



Quest® Identity Recovery for Microsoft Entra ID

Security Guide



© 2026 Quest Software Inc. ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software Inc.

The information in this document is provided in connection with Quest Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST SOFTWARE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest Software does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.
Attn: LEGAL Dept
10801 N. Mopac Expressway, Building 3, Suite 400
Austin, TX 78759

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.

Contents

Introduction	1
About Identity Recovery for Microsoft Entra ID	2
Architecture overview	3
Azure datacenter security	5
Overview of data handled by Identity Recovery for Microsoft Entra ID	6
Admin consent and service principals	7
Location of customer data	11
For US organizations	11
For Canadian organizations	11
For European organizations	11
For UK organizations	12
For Australian organizations	12
Privacy and protection of customer data	13
Separation of customer data	14
Network communications	15
User Authentication	16
Role based access control	17
FIPS 140-2 compliance	18
SDLC and SDL	19
Third party assessments and certifications	20
Penetration testing	20
Certification	20
Operational security	21
Permissions required to configure and operate Identity Recovery for Microsoft Entra ID	21
Prerequisites	21
OAuth 2.0 permission grants	22
Customer measures	23

About us **24**
 Technical support resources 24

Introduction

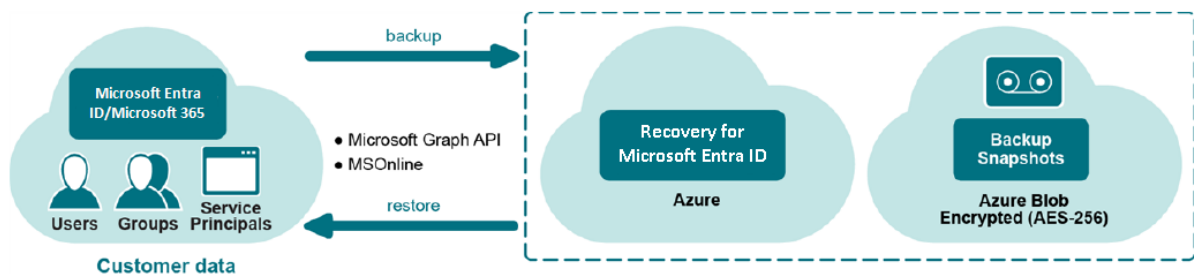
Managing information system security is a priority for every organization. In fact, the level of security provided by software vendors has become a differentiating factor for IT purchase decisions. Quest Software strives to meet standards designed to provide its customers with their desired level of security, whether it relates to privacy, authenticity and integrity of data, availability, or protection against malicious users and attacks.

This document describes the security features of Quest® Identity Recovery for Microsoft Entra ID. This includes access control, protection of customer data, secure network communication, and cryptographic standards.

About Identity Recovery for Microsoft Entra ID

Identity Recovery for Microsoft Entra ID cloud application automatically backs up Microsoft Entra ID and Microsoft 365 users, groups, service principals, device information, conditional access policies and navigation properties and lets you restore deleted or damaged data selectively.

Figure 1: Identity Recovery for Microsoft Entra ID overview



Identity Recovery for Microsoft Entra ID offers:

- **Back up Microsoft Entra ID and Microsoft 365 users, groups, service principals, device information, conditional access policies, and navigation properties** - Identity Recovery for Microsoft Entra ID automatically backs up a directory on a regular basis.
- **Granular, selective restore** – Objects can be selected in a backup and then restored to Microsoft Entra ID or Microsoft 365 without affecting other objects or attributes.
- **Restore users from the Recycle Bin** - Restore or recreate users that were inadvertently moved to the Recycle Bin.
- **Cloud solution** - Identity Recovery for Microsoft Entra ID does not require that you install or maintain any additional software. Backup snapshots are stored in the cloud.

Architecture overview

The following scheme shows the key components of the Identity Recovery for Microsoft Entra ID configuration.

