On Demand Migration Permissions

Reference Guide

Contents

Permissions Summary

Consent Permission Types are Application (A) and Delegated (D).

Quest On Demand - Core - Basic

Purpose: Initial tenant setup. Required for source and target tenant

Permission	Description	API	Type
AuditLog.Read.All	READ ALL AUDIT LOG DATA	Graph	A
Directory.Read.All	READ DIRECTORY DATA	Graph	A
Organization.Read.All	ORGANIZATION.READ.ALL	Graph	A, D
profile	VIEW USERS' BASIC PROFILE	Graph	D
Reports.Read.All	READ ALL USAGE REPORTS	Graph	A

Quest On Demand - Migration - Basic - Minimal

Purpose: Account discovery and migration. Required for source tenant

Permission	Description	API	Type
Application.Read.All	READ DIRECTORY DATA	Graph	A
Group.Read.All	READ ALL GROUPS	Graph	A
RoleManagement.ReadWrite.Directory	READ AND WRITE ALL DIRECTORY RBAC SETTINGS	Graph	A
Exchange.ManageAsApp	MANAGE EXCHANGE AS APPLICATION	Exchange Online	A

Quest On Demand - Migration - Basic - Full

Purpose: Account discovery and migration. Required for target tenant

Permission	Description	API	Type
Directory.AccessAsUser.All	ACCESS DIRECTORY AS THE SIGNED IN USER	Graph	D
Directory.ReadWrite.All	READ AND WRITE DIRECTORY DATA	Graph	A
Group.ReadWrite.All	READ AND WRITE ALL GROUPS	Graph	A

Permission	Description	API	Type
RoleManagement.ReadWrite.Directory	READ AND WRITE ALL DIRECTORY RBAC SETTINGS	Graph	A
Exchange.ManageAsApp	MANAGE EXCHANGE AS APPLICATION	Exchange Online	A

Quest On Demand - Migration - Mailbox Migration - Minimal

Purpose: Mailbox discovery and migration. Required for source tenant

Permission	Description	API	Type
Calendars.Read	READ CALENDARS IN ALL MAILBOXES	Graph	A
full_access_as_app	USE EXCHANGE WEB SERVICES WITH FULL ACCESS TO ALL MAILBOXES	Exchange Online	A

Quest On Demand - Migration - Mailbox Migration - Full

Purpose: Mailbox discovery and migration. Required for target tenant.

Permission	Description	API	Type
Calendars.Read.Shared	READ USER AND SHARED CALENDARS	Graph	D

Permission	Description	API	Type
Calendars.ReadWrite	READ AND WRITE CALENDARS IN ALL MAILBOXES	Graph	A
full_access_as_app	USE EXCHANGE WEB SERVICES WITH FULL ACCESS TO ALL MAILBOXES	Exchange Online	A

Quest On Demand - Migration - Mailbox Migration - Custom RBAC

Purpose: Authorize the migration of selected mailboxes only. Exchange Online RBAC permissions must be set up in the tenant for Exchange Web Services (EWS) to ensure that On Demand Migration can migrate mailbox data for users within the scope of the RBAC configuration. Additional consents are required when used in source or target tenants. Detailed implementation instructions are available in the Knowledge Base or you can contact Quest Technical Support for assistance.

Permission	Description	API	Type
Directory.Read.All	READ DIRECTORY DATA	Graph	A

Quest On Demand - Migration - OneDrive - Minimal

Purpose: OneDrive discovery. Required for source tenant

Permission	Description	API	Type
Files.Read.All	READ FILES IN ALL SITE COLLECTIONS	Graph	A

Permission	Description	API	Type
Sites.FullControl.All	HAVE FULL CONTROL OF ALL SITE COLLECTIONS	SPO	A

Quest On Demand - Migration - OneDrive - Full

Purpose: OneDrive migration. Required for target tenant

Permission	Description	API	Type
Directory.Read.All	READ DIRECTORY DATA	Graph	A
Files.Read.All	READ FILES IN ALL SITE COLLECTIONS	Graph	A
Sites.FullControl.All	HAVE FULL CONTROL OF ALL SITE COLLECTIONS	SPO	A

Quest On Demand - Migration - Power BI

Purpose: Power BI migration. Required for source and target tenant

Permission	Description	API	Type
profile	VIEW USERS' BASIC PROFILE	Graph	D

Quest On DemandQuest On Demand - Migration - SharePoint - Minimal

Purpose: SharePoint discovery. Required for source tenant

Permission	Description	API	Type
Directory.Read.All	READ DIRECTORY DATA	Graph	A
Files.Read.All	READ FILES IN ALL SITE COLLECTIONS	Graph	A
Sites.FullControl.All	HAVE FULL CONTROL OF ALL SITE COLLECTIONS	SPO	A
Sites.Read.All	READ ITEMS IN ALL SITE COLLECTIONS	SPO	A
TermStore.Read.All	READ MANAGED METADATA	SPO	A
TermStore.Read.All	READ MANAGED METADATA	Graph	A

