

Quest® On Demand Migration  
**Account Activity and Permissions Guide**

## 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  
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, 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 <https://www.quest.com/legal>. 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, TIP, MOBILE, or VIDEO:** An information icon indicates supporting information.

# ACCOUNT ACTIVITY MATRIX

## ACCOUNTS

Account \ Activity	ROLES	DEPLOY	DISCOVER	MATCH	MIGRATE
<p><b>Consent Account</b></p> <p>This is the account the client brings to register each tenant with ON DEMAND.</p> <p>The account for granting consent is not stored or used for later activities. The Quest Application Service Principle "Quest On Demand - Migration - Basic" is used for later automation activities using <b>PowerShell</b> and the <b>MS Graph APIs</b>.</p> <p>Credentials are never saved within the application.</p>	<p>ADDING TENANTS Global Administrator</p>	<p>DEPLOY MIGRATION PROJECT During deployment, this account is used to install the Quest application to each tenant.</p>	<p>DISCOVER OBJECTS Using OAuth token-based app authentication, ON DEMAND discovers objects, properties and basic stats within each tenant for the selected workload.</p>	<p>MATCH SOURCE TO TARGET ACCOUNTS AND GROUPS This task will read each tenant to determine which target objects match the source based on the selected attributes.</p>	<p>MIGRATE ACCOUNTS This task will begin the creation of selected accounts or groups in the target tenant.</p>
		<p>INITIAL TENANT DISCOVERY Automated verifications of Tenant settings such as region, Multi-Geo settings and domains are collected during project set up.</p>			
<p><b>Optional Service Account</b></p> <p>This account's credentials are supplied by the customer for each tenant.</p> <p>This account is used for automation purposes when Graph isn't sufficient. Utilizing APIs such as <b>PowerShell</b> or <b>EWS</b>.</p>	<p>MIGRATE GUEST USER Target Guest Inviter</p>	<p>*No Activity</p>	<p>*No Activity</p>	<p>*No Activity</p>	<p>GUESTS This task will create a guest target account based on the source target account.</p>

# ACCOUNT ACTIVITY MATRIX

## MAILBOXES

Activity Account	ROLES	DEPLOY	COEXISTENCE	CALENDAR	DISCOVER	MATCH	STATS	MIGRATE	SWITCH	DESKTOP
<p><b>Consent Account</b></p> <p>This is the account the client brings to register each tenant with ON DEMAND.</p> <p>The account for granting consent is not stored or used for later activities. The Quest Application Service Principle "Quest On Demand - Migration – Mailbox Migration" is used for later automation activities using <b>PowerShell</b> and the <b>MS Graph APIs</b>.</p> <p>Credentials are never saved within the application.</p>	<p>ADDING TENANTS Global Administrator</p>	<p>DEPLOY MIGRATION PROJECT During deployment, this account is used to install the Quest application to each tenant.</p>	<p>DEPLOY DOMAIN COEXISTENCE When a customer chooses to enable Domain coexistence services, better known as address rewrite, a series of events occurs to fully configure the service within each tenant.</p> <p>During deployment ON DEMAND will create in each tenant a set of Transport Rules and Connectors to route mail that is eligible for address rewrite services.</p>	<p>CREATE ORG RELATIONSHIP Automatically create an <b>organizational relationship</b> between the source and the target tenants to allow source users to retrieve calendar availability information from target calendars only.</p> <p>The organizational relationship settings may be modified post deployment to allow for greater access and permissions between tenants if desired.</p>	<p>DISCOVER OBJECTS Using OAuth token-based app authentication, ON DEMAND discovers objects, properties and basic stats within each tenant for the selected workload.</p>	<p>MATCH SOURCE TO TARGET ACCOUNTS AND GROUPS This task will read each tenant to determine which target objects match the source based on the selected attributes.</p>	<p>MAILBOXES This task collects statistics about source mailboxes such as size, number of items &amp; folders, archive info., legal hold settings and permissions.</p>	<p>LICENSE ACCOUNTS Applies selected subscription plan for the selected workload for the target account. Also enables Archive Mailboxes if enabled in source.</p>	<p>SWITCH APPLICATIONS This task will trigger the process to prompt the end-user to begin reconfiguring their local desktop applications &amp; MS 365 apps subscription. Application.</p>	<p>SOURCE &amp; TARGET MAILBOX ACCESS This Desktop Update task requires access to the source mailbox in order to deposit a hidden email message to trigger the switch over of the user's desktop applications.</p>
		<p>INITIAL TENANT DISCOVERY Automated verifications of Tenant settings such as region, Multi-Geo settings and domains are collected during project set up.</p>	<p>FORWARDING RULES This migration task option allows you to set the Mailbox Forwarding to ensure any new mail is sent to the desired mailbox either before or after the migration.</p>	<p>MIGRATE WORKLOAD CONTENT This task will begin the content migration for the selected workload(s).</p> <p>Content migrations copy data but also permissions and common settings.</p>	<p>NOTIFICATIONS During this task email notifications will be sent to the source and/or target mailboxes upon completion of the switch over.</p>	<p>RE-SEND NOTIFICATION The Desktop Update Agent offers an optional task to resend the switch applications email to the selected user's source mailbox to remind them this task must be completed by them to finalize their migration.</p>				