Figure 2: Main architecture diagram

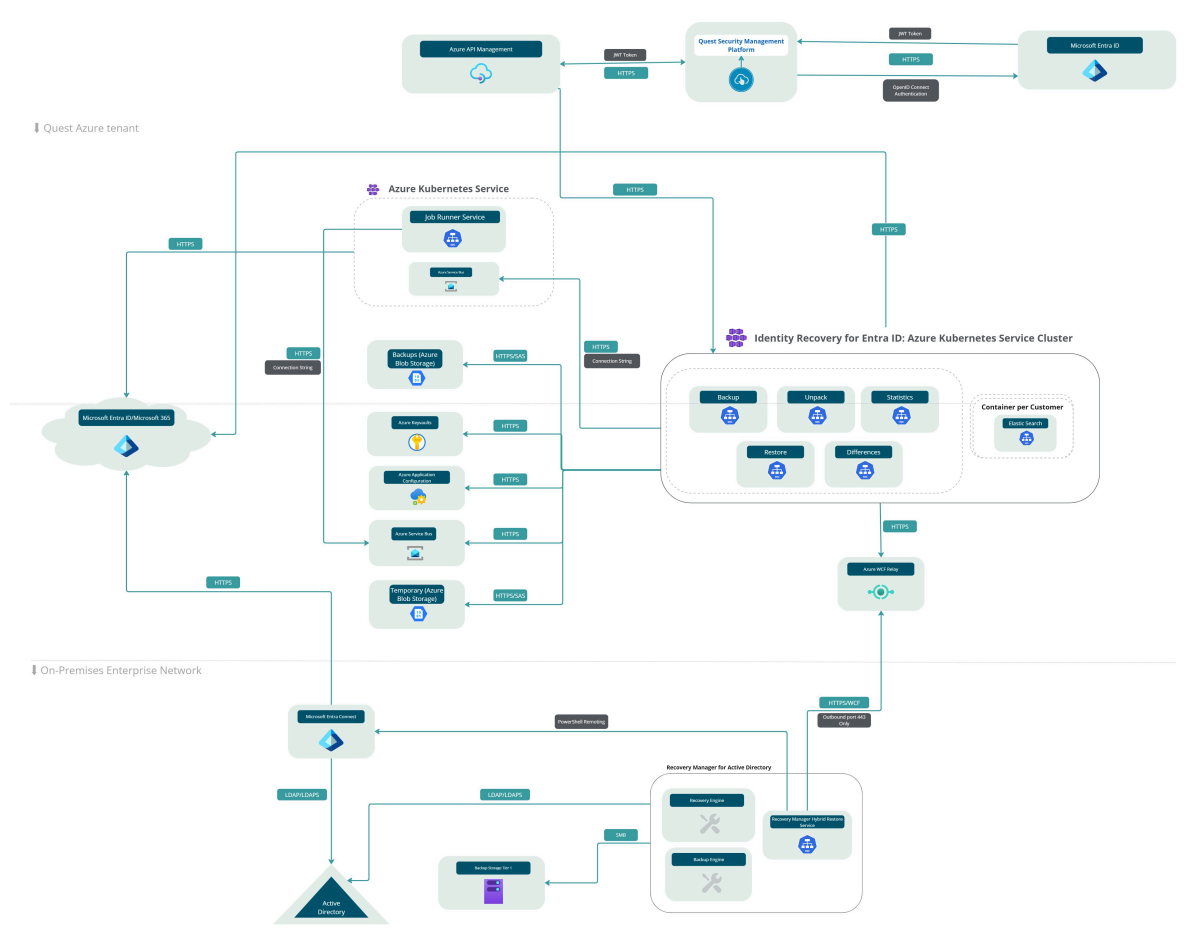


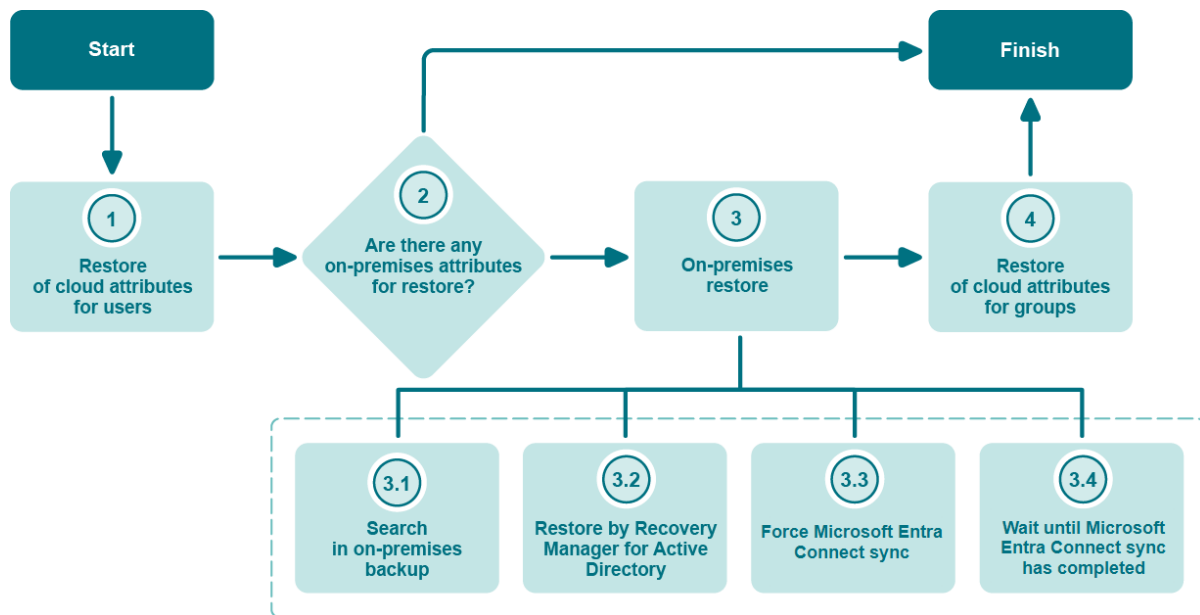
Table 1: Identity Recovery for Microsoft Entra ID and Recovery Manager for Active Directory ports and protocols

Protocol	Ports	Direction
HTTPS	443 (TCP/UDP)	Outbound

Hybrid configuration with Recovery Manager for Active Directory requires only outbound TCP/UDP port 443 to be opened on the Recovery Manager Portal server to access the internet. If the Recovery Manager Portal server already has access to the internet, you do not need to change the Firewall configuration.

If you do not want to open all outbound IP addresses and your firewall or proxy lets you specify a DNS allow list, you can add connections to <your name space>.servicebus.windows.net to your allow list.

Figure 3: Hybrid restore operation flow diagram



- All attributes that can be modified by Microsoft Graph API are considered as cloud attributes and restored on the first step. For example, assignedLicense, usageLicense, and membership in cloud groups.
- Identity Recovery for Microsoft Entra ID also restores users from the Recycle Bin or recreates them before the on-premises restore with the Undelete option. Microsoft Entra Connect matches these objects after the cloud restore by the immutableID attribute which is restored from the Identity Recovery for Microsoft Entra ID backup.
- On-premises restore is always performed for member, memberOf, accountEnabled, manager, and directReports attributes.
- If the Restore all attributes option is select in the Restore Objects dialog, we always perform the on-premises restore even if the cloud restore was successful.
- Groups are restored always after the on-premises restore, because in case of permanent deletion, Identity Recovery for Microsoft Entra ID needs to wait until a group is recreated by Microsoft Entra Connect.

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.

