Quest®

Quest® On Demand

Group Management User Guide

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

Quest Software Inc.

Attn: LEGAL Dept

4 Polaris Way

Aliso Viejo, CA 92656

Refer to our Web site (https://www.quest.com) for regional and international office information.

Patents

Trademarks

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 Group Management User Guide
Updated - 2019/04/16

Contents

1

Documentation roadmap

Global settings

On Demand global settings refers to management tools and configuration settings that apply to all On Demand modules. This includes tenant management tasks and downloading audit logs.

Modules

Each management tool is referred to as a module. Currently, the following modules are available:

- Audit
- Group Management
- Migration
- Policy Management for Skype for Business Online
- Policy Management for Exchange Online
- Recovery for Azure Active Directory

Documentation

For each module, and the global settings, there is a Release Notes document and a User Guide.

- The Release Notes contains a release history and details of new features, resolved issues, and known issues.
- User Guides contain descriptions and procedures for the management tasks you can perform with each module.

Use the links below to navigate to the content you require.

User Guides

- Global Settings
- Audit
- Group Management
- Migration
- Policy Managment for Exchange Online
- Policy Management for Skype for Business Online
- Recovery for Azure Active Directory

Release Notes

- Global Settings
- Audit
- Group Management
- Migration
- Policy Management for Exchange Online
- Policy Management for Skype for Business Online
- Recovery for Azure Active Directory

More resources

- For sales or other inquiries, visit http://quest.com/company/contact-us.aspx or call +1-949-754-8000.
- To sign up for a trial or purchase a subscription, go to https://www.quest.com/on-demand.
- 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 Quest On Demand Community provides a space for blog posts and a forum to disucss the On Demand products.

2

Introduction to Quest On Demand

Overview

On Demand is a cloud based management platform, providing access to multiple Quest Software Microsoft management tools through a single interface. Cloud based is a term that refers to applications, services or resources made available to users on demand via the Internet. Quest On Demand is a Software as a Service (SaaS) application where application software is hosted in the cloud and made available to users through quest-on-demand.com.

On Demand management is based on the concepts of organizations, modules, and Azure Active Directory (AD) tenants. When you sign up for the On Demand service, you create an organization. The organization can subscribe to modules. Organization administrators can use the tools provided by the modules to perform administrative actions on Azure AD tenants.

Modules

Each management tool is referred to as a module. Currently, the following modules are available:

- Audit
- Group Management
- Migration
- Policy Management for Skype for Business Online
- Policy Management for Exchange Online
- Recovery for Azure Active Directory

Global Settings

On Demand Global Settings refers to management tools and configuration settings that apply to all On Demand modules. This includes tenant management tasks and downloading audit logs.

Organizations

On Demand administration is based on organizations. When a user signs up for On Demand, an organization is created.

You can add users to an organization. To add a user, click **Settings** in the navigation panel on the left and then click **Permissions**.

Azure Active Directory tenants

Microsoft Azure also uses the concept of an organization. An Azure Active Directory (Azure AD) tenant is representative of an organization. It is a dedicated instance of the Azure AD service that an organization receive and owns when it signs up for a Microsoft cloud service such as Azure, Microsoft Intune, or Office 365. Each Azure AD tenant is distinct and separate from other Azure AD tenants.

A tenant houses the users in a company and the information about them - their passwords, user profile data, permissions, and so on. It also contains groups, applications, and other information pertaining to an organization and its security. For more information see this Microsoft help page.

3

Group Management overview

On Demand Group Management controls the chaos of managing Azure Active Directory (AD) and Office 365 groups with group creation policies for naming, attestation, expiration, quantity limits, and more. The Group Management module safely empowers users with self-service group creation, management, and group membership reporting.

