Quest

Quest® On Demand Migration for Active Directory

Security Guide

Legend

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

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

On Demand Migration for Active Directory - Security Guide
Updated – August 12, 2024

Contents

1

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.

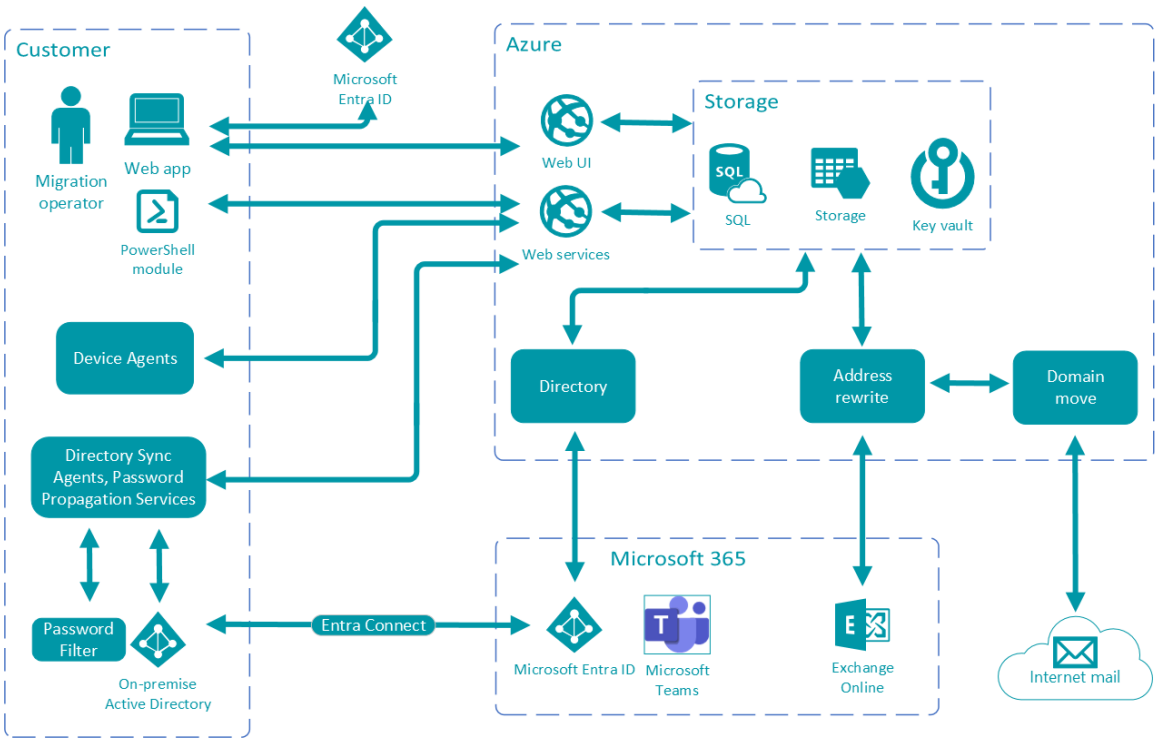
This document describes the security features of Quest On Demand Migration for Active Directory. It reviews access control, protection of customer data, secure network communication, cryptographic standards and more.

About On Demand Migration for Active Directory

Quest On Demand Migration for Active Directory provides the following functionality:

- Full tenant discovery of users, groups, domains and more.
- Move domains between tenants.
- Synchronize Active Directory and Microsoft Entra ID directories with customizable workflows.
- Migrate workstations, computers, servers, objects, users, groups and more.
- No servers, trusts, or network connectivity required.
- Data transformation and customizable mapping of directory attributes.
- Near-real time password hash synchronization.
- Password change propagation.
- Trustless SID History migration.

Architecture Overview



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 Migration for Active Directory

Domain Migrations

During domain migrations, On Demand Migration for Active Directory collects data for a variety of Microsoft Entra ID objects.

