Quest® On Demand Migration

Hybrid Content Matrix Security Guide

© 2023 Quest Software Inc. ALL RIGHTS RESERVED.

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

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

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

Quest Software Inc.

Attn: LEGAL Dept

4 Polaris Way

Aliso Viejo, CA 92656

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

Patents

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

Trademarks

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

Legend

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

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

On Demand Migration - Hybrid Content Matrix Security Guide
Updated - December 07, 2023

Contents

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

About On Demand Migration - Hybrid Content Matrix

On Demand Migration - Hybrid Content Matrix combines the powerful functionality of Metalogix® Content Matrix with the easy-to-use, cloud-based interface of On Demand for performing migrations of SharePoint on premises site collections to SharePoint Online.

You can enter all of the information needed to perform a migration tasks in On Demand, which includes discovering site collections, discovering and mapping users, selecting the site collection you want to migrate, and configuring and running the migration.

That information is then passed from On Demand to Content Matrix, which is installed in a SharePoint on-premises environment, for processing. Results are then returned to On Demand.

Architecture Overview

The following scheme shows the key components of the On Demand Migration – Hybrid Content Matrix configuration. Please refer to the Metalogix Content Matrix Security Guide for components of Metalogix® Content Matrix.

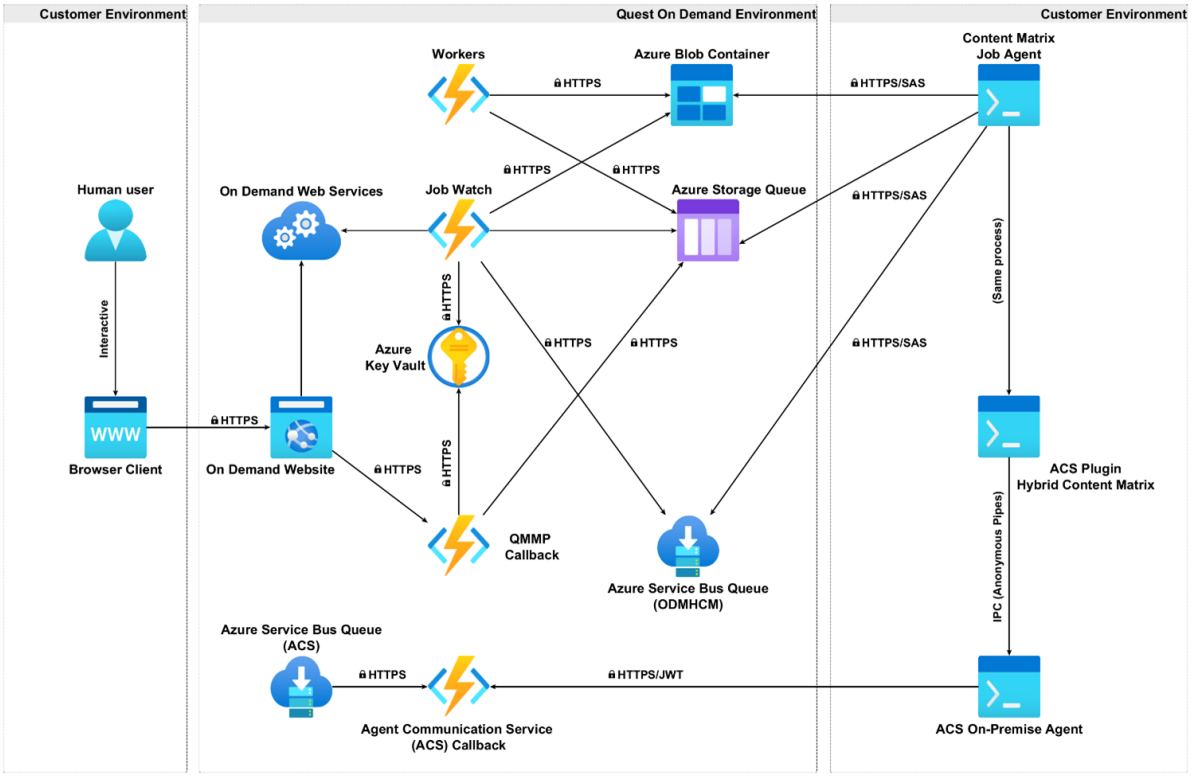


Figure 1: High-Level Architecture

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 - Hybrid Content Matrix

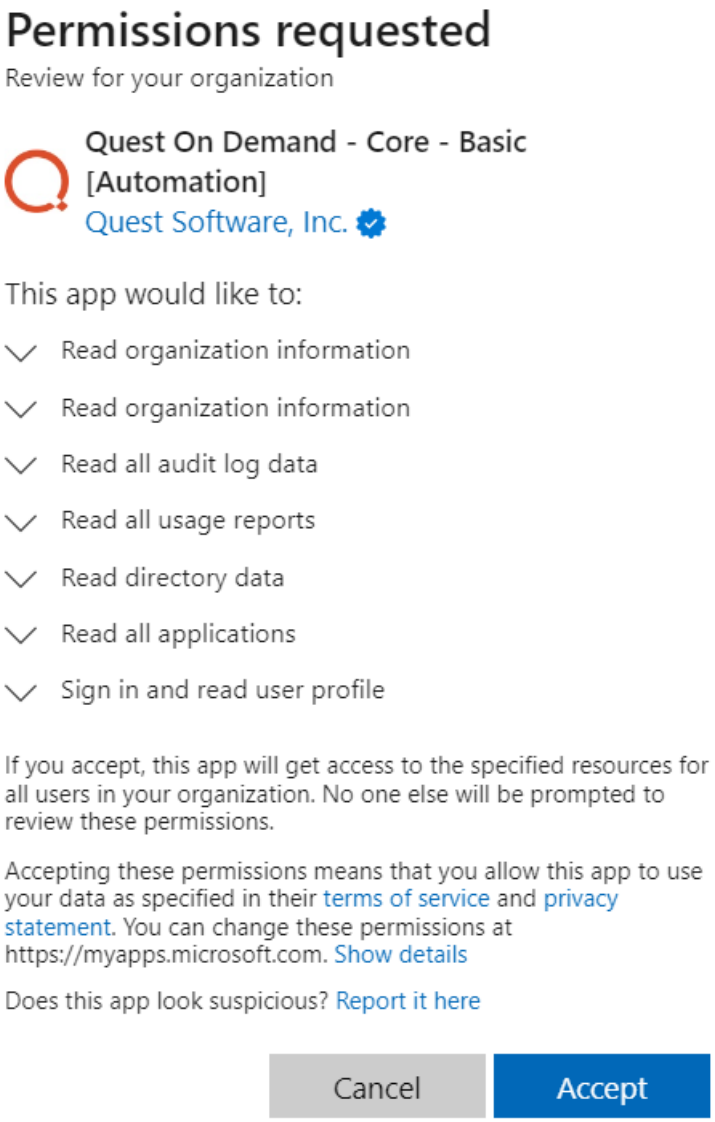
On Demand Migration – Hybrid Content Matrix manages the following type of customer data:

- SharePoint content. The content processed by the product is not persistently stored by the product. When a SharePoint 2013 or later database connection is used as source, large file content is fetched and temporarily stored in file system (on-premises) before it is copied to the target. Advanced Encryption Standard (AES) algorithm is used to encrypt this content.
- Some data from end-user SharePoint content can be stored by the product for troubleshooting purposes. This includes data to identify the items where some troubleshooting is required.
- The application stores administrative account name and password of source connection to perform migration operations. The data is stored in SQL database and is encrypted at rest (please refer to “Privacy and Protection of Customer Data” chapter for more details).
- The application does not store or deal with end-user passwords of Azure AD objects.

