Quest® On Demand Migration for Hybrid Exchange

Security Guide

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 for Hybrid Exchange Security Guide
Updated - November 2023

Contents

Introduction 1

About On Demand Migration Hybrid Exchange 2

Architecture overview 3

Azure datacenter security 4

Overview of data handled by On Demand Migration 5

Admin Consent and Service Principals 6

Location of customer data 9

Privacy and protection of customer data 10

Separation of customer data 11

Network communications 12

Authentication of users 14

Role based access control 15

FIPS 140-2 compliance 16

SDLC and SDL 17

Third Party assessments and certifications 18

Penetration testing 18

Certification 18

Operational security 19

Access to data 19

Permissions required to configure and operate On Demand Migration 19

Operational monitoring 20

Production incident response management 20

Customer measures 21

About us 22

Technical support resources 22

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 On Demand Migration for Hybrid Exchange. This includes access control, protection of customer data, secure communication, and cryptographic standards.

About On Demand Migration Hybrid Exchange

On Demand Migration for Hybrid Exchange (ODMHE) securely migrates data to Microsoft 365 from on-premises Microsoft Exchange without requiring organizations to install or maintain migration servers for the move. From a single console, administrators can migrate multiple users simultaneously and migrate data such as email, calendars and folders in a phased approach. Administrators can filter to clean up unwanted data and shorten the time it takes to migrate.

Architecture overview

The following scheme shows the key components of the On Demand Migration for Hybrid Exchange configuration.

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/microsoft/
- 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

Overview of data handled by On Demand Migration

On Demand Migration for Hybrid Exchange migrates the following type of customer data.

- Email content
- Email attachments
- Calendar
- Contacts
- Personal distribution lists and tasks
- Mailbox settings

ODMHE does not retain the data or emails and their attachments that get migrated. They only exist in memory while they are in the process of being migrated.

The following customer data will, by default, be retained by ODMHE:

- Source and target mailbox names
- Product logs data which can include structured error message entries containing meta-data of email items that ODMHE failed to transport, such as subject line, date, size, the folder name (if any) in which the email resides, but not the email body, .
- MIME content of mailbox items to facilitate troubleshooting. The MIME content of mailbox items may be stored when an error occurs during migration. This is turned off by default, and activated only when the customer grants permission.

The persisted data is stored until a customer's subscription ends. The data is stored in Azure Storage such as Table, Queue and BLOB (binary large object) storage, and persists as long as a customer's subscription is active. If a customer decides to unsubscribe from Quest On Demand, the customer is notified 30 days before their subscription ends. When an organization is deleted, data related to the organization will be deleted after 30 days.

Admin Consent and Service Principals

On Demand Migration for Hybrid Exchange requires access to the customer's Microsoft Entra ID and Microsoft 365 tenancies. The customer grants that access using the Microsoft Admin Consent process, which creates a Service Principal in the customer's Microsoft Entra ID with minimum consents required by ODMHE.

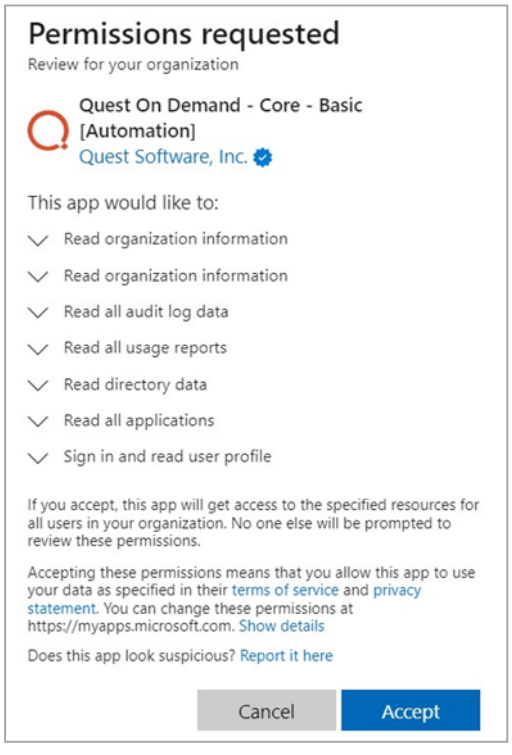
The Service Principal is created using Microsoft's OAuth2 certificate based client credentials grant flow. See https://docs.microsoft.com/en-us/azure/activedirectory/develop/v2-oauth2-client-creds-grant-flow for details.

