Quest

On Demand Migration

Security Guide

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

Quest Software Inc.

Attn: LEGAL Dept

4 Polaris Way

Aliso Viejo, CA 92656

Refer to our Web site (https://www.quest.com) for regional and international office information.

Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at https://www.quest.com/legal.

Trademarks

Quest, the Quest logo, and Join the Innovation are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit https://www.quest.com/legal/trademark-information.aspx. All other trademarks and registered trademarks are property of their respective owners.

Legend

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

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

On Demand Migration Security Guide
Updated - June 2022

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 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. This includes access control, protection of customer data, secure network communication, and cryptographic standards.

About On Demand Migration

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

- Analyzes Azure Active Directory structure and highlights the problems that might adversely affect the migration.
- Migrates users, groups, and the related information between Azure AD tenants or maps the existing source/target accounts.
- Migrates hybrid accounts (on-premises users/groups synchronized with Azure AD.)
- 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.

On Demand Migration is hosted in Microsoft Azure and delivers most of its functions via Microsoft Azure cloud services.

Hybrid accounts migration works via the secure connection with Quest Migration Manager for Active Directory, installed on premises.

Architecture overview

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

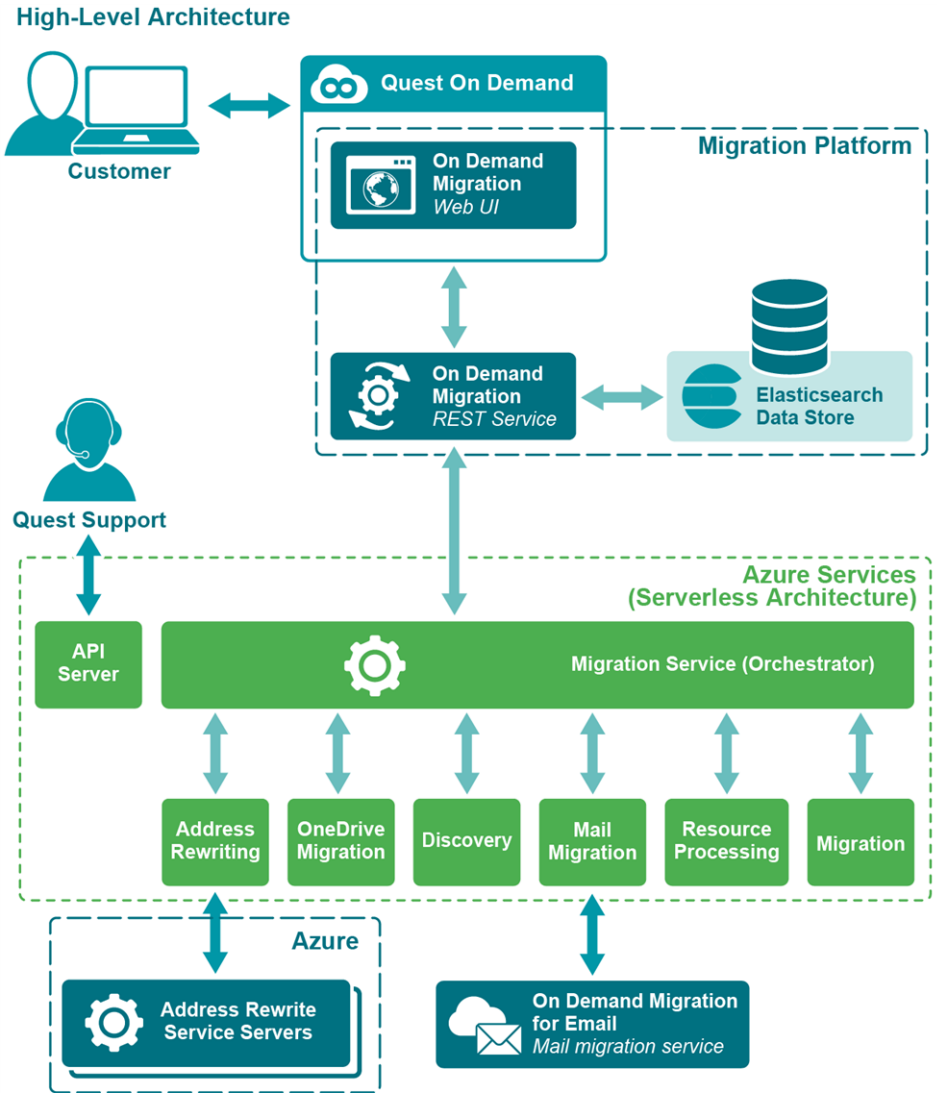


Figure 1: High-Level Architecture

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 manages the following type of customer data:

- Azure Active Directory and Office 365 users, groups and contacts with their properties returned by Azure Active Directory Graph API including account name, email addresses, contact information, department, membership and other properties. Part of the information is stored in the product database.
- Product works with end-user mailbox and OneDrive content. The content processed by the product is not persistently stored by the product. OneDrive data content is temporary stored in Azure blob storage and is encrypted at rest for the period of migrating particular OneDrive account.
- Some data from end-user mailbox/OneDrive content can be stored by the product for troubleshooting purposes. This includes data to identify the items where some troubleshooting is required, e.g., mail item subject, OneDrive file names. The data are stored in product Elasticsearch database, Azure table storage and Application Insight and is encrypted at rest.
- The application does not store or deal with end-user passwords of Azure AD objects.
- The application stores administrative account name and password to perform migration operations. The data are stored in Azure Key Vault and is encrypted at rest.

When domain coexistence is turned on, all outgoing mail traffic from the customer's source tenant is routed through Address Rewrite Service which changes the addresses in mail headers. The independent instance of Address Rewrite Service is created for each migration project.

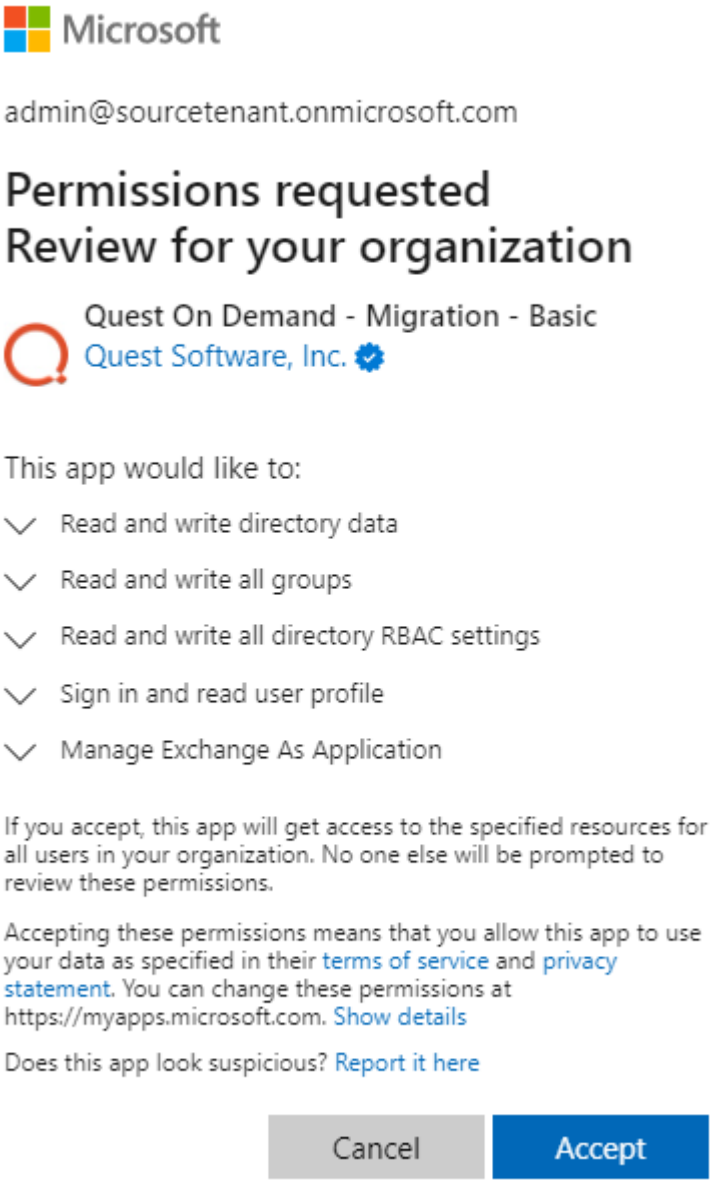
The domain coexistence can be disabled at any moment from the On Demand Migration UI, which completely removes the Address Rewrite Service from outgoing mail processing, thus all outgoing mail will be sent directly from Exchange Online.