Concepts in Goup Management

It is a good idea to understand the following concepts before working with Group Management:

- Understanding user and manager
- Understanding resource
- Understanding group

Understanding user and manager

User is a role in Group Management, a user usually does not have any administrative permissions assigned. However, a user can apply for other roles (such as HR, IT) via Self-Services to obtain corresponding permissions. A user can be assigned as a manager, and each users (except the top level ones in the organization structure) can only have one manager assigned in Group Management.

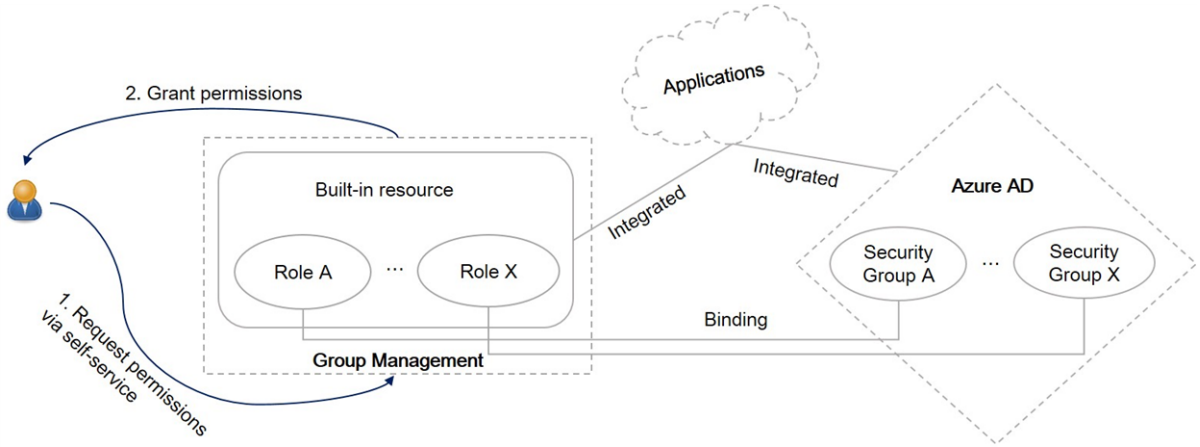
TIP: Group Management provides an organization chart based on the relationships between managers and their subordinates within a directory. Directory Administrators, and users with at least one permission (in the **Edit Permissions** list when editing a role) assigned can see the chart by clicking the organization-chart icon on the **Users** tab.

Understanding resource

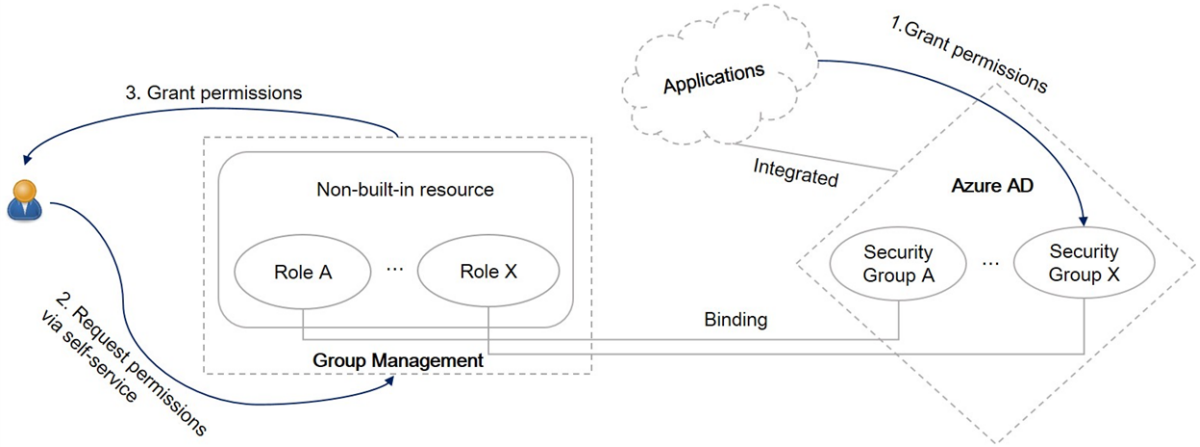
A resource is an application integrated with an on-premises AD or the Azure AD for identity management. Access to the application is based on roles which can be centrally created via Group Management, as creating a role for a resource also creates a bound group (security group) for access control.

