Quest

On Demand Core Services

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.

On Demand Core Security Guide
Updated - March 2024

Contents

About On Demand Shared Services

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 core services such as the On Demand Notification Service and other shared services. This includes access control, protection of customer data, secure network communication, and cryptographic standards.

About On Demand Core

On Demand Core is a cloud-based service that provides core services to other Quest Software as a Service (SaaS) product solutions.

The core services provided are as follows:

- Uniform user interface experience
- Microsoft Entra tenant registration and authorization (administrator consent)
- Common auditing and logging
- Quest Identity Broker integration for secure and seamless Single Sign-On (SSO) across all Quest SaaS products
- Notifications to other Quest SaaS products about key events, such as tenant registration
- Subscription management (records of purchases)
- Connectivity to on-premises Active Directory domains in hybrid environments to perform management activities
- Common storage services allowing storage and fast ad-hoc searching of big data in the form of activity data or snapshot data collected from integrated On Demand services.
- Services for providing alerting on changes to data stored with common storage services.

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

About the On-Premises Agent

The Quest On Demand On-Premises Agent provides On Demand connectivity to on-premises Active Directory domains in hybrid environments to perform management activities such as modifying group memberships and collecting Active Directory object attribute data. All On-Premises Agent communication with On Demand is secured by means of a MQTT-based Shared Access Signature (SAS) token authenticated connection.

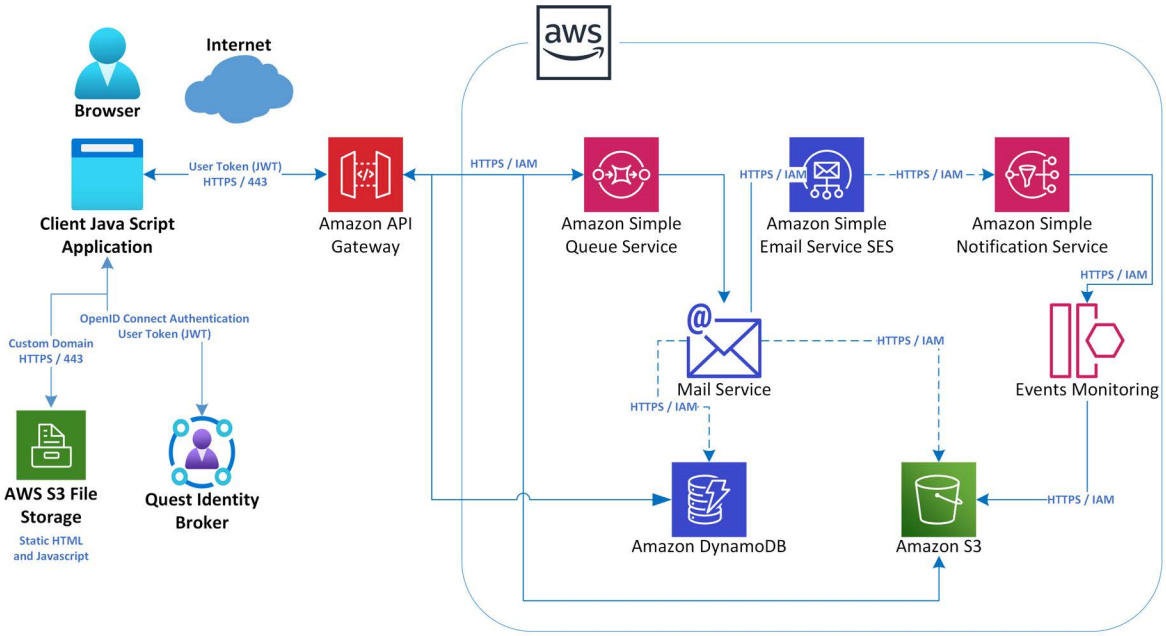
For more information about adding and configuring the On-Premises Hybrid Agent, see the “Adding an on-premises agent” section of the *Quest On Demand Global Settings User Guide*.

About the Notification Service

On Demand Notification Service (ODNS) is a cloud based service that provides core services to other Quest Software as a Service (SaaS) product solutions. The core service provided is email notifications. Every email sent by the Notification Service is scanned for viruses and malware.

This service is delivered via Amazon Web Services.