Check On Demand Migration User Guide for the detailed list of all customer configuration changes related to Domain Coexistence.

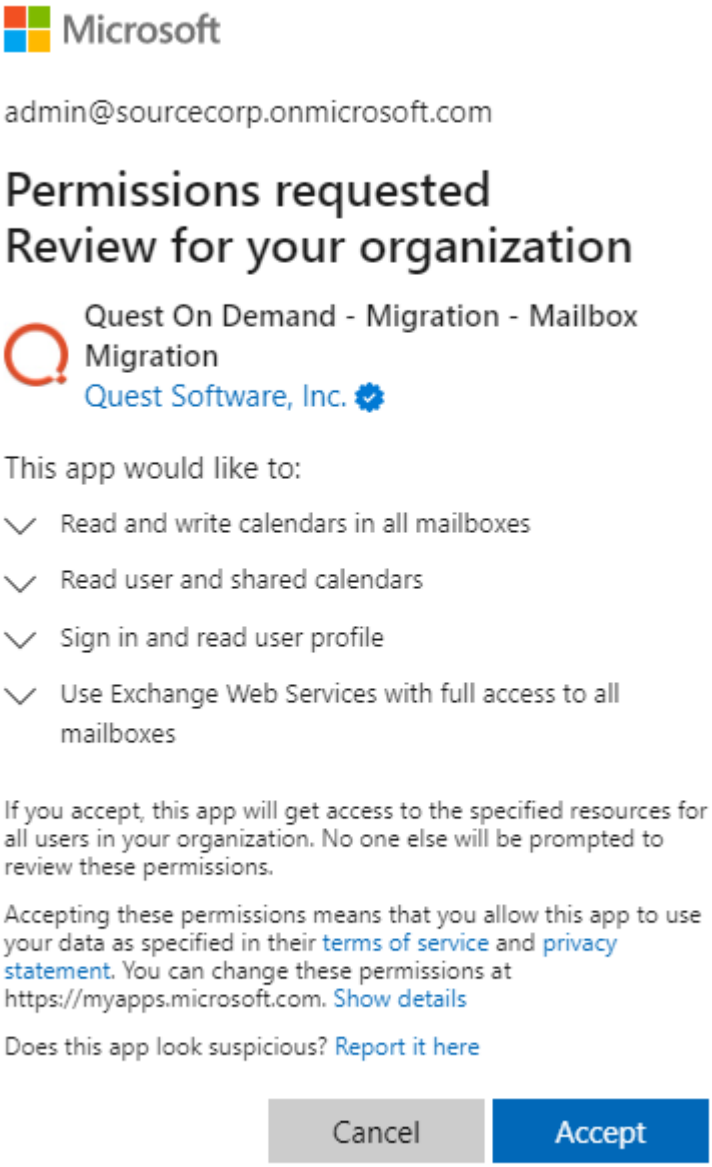
Admin Consent and Service Principals

On Demand Migration 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 Migration (Groups, Users, Contacts). 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 Migration.



In addition to the base consents required by On Demand and On Demand Migration, On Demand Migration (Email) requires the following consents:



On creating the On Demand Migration project, the Quest group is automatically added to the exchange administrator role for mailboxes.

On Demand Migration currently uses the Microsoft Exchange Online PowerShell API with support for the "limited permissions" model for Accounts, Email, SharePoint, Teams and OneDrive migrations, without needing global administrator permissions during migration. After the consent has been granted using the global administrator account, thereafter all migration operations will be driven by the token generated using app Service Principal.

The Admin Consent process of On Demand Migration (OneDrive) will create a Service Principal in the customer's Azure AD tenant with the following permissions.

- Permissions required for On Demand Migration (Groups, Users, Contacts) as per this Security Guide.
- Permissions required for On Demand Migration for SharePoint as per the *On Demand Migration for SharePoint Security Guide*.

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/.

Mail messages intended for processing by Address Rewrite Service servers are temporary stored at Azure Virtual Machine disks before being delivered to recipients. The data are encrypted at rest.