# ACCOUNT ACTIVITY MATRIX

## PUBLIC FOLDERS

Account \ Activity	ROLES	DISCOVER	MIGRATE
<p><b>Optional Service Account</b></p> <p>This account's credentials are supplied by the customer for each tenant.</p> <p>This account is used for automation purposes when Graph isn't sufficient. Utilizing APIs such as <b>PowerShell</b> or <b>EWS</b>.</p>	<p>PUBLIC FOLDERS</p> <p>Exchange Administrator</p>	<p>PUBLIC FOLDERS</p> <p>During this task, the source tenant's Public Folder(s) paths will be collected and displayed in the Public Folders tab for migration management.</p>	<p><b>PUBLIC FOLDERS CONTENT MIGRATION</b></p> <p>This migration task will copy all types of Public Folders content (appointment, contact, journal, mail, note, task, and permissions) to the target if supported in the target tenant.</p> <p>The task will provision the public folder(s) in target based on the source if it does not already exist.</p> <p>If the PF path does already exist on the target, the source public folder will not be migrated.</p> <p>To migrate PF permissions and related mail settings, all related user accounts must be matched under On Demand Accounts.</p>

# ACCOUNT ACTIVITY MATRIX

ONEDRIVE

Account \ Activity	ROLES	DEPLOY	DISCOVER	PROVISION	STATS	MIGRATE
<p><b>Consent Account</b></p> <p>This is the account the client brings to register each tenant with ON DEMAND.</p> <p>The account for granting consent is not stored or used for later activities. The Quest Application Service Principle "Quest On Demand - Migration - SharePoint" is used for later automation activities using the <b>MS Graph APIs</b>.</p> <p>Credentials are never saved within the application.</p>	<p>ADDING TENANTS Global Administrator</p>	<p>DEPLOY MIGRATION PROJECT</p> <p>During deployment, this account is used to install the Quest application to each tenant.</p>	<p>DISCOVER OBJECTS</p> <p>Using OAuth token-based app authentication, ON DEMAND discovers objects, properties and basic stats within each tenant for the selected workload.</p>	<p>* No Activity</p>	<p>ONEDRIVE</p> <p>This task collects statistics about source OneDrive such as size and number of items.</p>	<p>MIGRATE WORKLOAD CONTENT</p> <p>This task will begin the content migration for OneDrive. Content migrations copy data but also permissions and common settings.</p>
		<p>INITIAL TENANT DISCOVERY</p> <p>Automated verifications of Tenant settings such as region, Multi-Geo settings and domains are collected during project set up.</p>				
<p><b>Optional Service Account</b></p> <p>This account's credentials are supplied by the customer for each tenant.</p> <p>This account is used for automation purposes when Graph isn't sufficient. Utilizing APIs such as <b>PowerShell</b> or <b>EWS</b>.</p>	<p>PROVISION ONEDRIVE SharePoint Administrator</p>	<p>* No Activity</p>	<p>* No Activity</p>	<p>ONEDRIVE</p> <p>The OneDrive migration task will automatically provision the target OneDrive container if it has not already completed.</p> <p>If this account is not configured, then this task must be completed manually by the target administrator prior to any data migrations.</p>	<p>* No Activity</p>	<p>* No Activity</p>

