Quest

Quest® On Demand Group Management

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.

On Demand Group Management Security Guide
Updated - May 2022

Contents

3

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 Group Management, which includes access control, protection of customer data, secure network communication, and cryptographic standards.

About On Demand Group Management

On Demand Group Management is a cloud-based service on Azure, which provides group management services for Office 365 tenants and Hybrid Active Directory as a Service (SaaS) product solution. The core services provided are outlined in the following diagram.

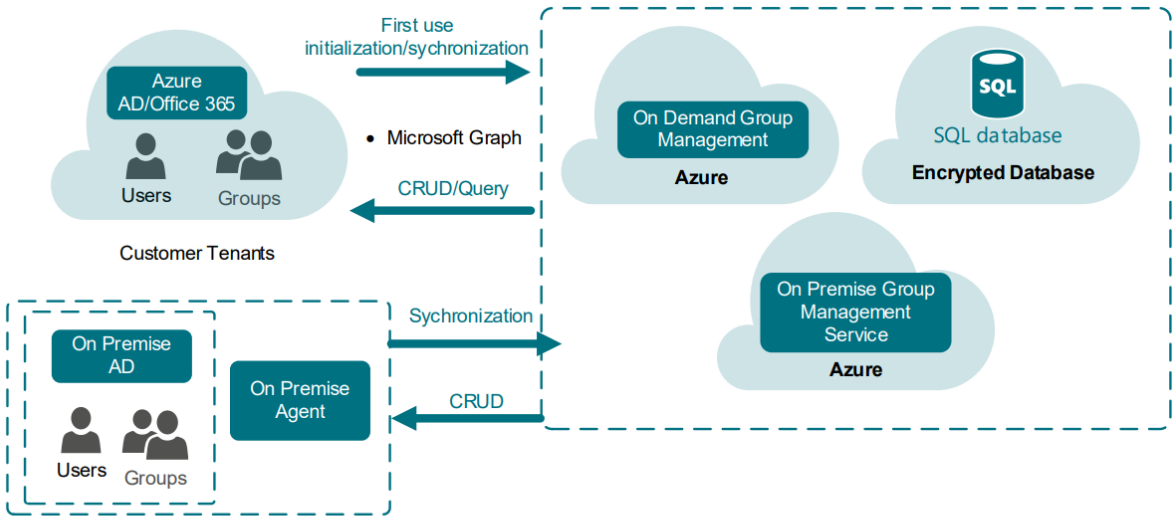


Figure 1: Core services of On Demand Group Management

Azure AD

Administration:

Administrators can manage, browse, and search Office 365 groups.

End-User Self-Service:

Users can create or manage groups and distribution lists. All these processes are controlled by management approval workflow.

Approval Workflow:

Administrators can manage and customize request approval workflow procedures for end-users who are requesting groups.

Attestation:

Users can periodically ensure their membership in the group or the group's existence.

Report:

The portal has a suite of modern visualizations to interactively show analytical data.

Hybrid Active Directory

Administration:

Administrators can manage, browse, and search groups within hybrid AD (also known as On-premises AD where AADC is enabled).

End-User Self-Service:

Users can manage Hybrid AD groups. All these processes are controlled by management approval workflow.

Approval Workflow:

Administrators can manage and customize request approval workflow procedures for end-users who are requesting Hybrid AD groups.

Attestation:

Users can periodically ensure the membership in the group is accurate or the group existence is necessary.

Architecture overview

The following schemes shows the key components of the On Demand Group Management configuration.