- Directory objects are processed using Microsoft Graph API and PowerShell.
- Objects include users, groups, contacts, teams, and Microsoft 365 groups.
- Properties include account name, email addresses, contact information, department, membership and more.
- Access to Microsoft Entra ID is granted by the customer using the Microsoft Admin Consent process and requires administrative credentials. Customers can revoke Admin Consent at any time. See https://msdn.microsoft.com/en-us/skype/trusted-application-api/docs/tenantadminconsent for details.
- On Demand Migration for Active Directory does not store credentials for administrative accounts.
- On Demand Migration for Active Directory generates and manages dedicated service accounts in each Microsoft 365 tenant used for PowerShell queries. The service accounts password is randomly generated to be unique and highly complex. The password is also encrypted with AES 256-bit encryption using Azure Key Vault and is never stored unencrypted.

Email Rewrite Service

During domain migrations and from domain rewrite enabled projects, On Demand Migration for Active Directory rewrites email message recipients to provide seamless message delivery.

- Email messages are temporarily stored during processing and deleted as soon as they are written to the target. The temporarily stored messages are encrypted using AES symmetric-key encryption with a 256-bit key that is unique per message, randomly generated and only held in memory.

Directory Synchronization & Migration

On Demand Migration for Active Directory collects data for a variety of on premises and Microsoft Entra ID objects. The directory locations, objects and properties collected are configurable to ensure only the desired objects and properties are processed.

Microsoft Entra ID

- Directory objects are processed using Microsoft Graph API and PowerShell.
- Objects include users, groups, contacts, teams, and Microsoft 365 groups.
- Properties include account name, email addresses, contact information, department, membership and more.
- Access to Microsoft Entra ID is granted by the customer using the Microsoft Admin Consent process and requires administrative credentials. Customers can revoke Admin Consent at any time. See https://msdn.microsoft.com/en-us/skype/trusted-application-api/docs/tenantadminconsent for details.
- On Demand Migration for Active Directory does not store credentials for administrative accounts.
- On Demand Migration for Active Directory generates and manages dedicated service accounts in each Microsoft 365 tenant used for PowerShell queries. The service accounts password is randomly generated to be unique and highly complex. The password is also encrypted with AES 256-bit encryption using Azure Key Vault and is never stored unencrypted.

On Premises Active Directory

- On-premises directory sync agents, running within the customers network, process Active Directory objects using LDAP or LDAPS (TLS 1.2) as configured within the user interface. Objects include users, groups, and contacts, computers, and servers. Properties include account name, email addresses, contact information, department, membership and more.
- When the optional password sync feature is enabled, the password hash of all user accounts in scope are collected using an encrypted connection to a signed Password Filter. The connection is encrypted using AES256 and a key derived from a customer-selected passphrase. Password hashes are stored encrypted with AES256 in Azure SQL Storage. The AES256 key is stored in Azure Key Vault. Once co-existence is no longer required for a specific user, the customer should use the reconcile option to ensure that information is promptly deleted.
- When the optional password change propagation feature is enabled, a signed Password Filter receives notifications when source users change their passwords. It relays those changes to the Password Change Propagation Service, which uses LDAPS to update the passwords of target users.

Passwords are stored on disk temporarily, doubly-encrypted, first using AES256 with a key derived from a customer-selected passphrase, then again using the Windows Data Protection API (DPAPI).