# ACCOUNT ACTIVITY MATRIX

## SHAREPOINT

Account \ Activity	ROLES	DEPLOY	DISCOVER	MATCH	MIGRATE	RESOURCE PROCESSING
<p><b>Consent Account</b></p> <p>This is the account the client brings to register each tenant with ON DEMAND.</p> <p>The account for granting consent is not stored or used for later activities. The Quest Application Service Principle "Quest On Demand - Migration - SharePoint" is used for later automation activities using the <b>MS Graph APIs</b>.</p> <p>Credentials are never saved within the application.</p>	<p>ADDING TENANTS Global Administrator</p>	<p>DEPLOY MIGRATION PROJECT</p> <p>During deployment, this account is used to install the Quest application to each tenant.</p>	<p>DISCOVER OBJECTS</p> <p>Using OAuth token-based app authentication, ON DEMAND discovers objects, properties and basic stats within each tenant for the selected workload.</p>	<p>MATCH SOURCE TO TARGET SHAREPOINT SITES</p> <p>This task will read the SharePoint Site collections to match the source site collections with the corresponding target site collections.</p>	<p>MIGRATE WORKLOAD CONTENT</p> <p>This task will begin the content migration for the selected workload(s).</p> <p>Content migrations copy data but also permissions and common settings.</p> <p>During a SharePoint Migration the task will provision the SharePoint Sites, Webs and Lists.</p>	<p>*No Activity</p>
		<p>INITIAL TENANT DISCOVERY</p> <p>Automated verifications of Tenant settings such as region, Multi-Geo settings and domains are collected during project set up.</p>				
<p><b>Optional Service Account</b></p> <p>This account's credentials are supplied by the customer for each tenant.</p> <p>This account is used for automation purposes when Graph isn't sufficient. Utilizing APIs such as <b>PowerShell or EWS</b>.</p>	<p>PROCESS RESOURCES SharePoint Administrator Source Guest Inviter</p>	<p>*No Activity</p>	<p>*No Activity</p>	<p>*No Activity</p>	<p>*No Activity</p>	<p>GRANT TARGET ACCOUNTS ACCESS TO SOURCE TENANT</p> <p>This task provides the access to source resources by creating a linked guest user in the source for each migrated matched target account.</p> <p>These guest users are granted the same permissions as the corresponding source accounts and become members of the same SharePoint groups.</p>

# ACCOUNT ACTIVITY MATRIX

## TEAMS

Account	Activity	ROLES	DEPLOY	DISCOVER	STATS	PROVISION	MIGRATE
<p>Consent Account</p> <p>This is the account the client brings to register each tenant with ON DEMAND.</p> <p>The Quest Application Service Principle "Quest On Demand - Migration - Teams" is used for later automation activities using the <b>MS Graph APIs</b>.</p> <p>The account's OAuth token is securely cached because this account is added to each Team and Channel during the migration process.</p> <p>Credentials are never saved within the application.</p>		<p>ADDING TENANTS Global Administrator</p> <p>TEAMS &amp; MICROSOFT 365 GROUPS Teams Administrator</p> <p><b>This account must remain intact during the entirety of the Microsoft 365 Teams &amp; Groups migration project because this account is added to each Team and Channel during the migration process.</b></p> <p>Post-Migration this account may be safely deleted or removed.</p>	<p>DEPLOY MIGRATION PROJECT</p> <p>During deployment, this account is used to install the Quest application to each tenant.</p>	<p>DISCOVER OBJECTS</p> <p>Using OAuth token-based app authentication, ON DEMAND discovers objects, properties and basic stats within each tenant for the selected workload.</p>	<p>TEAMS &amp; MS 365 GROUPS</p> <p>These statistics are collected during the discovery task. The source Teams' Total Channels, File size, Number of channels, members, messages, plans &amp; tasks are captured.</p>	<p>TEAMS</p> <p>This task will create or merge to the target Team and associated Group which will be owned by target Admin Consent account.</p>	<p>MIGRATE WORKLOAD CONTENT</p> <p>This task will begin the content migration for the selected workload(s).</p> <p>Content migrations copy data but also permissions and common settings.</p> <p>Please Note: Not all SharePoint related data of a MS Team is migrated. Plan to migrate this data using On Demand for SharePoint.</p>
			<p>INITIAL TENANT DISCOVERY</p> <p>Automated verifications of Tenant settings such as region, Multi-Geo settings and domains are collected during project set up.</p>			<p>MS 365 GROUPS</p> <p>This task will create or merge to the target Team and associated Group which will be owned by target Admin Consent account.</p>	



