Quest

Quest On Demand Audit

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 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 Audit Security Guide

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

About On Demand Audit

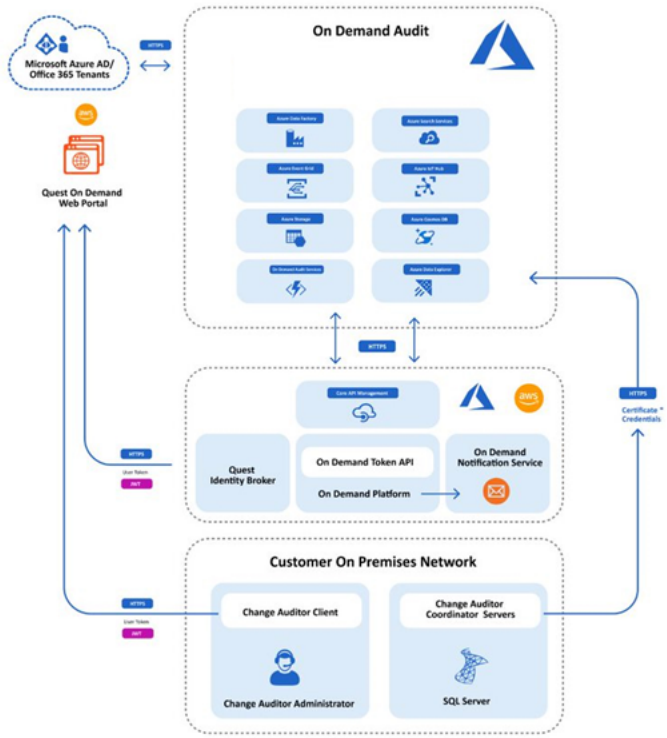
Quest On Demand Audit is an Azure hosted cloud service in the Quest On Demand platform that consolidates audit data from a variety of on premises and Office 365 workloads. Integrating with Quest Change Auditor provides the ability to search and correlate identities across both on premises and in the cloud to give a seamless view of activity in hybrid Microsoft environments.

On Demand Audit, specifically enables:

- Fast and flexible searches for easy investigation and accurate results across tenants and on premises environments
- Interactive visualizations and dashboards to summarize audit activity
- Easy to use customizable alerts based on audit event searches
- Long term storage of audit events outside of Office 365 and Change Auditor for a retention period of up to 10 years

Architecture Overview

The following scheme shows the key components of the On Demand Audit configuration



NOTE: Azure AD and Office 365 Tenants reference see OnDemand_CoreandNotificationServiceSecurityGuide.

Azure Datacenter Security

Microsoft Azure datacenters have the highest possible physical security and are considered among the most secure 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:

- 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 On Demand Audit

On Demand Audit collects events from a variety of on premises and Microsoft Cloud services that includes:

- Exchange Online
- SharePoint Online
- One Drive for Business
- Azure Active Directory
- Azure Sign-ins and Risk events
- On premises Change Auditor Active Directory

For further details on collected data, please consult the following references:

- https://msdn.microsoft.com/en-us/office-365/office-365-management-activity-api-schema.
- https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-audit-logs.
- https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-sign-ins.
- Change Auditor product documentation.

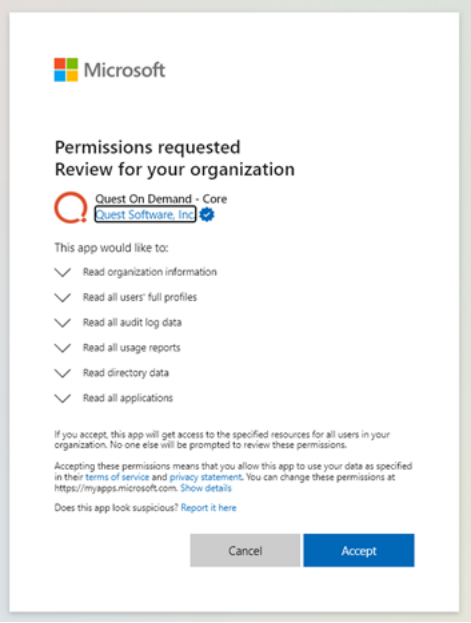
On Demand Audit does not record or store any user passwords.