Customers can revoke the 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.

The admin permission consents required by ODMHE are described below:

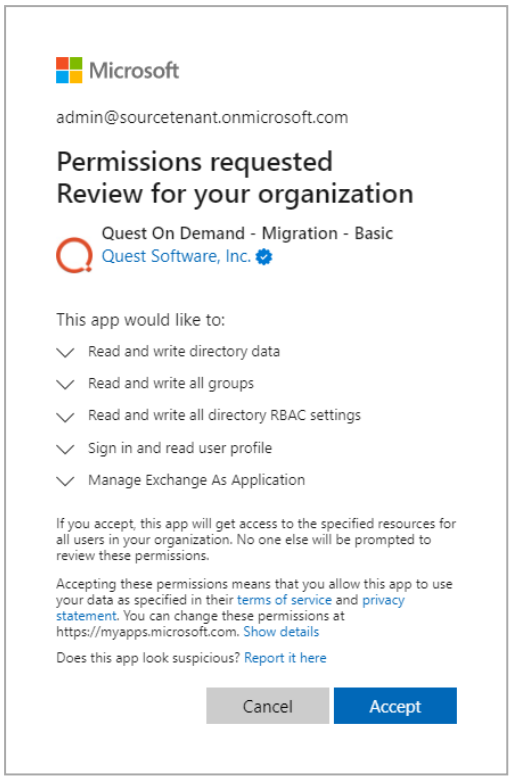
- **Quest On Demand - Core – Basic**

  These permissions are used by the Basic application, which extracts information from the user's tenant Microsoft Entra ID, such as display name, default domain name, and other properties such as B2C and cloud type.



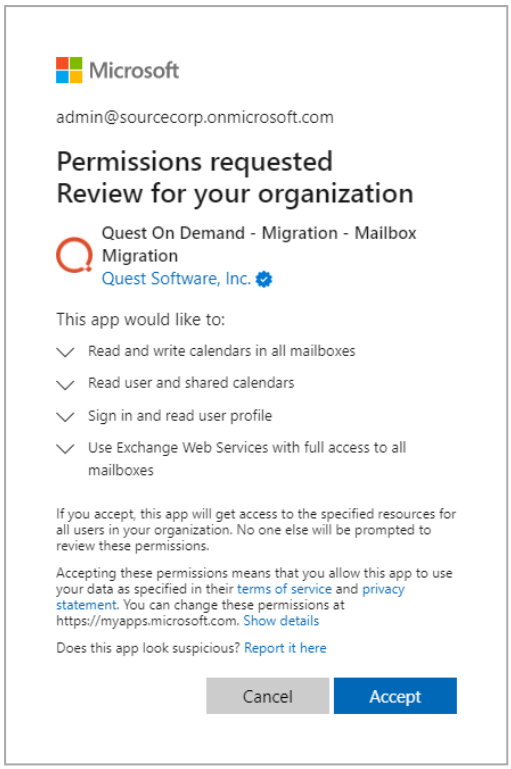
- **Quest On Demand - Migration – Basic**

The consent granted with this application allows On Demand Migration to access the Microsoft Entra ID and Exchange Online to read and write user and group in there.



- **Quest On Demand - Migration – Mailbox**

  The consent granted with this application allows On Demand Migration module to access mailboxes, calendars and Exchange Web Services to write Mailbox content to the target tenant.


Microsoft
admin@sourcecorp.onmicrosoft.com
Permissions requested
Review for your organization
Quest On Demand - Migration - Mailbox Migration
Quest Software, Inc.
This app would like to:
Read and write calendars in all mailboxes
Read user and shared calendars
Sign in and read user profile
Use Exchange Web Services with full access to all mailboxes
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

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 and all data is stored in the selected region. The currently supported regions can be found here: https://regions.quest-on-demand.com/.

Windows Azure Storage, including the Blobs, Tables, and Queues storage structures, are replicated three times in the same data center for resiliency against hardware failure. The data is replicated across different fault domains to increase availability. All replication data centers reside within the geographic boundaries of the selected region.

See this Microsoft reference for more details: https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy

8

Privacy and protection of customer data

The admin account credentials of the source email environment is an example of sensitive customer data that is collected and stored by ODMHE. These credentials are required by ODMHE to run email migration operations. ODMHE protects these credentials by storing them in Azure Key Vaults.