# ACCOUNT ACTIVITY MATRIX

## FOR DIRECTORY SYNCHRONIZATION

ACCOUNTS	ROLES	DEPLOY	DISCOVER	SYNC
<p><b>ADMIN CONSENT ACCOUNT</b> This is the account the client uses to register each tenant to a project. The account's OAuth token is securely cached for later automation activities using MS Graph. The account password is never saved within the application.</p>	<p>ACCOUNT SETUP User Administrator</p> <p>USERS, GROUPS &amp; CONTACTS Exchange Administrator</p> <p>TEAMS Teams Administrator</p>	<p>DEPLOYMENT During deployment, this account is used to configure all the required configuration components for directory sync. Such as creating the PowerShell Accounts and Distribution groups.</p>	<p>DISCOVER CHANGES Using OAuth token-based app authentication, On Demand discovers CHANGED objects and properties within each tenant. Such as users, groups, contacts, teams, etc.</p>	<p>SYNC ENVIRONMENT Using OAuth token-based app authentication. On Demand updates Azure AD properties during workflow synchronization.</p>
<p><b>POWERSHELL ACCOUNTS</b> Three (3) accounts are created by On Demand Directory Sync in each tenant. This account is used for PowerShell operations during workflow processing. One (1) mail-enabled security group, with the three (3) accounts above as members, is created by On Demand Directory Sync in each tenant and is used to synchronize group membership.</p>	<p>ALL WORKFLOWS User Administrator Exchange Administrator Teams Administrator</p>	<p>* NO ACTIVITY</p>	<p>DISCOVER ENVIRONMENT Using PowerShell, On Demand discovers objects and properties within each tenant. Such as the users, groups, contacts, teams, etc.</p>	<p>SYNC ENVIRONMENT Using PowerShell, On Demand creates, updates, renames, moves or deletes objects within each tenant as determined by the Workflow configuration.</p>
<p><b>ACTIVE DIRECTORY AGENT ACCOUNT</b> This account is created by the client in each AD Forest where a Directory Sync agent is deployed. This account is used for read and write access to the local AD during workflow synchronization.</p>	<p>DOMAIN USER WITH RIGHTS TO CREATE AND MODIFY OBJECTS IN LOCAL ACTIVE DIRECTORY</p>	<p>* NO ACTIVITY</p>	<p>* NO ACTIVITY</p>	<p>SYNC ENVIRONMENT Using LDAP, On Demand creates, updates, renames, moves or deletes objects within each local AD as determined by the workflow configuration.</p>