Figure 1. Notification architecture diagram



About the Data Egress Service

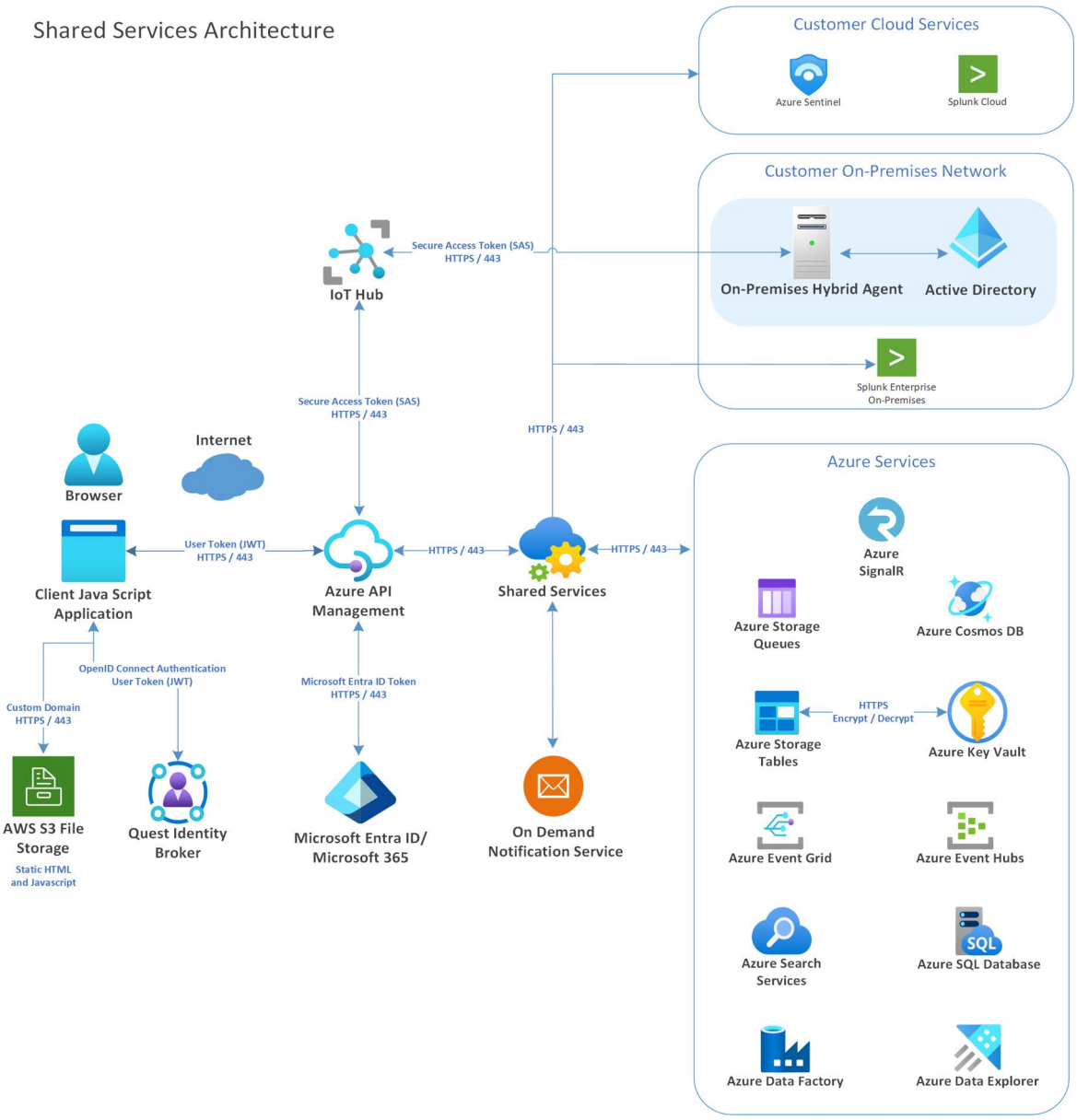
On Demand Data Egress Service (ODDE) is cloud based service delivered through Azure Services, which provides functionality to transfer incoming events to given destination.

Data egress service enables customers to set up event forwarding to SIEM Tools like Splunk, Sentinel or via Email Notifications.

Email forwarding leverages Notification Service (ODNS) to deliver emails.

Architecture Overview

The following schema shows the key shared components of the On Demand configuration.



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

AWS Datacenter Security

Amazon Web Services (AWS) 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 SOC 1, SOC 2 and ISO/IEC 27001:2005.