Quest On Demand - Migration - SharePoint - Full

Purpose: SharePoint migration. Required for target tenant

Permission	Description	API	Type
Directory.Read.All	READ DIRECTORY DATA	Graph	A

Permission	Description	API	Type
Files.Read.All	READ FILES IN ALL SITE COLLECTIONS	Graph	A
Sites.FullControl.All	HAVE FULL CONTROL OF ALL SITE COLLECTIONS	SPO	A
Sites.Read.All	READ ITEMS IN ALL SITE COLLECTIONS	SPO	A
TermStore.Read.All	READ MANAGED METADATA	Graph	A
TermStore.ReadWrite.All	READ AND WRITE MANAGED METADATA	SPO	A

Quest On Demand - Migration - Teams - Minimal

Purpose: Teams, M365 Groups, and Chat discovery. Required for source tenant

Permission	Description	API	Type
Authorization.ReadWrite	TEAMS AUTHORIZATION READWRITE	Teams	D
ChannelMember.ReadWrite.All	ADD AND REMOVE MEMBERS FROM ALL CHANNELS	Graph	A
ChannelMessage.Read.All	READ ALL CHANNEL MESSAGES	Graph	A
ChannelSettings.Read.All	READ THE NAMES, DESCRIPTIONS, AND SETTINGS OF ALL CHANNELS	Graph	A
Chat.Read.All	READ ALL CHAT MESSAGES	Graph	A
ChatMember.Read.All	READ MEMBERS FROM ALL CHATS	Graph	A
Directory.Read.All	READ DIRECTORY DATA	Graph	D
Group.ReadWrite.All	READ AND WRITE ALL GROUPS	Graph	A, D
Notes.Read.All	READ ALL ONENOTE NOTEBOOKS AND NOTES FOR ALL USERS	Graph, OneNote	A

Permission	Description	API	Type
Notes.ReadWrite.All	READ AND WRITE ALL ONENOTE NOTEBOOKS AND NOTES FOR ALL USERS	Graph, OneNote	A
Region.ReadWrite	READ OR WRITE USER REGION	Teams	D
Reports.Read.All	READ ALL USAGE REPORTS	Graph	A
Sites.Read.All	READ ITEMS AND LISTS IN ALL SITE COLLECTIONS	SPO	A
Tasks.Read.All	READ ALL USERS TASKS AND TASK LISTS	Graph	A
TeamMember.ReadWrite.All	ADD AND REMOVE MEMBERS FROM ALL TEAMS	Graph	A
TeamsAppInstallation.ReadWriteForTeam.All	MANAGE TEAMS APPS FOR ALL TEAMS	Graph	A
TeamSettings.Read.All	READ ALL TEAMS SETTINGS	Graph	A
TeamsTab.Read.All	READ TABS IN MICROSOFT TEAMS	Graph	A
Teamwork.Migrate.All	CREATE CHAT AND CHANNEL MESSAGES WITH ANYONE'S	Graph	A

Permission	Description	API	Type
	IDENTITY AND WITH ANY TIMESTAMP		
TeamworkTag.ReadWrite.All	READ AND WRITE TAGS IN TEAMS	Graph	A
User.Read.All	READ ALL USERS' FULL PROFILES	Graph	A, D
user_impersonation	HAVE FULL ACCESS TO THE CHAT SERVICE AGGREGATOR AND SKYPE TEAMS SERVICE	Teams	D

Quest On Demand - Migration - Teams - Full

Purpose: Teams, M365 Groups, and Chat migration. Required for target tenant

Permission	Description	API	Type
Authorization.ReadWrite	TEAMS AUTHORIZATION READWRITE	Teams	D
ChannelMember.ReadWrite.All	ADD AND REMOVE MEMBERS FROM ALL CHANNELS	Graph	A
ChannelMessage.Read.All	READ ALL CHANNEL MESSAGES	Graph	A
ChannelMessage.Send	SEND CHANNEL MESSAGES	Graph	D
ChannelSettings.ReadWrite.All	READ AND WRITE THE NAMES, DESCRIPTIONS, AND SETTINGS OF ALL CHANNELS	Graph	A
Chat.Read.All	READ ALL CHAT MESSAGES	Graph	A
Chat.ReadWrite	READ AND WRITE USER CHAT MESSAGES	Graph	D
ChatMember.ReadWrite.All	ADD AND REMOVE MEMBERS FROM ALL CHATS	Graph	A
Directory.Read.All	READ DIRECTORY DATA	Graph	D