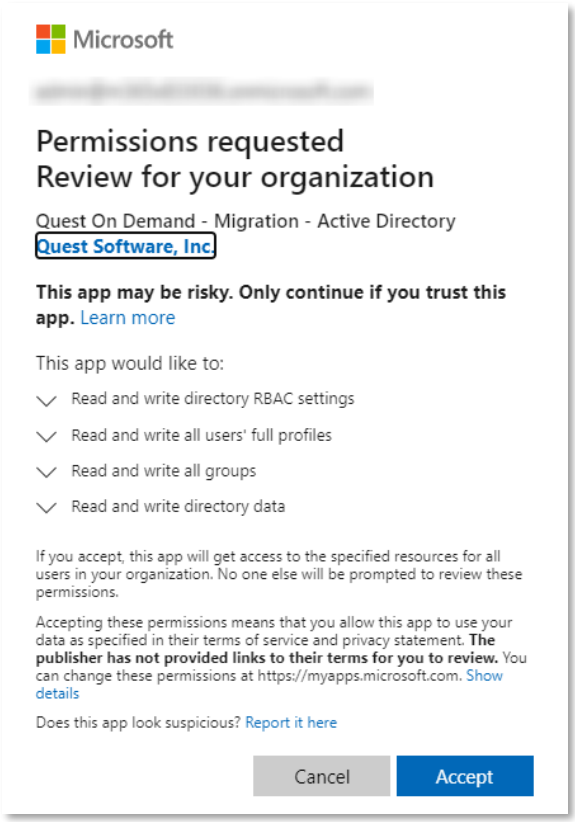
- On-premises directory sync agents, running within the customers network, securely encrypt and store administrative credentials locally on the agent's computer.
- On-premises device agents running locally on the end user's workstation collect device properties using WMI and PowerShell. Device properties include device name, domain name, user profile locations and more.
- On Demand Migration for Active Directory optionally stores credentials required for network share re-permission and Active Directory domain joins. These credentials are provided by migration operators and are encrypted with AES 256-bit encryption using Azure Key Vault and are never stored unencrypted.

Admin Consent and Service Principals

On Demand Migration for Active Directory requires access to the customer's Microsoft Entra ID and Office 365 tenants. The customer grants that access using the Microsoft Admin Consent process, which will create a Service Principal in the customer's Microsoft Entra ID with minimum consents required. The Service Principal is created using Microsoft's OAuth auth code grant flow https://docs.microsoft.com/en-us/azure/active-directory/develop/v2-oauth2-auth-code-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.

Below is the Admin Consent screen, see Operational Security > Permissions Required to Configure and Operate for a complete list of permissions required by On Demand Migration for Active Directory.


Microsoft
Permissions requested
Review for your organization
Quest On Demand - Migration - Active Directory
Quest Software, Inc.
This app may be risky. Only continue if you trust this app. Learn more
This app would like to:
Read and write directory RBAC settings
Read and write all users' full profiles
Read and write all groups
Read and write directory data
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. The publisher has not provided links to their terms for you to review. You can change these permissions at https://myapps.microsoft.com. Show details
Does this app look suspicious? Report it here
Cancel
Accept

Location of Customer Data

When a customer signs up for On Demand, they select the region in which to run their On Demand organization. All computation is performed in and all customer data is stored in the selected region. The currently supported regions can be found here: https://regions.quest-on-demand.com/. On Demand Migration for Active Directory customer data is stored in the selected region, entirely within Azure Services provided by Microsoft. For more information, see Achieving Compliant Data Residency and Security with Azure.

- Customer data is stored in Azure SQL and is automatically replicated for failover using Azure SQL Active Geo replication. See this Microsoft reference for details: https://docs.microsoft.com/en-us/azure/azure-sql/database/active-geo-replication-overview
- Application logs are stored in Azure storage tables. 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 are replicated across different fault domains to increase availability. All replication datacenters reside with the geographic boundaries of the selected region. See this Microsoft reference for details: https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy
- DKIM and TLS certificates used by On Demand Migration for Active Directory Email Rewrite Services are stored in Microsoft Key Vault.

When the optional password change propagation feature is enabled, passwords are stored temporarily on the local disks of source domain controllers and a server in the target domain, all within the customer's on-premises environment. Passwords are doubly-encrypted, first using AES256 with a key derived from a customer-selected passphrase, then again using the Windows Data Protection API (DPAPI)

Privacy and Protection of Customer Data

The most sensitive customer data collected and stored by On Demand Migration for Active Directory is the Microsoft Entra ID and on premises Active Directory data including users, password hashes, groups, contacts, and teams.