Relevant references with additional information about the AWS data center security are listed below.

- AWS Security and Infrastructure: https://aws.amazon.com/products/security/
- AWS Compliance: https://aws.amazon.com/compliance/

Overview of Data Handled by On Demand Core

This section describes how On Demand core services handle data.

Data Handled by Core

Managed Data Types

On Demand Core manages the following types of customer data. By default, the data is persisted in On Demand Core.

- Microsoft Entra Tenant Name
- Microsoft Entra Subscription Active Directory Object Id (GUID)
- Microsoft Entra Administration Consent Token
- Microsoft Entra User Object Identifiers (GUID)
- Microsoft Entra Group Object Identifiers (GUID)
- Audit log of On Demand Core user activities, including user name in email form (name@domain.com)

Quest Identity Broker

The Quest Identity Broker (QIB) stores the following personally identifiable information in its database:

- user email address
- user first name
- user last name

In addition, the QIB stores the unique identifier for each user account as provided by the Quest account database, Microsoft Entra ID, or Microsoft Live account during the authentication process. QIB creates an audit trail log for all interactions, including login, logout, and account creation. Access to the log is restricted to QIB administrators.

Subscription Services

The Subscription Service stores customer contact information and can process credit card transactions associated with subscription purchases and renewals.

- Cybersource is the credit card payment gateway. Cybersource receives the necessary information required for purchase transactions. Required fields are as follows:
  - credit card number

    - expiration date
    - name
    - address
    - email address
- Tradesphere is the trade compliance system. Tradesphere receives name, address, and country information.
- Salesforce is the subscription billing system. Salesforce receives all the product details along with the customer billing and shipping information that is required for invoicing. In addition, customer quotes are quoted in Salesforce using the account, contact, and product details housed in Salesforce. Orders are billed and invoiced through Salesforce billing. Details of a new subscription, subscription amendment, and subscription renewal orders are passed to the On Demand platform for the purposes of provisioning tenant environments on the On Demand platform.

Data Handled by the Notification Service

On Demand Notification Service manages customer email addresses. Every email sent by the Notification Service is scanned for viruses and malware.

All request data sent to On Demand Notification Service is persisted by default. This includes the notification recipients as well as any data placed inside the notification template. For more information about what customer data could be included in a notification, please refer to the security information for the relevant module.

Data Handled by Common Storage Services

Customer search configurations for both shared and private searches. This includes any user entered data that are used to parameterize the search.

Customer alerting configurations for both shared and private alert rules. This includes the email address of the receipts of alert emails.

- Activity data and object data collected from any configured tenants and on-premises environments originating from On Demand modules using Common Storage Services. For further details on data handled and stored, see the the On Demand Audit and Security Guardian Security Guides.

Admin Consent and Service Principals

As part of the on-boarding of the your organization into the On Demand solution, you (the customer) do not need to sign up for Quest account before going to On Demand. You can login with your Microsoft account to On Demand and your Quest account is automatically created. When your account is created with Quest, an On Demand organization is not automatically created. You must explicitly create your On Demand organization.

As part of the sign-up process, you (the customer) must provide a valid email address to receive and respond to a verification email from Quest Software.

On Demand Core requires some access to Microsoft Entra ID. You grant that access by using the Microsoft Admin Consent process. Customers can revoke Admin Consent at any time. See https://msdn.microsoft.com/en-us/skype/trusted-application-api/docs/tenantadminconsent.