# ACCOUNT ACITIVITY MATRIX

## FOR DOMAIN MOVES

ACCOUNTS	ROLES	DEPLOY	DISCOVERY	UPDATE SOURCE	MOVE DOMAIN	UPDATE TARGET
<b>ADMIN CONSENT ACCOUNT</b> This is the account the client uses to register each tenant to a project. The account's OAuth token is securely cached for later automation activities using MS Graph. The account password is never saved within the application.	ACCOUNT SETUP User Administrator  USERS, GROUPS & CONTACTS Exchange Administrator  DOMAIN MOVE Global Administrator	DEPLOYMENT During deployment, this account is used to configure all the required configuration components for directory sync. Such as creating the PowerShell Accounts, Distribution groups and assigning roles.	DISCOVER CLOUD ENVIRONMENT During the initial discovery, all source users and groups using this domain being cutover.	UPDATE CLOUD ENVIRONMENT Domain Move will replace the domain being moved with the desired domain for all cloud users and groups.	* NO ACTIVITY	UPDATE CLOUD ENVIRONMENT Domain Move will update the primary address for all matched cloud only users and groups.
<b>POWERSHELL ACCOUNTS</b> Three (3) accounts are created by On Demand Directory Sync in each tenant. This account is used for PowerShell operations during workflow processing. One (1) mail-enabled security group, with the three (3) accounts above as members, is created by On Demand Directory Sync in each tenant and is used to synchronize group membership.	ALL WORKFLOWS User Administrator Exchange Administrator  DOMAIN MOVE Global Administrator	PROJECT SETUP When the project is created, and the advanced relay mode is selected this account is used to configure the corresponding transport rules and connectors within Exchange Online to facilitate secure message transfer during the migration process.	DISCOVER MAIL ATTRIBUTES Using MS PowerShell, mail related attributes will be collected about users and groups.	UPDATE SELECT ATTRIBUTES Using MS PowerShell, some mail related attributes will be updated for users and groups.	REMOVE DOMAIN Using MS PowerShell, the domain is removed from the source tenant.  ADD DOMAIN Using MS PowerShell, the domain is added to the target tenant.  Manual validation is required by an administrator once the domain is added.	UPDATE SELECT ATTRIBUTES Using MS PowerShell, some mail related attributes will be updated for users and groups.
<b>ACTIVE DIRECTORY AGENT ACCOUNT</b> This account is created by the client in each AD Forest where a Directory Sync agent is deployed. This account is used for read and write access to the local AD during workflow synchronization as related to the domain move process.	DOMAIN USER WITH RIGHTS TO CREATE AND MODIFY SELECT OBJECTS IN LOCAL ACTIVE DIRECTORY	* NO ACTIVITY	DISCOVER LOCAL ENVIRONMENT The Active Directory Account for the local agent, is used to discovery AD OUs, and Schema.	UPDATE LOCAL ENVIRONMENT Domain Move will replace the domain being moved with the desired domain for all local users and groups.	* NO ACTIVITY	UPDATE LOCAL ENVIRONMENT Domain Move will update the primary address for all matched local hybrid users and groups.

# API PERMISSION MATRIX

## FOR BASIC CORE CONSENT

PERMISSION	profile	Directory.Read.All	Organization.Read.All	AuditLog.Read.All	Reports.Read.All
NAME	VIEW USERS' BASIC PROFILE	READ DIRECTORY DATA	ORGANIZATION.READ.ALL	READ ALL AUDIT LOG DATA	READ ALL USAGE REPORTS
TYPE	DELEGATED	APPLICATION	APPLICATION	APPLICATION	APPLICATION
DESCRIPTION	Allows the app to see your users' basic profile (name, picture, user name).	Allows the app to read data in your organization's directory, such as users, groups and apps, without a signed-in user.	Allows the app to read the organization and related resources, without a signed-in user. Related resources include things like subscribed skus and tenant branding information.	Allows the app to read and query your audit log activities, without a signed-in user.	Allows an app to read all service usage reports without a signed-in user. Services that provide usage reports include Office 365 and Azure Active Directory.
API	MICROSOFT GRAPH	MICROSOFT GRAPH	MICROSOFT GRAPH	MICROSOFT GRAPH	MICROSOFT GRAPH

# API PERMISSION MATRIX

## FOR BASIC CONSENT

PERMISSION	Exchange.ManageAsApp	Directory.ReadWrite.All	Group.ReadWrite.All	RoleManagement.ReadWrite.Directory
NAME	MANAGE EXCHANGE AS APPLICATION	READ AND WRITE DIRECTORY DATA	READ AND WRITE ALL GROUPS	READ AND WRITE ALL DIRECTORY RBAC SETTINGS
TYPE	APPLICATION	APPLICATION	APPLICATION	APPLICATION
DESCRIPTION	Allows the app to manage the organization's Exchange environment without any user interaction. This includes mailboxes, groups, and other configuration objects. To enable management actions, an admin must assign the appropriate roles directly to the app.	Allows the app to read and write data in your organization's directory, such as users, and groups, without a signed-in user. Does not allow user or group deletion.	Allows the app to create groups, read all group properties and memberships, update group properties and memberships, and delete groups. Also allows the app to read and write group calendar and conversations. All these operations can be performed by the app without a signed-in user.	Allows the app to read and manage the role-based access control (RBAC) settings for your company's directory, without a signed-in user. This includes instantiating directory roles and managing directory role membership, and reading directory role templates, directory roles and memberships.
API	OFFICE 365 EXCHANGE ONLINE	MICROSOFT GRAPH	MICROSOFT GRAPH	MICROSOFT GRAPH

