Quest® On Demand Migration Self-Service

Security Guide

© 2026 Quest Software Inc. ALL RIGHTS RESERVED.

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

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

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

Quest Software Inc.

Attn: LEGAL Dept

10801 N. Mopac Expressway

Building 3, Suite 400

Austin, TX 78759

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 Migration Self-Service Security Guide for Device Migration
Updated - September 2026

Contents

Introduction **4**

About On Demand Migration Self-Service (ODMSS) **5**

Architecture Overview **6**

Azure Datacenter Security **7**

Overview of Data Handled by ODMSS **8**

Admin Consent and Service Principals **9**

Location of Customer Data **11**

Privacy and Protection of Customer Data **12**

Separation of Customer Data **13**

Network Communications **14**

Authentication of Users **15**

Role Based Access Control **16**

FIPS 140-2 compliance **17**

SDLC and SDL **18**

Third party assessments and certifications **19**

Operational Security **20**

- Who at Quest has Access to Data 20
- Permissions Required to Configure and Operate 20
- Operational Monitoring 21
- Production Incident Response Management 21
- Security Incident Response Management 21

Customer Measures **22**

About us **23**

- Technical support resources 23

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 strives to meet standards designed to provide its customers with their desired level of security as it relates to privacy, confidentiality, integrity, and availability.

This document describes the security features of Quest On Demand Migration Self-Service (ODMSS). It reviews access control, protection of customer data, secure network communication, cryptographic standards and more.

About On Demand Migration Self-Service (ODMSS)

Quest On Demand Migration Self-Service (ODMSS) enables end users to schedule their own device migrations between Entra ID or local Active Directory and securely set passwords on their new target accounts. This feature is an add-on feature for On Demand Migration (ODM) and On Demand Migration for Active Directory (ODMAD).

For details about security in ODMAD, see the document On Demand Migration for Active Directory Security Guide.

ODMAD provides the following functionality:

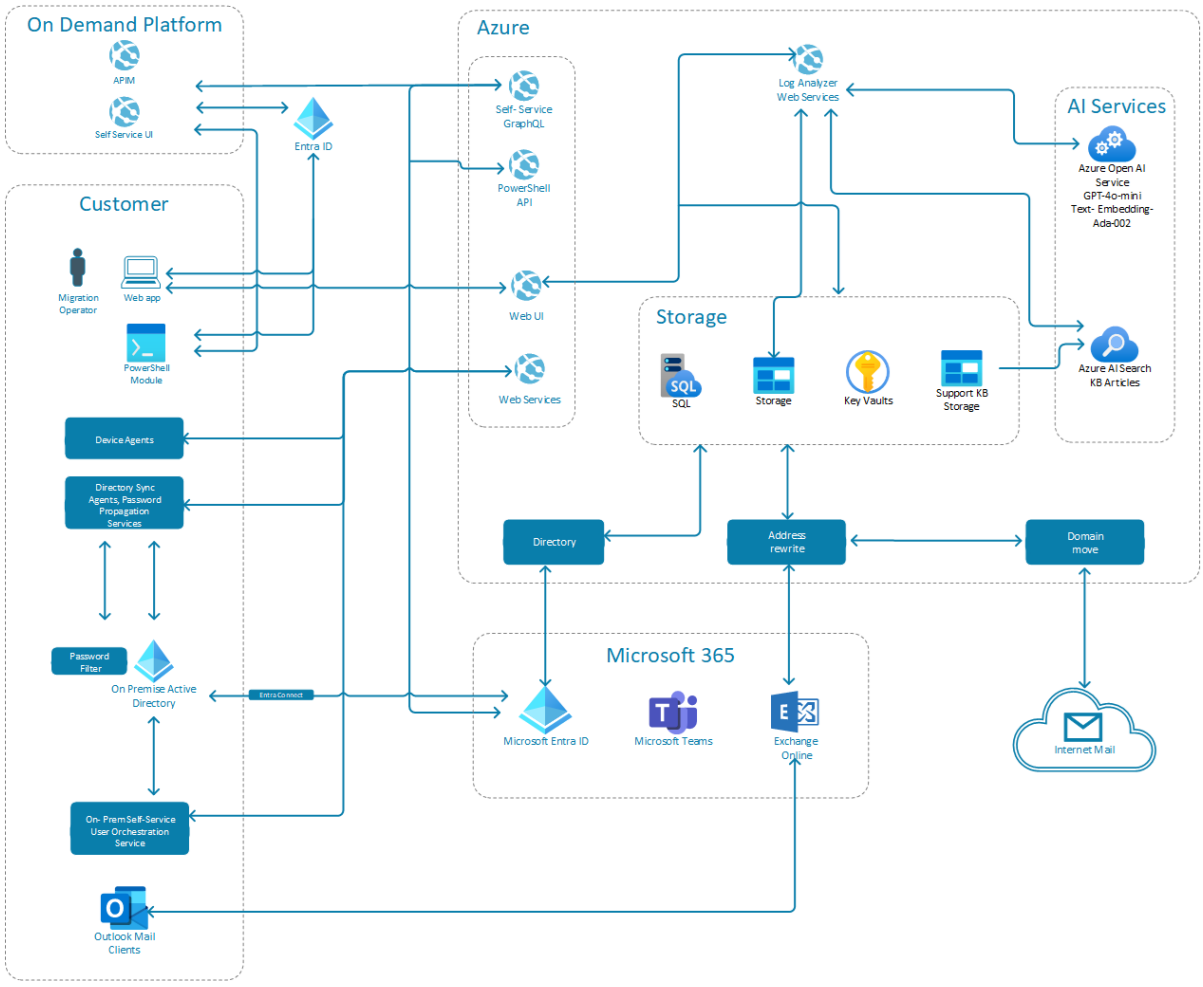
- Full tenant discovery of users, groups, domains and more.
- Move domains between tenants.
- Synchronize Active Directory and Microsoft Entra ID directories with customizable workflows.
- Migrate workstations, computers, servers, objects, users, groups and more.
- No servers, trusts, or network connectivity required.
- Data transformation and customizable mapping of directory attributes.
- Near-real time password hash synchronization.
- Password change propagation.
- Trustless SID History migration.