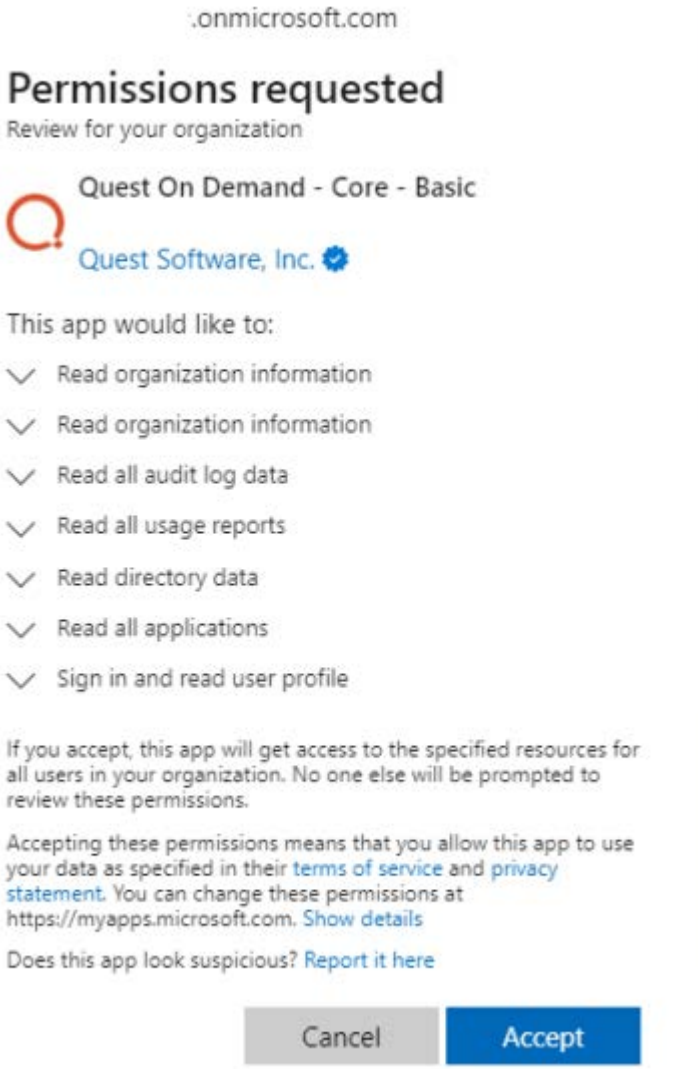
Quest is a Microsoft Verified Publisher and, as an additional security measure during the Admin Grant process, the customer can verify that the grant request is indeed initiated by Quest.

Details on Verified Publisher are available at https://learn.microsoft.com/en-us/entra/identity-platform/publisher-verification-overview.

The Admin Consent process of On Demand Core - Basic will create a Service Principal in the customer Microsoft Entra tenant with the following permissions.

- Read organization information
- Read all audit log data
- Read all usage reports
- Read directory data
- Read all applications
- Sign in and read user profile

Figure 2. Microsoft permissions needed for tenant.



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 in and all data is stored in the selected region. The currently supported regions can be found https://regions.quest-on-demand.com/.

On Demand customer data is stored in the selected On Demand region, entirely within Azure Services provided by Microsoft. For more information, see Achieving Compliant Data Residency and Security with Azure.

For US Organizations:

- All On Demand data is stored and processed within the United States, using a single Azure Datacenter. Azure “West US 2” is used for all processed data within On Demand. For disaster recovery duplicate copies of all data are stored in Azure “East US 2” and Azure “Central US”.

For Europe Organizations:

- All On Demand data is stored and processed within the European Union, using a single Azure Datacenter. Azure “Northern Europe” is used for all processed data within On Demand. For disaster recovery duplicate copies of all data are stored in Azure “Western Europe”.

For UK Organizations:

- All On Demand data is stored and processed within the UK, using a single Azure Datacenter. Azure “UK South” is used for all processed data within On Demand. For disaster recovery duplicate copies of all data are stored in Azure “UK West”.

For Canada Organizations:

- All On Demand data is stored and processed within Canada, using a single Azure Datacenter. Azure “Canada Central” is used for all processed data within On Demand. For disaster recovery duplicate copies of all data are stored in Azure “Canada East”.

For Australia Organizations:

- All On Demand data is stored and processed within Australia, using a single Azure Datacenter. Azure “Australia East” is used for all processed data within On Demand. For disaster recovery duplicate copies of all data are stored in Azure “Australia Southeast”.

Azure

Windows Azure Storage, including the Blobs, Tables and Queues storage structures, by default get 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.

AWS

All computation is performed in and all data is stored in the selected region. The only exception is transportation and delivery of email notifications for the Canada region is done through the US due to AWS Simple Email Service region availability. Amazon S3 and DynamoDB data is stored redundantly for resiliency against hardware failure. All replication datacenters reside within the geographic boundaries of the selected region.

See these AWS references for more details:

- https://aws.amazon.com/s3/details/#durability

- https://aws.amazon.com/s3/details/#security

Quest Identity Broker

Authentication Services are provided to On Demand by the Quest Identity Broker. The QIB is hosted in multiple availability zones in Azure US region and database backup and transaction logs are replicated to another Azure region for increased availability. Data is stored in an Azure Database for PostgreSQL Flexible Server.

