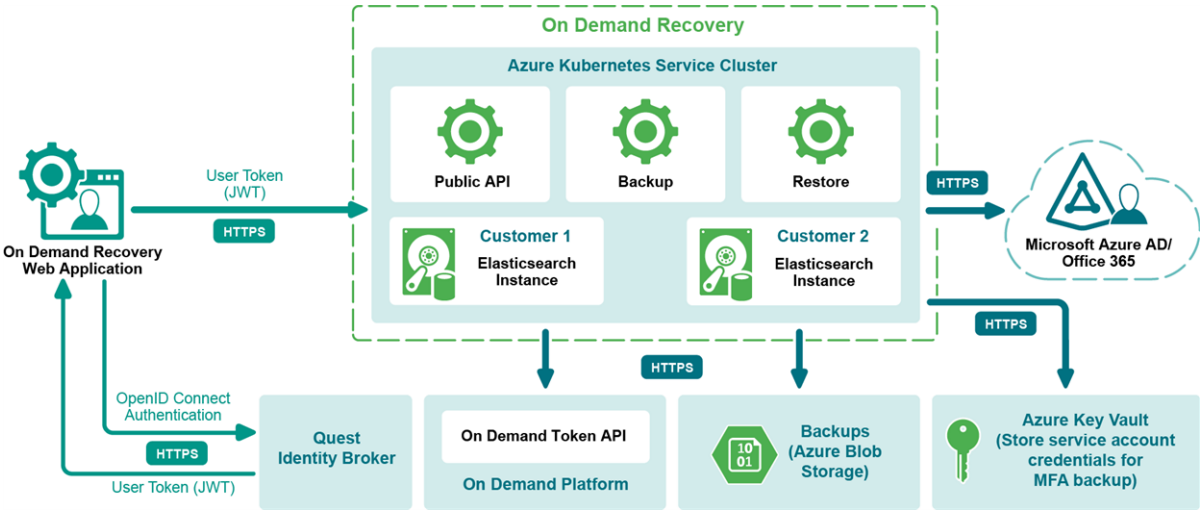


Figure 3: Hybrid restore components diagram

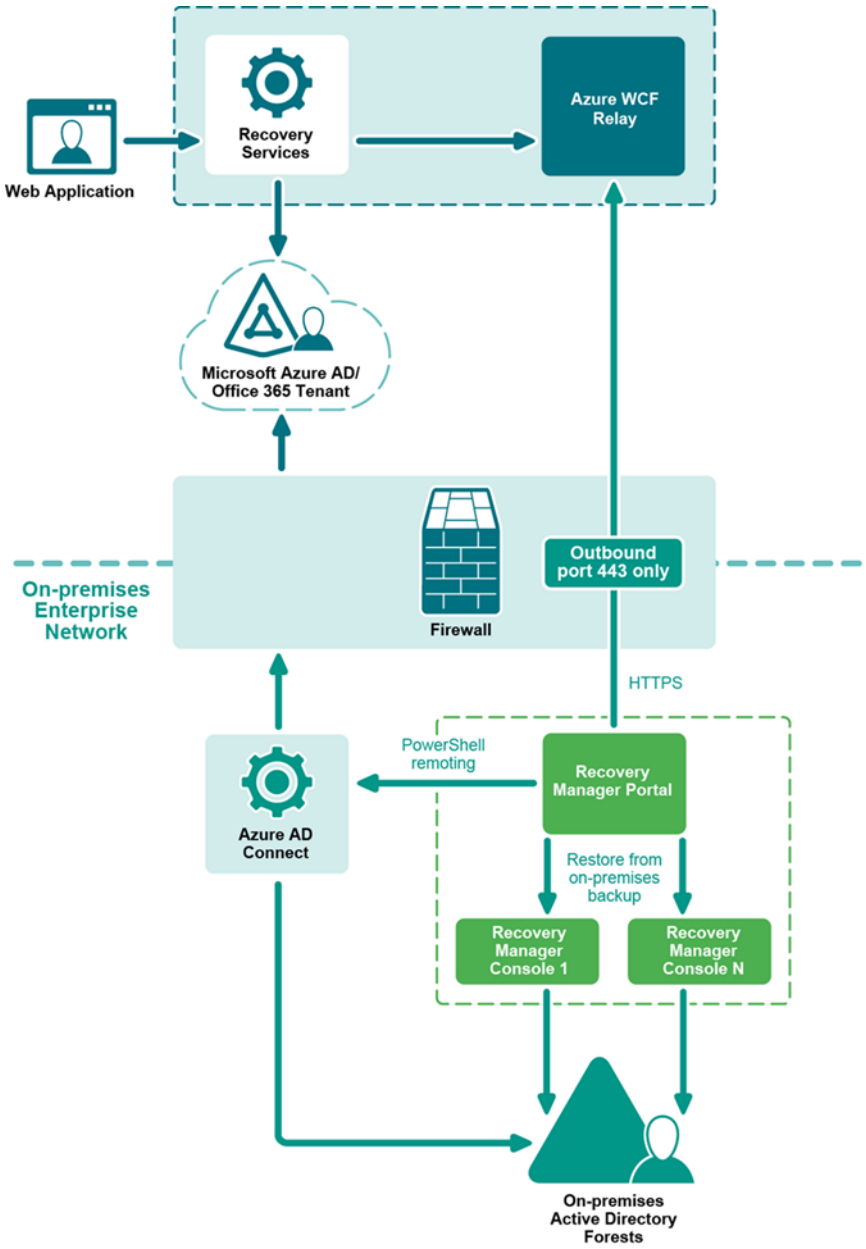


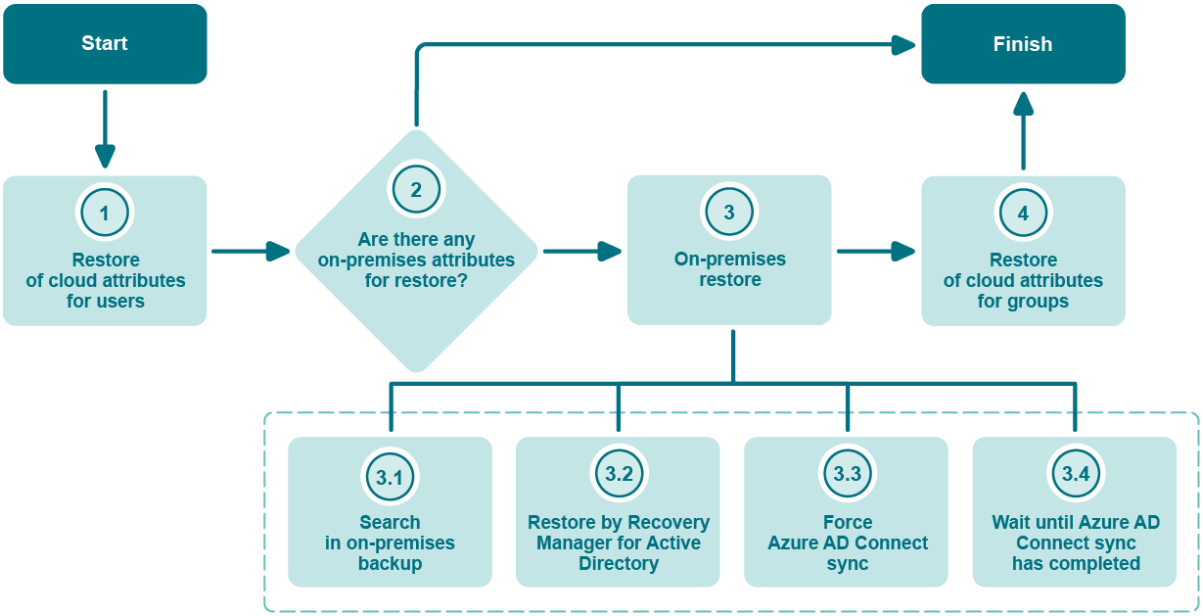
Table 1: On Demand Recovery and Recovery Manager for Active Directory ports and protocols

Protocol	Ports	Direction
HTTPS	443 (TCP/UDP)	Outbound

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.

If you do not want to open all outbound IP addresses and your firewall or proxy lets you specify a DNS allow list, you can add connections to <your name space>.servicebus.windows.net to your allow list.

Figure 4: Hybrid restore operation flow diagram



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

4

Azure datacenter security

Microsoft Azure datacenters have the highest possible physical security and are considered among the most secure and well protected datacenters in the world. They are subject to regular audits and certifications including Service Organization Controls (SOC) 1, SOC 2 and ISO/IEC 27001:2005.