Customer emails, attachments ant other mailbox items are obtained from the source on-premise mailbox via Exchange Web Services (EWS) over HTTPS[1]. They are processed by Azure Batched VM in memory and then sent into target M365 by EWS Online over HTTPS.

[1] A customer has the choice of using a non-encrypted connection using HTTP. For more details, see the Network Communication topic.

9

Separation of customer data

A common concern related to cloud-based services is the prevention of co-mingling of data that belongs to different customers. The On Demand Migration architecture specifically prevents such data co-mingling by logically and virtually separating customer data stores.

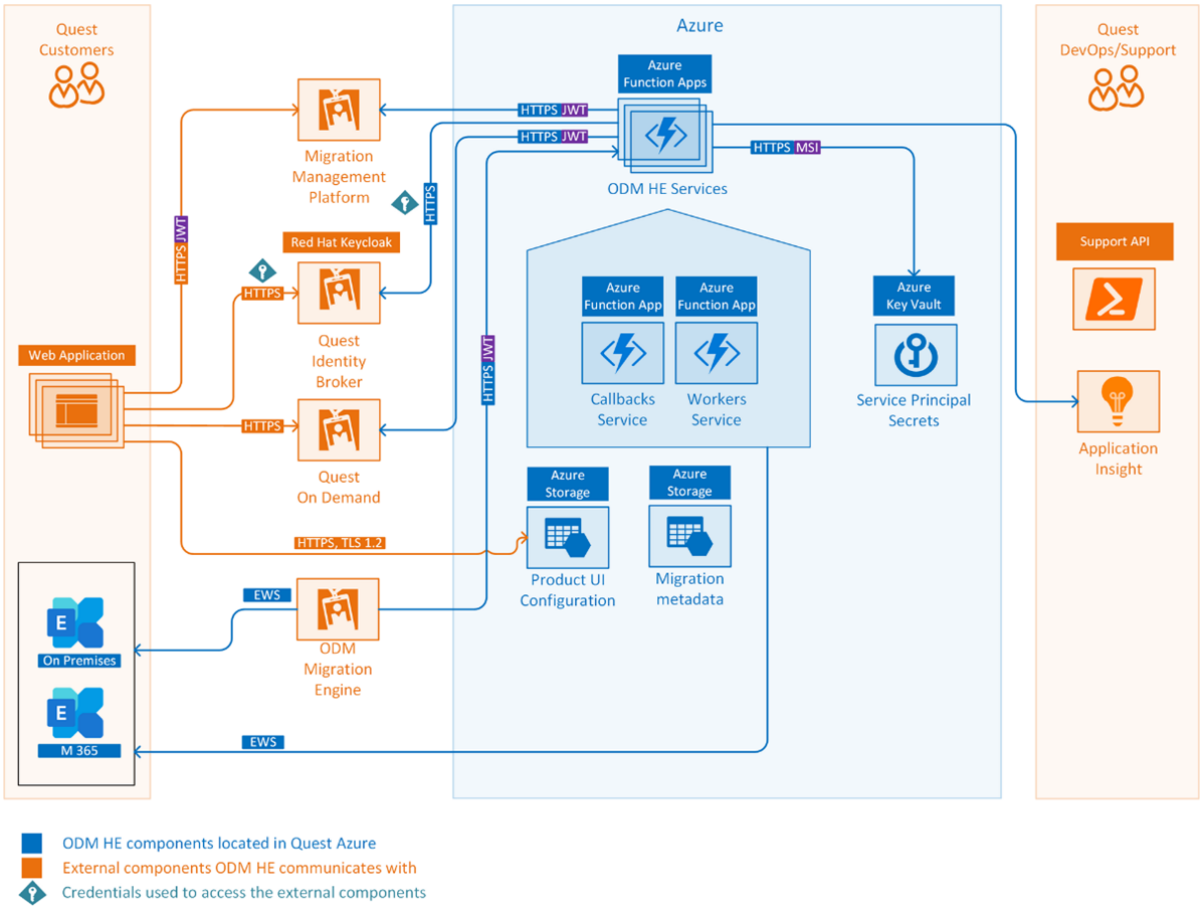
Customer data are differentiated using a Customer Organization Identifier. The Customer Organization Identifier is a unique identifier obtained from the Quest On Demand Core that is created when the customer signs up with the application.

This identifier used throughout the solution to ensure strict data separation of customers' data in Elasticsearch storage and during processing.