Group Management resources are classified into the following types:

- **Built-in resource**: Permissions to an application can be granted directly to users as they are successfully assigned a resource role. For more information about the available built-in resource types, see Resource settings.



- **Non-built-in resource**: Permissions to an application can be still granted to users via resource roles, but you must grant permissions to the bound security groups within the application in advance.



Permissions to a resource in Group Management are managed by roles. A resource in Group Management comes with a default role **Owner**, and can have multiple custom roles for different access permissions to the resource. Each role can be assigned to one or more users.

A resource owner can perform the following tasks via Self-Services:

- Manage members for all resource roles
- Create a resource attestation

Understanding group

Group Management supports for all the Office 365 and Azure AD groups, including:

- Office 365 groups
- Security groups (including mail-enabled security groups)
- Distribution lists

Group roles in Group Management include **Owner** and **Member**, and both of them can be assigned to one or more users.
A group owner can perform the following tasks via Self-Services:

- Manage group owners
- Manage group members
- Create a group attestation

Roles and permissions

Access to the Group Management features is based on roles. Group Management provides the following built-in roles:

- Global Administrator
- Directory Administrator
- General User

A Directory Administrator can also create custom roles and edit their permissions, see Roles.

Global Administrator

The users who are added as "Organization administrator" and "Group Management module administrator" for the organization at On Demand Home are automatically assigned this role. For more information about these types of administrators, refer to *On Demand Global Settings User Guide*.
Permissions include:

- Manage all directories in the organization.
- Manage Directory Administrators for all directories.

Directory Administrator

A Global Administrator can assign Directory Administrator for a directory, see Assigning Directory Administrator.
A Directory Administrator can also assign this role to other users, see Directory Administrators.
Permissions include:

- Access to all the directory's administrative features.
- Manage Directory Administrators for the directory.

General User

All users in a directory are automatically assigned this role.
Permissions include:

- Access to all Group Management self-services.

4

Getting started

Before getting started with Group Management, the tenant must have already been added to On Demand, and admin consent has been granted for the Group Management module on the On Demand Home site. For more information about adding a tenant and granting admin consent, refer to On Demand Global Settings User Guide.

To get started on a new tenant in Group Management

1. Assigning Directory Administrator
2. Initializing data for new tenant

Assigning Directory Administrator

The Global Administrator can assign the Directory Administrator role to one or more users. For more information about the Directory Administrator permissions, see Roles and permissions.

To assign Directory Administrator to users

1. In the Group Management Portal, select **Directories** under **GLOBAL ADMINISTRATOR** in the side navigation panel.
2. Click **MANAGE DIRECTORY ADMINISTRATORS** on the tenant.
3. Add one or more users to the list.
4. Click **SAVE**.

Initializing data for new tenant

When a Directory Administrator opens the tenant page in Group Management for the first time, an initialization process is available on the page. The process imports the existing users and groups from tenant, and makes them ready for Group Management.

To initialize data for a new tenant

1. In the Group Management Portal, select the new tenant under **DIRECTORY ADMINISTRATOR** in the side navigation panel.
2. On the initialization start page, click **START**.
3. After the initialization is complete, click **PROCEED**.

See also: Appendix: Attribute mappings between Azure AD and Group Management

Working as Global Administrator

Global Settings

The following settings are available to Global Administrators on the **Global Settings** page:

Notification

A Global Administrator can set the number of days to retain user notifications in Group Management. This setting applies to all the directories in the organizaiton. The default value is 0, meaning the notifications are retained forever.