- All data is secured at rest using SQL Transparent Data Encryption (TDE) with Microsoft managed keys. For more information see https://docs.microsoft.com/en-us/azure/azure-sql/database/transparent-data-encryption-tde-overview
- Azure storage account data is secured at rest using storage service encryption with Microsoft managed keys. For more information see https://docs.microsoft.com/en-us/azure/storage/common/storage-service-encryption
- Service account passwords and password hashes (while already encrypted at-rest) are additionally encrypted with AES 256-bit encryption using Azure Key Vault.
- On Demand Migration for Active Directory Email Rewrite Services encrypt email messages using AES encryption and a unique, randomly generated 256-bit key that is unique per message and only held in memory.
- When the optional password change propagation feature is enabled, passwords are stored temporarily on the local disks of source domain controllers and a server in the target domain, all within the customer's on-premises environment.

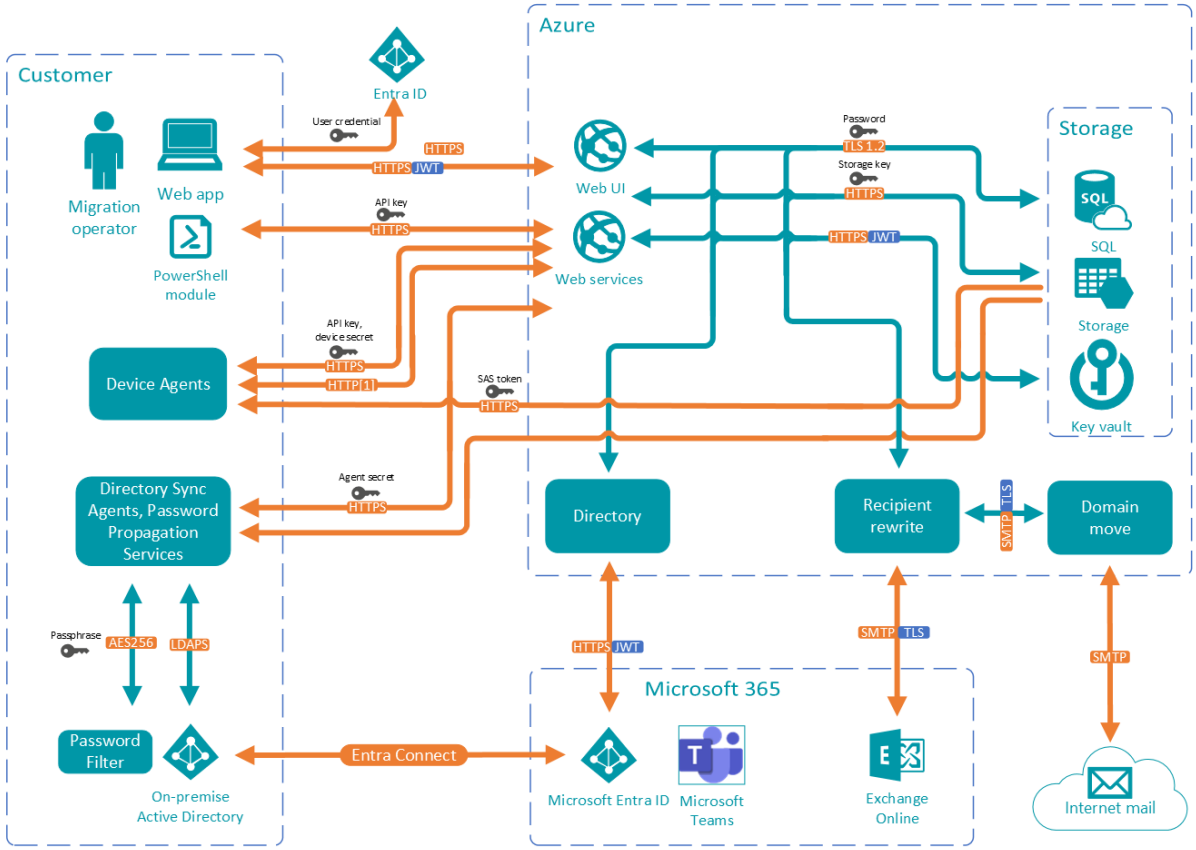
Separation of Customer Data

On Demand Migration for Active Directory is architected to prevent 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 Quest On Demand that is created when the customer signs up the application. This identifier is used throughout the solution to ensure strict data separation of customers' data.

Customer data is further separated as customer related services are isolated from any other OS process by the Microsoft Service Fabric exclusive process model. See https://docs.microsoft.com/en-us/azure/service-fabric/service-fabric-hosting-model#exclusive-process-model for more information.

Network Communications

- All communication to the On Demand Migration for Active Directory - including the user interface and associated Azure services - are secured with HTTPS. There are no unsecured external HTTP calls within On Demand Migration for Active Directory.
- All communication with Microsoft Entra ID uses OAuth2 access tokens for Microsoft Graph API operations and HTTPS for PowerShell operations.
- On-premises directory sync agents communicate with on-premises Active Directory using LDAP or LDAPS over TLS 1.2 as configured within the user interface and communicate with On Demand Migration for Active Directory cloud services using HTTPS.