Subscription Services

Subscription services are provided to On Demand through a combination of internal software and our partners CyberSource, TradeSphere, and Salesforce, all of which are in the US.

Privacy and Protection of Customer Data

Customer data is differentiated using a unique organization identifier. This organization identifier is generated securely during customer sign-up. This organization identifier is passed to the user interface via a tamper proof (signed) token (JSON Web Token). This is passed with all requests made and is used to provide the organization context for all back-end services. The signed token (JSON Web Token) has a 'Time to Live' of 5 minutes and must be refreshed and re-authorized at this time. Failure to do so results in access being lost to On Demand Core.

The most sensitive customer data collected and stored by On Demand Core is the refresh token for Microsoft Entra ID. This token is only accessible by service accounts. The user cannot access this token. This token is protected through encryption within the Azure Key Vault service. The process of encryption and decryption is transparent to On Demand Core.

Quest Software employees and Microsoft employees do not have access to and cannot see the keys used for encryption and decryption. The process of encryption and decryption is transparent to On Demand and takes place between the Azure Key Vault Service and Azure Storage Tables. The keys are stored in a Hardware Service Module within the Azure Key Vault which is FIPS-2 level validated by Microsoft Azure. These keys are rotated hourly. For more information, see: https://azure.microsoft.com/en-us/services/key-vault/.

Customer data passed within a notification to the Notification Service is stored but cannot be retrieved.

Separation of Customer Data

For Azure Data Explorer, each organization is contained within a separate database ensuring no mixture of data.

For Azure Storage, a combination of techniques is employed. In Azure Blob Storage the primary technique employed is to keep each organization in a separate container. For other Azure Storage services and when Azure Blob Storage data cannot be separated using containers, the architecture will employ careful use of the organization identifier to ensure data is kept separate.

For Azure Cosmos DB, the architecture will employ careful use of the organization identifier to ensure data is kept separate.

Network Communications

- All external communication is secured with HTTPS to the On Demand User Interface.
- The external HTTPS certificate used on AWS S3 Content Delivery Network is a Level 2 domain certificate created and managed by Quest DevOps.
- There are no unsecured external HTTP calls within On Demand.
- All internal network communication within Azure among On Demand services and components is secured with HTTPS and is not visible to the external public internet.
- Integration with on-premises Change Auditor installations:

  All communication with on-premises Change Auditor uses secure TLS 1.2 connections over Web Sockets.

Authentication of Users

All users must sign up and be approved by their internal On Demand administrator user before they can use On Demand. Sign in is via the Quest Identity Broker (QIB) which provides a tamper proof token for all user operations in the user interface. This token has a limited lifetime (5 minutes), after which it must be refreshed with the QIB. Failure to refresh causes all interactions with On Demand to fail. If a user's access is revoked by the QIB, they continue to have access until their valid token expires, which is a maximum of 5 minutes. If a user's access is revoked within On Demand by an On Demand administrator, their access and actions fail once the token expires.

The QIB provides authentication services linking identities and applications. Identities are sourced from several services:

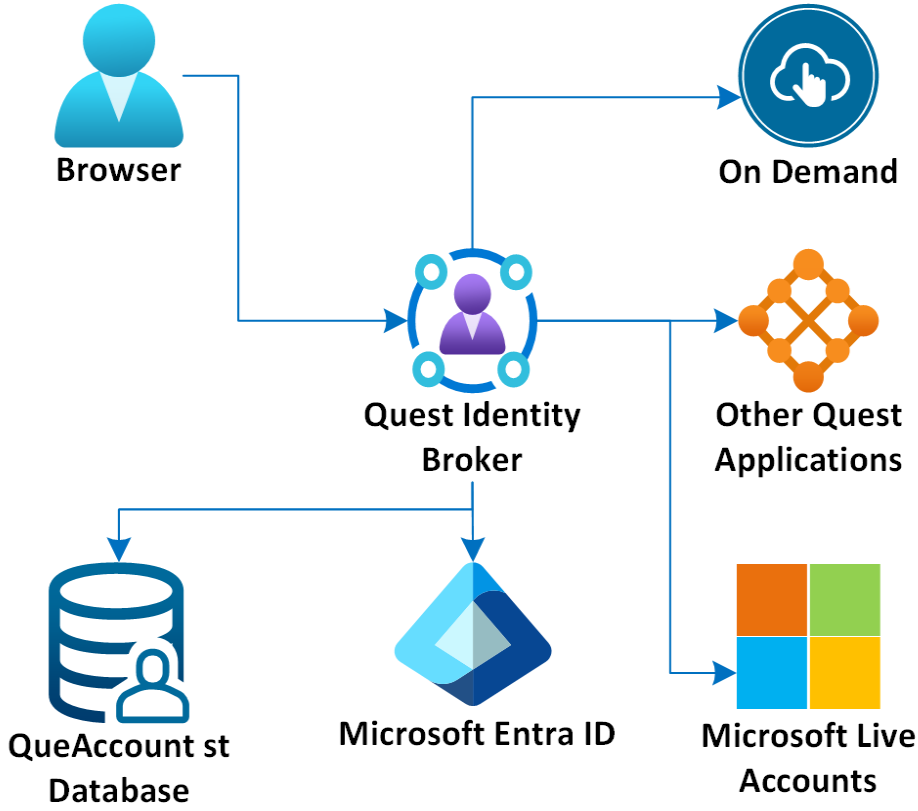
- Quest accounts (username and hashed passwords stored in a Quest database)
- Microsoft Entra ID (business)
- Microsoft Live (personal) account credentials