Admin Consent and Service Principals

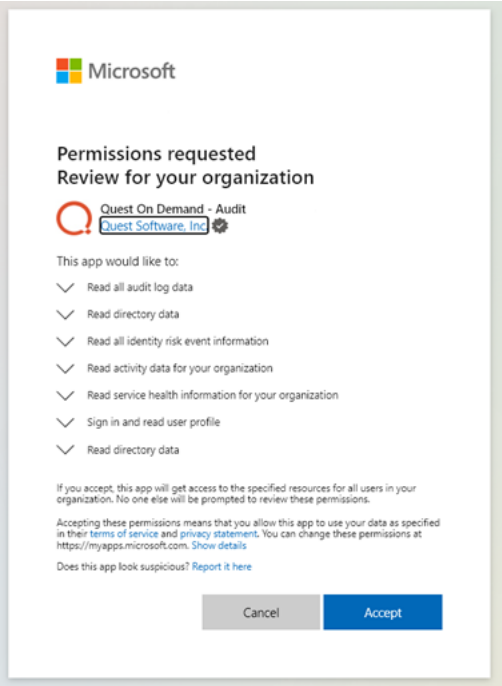
On Demand Audit requires access to the customer's Azure Active Directory and Office 365 tenancies. The customer grants that access using the Microsoft Admin Consent process, which will create a Service Principal in the customer's Azure Active Directory with minimum consents required by On Demand Audit (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.



In addition to the base consents required by On Demand, On Demand Audit requires the following consents:



On Demand Audit currently uses the Office 365 Management Activity API, Microsoft Graph API, and Azure AD Graph API for reading events from Office 365 and Azure AD using a “limited permissions model” which does not require global administrator permissions. After the consent has been granted using the global administrator account, thereafter all auditing operations will be driven by the token generated using the Application Service Principal.

The Admin Consent process of On Demand Audit will create a Service Principal in the customer's Azure AD tenant with the following permissions.

- Permissions required for On Demand Audit to read audit log activities and activity data from Azure AD and Office 365.
- Permissions required for On Demand Audit to read the identity risk event information.
- Permissions required for On Demand Audit to read service health information.
- Permissions required for On Demand Audit to read user profile data and directory data such as users, groups, and applications.

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 here https://regions.quest-on-demand.com/.

On Demand Audit 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 Audit 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 Audit. 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 Audit 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 Audit. For disaster recovery duplicate copies of all data are stored in Azure “Western Europe”.

For UK Organizations:

- All On Demand Audit 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 Audit. For disaster recovery duplicate copies of all data are stored in Azure “UK West”.

For Canada Organizations:

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

For Australia Organizations:

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

All on premises data from Change Auditor is transmitted to and retained in the selected On Demand organization and region.

On Demand Audit makes use of Amazon SES (Simple Email Service) to provide email alerting capabilities via the On Demand Notification Service. These services require Amazon data centers outside of Azure data centers. All data is stored and processed within the matching region selected in On Demand. For further details, see the On Demand Core Security Guide

Privacy and Protection of Customer Data

The most sensitive customer data collected and stored by On Demand Audit is the event data from activity occurring in the Azure Active Directory and Office 365 environment and event data from all connected Change Auditor installations. All data is segregated based on the organizational identifier. Whenever event data is stored or retrieved within the system the organizational identifier ensures data remains separate.

All event data is protected by service-level encryption present in Microsoft Azure Services.

For information on privacy and protection of customer data within On Demand and email alerting provided by Amazon SES, please refer to the On Demand and On Demand Notification Services security guides.

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 Audit 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 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. The technique used to separate custom data varies depending on the type service and storage.

- 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 Power BI, each organization is contained within a separate workspace.
- 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 Core 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 Audit.

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

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

The process of registering an Azure AD tenant into On Demand Audit 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.

The initial configuration of the connection of Change Auditor to On Demand is done by the Change Auditor administrator using On Demand login credentials previously established in the On Demand web portal. For further details, see the On Demand Core security guide.

Role Based Access Control

Quest On Demand provides permission-based roles to determine what permission level a user has and what tasks the user can perform.