- Microsoft Azure Trust Center:
<https://azure.microsoft.com/en-us/explore/trusted-cloud/>
- Microsoft Trust Center Compliance:
<https://www.microsoft.com/en-us/trust-center/compliance/compliance-overview?service=Azure#Icons>
- Microsoft's submission to the Cloud Security Alliance STAR registry:
<https://cloudsecurityalliance.org/star/registry/microsoft>
- Whitepaper: Standard Response to Request for Information – Security and Privacy:
<http://www.microsoft.com/en-us/download/details.aspx?id=26647>
- Azure global infrastructure, security, and compliance:
<https://azure.microsoft.com/en-us/explore/global-infrastructure/>
- Azure data security and encryption best practices:
<https://learn.microsoft.com/en-us/azure/security/fundamentals/data-encryption-best-practices>

Overview of data handled by Identity Recovery for Microsoft Entra ID

Identity Recovery for Microsoft Entra ID manages the following type of customer data:

- Microsoft Entra ID and Microsoft 365 users, groups, conditional access policies, service principals with their properties, and device information returned by Microsoft Graph API, including account name, email addresses, contact information, department, membership, and other properties.
- Identity Recovery for Microsoft Entra ID does not back up and does not store user passwords and password hashes.

For more information about Microsoft Entra connection information and security tokens, see the Security Management Platform Global Settings product documentation:

- [User Guide](#)
- [Release Notes](#)
- [Security Guide](#)

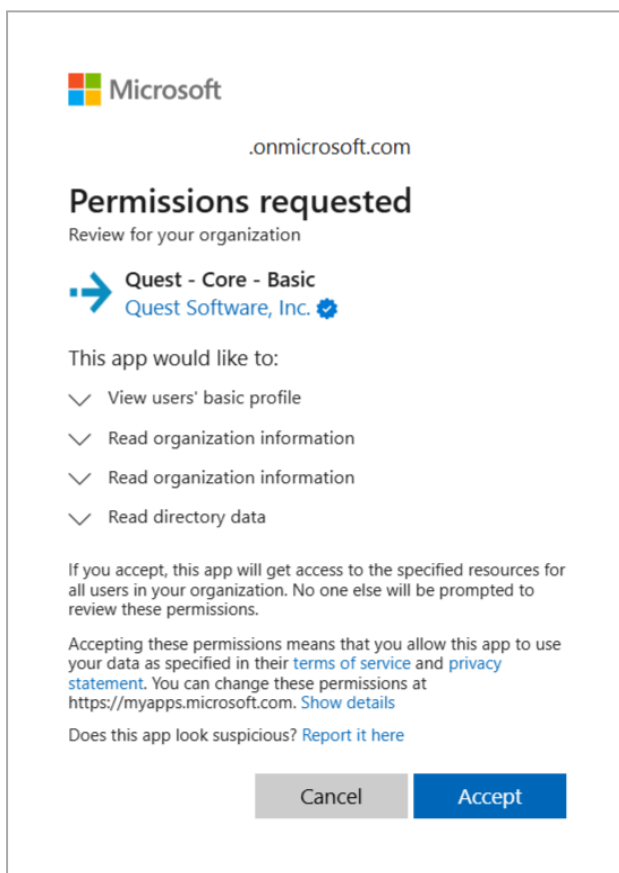
Admin consent and service principals

Identity Recovery for Microsoft Entra ID requires access to the customer's Microsoft Entra ID and Microsoft 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 by Identity Recovery for Microsoft Entra ID.

The service principal is created using Microsoft's OAuth certificate based client credentials grant flow (see [OAuth 2.0 client credentials grant flow](#) in Microsoft Learn). Customers can revoke Admin Consent at any time (see [Delete an enterprise application](#) in Microsoft Learn).