For details about security in ODM, see the document On Demand Migration Current - Security Guide - General Migration.

ODM provides the following functionality in a robust project management interface with in-depth monitoring and reporting:

- Analyzes Microsoft Entra ID structure and highlights the problems that might adversely affect the migration.
- Migrates users, groups, and the related information between Microsoft Entra ID tenants or maps the existing source/target accounts.
- Migrates hybrid accounts (on-premises users/groups synchronized with Microsoft Entra ID).
- Migrates Microsoft Office 365 mailboxes.
- Automatically redirects on-premise Outlook clients to the new Exchange Online.
- Grants access to the source tenant's resources and applications for the migrated/mapped accounts.
- Transfers OneDrive for Business content and permissions between tenants.
- Ensures uninterrupted workflows during the migration:
    - Automatically replaces email addresses in outgoing and incoming messages, as if the senders have already been migrated to the target tenant (Domain Coexistence feature) .
    - Shares free/busy information between tenants.

Architecture Overview



4

Azure Datacenter Security

Microsoft Azure datacenters have the highest possible physical security and are considered among the most secure 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:

- Azure Trust Center: https://azure.microsoft.com/en-us/support/trust-center/
- Microsoft Trust Center Compliance: https://www.microsoft.com/en-us/TrustCenter/Compliance?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-at-rest Encryption Best Practices: https://docs.microsoft.com/en-us/azure/security/azure-security-data-encryption-best-practices

5

Overview of Data Handled by ODMSS

ODMSS user data is stored in On Demand which collects data for a variety of on premises and Microsoft Entra ID objects. The directory locations, objects and properties collected are configurable to ensure only the desired objects and properties are processed.

Microsoft Entra ID

- Directory objects are processed using Microsoft Graph API and PowerShell.
- Objects include users, groups, contacts, teams, and Microsoft 365 groups.
- Properties include account name, email addresses, contact information, department, membership and more.
- Access to Microsoft Entra ID is granted by the customer using the Microsoft Admin Consent process and requires administrative credentials. Customers can revoke Admin Consent at any time. See https://msdn.microsoft.com/en-us/skype/trusted-application-api/docs/tenantadminconsent for details.
- Neither ODMAD nor ODMSS store credentials for administrative accounts.
- For User Cutover, passwords are never stored in On Demand Migration. The end user authenticates with Microsoft Entra ID via HTTPS using the application permission consented by the Migration Administrator and sets their password.