Windows Azure Storage, including the Blobs, Tables, and Queues storage structures, are replicated three times in the same datacenter for resiliency against hardware failure. The data is replicated across different fault domains to increase availability. All replication datacenters 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 most sensitive customer data processed by On Demand Migration is the Azure Active Directory and Office 365 data including users, groups and contacts and their associated properties, content of emails and OneDrive for Business. On Demand Migration does not store or deal with end-user passwords of Azure AD objects.

- Email attachments and OneDrive for Business content for a particular user is temporary stored during migration. The data are deleted once migration task for the user is finished. The data are encrypted at rest when stored.
- Mail messages processed by Address Rewrite Service are temporary stored on the disks of Azure Virtual Machine where Address Rewrite Service is deployed. Once delivered, they are deleted from mail queues and removed from the disks. The data are encrypted at rest.
- Some user, group, contact properties are stored as a part of migration project to be displayed in UI and handled correctly during migration. The data are deleted once migration project is deleted.
- All migration project data and logs are encrypted at rest.
- Hybrid accounts are processed by Quest Migration Manager for Active Directory, deployed in on-premises environment. On Demand Migration has access to the migration progress only (events, errors, etc.) Account properties and other data are not stored and processed in the cloud.

To ensure that customer data is kept separate during processing, the following policies are strictly applied in On Demand Migration:

- The data for each customer is stored in separate Azure storage containers. 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.
- A separate Elasticsearch server instance is used for each customer.
- A separate Azure Virtual Machine is used as mail transfer agent for each customer.
- On-premises deployment of Quest Migration Manager for Active Directory can be configured by customer to ensure required level of security and data protection. Refer to the Quest Migration Manager for Active Directory technical documents for details.
- The integration of On Demand Migration with Quest Migration Manager for Active Directory is secured by a secret that can be re-issued at any moment. Once re-issued, the original secret is immediately revoked.

More information about Azure queues, tables, and blobs:

- 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

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 Migration 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 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.

When domain coexistence is turned on, separate Azure Virtual Machines, Network Security Groups and inbound IP address are used as an outgoing mail transfer agent for each migration project.

Network communications

Internal network communication within Azure includes:

- Inter-service communication between On Demand Migration components, On Demand Core and the On Demand Platform
- Communication to customer Azure AD/Office 365 tenants

The following scheme shows the communication configuration between key components of On Demand Migration.