- When the optional password sync feature is enabled, on-premises directory sync agents communicate with a signed Password Filter over an encrypted named pipe. The connection is encrypted using AES256 and a key derived from a customer-selected passphrase. On-premises device agents poll the Device Agent Cache Service (DACS) using unencrypted UDP or HTTP for efficiency. No sensitive information is exchanged, just a Boolean value indicating when there are jobs queued for the device agent. If DACS indicates there are jobs queued, the device agent communicates securely with the On Demand Migration for Active Directory web service using HTTPS to retrieve the job details.
- When the optional password change propagation feature is enabled, password changes are relayed between on-premises servers doubly-encrypted, first using AES256 and a key derived from a customer-selected passphrase, then using HTTPS over TLS 1.2. Target passwords are updated using LDAPS, with optional SSL certificate pinning to verify the identity of the target domain controller.
- On Demand Migration for Active Directory reads and writes content using HTTPS over TLS 1.2 data channels.
- On Demand Migration for Active Directory Email Rewrite Services communicates with Microsoft 365 tenants using TLS 1.2 encrypted data channels.



Credential/secret used to authenticate

Communication over internet

Communication within Azure

[1] High efficiency poll, no sensitive data exchanged

Authentication of Users

- On Demand Migration for Active Directory relies Microsoft Entra ID for authentication which provides customers with an integrated authentication experience where you can move from On Demand Migration for Active Directory to a Microsoft portal seamlessly, without multiple logins and passwords. All while keeping your account security under your organization's policies, rules, and security protocols.
- On Demand Migration for Active Directory also supports Multi Factor Authentication (MFA) for organizations that have enabled MFA within Microsoft 365.
- Registering a Microsoft Entra tenant into On Demand Migration for Active Directory is handled through the Azure Admin Consent workflow and customers can revoke Admin Consent at any time. See https://msdn.microsoft.com/en-us/skype/trusted-application-api/docs/tenantadminconsent for details.

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 information on role-based access control, please refer to the Quest On Demand product documentation.

FIPS 140-2 compliance

On Demand Migration for Active Directory cryptographic usage is based on Azure FIPS 140-2 compliant cryptographic functions. On Demand Migration for Active Directory makes use of FIPS 140-2 compliant encryption keys that are stored in Microsoft Key Vault.