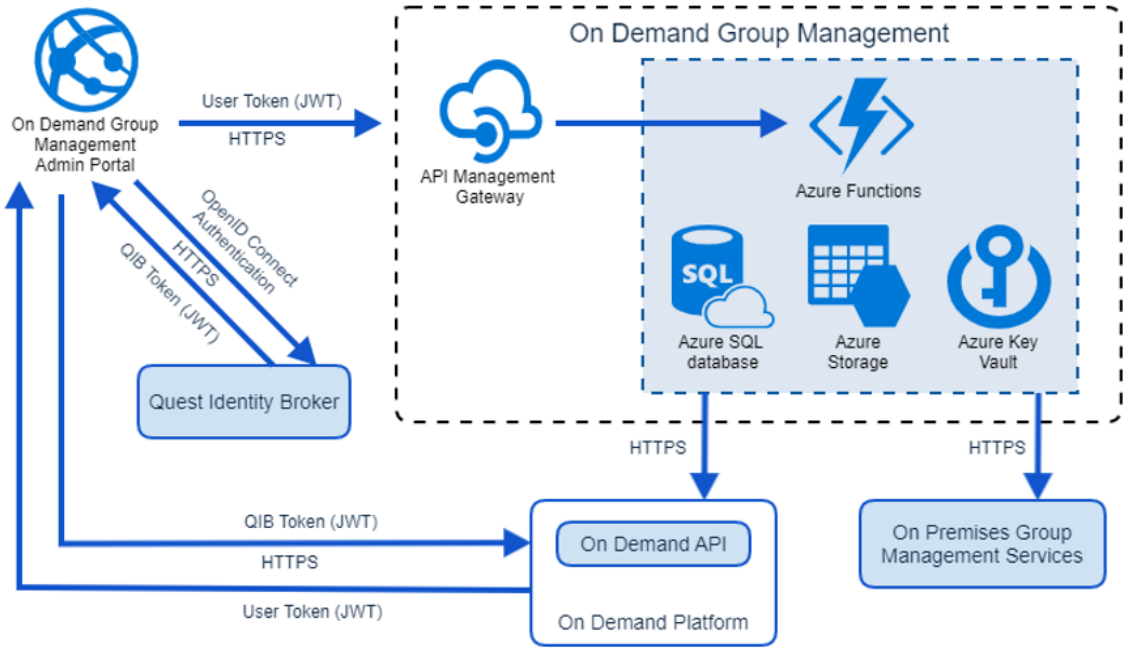


Figure 2: Admin Portal Architecture Diagram

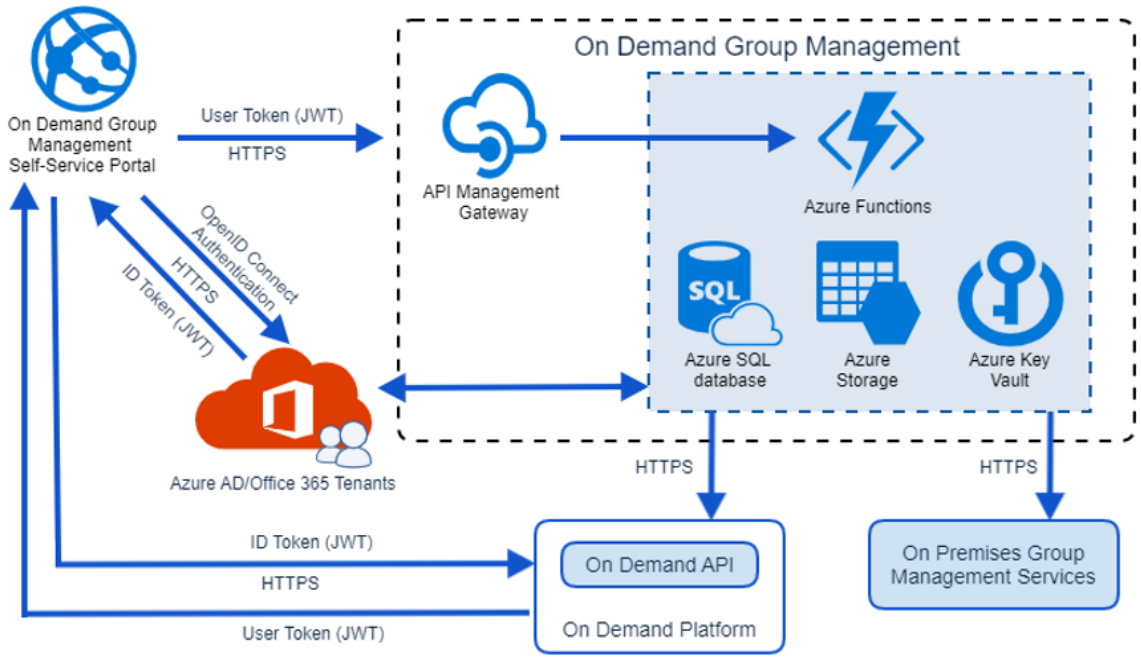


Figure 3: End-User Self Service Architecture Diagram

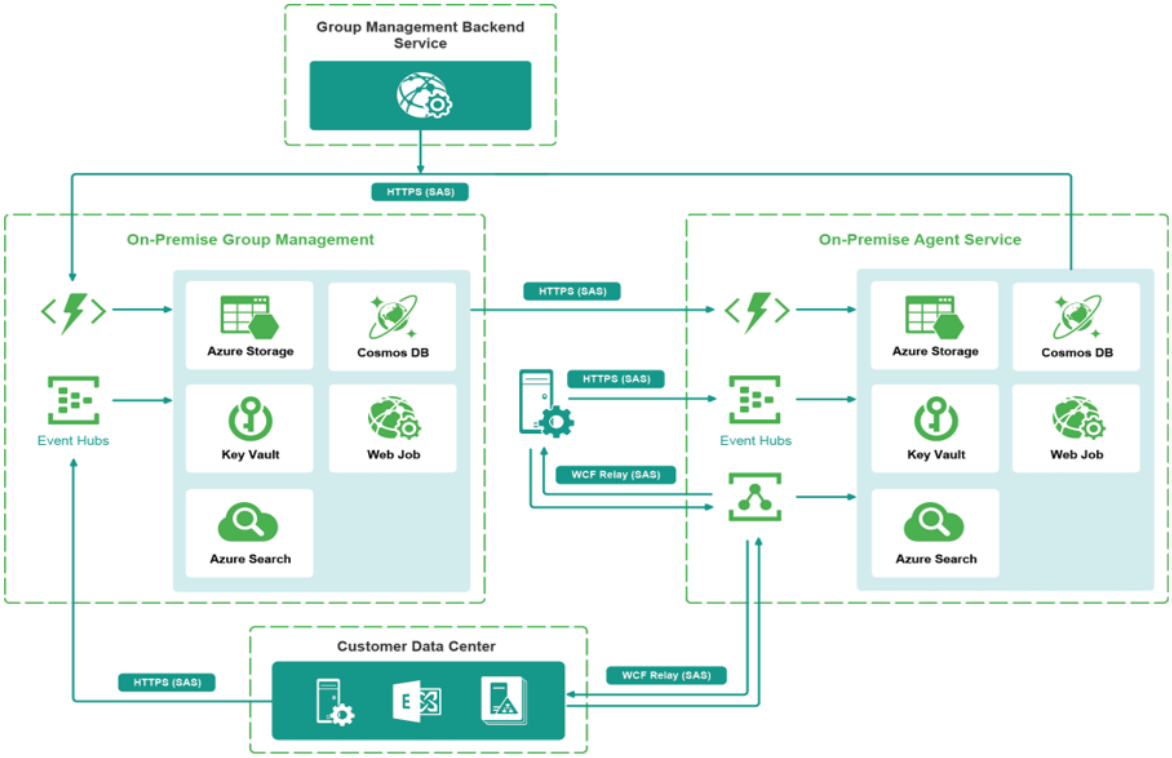


Figure 4: On-Premises Group Management Architecture

6

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/v
- 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/
- Whitepaper: Standard Response to Request for Information – Security and Privacy:http://www.microsoft.com/en-us/download/details.aspx?id=26647
- Microsoft Global Datacenters: Security & Compliance: https://www.microsoft.com/en-us/cloud-platform/global-datacenters
- Azure data-at-rest Encryption Best Practices: https://microsoft.com/en-us/azure-security-data-encryption-best-practices
- 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 Group Management

On Demand Group Management takes advantage of Microsoft Graph API to manage and store customer's Azure Active Directory and Office 365 users, groups, membership, and so on. On Demand Group Management manages the following types of customer data:

- On Demand Group Management stores customer's data, such as Azure Active Directory user/group information, naming rules, security levels, categories, and son on, in Azure SQL database.
- On Demand Group Management stores intermediate data for functionality, such as to request payload, data to be processed and son on, in Azure tables and blobs.
- On Demand Group Management stores Office 365 Service Account in Azure Key Vault as remote PowerShell credentials to manage Distribution Lists and Mail-enabled Security Groups.

On Demand Hybrid Group Management uses Microsoft WCF Service to manager and store customer's Active Directory users/groups, organizations, domains, group memberships, and so on. On Demand Hybrid Group Management manages the following types of customer data:

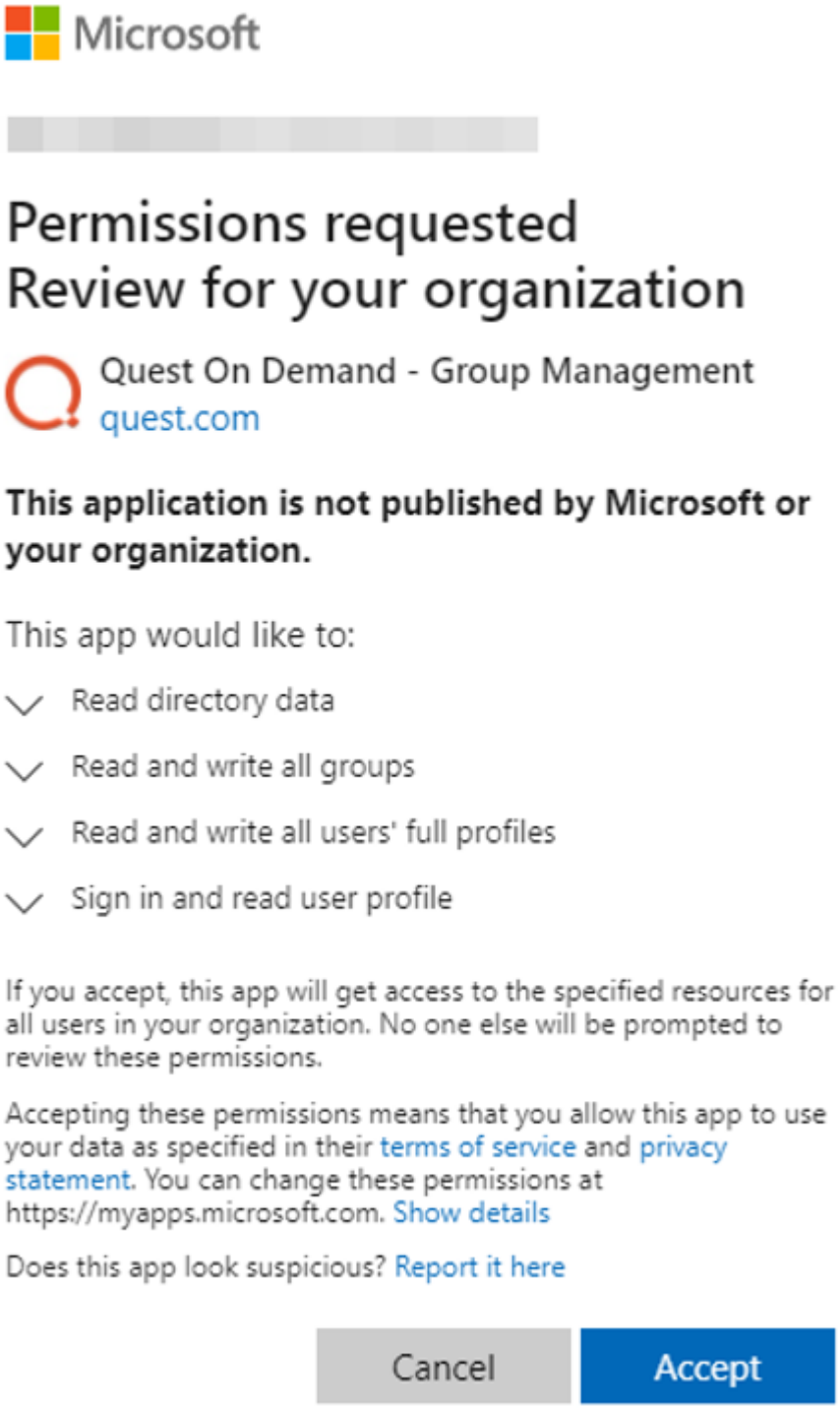
- On Demand Hybrid Group Management stores customer's data, such as on-premises Active Directory user/group information, organization information, domain information, synchronization information, and so on, in Azure Cosmos DB.
- On Demand Hybrid Group Management stores intermediate data for functionality, such as request payload, data to be processed and so on (excluding password), in Azure message queues
- On Demand Hybrid Agent Service stores the Active Directory Administrator account and Exchange Service credentials in Azure Key Vaults to synchronize Active Directory user/group information.

8

Admin Consent and Service Principals

On Demand Group Management requires access to the customer’s Azure Active Directory. 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 Group Management (Groups, Users). 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-pps/delete-application-portal and https://docs.microsoft.com/en-us/skype-sdk/trusted-application-api/docs/tenantadminconsent for details.

The following is the base consent required by On Demand Group Management.


Microsoft
Permissions requested
Review for your organization
Quest On Demand - Group Management
quest.com
This application is not published by Microsoft or your organization.
This app would like to:
Read directory data
Read and write all groups
Read and write all users' full profiles
Sign in and read user profile
If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.
Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. You can change these permissions at https://myapps.microsoft.com. Show details
Does this app look suspicious? Report it here
Cancel
Accept

9

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/.

- On Demand Group Management stores customer data in Azure SQL database, Azure Cosmos DB (Hybrid only) and Azure Table, Queues (Hybrid only), Blobs, Key Vault – encrypted at rest, in Azure US (West US 2), CA (Canada Central), EU (North Europe), UK (UK South), AU (Australia East) datacenter.