Permission	Description	API	Type
Directory.ReadWrite.All	READ AND WRITE DIRECTORY DATA	Graph	A
Group.ReadWrite.All	READ AND WRITE ALL GROUPS	Graph	A, D
Notes.ReadWrite.All	READ AND WRITE ALL ONENOTE NOTEBOOKS AND NOTES FOR ALL USERS	Graph, OneNote	A
Region.ReadWrite	READ OR WRITE USER REGION	Teams	D
Reports.Read.All	READ ALL USAGE REPORTS	Graph	A
Sites.Manage.All	READ AND WRITE ITEMS AND LISTS IN ALL SITE COLLECTIONS	SPO	A
Sites.ReadWrite.All	READ AND WRITE ITEMS IN ALL SITE COLLECTIONS	Graph	A
Tasks.ReadWrite.All	READ AND WRITE ALL USERS TASKS AND TASKLISTS	Graph	A
TeamMember.ReadWrite.All	ADD AND REMOVE MEMBERS FROM ALL TEAMS	Graph	A, D
TeamsAppInstallation.ReadWriteForTeam.All	MANAGE TEAMS APPS FOR ALL TEAMS	Graph	A

Permission	Description	API	Type
TeamSettings.ReadWrite.All	READ AND CHANGE ALL TEAMS SETTINGS	Graph	A
TeamsTab.ReadWrite.All	READ AND WRITE TABS IN MICROSOFT TEAMS	Graph	A
Teamwork.Migrate.All	CREATE CHAT AND CHANNEL MESSAGES WITH ANYONE'S IDENTITY AND WITH ANY TIMESTAMP	Graph	A
TeamworkTag.ReadWrite.All	READ AND WRITE TAGS IN TEAMS	Graph	A
User.Read.All	READ ALL USERS' FULL PROFILES	Graph	A, D
user_impersonation	HAVE FULL ACCESS TO THE CHAT SERVICE AGGREGATOR AND SKYPE TEAMS SERVICE	Teams	D

You can enhance the security of SharePoint Online (SPO), by ensuring that On Demand Migration for Teams has access only to specific SharePoint sites, preventing unnecessary exposure to other sites in the environment. To achieve selected access, you must configure the **Sites.Selected** permission which is part of the permissions model for controlling access to specific SharePoint sites or site collections. See the Knowledge Base for more details or contact Quest Technical Support for assistance with this implementation.

When implemented, **Site.Selected** replaces the Sites.Read.All permissions.

Quest On Demand - Migration - Active Directory

Purpose: Active Directory and EntraID Migration, Device Migration, Directory Sync, Domain Rewrite, and Domain Move. Required for source and target tenant.

Permission	Description	API	Type
DeviceManagementConfiguration. ReadWrite.All	READ AND WRITE MICROSOFT INTUNE DEVICE CONFIGURATION AND POLICIES	Graph	A
DeviceManagementManagedDevic es.ReadWrite.All	READ AND WRITE MICROSOFT INTUNE DEVICES	Graph	A
DeviceManagementServiceConfig. ReadWrite.All	READ AND WRITE MICROSOFT INTUNE CONFIGURATION	Graph	A
Directory.AccessAsUser.All	ACCESS DIRECTORY AS THE SIGNED IN USER	Graph	D
Directory.ReadWrite.All	READ AND WRITE DIRECTORY DATA	Graph	D
Domain.ReadWrite.All	READ AND WRITE DOMAINS	Graph	D
Group.ReadWrite.All	READ AND WRITE ALL GROUPS	Graph	D
RoleManagement.ReadWrite.Direc tory	READ AND WRITE ALL DIRECTORY RBAC SETTINGS	Graph	D

Permission	Description	API	Type
User.Read.All	READ ALL USERS' FULL PROFILES	Graph	A, D

Quest On Demand - Migration - AIP protected content migration - Read

Purpose: Required for the source tenant. Allows On Demand Migration to read sensitivity labels from the Microsoft Information Protection Sync Service and the Azure Rights Management Service.

Permission	Description	API	Type
Content.SuperUser	READ ALL PROTECTED CONTENT FOR THIS TENANT	Graph	A
UnifiedPolicy.Tenant.Read	READ ALL UNIFIED POLICIES FOR THIS TENANT	Graph	A

Quest On Demand - Migration - AIP protected content migration - Write

Purpose: Required for the target tenant only, and not the source. Allows On Demand Migration to read sensitivity labels from the Microsoft Information Protection Sync Service and write to the Azure Rights Management Service..