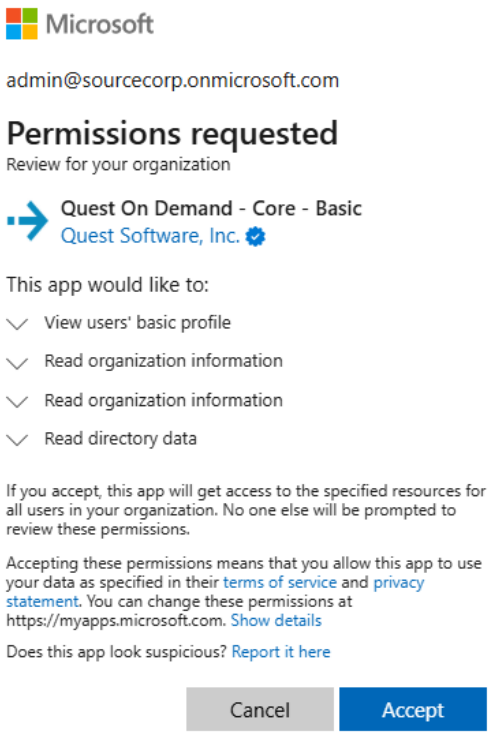
On Premises Active Directory

- On-premises directory sync agents, running within the customers network, process Active Directory objects using LDAP or LDAPS (TLS 1.2) as configured within the user interface. Objects include users, groups, and contacts, computers, and servers. Properties include account name, email addresses, contact information, department, membership, and more.
- On-premises directory sync agents, running within the customers network, securely encrypt and store administrative credentials locally on the agent's computer.
- On-premises device agents running locally on the end user's workstation collect device properties using WMI and PowerShell. Device properties include device name, domain name, user profile locations, and more.
- ODMAD optionally stores credentials required for network share re-permission, and Active Directory domain joins. These credentials are provided by migration operators and are encrypted with AES 256-bit encryption using Azure Key Vault and are never stored unencrypted.

Admin Consent and Service Principals

As part of the login process with Microsoft Entra ID, users must consent to the set of minimal permissions required by the Quest On Demand application. By default, all users are allowed to consent to applications for permissions that do not require administrator consent. This behavior might be deactivated in some Microsoft Entra ID tenants and may require tenant administrators to enable user consent flow for the Quest On Demand application.

The base consents required by Quest On Demand are shown below.

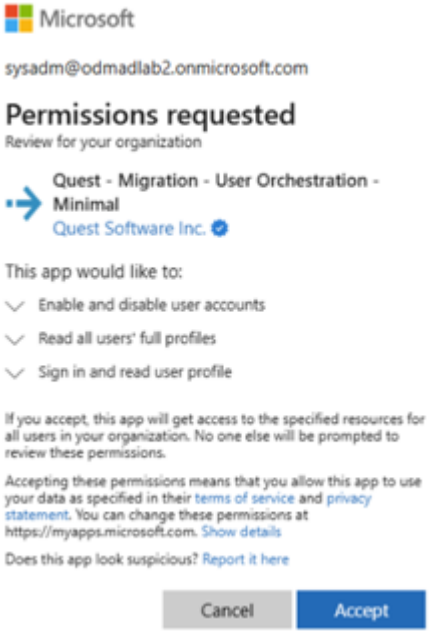


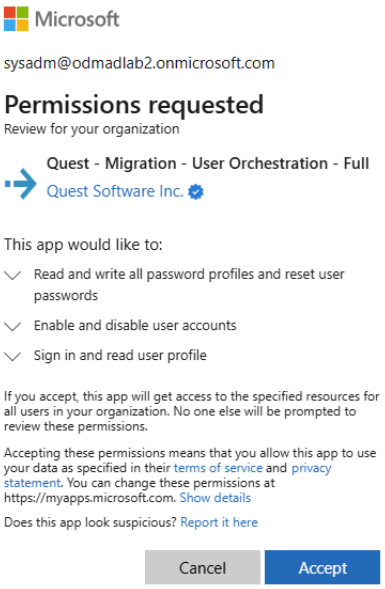
Additional Admin consents are required when using ODMSS with ODMAD.

In addition to the On Demand application consent, user cutover feature also requires the following consents:

Quest - Migration - User Orchestration - Minimal for the source tenant.

Quest - Migration - User Orchestration - Full consent for the target tenant.


Microsoft
sysadm@odmadlab2.onmicrosoft.com
Permissions requested
Review for your organization
Quest - Migration - User Orchestration - Minimal
Quest Software Inc.
This app would like to:
Enable and disable user accounts
Read all users' full profiles
Sign in and read user profile
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


Microsoft
sysadm@odmadlab2.onmicrosoft.com
Permissions requested
Review for your organization
Quest - Migration - User Orchestration - Full
Quest Software Inc.
This app would like to:
Read and write all password profiles and reset user passwords
Enable and disable user accounts
Sign in and read user profile
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

7

Location of Customer Data

When a customer signs up for On Demand, they select the region in which to run their On Demand organization. All computation is performed in and all customer data is stored in the selected region. The currently supported regions can be found here: https://regions.quest-on-demand.com/. ODMSS customer data is stored in the selected region, entirely within Azure Services provided by Microsoft. For more information, see Achieving Compliant Data Residency and Security with Azure.