Relevant references with additional information about the Windows Azure datacenter security can be found here:

- Microsoft Azure Trust Center: https://azure.microsoft.com/en-us/overview/trusted-cloud/
- Microsoft Trust Center Compliance: https://www.microsoft.com/en-us/trust-center/compliance/compliance-overview?service=Azure#Icons
- Microsoft's submission to the Cloud Security Alliance STAR registry:https://cloudsecurityalliance.org/star/registry/
- Whitepaper: Standard Response to Request for Information – Security and Privacy: http://www.microsoft.com/en-us/download/details.aspx?id=26647
- Microsoft Global Datacenters: Security & Compliance: https://www.microsoft.com/en-us/cloud-platform/global-datacenters
- Azure data security and encryption best practices: https://docs.microsoft.com/en-us/azure/security/fundamentals/data-encryption-best-practices

5

Overview of data handled by On Demand Recovery

On Demand Recovery manages the following type of customer data:

- Azure Active Directory and Office 365 users, groups, conditional access policies, service principals with their properties, and device information returned by Azure Active Directory Graph API, including account name, email addresses, contact information, department, membership, and other properties.
- On Demand Recovery does not back up and does not store user passwords and password hashes.

For more information about Azure Active Directory connection information and security tokens, refer to the On Demand Core product documentation:

- User Guide
- Release Notes
- Security Guide

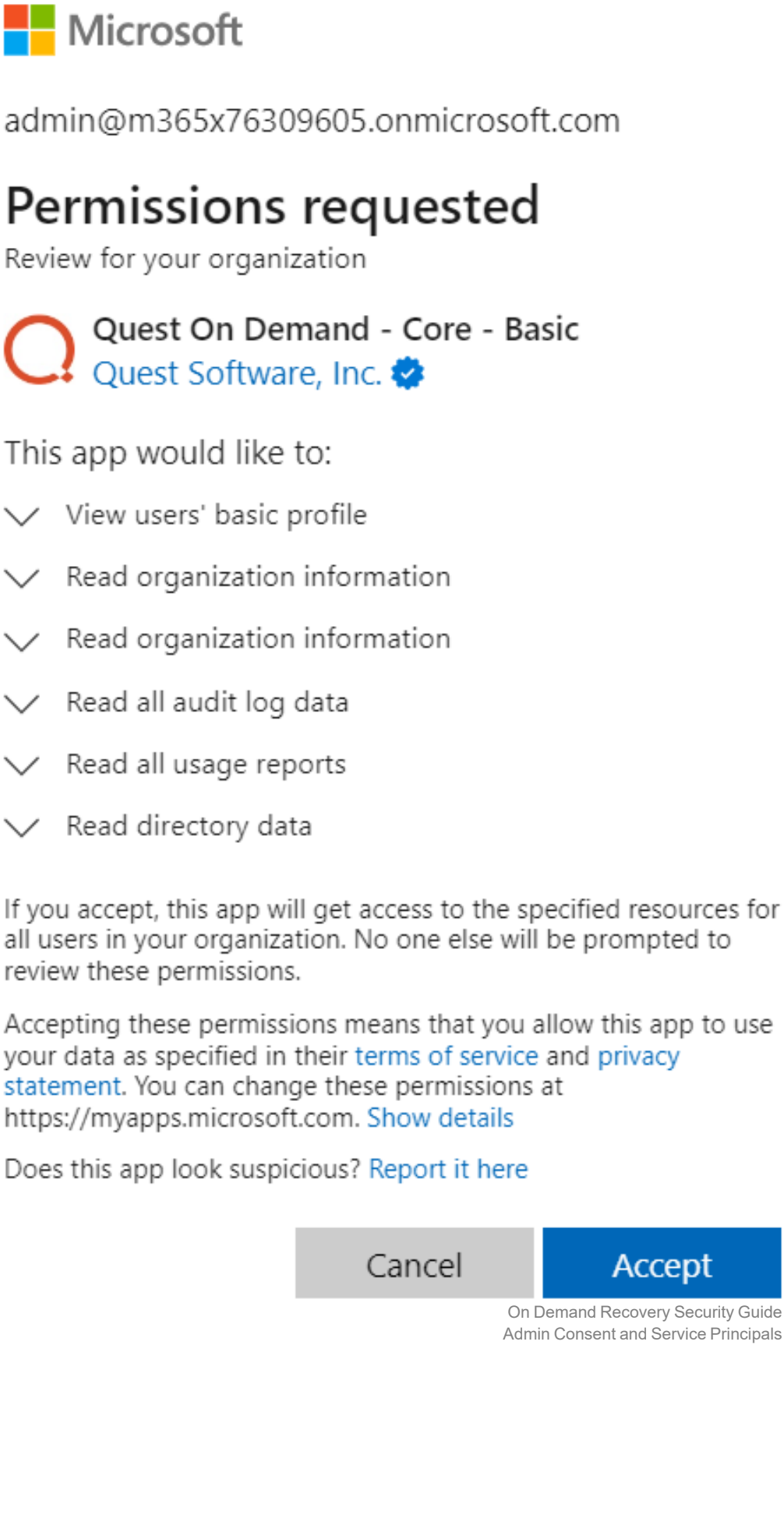
6

Admin Consent and Service Principals

On Demand Recovery requires access to the customer’s Azure Active Directory and Office 365 tenancies. The customer grants that access using the Microsoft Admin Consent process, which will create a Service Principal in the customer's Azure Active Directory with minimum consents required by On Demand Recovery (Groups and Users).

The Service Principal is created using Microsoft's OAuth certificate based client credentials grant flow https://docs.microsoft.com/en-us/azure/active-directory/develop/v2-oauth2-client-creds-grant-flow. Customers can revoke Admin Consent at any time. See https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/delete-application-portal and https://docs.microsoft.com/en-us/skype-sdk/trusted-application-api/docs/tenantadminconsent for details.

Following is the base consent required by On Demand.


Microsoft
admin@m365x76309605.onmicrosoft.com
Permissions requested
Review for your organization
Quest On Demand - Core - Basic
Quest Software, Inc.
This app would like to:
View users' basic profile
Read organization information
Read organization information
Read all audit log data
Read all usage reports
Read directory data
If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.
Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. You can change these permissions at https://myapps.microsoft.com. Show details
Does this app look suspicious? Report it here
Cancel
Accept

In addition to the base consents required by On Demand, On Demand Recovery requires the following consents:

Microsoft

admin@newframeworksorg.onmicrosoft.com

Permissions requested

Review for your organization

Quest On Demand - Recovery - Basic

Quest Software, Inc.

This app would like to:

- Read and write directory data
- Read and write directory data
- Access directory as the signed in user
- Read all groups
- Read and write all groups
- Read directory data
- Read all groups
- Read and write all groups
- Read directory data
- Read and write all directory RBAC settings
- Read and write directory RBAC settings
- Manage app permission grants and app role assignments
- Manage app permission grants and app role assignments

If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. You can change these permissions at

In addition to the base consents required by On Demand and On Demand Recovery, to restore Office 365 and Azure Active Directory data the following consent is required:

Microsoft

admin@newframeworksorg.onmicrosoft.com

Permissions requested

Review for your organization

Quest On Demand - Recovery - Restore

Quest Software Inc.

This app would like to:

- Read and write directory data
- Read and write directory data
- Access directory as the signed in user
- Read and write all groups
- Read and write all groups
- Read and write all directory RBAC settings
- Read and write directory RBAC settings
- Manage app permission grants and app role assignments
- Manage app permission grants and app role assignments
- Read and write all users' full profiles
- Read and write all users' full profiles
- Read and write devices

If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. You can change these permissions at https://myapps.microsoft.com. Show details

Does this app look suspicious? Report it here

Exchange Online PowerShell

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

Location of customer data

The following datacenters are used to store customer data:

For US organizations

- Backups are stored in Geo-redundant Azure Blob Storage – encrypted at rest:
  - Primary replica - West US 2 (Washington)
  - Secondary replica - West Central US (Wyoming)
- Unpacked backups are stored on Azure virtual disks that are associated with independent Elasticsearch nodes (per customer) which are part of Azure Kubernetes Service West US 2 (Washington) - encrypted at rest
- Logs are stored in Log Analytics East US (Virginia) – encrypted at rest
- Service account credentials that are used to backup MFA settings, inactive mailboxes, conditional access policies, Gallery applications, and SSO settings data (if the corresponding option is selected) are stored in Azure Key Vault Central US (Iowa).

For Canadian organizations

- Backups are stored in Geo-redundant Azure Blob Storage – encrypted at rest
  - Primary replica – Canada Central (Toronto)
  - Secondary replica – Canada East (Quebec City)
- Unpacked backups are stored on Azure virtual disks that are associated with independent Elasticsearch nodes (per customer) which are part of Azure Kubernetes Service Canada Central (Toronto) – encrypted at rest
- Logs are stored in Log Analytics Canada Central (Toronto) – encrypted at rest
- Service account credentials that are used to backup MFA settings, inactive mailboxes, conditional access policies, Gallery applications, and SSO settings data (if the corresponding option is selected) are stored in Azure Key Vault Canada Central (Toronto).

