Quest™

On Demand License Management
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 website (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 www.quest.com/legal.

Trademarks

Quest and the Quest logo are trademarks and registered trademarks of Quest Software Inc. in the U.S.A. and other countries. For a complete list of Quest Software trademarks, please visit our website at www.quest.com/legal. Microsoft, Active Directory, ActiveSync, Excel, Lync, and Skype are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. All other trademarks, servicemarks, registered trademarks, and registered servicemarks are the 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, **NOTE**, **TIP**, **MOBILE**, or **VIDEO:** An information icon indicates supporting information.

UC Analytics Security Guide
Updated - May 2022

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 Quest On Demand License Management. This includes access control, protection of customer data, secure network communication, and cryptographic standards.

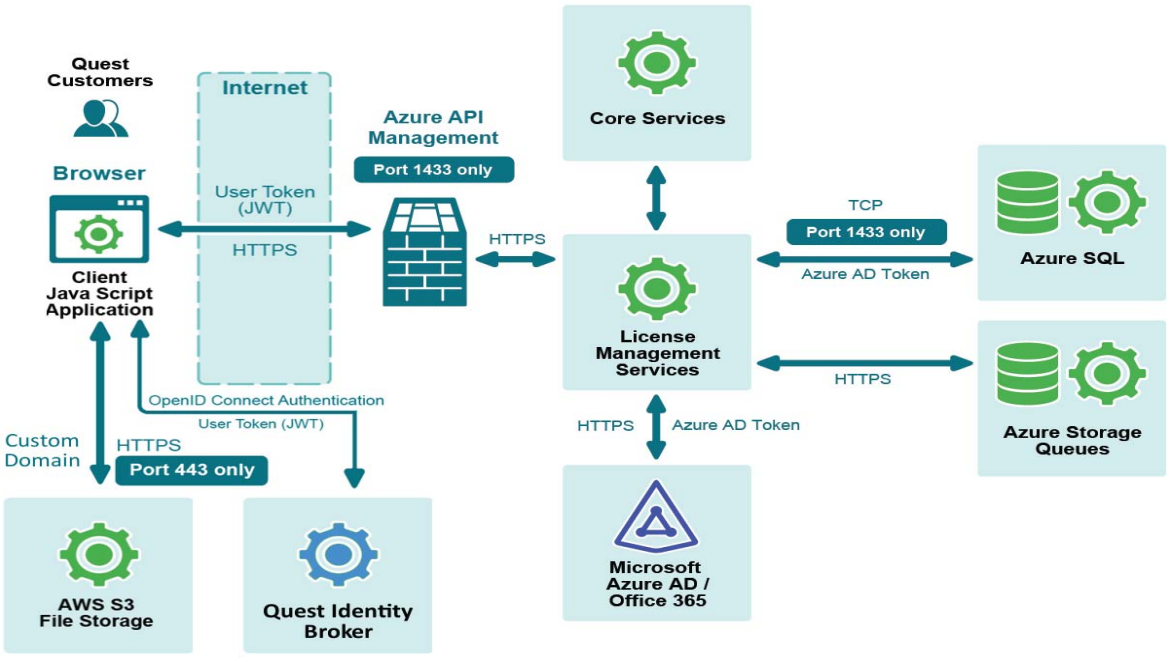
About On Demand License Management

On Demand License Management is a cloud based service that provides license management services for Office 365 tenants. License Management optimizes your Office 365 license investment by identifying cost saving measures and areas of underutilization to get more return from existing licenses.

The majority of these services are delivered via Microsoft Azure cloud services. The exception being the user interface, which is delivered using Amazon Web Services CDN network.

On Demand License Management is dependent on On Demand Core.

Figure 1. License Management architecture diagram.



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 are listed below.

- Azure Trust Center: https://azure.microsoft.com/en-us/support/trust-center/
- Microsoft Trust Center Compliance: https://www.microsoft.com/en-us/TrustCenter/Compliance?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://docs.microsoft.com/en-us/azure/security/azure-security-data-encryption-best-practices

Overview of data handled by License Management

Each relational database module defines roles for services and grants granular access rights to a single database schema. Those object-level permissions include select grant for views and table valued functions and execute for stored procedures.

The data synchronization process ingests AAD data into staging tables using Bulk Copy and is discarded immediately. Data is not persistent or cached in transit.