On Demand is among many Quest applications that rely on the QIB for authentication services. The QIB uses industry-standard Open ID Connect and SAML protocols, as well as secure direct connections to the Quest account database. All traffic in transit is encrypted using HTTPS and all data stored in the QIB database is encrypted at rest. No credentials are stored in the QIB database.

The QIB does not provide Multi-Factor Authentication (MFA) at this time. End users wishing to use Microsoft Entra ID for authentication can take advantage of MFA as provided by AAD, which is honored by the QIB.

The QIB is based on the open source Keycloak project sponsored by Red Hat. Quest regularly updates our customizations to match the most recent released version of Keycloak.

Figure 3. User authentication with QIB (Quest Identity Broker).



A valid Microsoft Entra ID JWT token is required to make notification requests and a valid On Demand JWT token is required to make additions or modifications to the Notification Service settings.

NOTE: Azure Active Directory is now Microsoft Entra ID.

Role Based Access Control

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 details, see Adding users to an organization in the On Demand Global Settings User Guide.

FIPS 140-2 Compliance

On Demand Core cryptographic usage is based on Azure and AWS FIPS 140-2 compliant cryptographic functions.

- On Demand Core leverages the Azure Key Vault and AWS KMS data-in-transit and data-at-rest built-in mechanisms.

- Quest Identity Broker uses AWS KMS to encrypt data-at-rest stored in RDS.
- More information on Azure Key Vault is available at https://azure.microsoft.com/en-us/services/key-vault/
- More information on AWS KMS is available at https://aws.amazon.com/kms/
- More information on approved crypto functions is available at NIST FIPS 140-2 https://csrc.nist.gov/publications/detail/fips/140/2/final
- The Notification Service uses AES-256 server-side encryption with Amazon S3 managed keys.
- Azure Storage: https://docs.microsoft.com/en-us/azure/storage/common/storage-security-guide
- Azure Data Explorer: Enable infrastructure encryption: https://docs.microsoft.com/en-us/azure/data-explorer/double-encryption
- Enable infrastructure encryption for double encryption of data: https://docs.microsoft.com/en-us/azure/storage/common/infrastructure-encryption-enable

Auditing

On Demand Core provides an activity trail log for the following actions:

- Adding and removing an Office 365 tenant
- Granting of Admin Consent for the tenant
- Adding and removing hybrid agents, domains and relevant capabilities
- Authorizing and de-authorizing users as an On Demand administrator
- Notification settings modification
- Privileged actions on system objects for On Demand modules

Audit data is stored in Azure SQL database and is available via JWT authenticated access to On Demand administrators only.

The Quest Identity Broker provides an audit trail log for all interactions, including login, logout, and account creation. Access is limited to the QIB administrators only.

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 the Quest corporate network have access to these systems. Therefore, should an On Demand developer leave the company, this individual can no longer 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.

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

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 On Demand

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 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.

Our brand, our vision. Together.

Our logo reflects our story: innovation, community and support. An important part of this story begins with the letter Q. It is a perfect circle, representing our commitment to technological precision and strength. The space in the Q itself symbolizes our need to add the missing piece—you—to the community, to the new Quest.

Contacting Quest

For sales or other inquiries, visit www.quest.com/contact.

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.