

On Demand Migration for SharePoint

Security Guide



© 2022 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.

Contents

Introduction	1
About On Demand Migration for SharePoint	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	8
Privacy and protection of customer data	9
Separation of customer data	10
Network communications	11
Authentication of users	13
Role based access control	14
FIPS 140-2 compliance	15
SDLC and SDL	16
Third Party assessments and certifications	17
Penetration testing	17
Certification	17
Operational security	18
Access to data	18
Permissions required to configure and operate On Demand Migration	18
Operational monitoring	19
Production incident response management	19
Customer measures	20
About us	21
Technical support resources	21

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

About On Demand Migration for SharePoint

Use On Demand Migration for SharePoint to migrate Microsoft SharePoint site collections, and the sites, lists, list items, document libraries, and documents contained in the site collections, between Office 365 tenancies.

Most of these services are delivered via Microsoft Azure cloud services.

Architecture overview

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

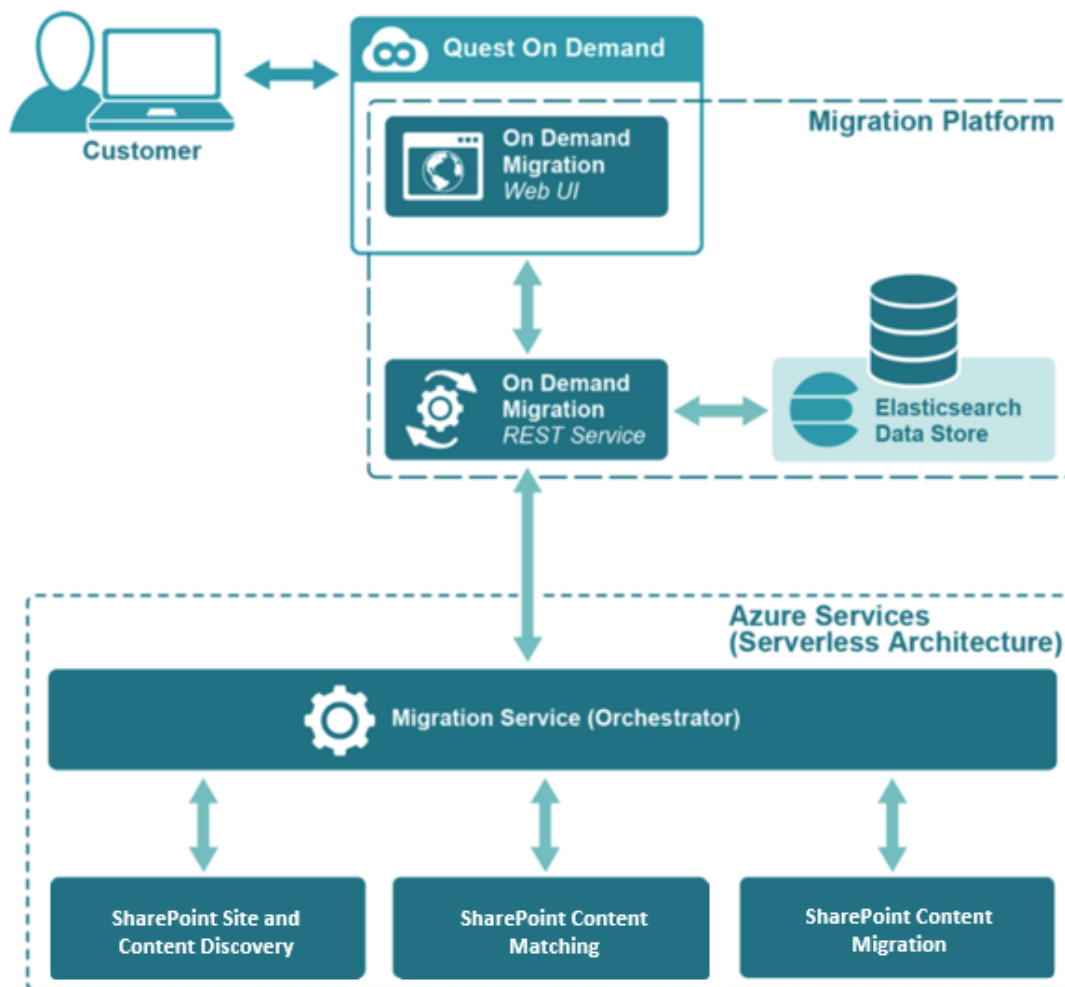


Figure 1: High-Level Architecture

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 SharePoint accesses customer SharePoint data (content) from the source tenancy and writes the data to a SharePoint site on the target tenancy.

- Metadata that defines the SharePoint site structure and properties is temporarily stored in memory and deleted when the migration is completed.
- Documents stored in the document libraries and lists of the SharePoint site are temporarily stored in Azure blob storage for the duration of the migration. The storage account is deleted when the migration is complete.
- Manifest files and associated migration log files may be retained by the application for troubleshooting purposes. Manifest files contain data to identify the list items and documents. The troubleshooting data is stored in a separate storage account. Troubleshooting data is automatically deleted after 30 days.
- The application does not require or store any passwords

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 for SharePoint. 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.