# API PERMISSION MATRIX

## FOR MAILBOX MIGRATION CONSENT

PERMISSION	User.Read	Directory.ReadWrite.All	Calendars.ReadWrite	full_access_as_app
NAME	SIGN IN AND READ USER PROFILE	READ AND WRITE DIRECTORY DATA	READ AND WRITE CALENDARS IN ALL MAILBOXES	USE EXCHANGE WEB SERVICES WITH FULL ACCESS TO ALL MAILBOXES
TYPE	DELEGATED	APPLICATION	APPLICATION	APPLICATION
DESCRIPTION	Allows the app to read and write data in your organization's directory, such as users, and groups, without a signed-in user. Does not allow user or group deletion.	Allows the app to create, read, update, and delete events of all calendars without a signed-in user.	Allows users to sign-in to the app and allows the app to read the profile of signed-in users. It also allows the app to read basic company information of signed-in users.	Allows the app to have full access via Exchange Web Services to all mailboxes without a signed-in user.
API	MICROSOFT GRAPH	MICROSOFT GRAPH	MICROSOFT GRAPH	OFFICE 365 EXCHANGE ONLINE

# API PERMISSION MATRIX

## FOR SHAREPOINT CONSENT

PERMISSION	Directory.ReadWrite.All	Files.Read.All	Directory.ReadWrite.All	Sites.ReadWrite.All	Sites.FullControl.All	Sites.Manage.All	TermStore.ReadWrite.All	User.ReadWrite.All
NAME	READ AND WRITE DIRECTORY DATA	READ FILES IN ALL SITE COLLECTIONS	READ AND WRITE DIRECTORY DATA	READ AND WRITE ITEMS IN ALL SITE COLLECTIONS	HAVE FULL CONTROL OF ALL SITE COLLECTIONS	READ AND WRITE ITEMS AND LISTS IN ALL SITE COLLECTIONS	READ AND WRITE MANAGED METADATA	READ AND WRITE USER PROFILES
TYPE	APPLICATION	APPLICATION	APPLICATION	APPLICATION	APPLICATION	APPLICATION	APPLICATION	APPLICATION
DESCRIPTION	Allows the app to read and write data in your organization's directory, such as users, and groups, without a signed-in user. Does not allow user or group deletion.	Allows the app to read all files in all site collections without a signed in user.	Allows the app to read and write data in your company or school directory, such as users, and groups. Does not allow user or group deletion.	Allows the app to create, read, update, and delete documents and list items in all site collections without a signed in user.	Allows the app to have full control of all site collections without a signed in user.	Allows the app to read, create, update, and delete document libraries and lists in all site collections without a signed in user.	Allows the app to write enterprise managed metadata and to read basic site info without a signed in user.	Allows the app to read and update user profiles and to read basic site info without a signed in user.
API	MICROSOFT GRAPH	MICROSOFT GRAPH	WINDOWS AZURE ACTIVE DIRECTORY	OFFICE 365 SHAREPOINT ONLINE	OFFICE 365 SHAREPOINT ONLINE	OFFICE 365 SHAREPOINT ONLINE	OFFICE 365 SHAREPOINT ONLINE	OFFICE 365 SHAREPOINT ONLINE