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

Customer data is differentiated and separated by customer's organization and customer's tenant. Each organization has its own organization ID(GUID). Tenant data is differentiated by Office 365 Tenant ID (GUID). The database stores the customer's data, including Azure Active Directory and Office 365 users, groups, and their associated properties. The Azure SQL database and Azure Storage where the customer's data is stored, protected, and encrypted by Azure SQL database and Azure Storage encryption at rest.

Customer data is differentiated and separated by customer's organization and customer's tenant. Each organization has its own organization ID(GUID). Tenant data is differentiated by Office 365 Tenant ID (GUID). The database stores the customer's data, including Azure Active Directory and Office 365 users, groups, and their associated properties. The Azure SQL database and Azure Storage where the customer's data is stored, protected, and encrypted by Azure SQL database and Azure Storage encryption at rest.

For more information about Azure Cosmos DB database, Azure SQL Database, and Azure Storage encryption at rest, click the following links:

- https://docs.microsoft.com/en-us/azure/cosmos-db/database-encryption-at-rest
- https://docs.microsoft.com/en-us/azure/storage/common/storage-service-encryption
- https://docs.microsoft.com/en-us/azure/azure-sql/database/transparent-data-encryption-tde-overview?tabs=azure-portal

11

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 Group Management has architected its solution to specifically prevent such data commingling by logically separating customer data.

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

This identifier is used throughout the solution to ensure strict data separation of customers' data in Azure SQL database and during processing.

12

Network communications

All external communications are secured with HTTPS (TLS 1.2) to theOn Demand Group Management User Interface. No internal service can be accessed without a valid JWT token. See Figure 2 and Figure 3 for the communication paths using HTTPS.

- The external HTTPS certificate for On Demand Group Management End-user self service uses a level 2 domain certificate for *.quest-on-demand.com by GoDaddy.
- There are no unsecured HTTP calls within On Demand Group Management.

For authentication, the communication between a customer's browser and the Quest Identity Broker is secured using HTTPS. The browser securely stores the access tokens and transmits the access token to the On Demand application using HTTPS when making authenticated REST calls.

The Group Management on-premises agents communicate via the Azure WCF Relay service. This service communicates via TCP using HTTPS and ports 5671 and 9532. All communications between the On-Premises management service and the agent requires a valid shared-access-signature (SAS).

13

Authentication of users

The customer of Azure Active Directory logs in to the End-user self-service portal by providing their own Office 365 Tenant account credentials (Microsoft OAuth 2.0 authorization code flow).

The customer logs in to the On Demand Group Management Admin Portal by providing On Demand user account credentials.

Customer login is authenticated by independent region service.

14

Role based access control

On Demand Group Management 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 to the Quest On Demand product documentation.

15

FIPS 140-2 compliance

On Demand Group Management cryptographic usage is based on Azure FIPS 140-2 compliant cryptographic functions.

On Demand Group Management FIPS 140-2 compliance refers to Azure FIPS 140-2 at https://www.microsoft.com/en-us/trustcenter/Compliance/FIPS.

Microsoft and FIPS: https://docs.microsoft.com/en-us/compliance/regulatory/offering-FIPS-140-2?view=o365-worldwide

16

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.

17

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**.

18

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 Group Management) 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 Group Management data is restricted to Quest Operations team members. On Demand Group Management developers have no access to customer production data.

Permissions required to configure and operate On Demand Group Management

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 Group Management developers have no access to Quest's production Azure Subscription.

To access On Demand Group Management, 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 Group Management for the customer's Azure Active Directory with the following permissions:

Microsoft Graph

- Read directory data
- Read and write all groups
- Read and write all users' full profiles

Windows Azure Active Directory

- Sign in and read user profile

Operational monitoring

On Demand Group Management internal logging is available to Quest Operations and On Demand Group Management development teams during the normal operation of the platform. No customer or Personally Identifiable Information (PII) data is placed in internal logging and this is reviewed as part of the SDL process.

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 Group Management 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/

Security incident response management

Quest has established a formal process of preparation, detection, analysis, containment, eradication, recovery, and post-incident activities for theOn Demand Group Management solution. In accordance with intentional privacy laws, Quest has established a Security Breach Notice process as well.

19

Customer measures

On Demand Group Management security features are only one part of a secure environment. Customers must implement their own security practices when proceeding with data recovery. Special care needs to be given to protecting the credentials of the Azure Active Directory tenants global administrator accounts and the Active Directory 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