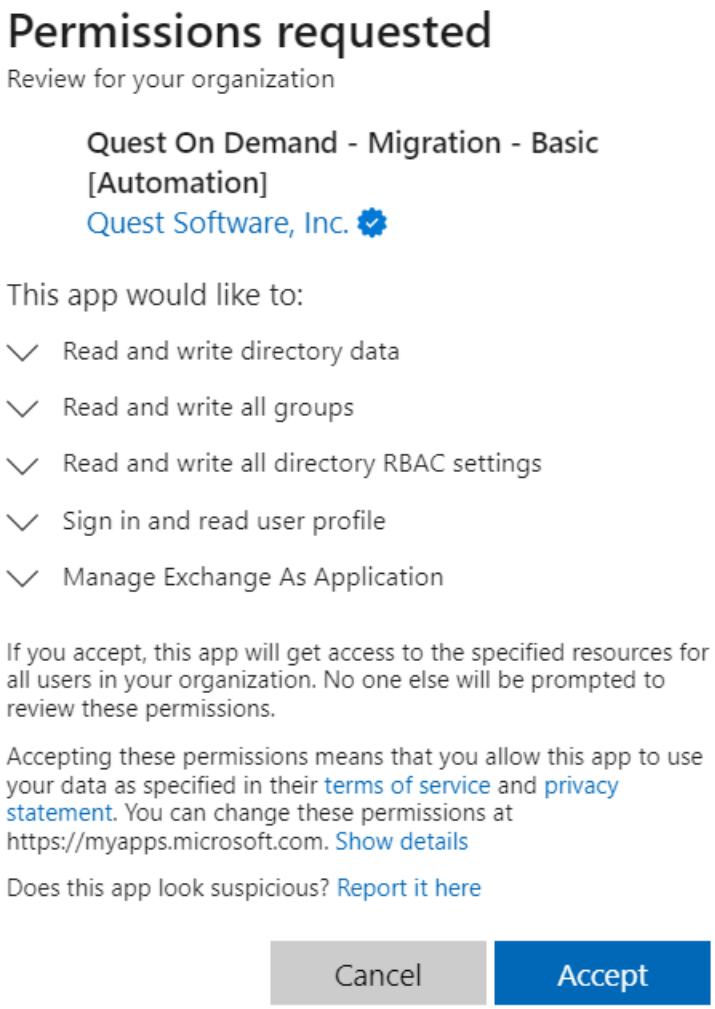
Admin Consent and Service Principals

On Demand Migration – Hybrid Content Matrix 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 – Hybrid Content Matrix (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.

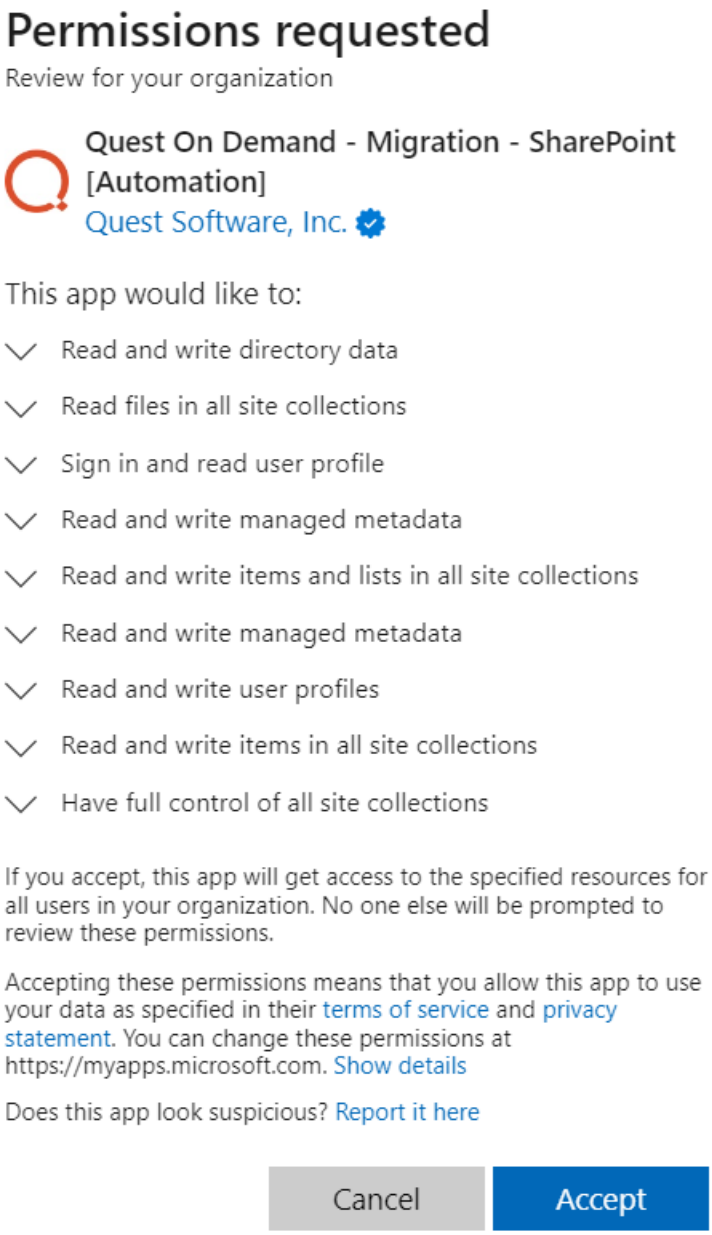
Following is the base consent required by On Demand Migration – Hybrid Content Matrix. These permissions are used by Basic application, which extracts information from user's Azure AD tenant such as display name, default domain name, and other properties such as B2C and cloud type.