# API PERMISSION MATRIX

## FOR TEAMS CONSENT Part 2

PERMISSION	Notes.ReadWrite.All	TeamMember.ReadWrite.All	ChannelMember.ReadWrite.All	Teamwork.Migrate.All	ChatMember.ReadWrite.All	Notes.ReadWrite.All	user_impersonation	user_impersonation	Region.ReadWrite
NAME	READ AND WRITE ALL ONENOTE NOTEBOOKS	ADD AND REMOVE MEMBERS FROM ALL TEAMS	ADD AND REMOVE MEMBERS FROM ALL CHANNELS	CREATE CHAT AND CHANNEL MESSAGES WITH ANYONE'S IDENTITY AND WITH ANY TIMESTAMP	ADD AND REMOVE MEMBERS FROM ALL CHATS	VIEW AND MODIFY NOTES FOR ALL USERS	HAVE FULL ACCESS TO THE CHAT SERVICE AGGREGATOR	HAVE FULL ACCESS TO THE SKYPE TEAMS SERVICE	READ OR WRITE USER REGION
TYPE	APPLICATION	APPLICATION	APPLICATION	APPLICATION	APPLICATION	APPLICATION	DELEGATED	DELEGATED	DELEGATED
DESCRIPTION	Allows the app to read all the OneNote notebooks in your organization, without a signed-in user.	Add and remove members from all teams, without a signed-in user. Also allows changing a team member's role, for example from owner to non-owner.	Add and remove members from all channels, without a signed-in user. Also allows changing a member's role, for example from owner to non-owner.	Allows the app to create chat and channel messages, without a signed in user. The app specifies which user appears as the sender and can backdate the message to appear as if it was sent long ago. The messages can be sent to any chat or channel in the organization.	Add and remove members from all chats, without a signed-in user.	Allows the app to view and modify the OneNote notes of other users in your organization, without a signed-in user. The app cannot access notes under password-protected sections.	Allow application full access to the Chat service aggregator on behalf of the signed-in user	Allow the application full access to the Skype Teams Service on behalf of the signed-in user	Allows the app to read or write the region for all users in your organization
API	MICROSOFT GRAPH	MICROSOFT GRAPH	MICROSOFT GRAPH	MICROSOFT GRAPH	MICROSOFT GRAPH	ONENOTE	MICROSOFT TEAMS CHAT AGGREGATOR	MICROSOFT TEAMS SERVICES	MICROSOFT TEAMS SERVICES



# API PERMISSION MATRIX

## FOR DIRECTORY SYNCRONIZATION

PERMISSION	Group.ReadWrite.All	Directory.ReadWrite.All	RoleManagement.ReadWrite.Directory	User.Read.All
NAME	READ AND WRITE ALL GROUPS	READ AND WRITE DIRECTORY DATA	READ AND WRITE DIRECTORY RBAC SETTINGS	READ ALL USERS' FULL PROFILES
TYPE	DELEGATED	DELEGATED	DELEGATED	DELEGATED
DESCRIPTION	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.	Allows the app to read and write data in your organization's directory, such as users, and groups. It does not allow the app to delete users or groups or reset user passwords.	Allows the app to read and manage the role-based access control (RBAC) settings for your company's directory, on behalf of the signed-in user. This includes instantiating directory roles and managing directory role membership, and reading directory role templates, directory roles and memberships.	Allows the app to read the full set of profile properties, reports, and managers of other users in your organization, on behalf of the signed-in user.
API	MICROSOFT GRAPH	MICROSOFT GRAPH	MICROSOFT GRAPH	MICROSOFT GRAPH

# API PERMISSION MATRIX

## FOR DOMAIN MOVE

PERMISSION	Group.ReadWrite.All	Directory.ReadWrite.All	RoleManagement.ReadWrite.Directory	User.Read.All
NAME	READ AND WRITE ALL GROUPS	READ AND WRITE DIRECTORY DATA	READ AND WRITE DIRECTORY RBAC SETTINGS	READ ALL USERS' FULL PROFILES
TYPE	DELEGATED	DELEGATED	DELEGATED	DELEGATED
DESCRIPTION	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.	Allows the app to read and write data in your organization's directory, such as users, and groups. It does not allow the app to delete users or groups or reset user passwords.	Allows the app to read and manage the role-based access control (RBAC) settings for your company's directory, on behalf of the signed-in user. This includes instantiating directory roles and managing directory role membership, and reading directory role templates, directory roles and memberships.	Allows the app to read the full set of profile properties, reports, and managers of other users in your organization, on behalf of the signed-in user.
API	MICROSOFT GRAPH	MICROSOFT GRAPH	MICROSOFT GRAPH	MICROSOFT GRAPH

## Contacting Quest

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](http://www.quest.com).

## Technical support resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at <https://support.quest.com>.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to-videos
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product.