For European organizations

- Backups are stored in Geo-redundant Azure Blob Storage – encrypted at rest:
    - Primary replica – North Europe (Ireland)
    - Secondary replica – West Europe (Netherlands)
- Unpacked backups are stored on Azure virtual disks that are associated with independent Elasticsearch nodes (per customer) which are part of Azure Kubernetes Service North Europe (Ireland) – encrypted at rest
- Logs are stored in Log Analytics North Europe (Ireland) – encrypted at rest
- Service account credentials that are used to backup MFA settings, inactive mailboxes, conditional access policies, Gallery applications, and SSO settings data (if the corresponding option is selected) are stored in Azure Key Vault North Europe (Ireland).

For UK organizations

- Backups are stored in Geo-redundant Azure Blob Storage – encrypted at rest:
    - Primary replica – UK South
    - Secondary replica – UK West
- Unpacked backups are stored on Azure virtual disks that are associated with independent Elasticsearch nodes (per customer) which are part of Azure Kubernetes Service UK South – encrypted at rest
- Logs are stored in Log Analytics UK South – encrypted at rest
- Service account credentials that are used to backup MFA settings, inactive mailboxes, conditional access policies, Gallery applications, and SSO settings data (if the corresponding option is selected) are stored in Azure Key Vault UK South.

For Australian organizations

- Backups are stored in Geo-redundant Azure Blob Storage – encrypted at rest:
    - Primary replica – Australia East
    - Secondary replica – Australia Southeast
- Unpacked backups are stored on Azure virtual disks that are associated with independent Elasticsearch nodes (per customer) which are part of Azure Kubernetes Service Australia East – encrypted at rest
- Logs are stored in Log Analytics Australia East– encrypted at rest
- Service account credentials that are used to backup MFA settings, inactive mailboxes, conditional access policies, Gallery applications, and SSO settings data (if the corresponding option is selected) are stored in Azure Key Vault Australia East.

Other regions are supported on customer request.

8

Privacy and protection of customer data

The most sensitive customer data collected and stored by On Demand Recovery is the Azure Active Directory and Office 365 data including users, groups, service principals, conditional access policies, devices and their associated properties. All properties which are available in Microsoft Azure AD Graph API and MSOnline – such as users email, work title, department, phone number, address and others – are stored in the backup. On Demand Recovery does not back up and does not store user passwords and password hashes.

The backup data for each customer is stored in a separate Azure Blob Container. This information is protected through the Azure built in data at rest Server-Side encryption mechanism. It uses the strongest FIPS 140-2 approved block cipher available, Advanced Encryption Standard (AES) algorithm, with a 256-bit key.

Geo-redundant storage is used which means that backup data is replicated to a secondary region that is hundreds of miles away from the primary region. Backup data is durable even in the case of a complete regional outage or a disaster in which the primary region is not recoverable.

Service account credentials that are used to backup MFA settings and conditional access policies (if the corresponding option is selected) and security tokens are stored in Microsoft Azure Key Vault. For details about encryption within Azure Key Vault, see the Privacy and Protection of Customer Data section in the Quest On Demand Core Security Guide.

For more information about Azure Blob Storage, see the following links:

- https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blobs-introduction
- https://docs.microsoft.com/en-us/azure/security/security-storage-overview
- https://docs.microsoft.com/en-us/azure/storage/common/storage-service-encryption
- https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy#geo-redundant-storage

9

Separation of customer data

A common concern related to cloud based services is the prevention of commingling of data that belongs to different customers.On Demand Recovery has architected its solution to specifically prevent such data commingling by logically separating customer data stores.

Customer data are differentiated using a Customer Organization Identifier. The Customer Organization Identifier is a unique identifier obtained from the Quest On Demand Core that is created when the customer signs up with the application.

This identifier is used throughout the solution to ensure strict data separation of customers' backups in the Azure Blob storage.

Furthermore, each customer has its own instance of Elasticsearch that is used for unpack, object search, and restore operations. Elasticsearch index is stored on a separate Azure Disk with enabled encryption in the Quest Azure subscription.

10

Network communications

All communications to and from the On Demand Recovery web application go over HTTPS, and the SSL certificates are issued by trusted certificate authorities. As for the On Demand Recovery web application itself, it enforces that all communications occur over HTTPS connections. If a user tries to access via a regular HTTP, the application will redirect the request to HTTPS version of the endpoint's enabled connection. On Demand Recovery communicates with Azure Active Directory Graph API over HTTPS. TLS 1.2 is enforced for this communication.