In addition to the base consents On Demand Migration – Hybrid Content Matrix requires the following consents (Quest On Demand - Migration – Basic).The consent granted with this application allows On Demand Migration access to Azure Active Directory and Exchange Online to read and write user and group in



Another set of consents is Quest On Demand - Migration – SharePoint. These consents are required for SharePoint migrations. They allow On Demand Migration module to access Azure Active Directory and SharePoint Online to write SharePoint content to the target tenant.


Permissions requested
Review for your organization
Quest On Demand - Migration - SharePoint [Automation]
Quest Software, Inc.
This app would like to:
Read and write directory data
Read files in all site collections
Sign in and read user profile
Read and write managed metadata
Read and write items and lists in all site collections
Read and write managed metadata
Read and write user profiles
Read and write items in all site collections
Have full control of all site collections
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 computations of Azure cloud services are performed and all data is stored in the selected region. The currently supported regions can be found here https://regions.quest-on-demand.com/.

Content Matrix Job Agent performs computations on server provided by the customer. All data and application logs are stored in an SQL server or file provided by the customer.

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

Content Matrix Job Agent components use MS DPAPI (PBKDF2, AES) for encryption of connection credentials (passwords for source connection), and OAuth tokens to target SharePoint connections.

SharePoint Database Connections

When a SharePoint 2013 or later database connection is used as source, large file content is fetched and temporarily stored in file system (on-premises) before it is copied to the target. Advanced Encryption Standard (AES) algorithm is used to encrypt this content, with key size 128 bits (AES-128).

Azure Import Pipeline

In order to migrate on-premises source SharePoint site to target (SharePoint Online, SPO), Azure Import Pipeline is used. Refer to the Migrating to SharePoint Online Using the Import Pipeline help topic of Metalogix® Content Matrix for more details of support objects and actions.

Note, that for ODMHCM product, Azure Private Containers are not available (as they are in Metalogix® Content Matrix migration), and SPO Provided Azure Containers will be used. That is the default container which is provided to tenant while using the migration API. Note, that once a container is given to tenant this container will not be reused or shared.

- When the Import Pipeline is used, security-sensitive information about azure blob storage SASS URLs stored with Microsoft DPAPI encryption.
- The files uploaded to Azure storage are encrypted with Advanced Encryption Standard (AES) algorithm (AES-128).

Job Database Connection Credentials

On premises SQL database or Azure SQL database could be used as a Job Database. While connecting to database, the user could enable encrypted connection to database. In that case, TLS/SSL encrypted connection will be established. Job database (SQL Server) connection credentials are encrypted with Microsoft DPAPI and are stored by Metalogix® Content Matrix locally (on premises).

To ensure that customer data is kept separate during processing on ODM, the following policies are strictly applied in On Demand Migration – Hybrid Content Matrix:

- 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.

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 – Hybrid Content Matrix 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

he following scheme shows the communication configuration between key components of On Demand Migration – Hybrid Content Matrix.