A separate Elasticsearch server instance is used for each customer.

Network communications

The following schema shows the communication configuration between key components of On Demand Migration for Hybrid Exchange.



The network communication is secured with HTTPS TLS 1.2.

Inter-service communication uses OAuth authentication using a Quest Microsoft Entra ID service account with the rights to access the services. No back end services of ODMHE can be used by end-users.

On Demand Services accepts the following network communication from outside Azure:

- Customer access to ODMHE web UI.
- PowerShell cmdlets accessing ODMHE back end (PowerShell cmdlets are used internally by Quest Authorized Support personnel.)

The ODMHE user interface uses OAuth 2.0 authentication with JWT token issued to a logged in user.

PowerShell cmdlets used by Quest Authorized Support personnel are using Microsoft Entra ID authentication to access the ODMHE service.

For on-premise Microsoft Exchange migrations, the default port used (during the migration) is port 443 (HTTPS). A customer has the choice of using a non-encrypted connection using HTTP. It is also possible for a customer to use non-standard ports, and specifying these port numbers in the URL (e.g. https://xyz:454).

ODMHE communicates with on-premise Microsoft Exchange servers over port 443 by default. Port 80 may be used if the customer configures their on-premise server that way.

Self-signed certificates are allowed as well when connecting to on-premises servers. Such certificate must be valid and its Issuer DN must match its Subject DN.

11

Authentication of users

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

The process of registering a Microsoft Entra ID tenant in On Demand Migration is handled through the well established Azure Admin Consent workflow. For more information about the Microsoft Entra ID Admin Consent workflow, please refer the Quest On Demand Global Settings User Guide.

12

Role based access control

On Demand Migration does provide the common authentication via Quest Identity Broker. 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 the Quest On Demand product documentation.

13

FIPS 140-2 compliance

On Demand Migration 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 team follows a strict Quality Assurance cycle.

- Access to source control and build systems is protected by domain security, meaning that only employees on Quest's corporate network have access to these systems. Therefore, should an On Demand developer leave the company, this individual 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 check in.

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

- MS-SDL best practices
- Threat modeling.
- OWASP guidelines.
- Automated static code analysis is performed on a regular basis.
- Automated 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 developers go through the same set of hiring procesdey0000ses and background checks as other Quest employees.

Third Party assessments and certifications

Penetration testing

On Demand has undergone a third-party security assessment and penetration testing yearly since 2017. The 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.

Certification

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

- 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 31st, 2023**

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

16

Operational security

Source control and build systems can only be accessed by Quest employees on Quest's corporate network (domain security.) If a developer (or any other employee with access to On Demand Migration) leaves the company, the individual immediately loses access to the systems.

All code is versioned in source control.

Access to data

Access to On Demand Migration for Hybrid Exchange data is restricted to:

- Quest Operations team members
- Particular Quest Support team members working closely with On Demand Migration product issues.
- The On Demand Migration for Hybrid Exchange development team to provide support for the product

Access to On Demand Migration for Hybrid Exchange data is restricted through the dedicated Quest Azure AD security groups. For different types 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 On Demand Migration

Quest Operations team members have access to Quest's production Azure Subscription and monitor this as part of normal day to day operations. On Demand Migration developers have no access to Quest's production Azure Subscription.

To access On Demand Migration, a customer representative opens the On Demand website and signs up for an On Demand account. The account is verified via email; thus a valid email address must be provided during registration.

An organization is automatically created once the new account is created.

Prerequisites:

Microsoft Entra ID Global Administrator must give the Admin Consent to provision On Demand Migration for Hybrid Exchange for the customer's Microsoft Entra ID with the following permissions:

Microsoft Graph

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

Windows Microsoft Entra ID

- 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 Microsoft Entra ID

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

Microsoft Graph permissions reference - Microsoft Graph | Microsoft Docs

Operational monitoring

On Demand Migration for Hybrid Exchange internal logging is available to Quest Operations and ODMHE development teams during the normal operation of the platform. Some customer or Personally Identifiable Information (PII) data can become a part of internal logging for troubleshooting purposes.

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. On Demand Migration for Hybrid Exchange relies an Azure infrastructure and as such, is subject to 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/

17

Customer measures

On Demand Migration security features are only one part of a secure environment. Customers must implement their own security practices when proceeding with data handling. Special care needs to be given to protecting the tenant credentials of the Microsoft Entra ID global administrator accounts and Office 365 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