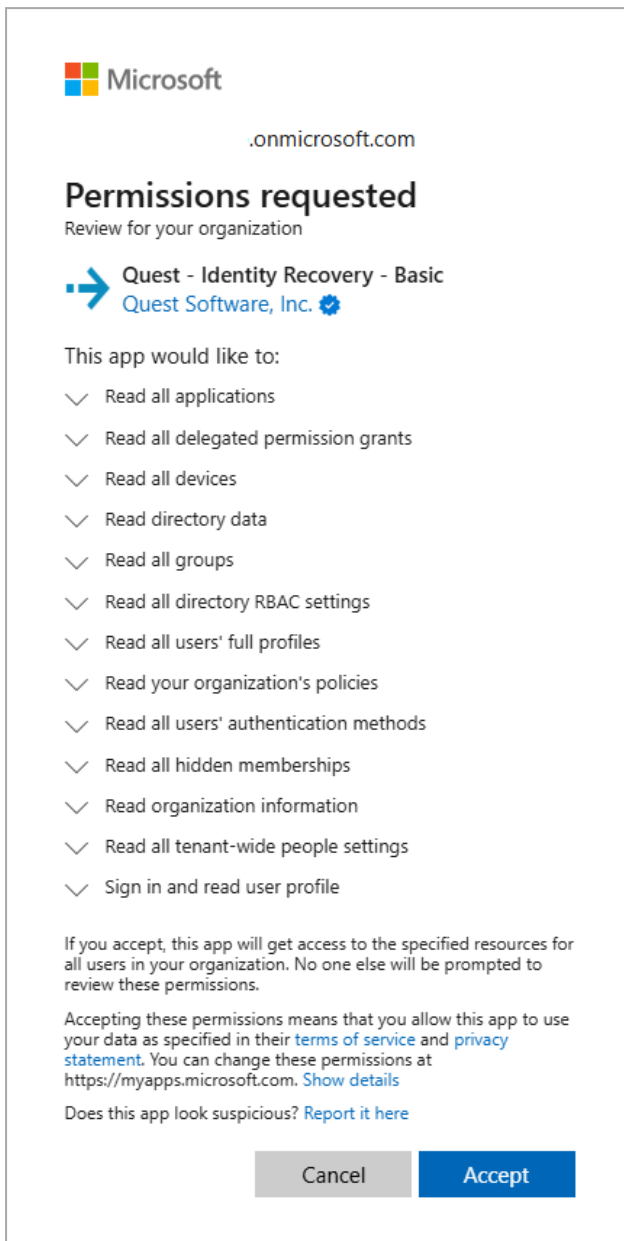
The following is the base consent required by Security Management Platform Core:

Figure 4: Quest - Core - Basic consent.



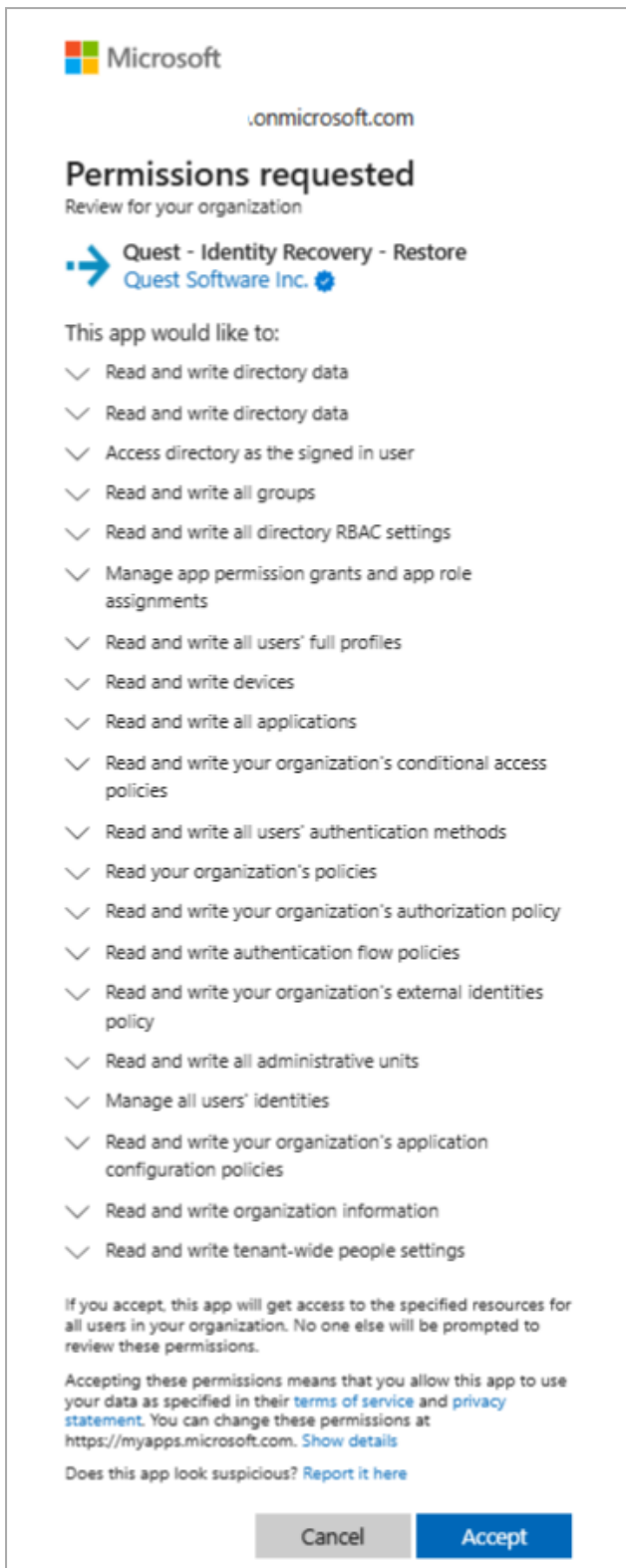
In addition, the following base consent is required by Identity Recovery for Microsoft Entra ID:

Figure 5: Quest - Identity Recovery - Basic consent.



To restore Microsoft 365 and Microsoft Entra data, the following consent is required by Identity Recovery for Microsoft Entra ID:

Figure 6: Quest - Identity Recovery - Restore consent.



Exchange Online PowerShell

To perform Exchange tasks, you will need to grant consent to Exchange Online PowerShell, and assign the Exchange Admin Role. For more information, see [About admin consent status](#) and [Granting and regranting admin consent](#) in the *Security Management Platform Global Settings User Guide*.

Location of customer data

The following data centers are used to store customer data:

For US organizations

- Backups are stored in Geo-redundant Azure Blob Storage – encrypted at rest:
 - Primary replica - West US 2 (Washington)
 - Secondary replica - West Central US (Wyoming)
- Unpacked backups are stored on Azure virtual disks that are associated with independent Elasticsearch nodes (per customer) which are part of Azure Kubernetes Service West US 2 (Washington) - encrypted at rest
- Logs are stored in Log Analytics East US (Virginia) – encrypted at rest

For Canadian organizations

- Backups are stored in Geo-redundant Azure Blob Storage – encrypted at rest
 - Primary replica – Canada Central (Toronto)
 - Secondary replica – Canada East (Quebec City)
- Unpacked backups are stored on Azure virtual disks that are associated with independent Elasticsearch nodes (per customer) which are part of Azure Kubernetes Service Canada Central (Toronto) – encrypted at rest
- Logs are stored in Log Analytics Canada Central (Toronto) – encrypted at rest

For European organizations

- Backups are stored in Geo-redundant Azure Blob Storage – encrypted at rest:
 - Primary replica – North Europe (Ireland)
 - Secondary replica – West Europe (Netherlands)
- Unpacked backups are stored on Azure virtual disks that are associated with independent Elasticsearch nodes (per customer) which are part of Azure Kubernetes Service North Europe (Ireland) – encrypted at rest
- Logs are stored in Log Analytics North Europe (Ireland) – encrypted at rest

For UK organizations

- Backups are stored in Geo-redundant Azure Blob Storage – encrypted at rest:
 - Primary replica – UK South
 - Secondary replica – UK West
- Unpacked backups are stored on Azure virtual disks that are associated with independent Elasticsearch nodes (per customer) which are part of Azure Kubernetes Service UK South – encrypted at rest
- Logs are stored in Log Analytics UK South – encrypted at rest

For Australian organizations

- Backups are stored in Geo-redundant Azure Blob Storage – encrypted at rest:
 - Primary replica – Australia East
 - Secondary replica – Australia Southeast
- Unpacked backups are stored on Azure virtual disks that are associated with independent Elasticsearch nodes (per customer) which are part of Azure Kubernetes Service Australia East – encrypted at rest
- Logs are stored in Log Analytics Australia East– encrypted at rest

Other regions are supported on customer request.