- Customer data is stored in Azure SQL and is automatically replicated for failover using Azure SQL Active Geo replication. See this Microsoft reference for details: https://docs.microsoft.com/en-us/azure/azure-sql/database/active-geo-replication-overview
- Application logs are stored in Azure storage tables. Windows Azure Storage, including the Blobs, Tables and Queues storage structures, by default get replicated three times in the same datacenter for resiliency against hardware failure. The data are replicated across different fault domains to increase availability. All replication datacenters reside with the geographic boundaries of the selected region. See this Microsoft reference for details: https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy

8

Privacy and Protection of Customer Data

Sensitive customer data collected and stored by ODMSS includes end user UserPrincipalName and Email Addresses. This data is uploaded by the customer's Migration Administrator and stored in On Demand.

- All data is secured at rest using SQL Transparent Data Encryption (TDE) with Microsoft managed keys. For more information see https://docs.microsoft.com/en-us/azure/azure-sql/database/transparent-data-encryption-tde-overview
- Azure storage account data is secured at rest using storage service encryption with Microsoft managed keys. For more information see https://docs.microsoft.com/en-us/azure/storage/common/storage-service-encryption

9

Separation of Customer Data

ODMSS is designed to prevent data from commingling by logically separating customer data. Customer data are differentiated using a Customer Organization Identifier. The Customer Organization Identifier is a unique identifier obtained from Quest On Demand that is created when the customer signs up for the application. This identifier is used throughout the solution to ensure strict data separation of customers' data.

Customer data is further separated as customer related services are isolated from any other OS process by the Microsoft Service Fabric exclusive process model. See https://docs.microsoft.com/en-us/azure/service-fabric/service-fabric-hosting-model#exclusive-process-model for more information.

10

Network Communications

- All communication to the ODMSS - including the user interface and associated Azure services - are secured with HTTPS. There are no unsecured external HTTP calls within ODMAD.
- All communication with Microsoft Entra ID uses OAuth2 access tokens for Microsoft Graph API operations and HTTPS for PowerShell operations.
- Internal network communication within Azure includes Inter-service communication between ODMAD, On Demand Core and the On Demand Platform.

11

Authentication of Users

- ODMSS relies Microsoft Entra ID for authentication which provides customers with an integrated authentication experience where you can move from ODMSS to a Microsoft portal seamlessly, without multiple logins and passwords. All while keeping your account security under your organization's policies, rules, and security protocols.
- ODMSS also supports Multi Factor Authentication (MFA) for organizations that have enabled MFA within Microsoft 365.
- Registering a Microsoft Entra tenant into ODMSS is handled through the Azure Admin Consent workflow and customers can revoke Admin Consent at any time. See https://msdn.microsoft.com/en-us/skype/trusted-application-api/docs/tenantadminconsent for details.

12

Role Based Access Control

Quest On Demand is configured with default roles that cannot be edited or deleted and also allows you to add custom roles to make permissions more granular. Each access control role has a specific set of permissions that determines what tasks a user assigned to the role can perform. For more information on role-based access control, please refer to the Quest On Demand product documentation.

13

FIPS 140-2 compliance

ODMSS cryptographic usage is based on Azure FIPS 140-2 compliant cryptographic functions. ODMSS makes use of FIPS 140-2 compliant encryption keys that are stored in Microsoft Key Vault.

More information:

- Microsoft and FIPS: https://www.microsoft.com/en-us/trustcenter/compliance/fips
- Microsoft FIPS backgrounder: https://aka.ms/fips-backgrounder
- Encryption in the Microsoft Cloud: https://docs.microsoft.com/en-us/office365/securitycompliance/office-365-encryption-in-the-microsoft-cloud-overview
- Azure Storage: https://docs.microsoft.com/en-us/azure/storage/common/storage-security-guide

14

SDLC and SDL

The ODMSS Development team follows a managed Software Development Lifecycle (SDLC).
The ODMSS team follows a strict Quality Assurance cycle.

- Access to source control and build systems is protected by domain security. Only employees on Quest's corporate network have access to these systems. If an On Demand developer leaves the company, they will no longer be able to access On Demand systems.
- All code is versioned in source control.
- All product code is reviewed by another developer before checking in.

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

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

ODMSS developers go through the same set of hiring processes and background checks as other Quest employees.

15

Third party assessments and certifications

Penetration testing

On Demand has undergone a third-party security assessment and penetration testing yearly since 2017. Assessment includes but is not limited to:

- Manual penetration testing
- Static code analysis with Third Party tools to identify security flaws

A summary of the results is available upon request. All security recommendations are planned to be incorporated in near-term product releases.