For all users, On Demand License Management requests and stores the following data:

- UserId
- GroupId
- GroupName
- Group Membership
- SubscribedSkus
- On Premises Distinguished Name

For groups, the following data is also requested and stored:

- On Premises Domain Name
- On Premises Security Identifier

In addition to the above, for users with a trial or paid subscription, On Demand License Management requests and stores the following data:

- User Display Name
- User Principal Name (UPN)
- Email
- Department
- State, Province, and Country.

The User Display Name is used for searching. Email is displayed in user details. Department, Province, and Country are used for filtering, sorting, and data grouping for analytical purposes. The UPN is used for matching with data in the usage data report. The usage data report is pulled daily from Graph API and contains Product Name, UPN, and Last Used Date.

On Demand License Management keeps the Directory Tenant ID for data sync purposes and token retrieval from On Demand. The tenant domain name is used for tenant identification during internal troubleshooting and is not exposed in the API.

Location of customer data

When a customer signs up for On Demand, they select the Microsoft Azure region in which to run their On Demand organization. All computation is performed in and all data is stored in the selected region. The currently supported regions are the United States, Canada, European Union, United Kingdom, and Australia. Other regions may be added over time. For the most up-to-date information, see https://regions.quest-on-demand.com/ .

Windows Azure Storage, including the Blobs, Tables and Queues storage structures, by default 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/storage-redundancy.

Privacy and protection of customer data

When a Microsoft Global Administrator adds a tenant to On Demand, they must grant admin consent for a set of permissions. The basic permission setting for all modules is Directory.ReadAll. On Demand modules require additional permissions depending on the tasks performed.

Any user that signs into On Demand and adds a tenant can view basic License Management data for their tenant. With a trial or paid subscription to License Management, users have access to additional license data and features. The On Demand License Management module requires admin consent for the Reports.Read.All permission setting in order to read product usage reports.

Network Communication

All network communications are executed using HTTPS. Compute nodes are enforced to use TLS 1.2 and don't support fallback to previous versions. All other protocols such as http, ftp, ftps, msdeploy, and msvsmon are explicitly disabled. All ports are explicitly disabled.

All connections to the Azure SQL Database are encrypted (TLS/SSL) at all time. Connections are set to force encryption and disable server certificate trust.

For authentication, all communication between a customer browser and the Quest Identity Broker is secured using HTTPS. The browser securely stores the session access and refresh tokens and transmits the access token to the On Demand application using HTTPS when making authenticated REST calls. For further details see the On Demand Core and Notification Service Security Guide.

Authentication of Users

For information on user authentication, see the *On Demand Core and Notification Service Security Guide*.

To view an architecture diagram, see About On Demand License Management.

On Demand License Management does not store any credentials in configuration files or database tables. All communication with the database is based on System Managed Identities. Database connection strings never include credentials and use Azure AD Authentication only.

FIPS 140-2 compliance

On Demand License Management cryptographic usage is based on Azure FIPS 140-2 compliant cryptographic functions. On Demand License Management makes use of FIPS 140-2 compliant encryption provided in the Microsoft Azure Cloud services that On Demand License Management uses.

For more information, see

- Microsoft and FIPS:https://docs.microsoft.com/en-us/compliance/regulatory/offering-FIPS-140-2?view=o365-worldwide
- Encryption in the Microsoft Cloud: https://docs.microsoft.com/en-us/office365/securitycompliance/office-365-encryption-in-the-microsoft-cloud-overview
- Azure Storage: https://docs.microsoft.com/en-us/azure/storage/common/storage-security-guide

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:

- 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

Access to data

Access to On Demand Core data is restricted to Quest Operations team members. On Demand developers have no access to customer production data.

Permissions required to configure and operate

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

Operational Monitoring

On Demand internal logging is available to Quest Operations and On Demand 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 relies on Azure and AWS 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/
- AWS services status page is available at https://status.aws.amazon.com/

Security incident response management

For its On Demand solution, Quest has established a formal process of preparation, detection, analysis, containment, eradication, recovery, and post-incident activities. As well, in accordance with international privacy laws, Quest has established a Security Breach Notice process.

Customer measures

On Demand License Management security features are only one part of a secure environment. Customers must implement their own security best practices.

About us

Quest provides software solutions for the rapidly-changing world of enterprise IT. We help simplify the challenges caused by data explosion, cloud expansion, hybrid datacenters, security threats, and regulatory requirements. We are a global provider to 130,000 companies across 100 countries, including 95% of the Fortune 500 and 90% of the Global 1000. Since 1987, we have built a portfolio of solutions that now includes database management, data protection, identity and access management, Microsoft platform management, and unified endpoint management. With Quest, organizations spend less time on IT administration and more time on business innovation. 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.