Permission	Description	API	Type
Content.Writer	CREATE PROTECTED CONTENT	Graph	A
UnifiedPolicy.Tenant.Read	READ ALL UNIFIED POLICIES FOR THIS TENANT	Graph	A

Office 365 Permission Requirements

For Tenant Administrator

Asset	Tenant	Required Privileges	MFA Allowed	Purpose	Additional Notes
Accounts, Mailboxes, OneDrive, SharePoint	Source, Target	Global Admin role, which can be removed after consents are granted.	Yes	Grant consents, which creates ODM application service principals in the tenant.	The same Tenant Administrator Account can be used for all assets and features.
Teams, M365 Groups	Source, Target	Global Admin role, which can be removed after consents are granted. Teams Admin role, with active Teams license.	Yes	Grant consents, which creates ODM application service principals in the tenant. Provisions target Teams and M365 Groups, updates membership, and migrates Teams chats. Migrates Group mailboxes for Teams and M365 Groups.	The Tenant Administrator Account name appears in migrated Teams chats unless you specify another default target user.

For Tenant Administrator

Feature	Tenant	Required Privileges	MFA Allowed	Purpose	Additional Notes
Public Folders Migration	Source, Target	Owner permission for root Public Folders	Yes	Migrates public folders	Required if public folder migrations are in scope. ODM needs only the username; password is not required.
OneDrive Provisioning	Target	SharePoint Admin role	No	Provisions target OneDrives	Required if target OneDrives are not pre-provisioned.

Active Directory Permission Requirements

For Tenant Administrator

Activity	Tenant	Required Privileges	MFA Allowed	Purpose	Additional Notes
Domain Rewrite, Domain Move, Directory Sync, Active Directory Migration	Source, Target	Global Admin role, which can be removed after consents are granted and PowerShell accounts are created. Exchange Admin, Teams Admin, User Admin roles.	Yes	Grant consents, which creates an ODM application service principal in the tenant. Auto-creates PowerShell accounts and a mail-enabled security group using an OAuth Token. Auto-assigns required privileges to the PowerShell accounts.	Global Admin role must be reactivated during a Domain Move to auto-elevate the PowerShell accounts.

For PowerShell Accounts

Activity	Tenant	Required Privileges	MFA Allowed	Purpose	Additional Notes
Directory Sync, Active Directory Migration	Source, Target	Exchange Admin, Teams Admin, User Admin roles.	No	Reads and updates tenant objects.	Account names will be in the format of BinaryTreeCDSPowerShell.[GUID]
Domain Rewrite, Domain Move	Source, Target	Exchange Admin, Teams Admin, User Admin roles, with active Exchange Online license. Account will be auto-elevated to Global Admin during a Domain Move.	No	Reads and updates tenant objects. Auto-creates transport rules, connectors, and distribution groups for domain rewrite and advanced domain move functions.	Account names will be in the format of BinaryTreePowerShell.[GUID] and BinaryTreeCDSPowerShell.[GUID]

For Domain Account

Activity	Directory	Required Privileges	MFA Allowed	Purpose	Additional Notes
Domain Rewrite, Domain Move, Directory Sync, Active Directory Migration	Source, Target	Permissions to read and update Active Directory objects in scope.	N/A	Reads and updates Active Directory objects.	Required if local Active Directory environments are in scope.
Password Sync	Source, Target	Member of Administrators group or Domain Admins group	N/A	Sync passwords from source Active Dircetory to target Active Directory.	Required if password sync is in scope.
SID History Migration	Source	Member of Administrators group or Domain Admins group	N/A	Sync SID History from source Active Directory to target Active Directory	Required if SID History migration is in scope
SID History Migration	Target	Member of Administrators group or Domain Admins group or assigned Delegated migrateSIDHistory permissions	N/A	Sync SID History from source Active Directory to target Active Directory	Required if SID History migration is in scope

About Us

Quest creates software solutions that make the benefits of new technology real in an increasingly complex IT landscape. From database and systems management, to Active Directory and Office 365 management, and cyber security resilience, Quest helps customers solve their next IT challenge now. Around the globe, more than 130,000 companies and 95% of the Fortune 500 count on Quest to deliver proactive management and monitoring for the next enterprise initiative, find the next solution for complex Microsoft challenges and stay ahead of the next threat. Quest Software. Where next meets now. For more information, visit www.quest.com.

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 allows 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