11

Authentication of users

The customer logs in to the application by providing On Demand user account credentials.

The process of registering an Azure AD tenant into On Demand Recovery is handled through the well established Azure Admin Consent workflow. For more information about Azure Active Directory Admin Consent workflow, refer to the Quest On Demand Core product documentation:

- User Guide
- Release Notes
- Security Guide

Role based access control

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

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

List of permissions that can be assigned to Recovery module users

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

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

13

FIPS 140-2 compliance

On Demand Recovery cryptographic usage is based on Azure FIPS 140-2 compliant cryptographic functions. For more information, see https://docs.microsoft.com/en-us/azure/storage/blobs/security-recommendations.

14

SDLC and SDL

The On Demand Recovery Development team follows a managed Software Development Lifecycle (SDLC).

The On Demand Recovery team follows a strict Quality Assurance cycle.

All product code is reviewed by another developer before check in.

In addition, the On Demand Recovery Development team follows a managed Security Development Lifecycle (SDL) which includes:

- MS-SDL best practices
- Threat modeling
- OWASP guidelines
- Static code analysis is performed on a regular basis.
- Vulnerability scanning is performed on a regular basis.
- Segregated Development, Pre-Production, and Production environments. Customer data is not used in Development and Pre-Production environments.

On Demand Recovery developers go through the same set of hiring processes and backgrounds checks as other Quest employees.

15

Third Party assessments and certifications

Penetration testing

On Demand Recovery has undergone a third party security assessment and penetration testing yearly since 2018. A summary of the results is available upon request.

Certification

On Demand is included in the scope of the Platform Management ISO/IEC 27001, 27017 and 27018 certification:

- ISO/IEC 27001 Information technology — Security techniques — Information security management systems — Requirements: **Certificate Number: 1156977-3**, valid until **2025-07-28.**
- ISO/IEC 27017 Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services: **Certificate Number: 1156977-3**, valid until **2025-07-28**.
- ISO/IEC 27018 Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors: **Certificate Number: 1156977-3**, valid until **2025-07-28**.

Quest Software, Inc. has successfully completed a SOC 2 examination of its On Demand solution. The examination was performed by an independent CPA firm for the scope of service described below.

Examination Scope: **Quest On Demand Platform**

Selected SOC 2 Categories: **Security**

Examination Type: **Type 2**

Review Period: **August 1, 2022** to **July 31, 2023**

Service Auditor: **Schellman & Company, LLC**

16

Operational security

Access to source control and build systems is protected by domain security, meaning that only employees that are on Quest's corporate network have access to these systems. Therefore, if an On Demand Recovery developer departs from the company, this individual will no longer be able to access On Demand Recovery systems. All code is versioned in source control.

Permissions required to configure and operate On Demand Recovery

On Demand Recovery is a part of Quest On Demand cloud-based management platform. The main interface through which the customer interacts with and configures On Demand Recovery is its web application. It does not require the installation of any software components on the customer's systems.

In order to access the On Demand Recovery tool, a customer representative goes to the On Demand website and signs up for an On Demand account. When you create an account, an organization is automatically created. As part of the sign up process, you must provide a valid email address. You must have access to the email account in order to receive and respond to a verification email from Quest Software.

Prerequisites

Azure Active Directory Global Administrator must give the Admin Consent to provision On Demand Recovery for customer's Azure Active Directory with the following permissions:

Microsoft Graph

- Read all groups
- Read and write all groups
- Read and write directory data
- Read directory data

Windows Azure Active Directory

- Read and write directory data
- Read directory data

OAuth 2.0 permission grants

Microsoft Graph

- Access directory as the signed in user
- Read all groups
- Read and write all groups
- Read and write directory data
- Read directory data

Windows Azure Active Directory

- Read all groups
- Read and write all groups
- Read and write directory data
- Read directory data
- Sign in and read user profile

On Demand Recovery does not use and does not store the user account with the Azure AD Global Administrator role. This account is used only to provision the Quest Azure application.

17

Customer measures

On Demand Recovery security features are only one part of a secure environment. Customers need to operate by their own best security practices when proceeding with data recovery. Special care needs to be given to protecting the credentials of the Azure Active Directory tenants Global Administrator accounts.

About us

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

Technical support resources

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

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

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