Certification

On Demand is included in the scope of the Platform Management ISO/IEC 27001, 27701, 27017 and 27018 certification:

- ISO/IEC 27001:2022 Information technology — Security techniques — Information security management systems — Requirements: Certificate Number: 1156977-8, valid until 2028-07-27.
- ISO/IEC 27701:2019 Information security, cybersecurity and privacy protection — Privacy information management systems — Requirements and guidance: Certificate Number: 1156977-8, valid until 2028-07-27
- ISO/IEC 27017:2015 Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services: Certificate Number: 1156977-8, valid until 2028-07-27.
- ISO/IEC 27018:2019 Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors: Certificate Number: 1156977-8, valid until 2028-07-27.

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, 2024, to July 31, 2025
- Service Auditor: Schellman & Company, LLC

16

Operational Security

Source control and build systems can only be accessed by Quest employees. If an employee with access to ODMSS leaves the company the individual loses access to all systems. All code is versioned in source control.

Who at Quest has Access to Data

Access to ODMSS data is restricted to:

- Quest Operations team members
- Selected Quest Support team members working on product issues.
- Selected development team members working with the Operations and Support teams.

Access to ODMSS data and resources is restricted through Azure RBAC and Microsoft Entra ID security groups. For each type of data (e.g., product logs, customer data, and sensitive data) different access levels and lists of allowed people are assigned.

Permissions Required to Configure and Operate

To access ODMSS, a customer representative goes to On Demand website and signs up for an On Demand account. When an account is created an organization is also automatically created. As part of the sign-up process, they must provide a valid email address and must have access to this email account to receive and respond to a verification email from Quest Software.

A Microsoft Entra ID Global Administrator must give the Admin Consent to provision ODMSS with the following Microsoft.Graph permissions:

Read and write all groups (Group.ReadWrite.All)

Permission Definition: Allows the app to create groups and read all group properties and memberships on behalf of the signed-in user. Additionally, allows group owners to manage their groups and allows group members to update group content.

Application Purpose: Used by the app to Sync services to provide OneDrive migration activities.

Read and write directory data (Directory.ReadWrite.All)

Permission Definition: Allows the app to have the same access to information in the directory as the signed-in user.

Application Purpose: Used by Discovery and Provisioning Services to discover all workloads (such as Organizations, available SKUs, users, groups, contacts, etc.) and to automate M365 licensing.

Read and write role management data for Microsoft Entra ID (RoleManagement.ReadWrite.Directory)

Permission Definition: Allows the app to assign roles to Microsoft Entra ID accounts.

Application Purpose: Used by the app to assign roles to service accounts to ensure the minimum effective rights are granted.

Read and write all groups (User.Read.All)

Permission Definition: Allows the app to read and write the full set of profile properties, reports, and managers of other users in your organization, on behalf of the signed-in user.

Application Purpose: Used by Discovery services to identify user mailbox properties.

Operational Monitoring

ODMSS internal logging is available to Quest Operations and ODMSS development teams during the normal operation of the platform. Some Personally Identifiable Information (PII) (e.g. usernames, email addresses, email aliases, etc.) can become a part of internal logging for troubleshooting purposes. Quest Operations team members have access to Quest's production Azure Subscription and monitor this as part of normal day-to-day operations.

Production Incident Response Management

Quest Operations and Quest Support have procedures in place to monitor the health of the system and ensure any degradation of the service is promptly identified and resolved. ODMSS relies on Azure infrastructure and as such, is subject to the possible disruption of these services.

- Quest On Demand services status page is available at https://status.quest-on-demand.com/
- Azure services status page is available at https://azure.microsoft.com/en-ca/status/

Security Incident Response Management

For its On Demand solution, Quest has established a formal process of preparation, detection, analysis, containment, eradication, recovery, and post-incident activities. In accordance with international privacy laws, Quest has also established a Security Breach Notice process.

17

Customer Measures

ODMSS security features are only one part of a secure environment. Customers need to operate by their own best security practices when proceeding with auditing their data. Special care needs to be given to protecting the credentials of the Microsoft Entra Tenants Global Administrator accounts and On Premises Active Directory Administrator accounts.

About us

Quest Software creates technology and solutions that build the foundation for enterprise AI. Focused on data management and governance, cybersecurity and platform modernization, Quest helps organizations address their most pressing challenges and make the promise of AI a reality. Around the globe, more than 45,000 companies including over 90% of the Fortune 500 count on Quest Software. For more information, visit www.quest.com or follow Quest Software on X (formerly Twitter) and LinkedIn.

Technical support resources

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

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

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