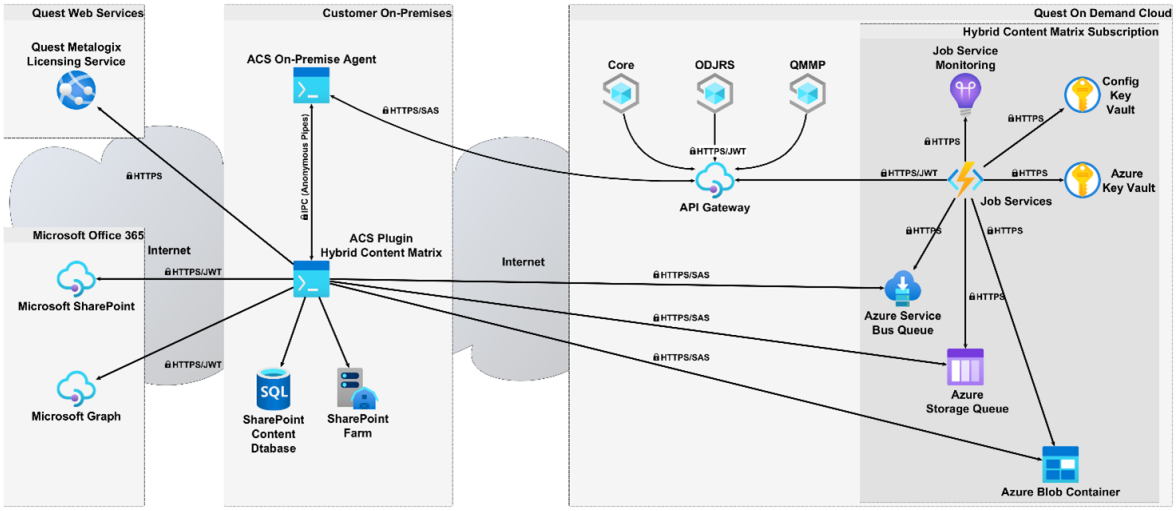


Figure 2: Component Communication Architecture

The network communication is secured with HTTPS.

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 – Hybrid Content Matrix can be used by end-users.

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

- Access to On Demand Migration – Hybrid Content Matrix web UI.
- ODJRS Agent running on customer on-premises workstations which updates ACS Hybrid Content Matrix plugin.
- ACS Hybrid Content Matrix plugin accessing to Azure resources (job queue, job storage, message queue)
- PowerShell cmdlets accessing On Demand Migration – Hybrid Content Matrix backend (PowerShell cmdlets are used internally by Quest Support.)

All external communication is secured with HTTPS.

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

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

Authentication of Users

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

The process of registering an Azure AD tenant into On Demand Migration – Hybrid Content Matrix 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.

Also, Metalogix® Content Matrix module relies upon Windows Authentication and Active Directory group membership to authenticate users.

Role Based Access Control

On Demand Migration – Hybrid Content Matrix is configured with default roles that cannot be edited or deleted, and also allows users 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 – Hybrid Content Matrix 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

Content Matrix Job Agent utilizes Metalogix® Content Matrix functions, and Metalogix® Content Matrix itself has undergone a Quest internal Self-Affirmation process to confirm that all cryptographic usage relies exclusively on Third-Party FIPS 140-2 validated modules.

More information:

- Microsoft and FIPS: https://www.microsoft.com/en-us/trustcenter/compliance/fips

SDLC and SDL

The On Demand Migration – Hybrid Content Matrix 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 the On Demand Migration – Hybrid Content Matrix 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 Migration – Hybrid Content Matrix Development team follows a managed Security Development Lifecycle (SDL) which includes:

- MS-SDL best practices
- Threat modelling.
- 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 Migration – Hybrid Content Matrix 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.

Certification

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

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

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

Examination Scope: **Quest On Demand Platform**

Selected SOC 2 Categories: **Security**

Examination Type: **Type 2**

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

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

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 – Hybrid Content Matrix) 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 – Hybrid Content Matrix data is restricted to:

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

Access to On Demand Migration – Hybrid Content Matrix 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 - Hybrid Content Matrix

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 – Hybrid Content Matrix developers have no access to Quest's production Azure Subscription.

To access On Demand Migration – Hybrid Content Matrix, 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 – Hybrid Content Matrix for the customer's Azure Active Directory with the following permissions:

Microsoft Graph

- Read organization information
- Read all audit log data
- Read all usage reports

- Read directory data
- Read all applications
- Read and write directory data
- Read and write all groups
- Read and write all directory RBAC settings
- Read files in all site collections

Office 365 SharePoint Online

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

Office 365 Exchange Online

- Manage Exchange As Application

Microsoft Graph permissions reference - Microsoft Graph | Microsoft Docs

In order to create connection to tenant from Metalogix® Content Matrix, the following consents are granted

Microsoft Graph

- Have full control of all site collections

Office 365 SharePoint Online

- Have full control of all site collections
- Read and write user files
- Run search queries as a user
- Read and write managed metadata
- Read user profiles

Operational Monitoring

On Demand Migration – Hybrid Content Matrix internal logging is available to Quest Operations and On Demand Migration – Hybrid Content Matrix 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 – Hybrid Content Matrix 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/

Customer Measures

On Demand Migration – Hybrid Content Matrix 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 tenant 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