In addition to the base consents required by On Demand and On Demand Migration, On Demand Migration for SharePoint requires the following consents:



ask-admin@contoso.com

Permissions requested Review for your organization



This app would like to:

- ✓ Read and write directory data
- ✓ Read files in all site collections
- ✓ Read and write directory data
- ✓ Read and write items in all site collections
- ✓ Have full control of all site collections
- ✓ Read and write items and lists in all site collections
- ✓ Read and write managed metadata
- ✓ Read and write user profiles

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 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>

Privacy and protection of customer data

The most sensitive customer data processed by On Demand Migration for SharePoint is the SharePoint content including documents and their associated metadata.

- While the migration task is running, SharePoint documents, list items, and associated metadata, are temporary stored in Azure Blob containers. When the migration task is complete, this data is deleted.
- All migration project data and logs are encrypted at rest.

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

- 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.

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.

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.

Component Communication Architecture

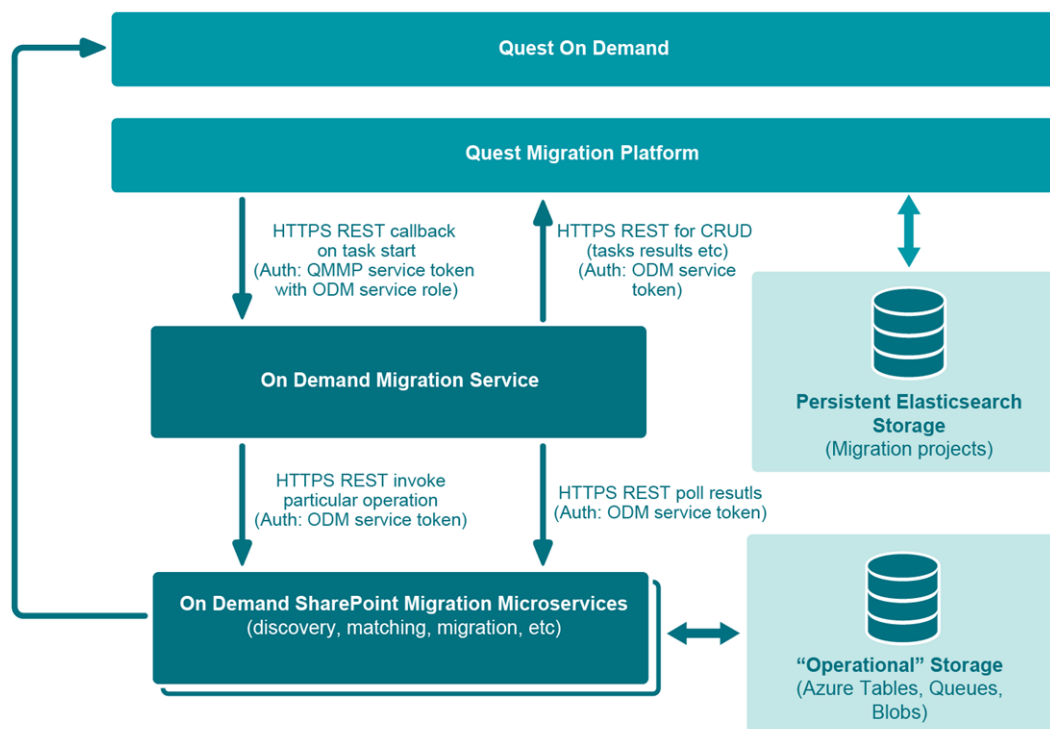


Figure 2: Component Communication Architecture

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 for SharePoint can be used by end-users.

External network communication from outside Azure to On Demand Services include:

- On Demand Migration user interface access

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.

There are no unsecured HTTP calls within On Demand Migration for SharePoint.

Authentication of users

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

The process of registering a SharePoint Office 365 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](#).

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>

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.

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 for SharePoint 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 SharePoint development team to provide support for the product

Access to On Demand Migration for SharePoint 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 SharePoint for the customer's Azure Active Directory with the following permissions:

OAuth 2.0 Permission Grants

Microsoft SharePoint Online

- Read and write directory data (Microsoft Graph)
- Read files in all site collections (Microsoft Graph)
- Read and write directory data (Windows Azure Active Directory)

- Read and write items and lists in all site collections (Office 365 SharePoint Online)
- Read and write managed metadata (Office 365 SharePoint Online)
- Read and write user profiles (Office 365 SharePoint Online)
- Read and write items in all site collections (Office 365 SharePoint Online)
- Have full control of all site collections (Office 365 SharePoint Online)

[Microsoft Graph permissions reference - Microsoft Graph | Microsoft Docs](#)

Operational monitoring

On Demand Migration for SharePoint internal logging is available to Quest Operations and On Demand Migration for SharePoint development teams during the normal operation of the platform. Some customer or Personally Identifiable Information (PII) data (e.g. document names, URLs, Metadata, error messages, 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 for SharePoint 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/>

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.

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