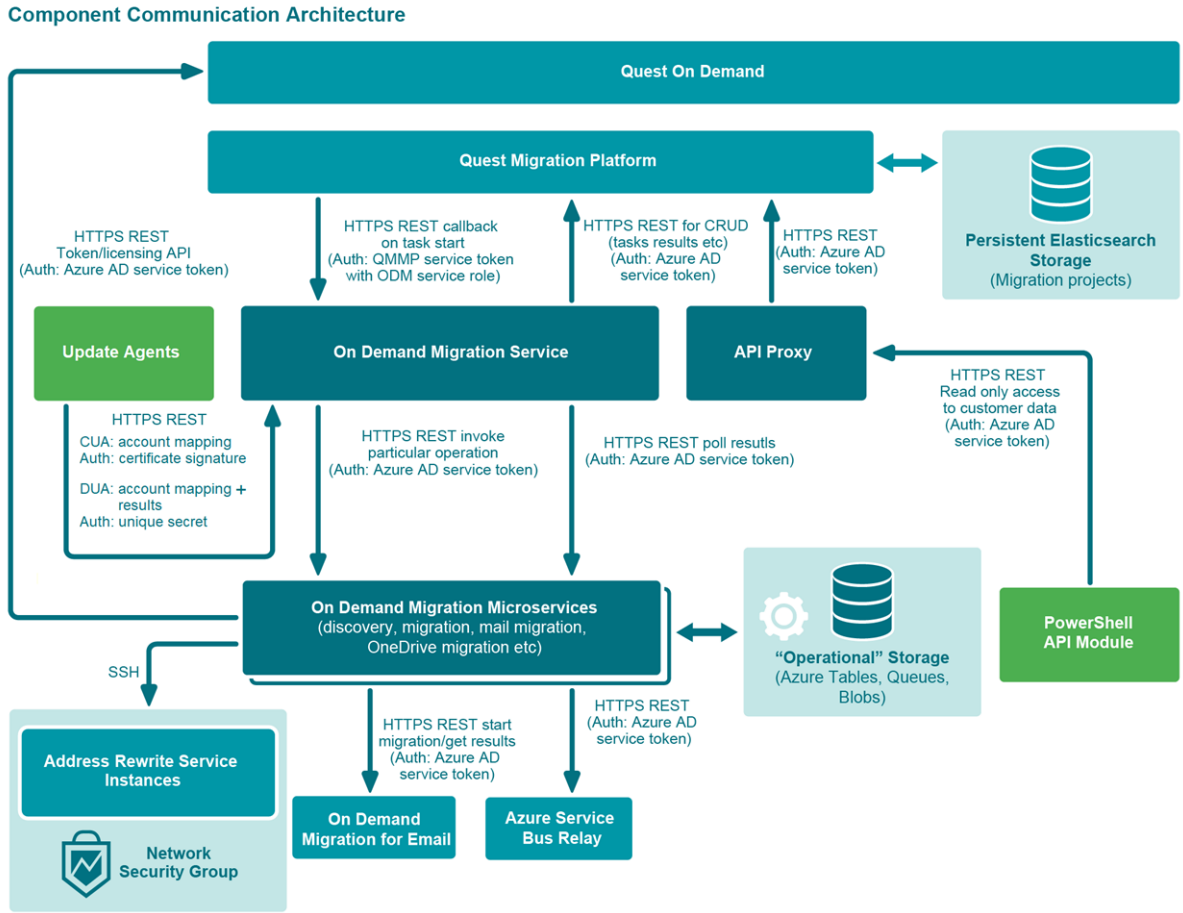


Figure 2: Component Communication Architecture

The network communication is secured with HTTPS and is not visible to the external public internet.

Inter-service communication uses OAuth authentication using a Quest Azure AD service account with the rights to access the services. No backend services of On Demand Migration can be used by end-users.

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

- Access to On Demand Migration web UI.
- Client Update Agent deployed on customer on-premise workstations accessing On Demand Migration backend.
- Desktop Update Agent deployed on customer on-premises workstations accessing On Demand Migration backend.
- PowerShell cmdlets accessing On Demand Migration backend (PowerShell cmdlets are used internally by Quest Support.)

All external communication is secured with HTTPS.

The On Demand Migration user interface uses OAuth authentication with JWT token issued to a logged in user.

All requests from Client Update Agents deployed on customer's workstations are signed with the certificate, issued by On Demand Migration. The certificate is deployed (either automatically or manually) by customer's IT specialist to each workstation's certificate store. The certificate can be revoked at any moment by generating a new one using On Demand Migration interface.

Communication between Desktop Update Agent and On Demand Migration is secured with HTTPS/TLS 1.2 and secret-based authentication.

PowerShell cmdlets used by Quest Support are using Azure AD authentication to access the On Demand Migration service. The user of the PowerShell API should be a Quest Azure AD member with the appropriate role assigned.

There are no unsecured HTTP calls within On Demand Migration.

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 Migration is handled through the well established Azure Admin Consent workflow. For more information about the Azure Active Directory Admin Consent workflow, please refer the Quest On Demand Core technical documents.

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.
- Regularly scheduled static code analysis is performed on regular basis.
- Regularly scheduled 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.

On Demand 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. 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. No OWASP Top 10 critical or high risk issues have been identified.

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 : **C710-ISMS222-07-19**, valid until **2022-07-29**.
- ISO/IEC 27017 Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services: **C711-ITCS2-07-19**, valid until **2022-07-29**.
- ISO/IEC 27018 Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors: **C712-ITPII2-07-19**, valid until **2022-07-29**.

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 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 development team to provide support for the product

Access to On Demand Migration 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 the 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:

Azure Active Directory Global Administrator must give the Admin Consent to provision On Demand Migration for the 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

Microsoft Graph permissions reference - Microsoft Graph | Microsoft Docs

Operational monitoring

On Demand Migration internal logging is available to Quest Operations and On Demand Migration development teams during the normal operation of the platform. Some customer or Personally Identifiable Information (PII) data (e.g. mail item subject, OneDrive file names, error messages reporting user names or email addresses, etc.) 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 relies an 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/

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 credentials of the Azure Active Directory tenants global administrator accounts and Office 365 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