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

List of permissions that can be assigned to On Demand Audit users:

- Can Configure Audit and Manage Searches
- Can View Dashboard
- Can Manage Azure AD Tenant Configurations for Audit
- Can Manage Change Auditor Installation Configuration
- Can View Event Retention Settings
- Can View Shared Searches
- Can Run Shared Searches
- Can Run Search Visualization
- Can Run Private Searches
- Can Manage Private Searches
- Can Manage Shared Searches
- View Event Details
- Can Run Quick Search Searches
- Can Export Search Results
- Can Manage Shared Alerts and Shared Alert Plans
- Can Manage Private Alerts and Private Alert Plans
- Can Export Data

On Demand Audit also makes use of one special role called *Manage Audit Organization Private Alerts* and *Private Alert Plans*. This built-in role is the only way that users can be delegated the rights to manage organization private alerts and private alert plans regardless of the user in the organization that owns the alert or alert plan. Users must be assigned to this role to receive the assigned rights because they cannot be granted this capability via a permission in the standard way. This role is not assigned by default to any user, nor is the right implicitly held by members of On Demand Administrator or Audit Administrator roles the way that other permissions are held.

FIPS 140-2 Compliance

On Demand Audit module cryptographic usage is based on Azure FIPS 140-2 compliant cryptographic functions.

On Demand Audit makes use of FIPS 140-2 compliant encryption provided in Microsoft Azure Cloud services.

More information:

- 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
- 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

SDLC and SDL

The On Demand Audit team follows a strict Quality Assurance cycle.

Access to source control and build systems is protected by domain security. Only employees on Quest's corporate network have access to these systems. Therefore, if an On Demand developer leaves the company, they 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 Audit team follows a managed Security Development Lifecycle (SDL) which includes:

- MS-SDL best practices
- Threat modeling
- OWASP guidelines
- Static code analysis is performed on regular basis
- 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 Audit 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 27001 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 27001 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 Audit data is restricted to:

- Quest Operations team members
- Particular Quest Support team members working closely with On Demand Audit product issues.
- The On Demand Audit development team to provide support for the product.

Access to On Demand Audit 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 Audit

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

To access On Demand Audit, a customer representative goes to the On Demand website and signs up for an On Demand account. When they create an account, an organization is automatically created. As part of the sign-up process, they must provide a valid email address. They must have access to the email account in order to receive and respond to a verification email from Quest Software.

Prerequisites:

Azure Active Directory Global Administrator must give the Admin Consent to provision On Demand Audit for the customer's Azure Active Directory with the following permissions:

Microsoft Graph

- Read all audit log data
- Read all identity risk event information

Azure Active Directory Graph

- Read directory data
- Office 365 Management APIs
- Read activity data for your organization
- Read service health information for your organization

Microsoft Graph permissions reference - Microsoft Graph | Microsoft Docs

Operational Monitoring

On Demand Audit internal logging is available to Quest Operations and On Demand Audit 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 Audit 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/

Customer Measures

On Demand Audit security features are only one part of a secure environment. Customers need to operate by their own best security practices when proceeding with auditing their data. Special care needs to be given to protecting the credentials of the Azure Active Directory Tenants Global Administrator accounts.

Change Auditor Integration

When On Demand Audit is configured to connect to an on premises Change Auditor installation, care must be taken to ensure that the Change Audit installation is configured according to security best practices to protect Change Auditor coordinators.

Secure the Change Auditor installation

Any Change Auditor users that have the Change Auditor administrator role can modify the configuration for On Demand Audit integration through the Change Auditor client and thereby expose data to other organizations. Therefore, the members of the Change Auditor administrators must be carefully managed.

Secure Change Auditor Coordinator Servers

All Change Auditor coordinators communicate with On Demand Audit cloud components and must be secured. This communication is secured and encrypted by means of a unique X.509 certificate installed on each coordinator in the Certificate Store. This certificate provides the identity and access for On Demand Audit from for on premises components and therefore must be protected so that the On Demand Audit organization and data remains protected. For correct operation, only the Change Auditor Coordinator service and local computer administrators can access certificates in the Certificate Store. To protect the certificate, it is essential that only trusted users have administrative rights on coordinators because these users may gain access to the certificate.

If a certificate is suspected of being compromised it should be replaced with a new unique certificate to secure the environment. Please contact Quest support for this procedure.

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.

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