Privacy and protection of customer data

The most sensitive customer data collected and stored by Identity Recovery for Microsoft Entra ID is the Microsoft Entra ID and Microsoft 365 data including users, groups, service principals, conditional access policies, devices and their associated properties. All properties which are available in Microsoft Graph API and MSOnline – such as users email, work title, department, phone number, address and others – are stored in the backup. Identity Recovery for Microsoft Entra ID does not back up and does not store user passwords and password hashes.

The backup data for each customer is stored in a separate Azure Blob Container. This information is protected through the Azure built in data at rest Server-Side encryption mechanism. It uses the strongest FIPS 140-2 approved block cipher available, Advanced Encryption Standard (AES) algorithm, with a 256-bit key.

Geo-redundant storage is used which means that backup data is replicated to a secondary region that is hundreds of miles away from the primary region. Backup data is durable even in the case of a complete regional outage or a disaster in which the primary region is not recoverable.

For more information about Azure Blob Storage, see the following Microsoft Learn topics:

- [Introduction to Azure Blob Storage](#)
- [Security recommendations for Blob storage](#)
- [Azure Storage encryption for data at rest](#)
- [Geo-redundant-storage](#)

Separation of customer data

A common concern related to cloud based services is the prevention of commingling of data that belongs to different customers. Identity Recovery for Microsoft Entra ID has architected its solution to specifically prevent such data commingling by logically separating customer data stores.

Customer data is differentiated using a unique organization identifier. This organization identifier is generated securely during customer sign-up to Security Management Platform.

This identifier is used throughout the solution to ensure strict data separation of customers' backups in the Azure Blob storage.

Furthermore, each customer has its own instance of Elasticsearch that is used for unpack, object search, and restore operations. Elasticsearch index is stored on a separate Azure Disk with enabled encryption in the Quest Azure subscription.

Network communications

All communications to and from the Identity Recovery for Microsoft Entra ID web application go over HTTPS, and the SSL certificates are issued by trusted certificate authorities. As for the web application itself, it enforces that all communications occur over HTTPS connections. If a user tries to access via a regular HTTP, the application will redirect the request to HTTPS version of the endpoint's enabled connection. The solution communicates with Microsoft Graph API over HTTPS. TLS 1.2 is enforced for this communication.

User Authentication

The customer logs in to the solution by providing Security Management Platform user account credentials.

The process of registering an Microsoft Entra tenant into Identity Recovery for Microsoft Entra ID is handled through the well established Azure admin consent workflow. For more information about user authentication, see the Security Management Platform Global Settings product documentation:

- [User Guide](#)
- [Release Notes](#)
- [Security Guide](#)

Role based access control

Quest Security Management Platform 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, see [Adding users and groups to an organization](#) in the *Security Management Platform Global Settings User Guide*.

List of permissions that can be assigned to Identity Recovery for Microsoft Entra ID users

- Can Mange Backup Settings
- Can Download Hybrid Credentials
- Can Manage Events
- Can Manage Project Settings
- Can Read Backup History
- Can Read Differences
- Can Read Events
- Can Read Restore Attributes
- Can Read Task History
- Can Read UI Projects
- Can Read UI Collections
- Can Read Unpacked Objects
- Can Restore from Differences
- Can Restore from Objects
- Can Run Backup Manually
- Can Run Difference Report
- Can Unpack Backups

i | **NOTE:** Platform administrators have full access to global settings and all module permissions.

FIPS 140-2 compliance

Identity Recovery for Microsoft Entra ID cryptographic usage is based on Azure FIPS 140-2 compliant cryptographic functions. For more information, see [Security recommendations for Blob storage](#) in Microsoft Learn.

SDLC and SDL

The Identity Recovery for Microsoft Entra ID Development team follows a managed Software Development Lifecycle (SDLC).