More information:

- Microsoft and FIPS: https://www.microsoft.com/en-us/trustcenter/compliance/fips
- Microsoft FIPS backgrounder: https://aka.ms/fips-backgrounder
- 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 Migration for Active Directory Development team follows a managed Software Development Lifecycle (SDLC).

The On Demand Migration for Active Directory 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. 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 Migration for Active Directory 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 Migration for Active Directory 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.

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. All security recommendations are planned to be incorporated in near-term product releases.

Certification

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

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

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

- Examination Scope: Quest On Demand Platform
- Selected SOC 2 Categories: **Security**
- Examination Type: **Type 2**
- Review Period: August 1, 2022, to July 31, 2023
- Service Auditor: Schellman & Company, LLC

Operational Security

Source control and build systems can only be accessed by Quest employees. If an employee with access to On Demand Migration for Active Directory leaves the company the individual loses access to all systems. All code is versioned in source control.

Who at Quest has Access to Data

Access to On Demand Migration for Active Directory data is restricted to:

- Quest Operations team members
- Selected Quest Support team members working on product issues.
- Selected development team members working with the Operations and Support teams.

Access to On Demand Migration for Active Directory data and resources is restricted through Azure RBAC and Microsoft Entra ID security groups. For each type 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

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

A Microsoft Entra ID Global Administrator must give the Admin Consent to provision On Demand Migration for Active Directory with the following Microsoft.Graph permissions:

Read and write all groups (Group.ReadWrite.All)

Permission Definition: Allows the app to create groups and read all group properties and memberships on behalf of the signed-in user. Additionally, allows group owners to manage their groups and allows group members to update group content.
Application Purpose: Used by the app to Sync services to provide OneDrive migration activities.

Read and write directory data (Directory.ReadWrite.All)
Permission Definition: Allows the app to have the same access to information in the directory as the signed-in user.

Application Purpose: Used by Discovery and Provisioning Services to discover all workloads (such as Organizations, available SKUs, users, groups, contacts, etc.) and to automate M365 licensing.

Read and write role management data for Microsoft Entra ID (RoleManagement.ReadWrite.Directory)
Permission Definition: Allows the app to assign roles to Microsoft Entra ID accounts.

Application Purpose: Used by the app to assign roles to service accounts to ensure the minimum effective rights are granted.

Read and write all groups (User.Read.All)
Permission Definition: Allows the app to read and write the full set of profile properties, reports, and managers of other users in your organization, on behalf of the signed-in user.
Application Purpose: Used by Discovery services to identify user mailbox properties.

Operational Monitoring

On Demand Migration for Active Directory internal logging is available to Quest Operations and On Demand Migration for Active Directory development teams during the normal operation of the platform. Some Personally Identifiable Information (PII) (e.g. usernames, email addresses, email aliases, etc.) can become a part of internal logging for troubleshooting purposes. Quest Operations team members have access to Quest's production Azure Subscription and monitor this as part of normal day-to-day operations.

Production Incident Response Management

Quest Operations and Quest Support have procedures in place to monitor the health of the system and ensure any degradation of the service is promptly identified and resolved. On Demand Migration for Active Directory relies on 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

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 Migration for Active Directory 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 Microsoft Entra Tenants Global Administrator accounts and On Premises Active Directory Administrator accounts.

About us

We are more than just a name

We are on a quest to make your information technology work harder for you. That is why we build community-driven software solutions that help you spend less time on IT administration and more time on business innovation. We help you modernize your data center, get you to the cloud quicker and provide the expertise, security and accessibility you need to grow your data-driven business. Combined with Quest's invitation to the global community to be a part of its innovation, and our firm commitment to ensuring customer satisfaction, we continue to deliver solutions that have a real impact on our customers today and leave a legacy we are proud of. We are challenging the status quo by transforming into a new software company. And as your partner, we work tirelessly to make sure your information technology is designed for you and by you. This is our mission, and we are in this together. Welcome to a new Quest. You are invited to Join the Innovation™.

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.