The Identity Recovery for Microsoft Entra ID team follows a strict Quality Assurance cycle.

All product code is reviewed by another developer before check in.

In addition, the Development team follows a managed Security Development Lifecycle (SDL) which includes:

- MS-SDL best practices
- Threat modeling
- OWASP guidelines
- Static code analysis is performed on a regular basis.
- Vulnerability scanning is performed on a regular basis.
- Segregated Development, Pre-Production, and Production environments. Customer data is not used in Development and Pre-Production environments.

Identity Recovery for Microsoft Entra ID developers go through the same set of hiring processes and background checks as other Quest employees.

Third party assessments and certifications

Penetration testing

Security Management Platform (formerly On Demand) has undergone a third party security assessment and penetration testing yearly since 2017. A summary of the results is available upon request.

Certification

Security Management Platform (formerly On Demand) is included in the scope of the Platform Management ISO/IEC 27001, 27701, 27017, and 27018 certification:

- ISO/IEC 27001:2022 Information technology — Security techniques — Information security management systems — Requirements: **Certificate Number: 1156977-8**, valid until **2028-07-27**.
- ISO/IEC 27701:2019 Information security, cybersecurity and privacy protection — Privacy information management systems — Requirements and guidance: **Certificate Number: 1156977-8**, valid until **2028-07-27**.
- ISO/IEC 27017:2015 Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services: **Certificate Number: 1156977-8**, valid until **2028-07-27**.
- ISO/IEC 27018:2019 Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors: **Certificate Number: 1156977-8**, valid until **2028-07-27**.

Quest Software, Inc. has successfully completed a SOC 2 examination of its Security Management Platform (formerly On Demand). 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, 2024, to July 31, 2025**

Service Auditor: **Schellman & Company, LLC**

Operational security

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, if a developer (or any other employee with access to Identity Recovery for Microsoft Entra ID) leaves the company, this individual immediately loses access to the systems. All code is versioned in source control.

Permissions required to configure and operate Identity Recovery for Microsoft Entra ID

Identity Recovery for Microsoft Entra ID is a part of Quest Security Management Platform cloud-based management platform. The main interface through which the customer interacts with and configures the solution is its web application. It does not require the installation of any software components on the customer's systems.

To access Identity Recovery for Microsoft Entra ID, a customer representative goes to the website quest-on-demand.com and signs up for a Security Management Platform account. When you create an account, an organization is automatically created. The account is verified through email; thus, a valid email address must be provided when signing up.

Prerequisites

A Microsoft Entra Global Administrator must grant admin consent to provision Identity Recovery for Microsoft Entra ID for customer's Microsoft Entra ID with the following permissions. Once consent is granted, the account can be downgraded if necessary.

Microsoft Graph

- Read all groups
- Read and write all groups
- Read and write directory data
- Read directory data

Microsoft Entra ID

- Read and write directory data
- Read directory data

OAuth 2.0 permission grants

Microsoft Graph

- Access directory as the signed in user
- Read all groups
- Read and write all groups
- Read and write directory data
- Read directory data

Microsoft Entra ID

- Read all groups
- Read and write all groups
- Read and write directory data
- Read directory data
- Sign in and read user profile

Identity Recovery for Microsoft Entra ID does not use and does not store Microsoft Entra Global Administrator account credentials. This account is used only to provision the Quest Azure application.

Customer measures

Identity Recovery for Microsoft Entra ID security features are only one part of a secure environment. Customers need to operate by their own best security practices when proceeding with data recovery. Particular care needs to be given to protecting the credentials of the Microsoft Entra tenants Global Administrator accounts.

Quest Software creates technology and solutions that build the foundation for enterprise AI. Focused on data management and governance, cybersecurity and platform modernization, Quest helps organizations address their most pressing challenges and make the promise of AI a reality. Around the globe, more than 45,000 companies including over 90% of the Fortune 500 count on Quest Software. For more information, visit www.quest.com or follow Quest Software on [X \(formerly Twitter\)](#) and [LinkedIn](#).

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