To set retention policy for user notifications

1. In the Group Management Portal, select **Global Settings** under **GLOBAL ADMINISTRATOR** in the side navigation panel.
2. Click the **Notification** tile.
3. Set the number of days to retain user notifications.
4. Click **Save**.

Directories

The **Directories** page lists all the directories managed by the Global Administrator. Each tile represents a directory, and the messages on the tile indicate:

- If the required admin consent has been granted to Group Management.
- If the directory is managed with the current organization.

To manage Directory Administrators for a directory, click **MANAGE DIRECTORY ADMINISTRATORS**. See Assigning Directory Administrator for more information.

Working as Directory Administrator

Viewing dashboard

Group Management provides a dashboard for each directory to display the following statistical information:

- The total number of resources
- The total number of groups (including Office 365 groups, distribution lists, security groups, and mail-enabled security groups)
- The total number of users
- The top 5 resource types that most resources are created with.
- The number of groups of each type (including Office 365 group, distribution list, security group, and mail-enabled security group)

To view the dashboard for a directory, select the directory under **DIRECTORY ADMINISTRATOR** in the side navigation panel, and select the **Dashboard** tab.

Managing resources

To manage resources and their roles, select the directory under **DIRECTORY ADMINISTRATOR** in the side navigation panel, and select the **Resources** tab.

Managing resources

- Adding a resource
- Editing a resource
- Deleting a resource

Adding a resource

Prerequisites

Before adding a resource, complete the Resource settings on **Settings** > **Polices** > **Resource**.

To add a resource

1. On the **Resources** tab, click **ADD**.
2. Edit the general information for the new resource.
3. Click **ADD**.

A resource owner must be selected when adding the resource. To edit roles and their members for the new resource, see Managing resource roles.

Editing a resource

The following general information of a resource can be edited after the resource has been added to Group Management:

- Resource category
- Location
- Expiration date
- Description

To edit general information of a resource

1. On the **Resources** tab, search for and select the resource you want to edit.
2. Click **MORE** > **EDIT**.
3. Edit general information for the resource.
4. Click **SAVE**.

To edit roles for the resource, see Managing resource roles.

Deleting a resource

To delete a resource

1. On the **Resources** tab, search for and select the resource you want to delete.
2. Click **MORE** > **DELETE**.
3. Click **YES**.

Managing resource roles

For information about the resource roles, see Understanding resource.
To manage roles for a resource, select the resource on the **Resources** tab and click **VIEW**.

- Adding a resource role
- Editing a resource role
- Assigning a resource role
- Unassigning a resource role
- Deleting a role

Adding a resource role

To add a resource role

1. Click **ADD ROLE** on the **Roles** subpage.
2. Edit the role information.
3. Click **SAVE**.

Editing a resource role

The following general information of a role can be edited:

- Description
- The setting **Allow users to apply for this role**.

To edit a resource role

1. On the **Roles** sub page, select the role you want to edit.
2. Click **EDIT ROLE** on the tab.
3. Edit the role information.
4. (For resource of built-in type only) Click **PERMISSIONS** to edit the role's permissions.
5. Click **SAVE**.

Assigning a resource role

To assign a resource role

1. On the **Roles** sub page, select the role you want to assign.
2. On the tab, click **ADD**.
3. Search for and select the user you want to assign to on the **Users** tab, and set an expiration date.
   TIP: The option **Membership Expires** is not available when you assign the role **Owner**.
4. Click **SELECT**.
5. Repeat step 3 and 4 to assign the role to more users.
6. Click **SUBMIT**.

Unassigning a resource role

To unassign a resource role

1. On the **Roles** sub page, select the role you want to unassign.
2. Select the users you want to unassign from.
3. Click **REMOVE**.
4. Click **YES**.

Deleting a resource role

To delete a resource role

1. On the **Roles** sub page, select the role you want to delete.
2. Click **DELETE ROLE**.
3. Click **YES**.

TIP: The default role **Owner** cannot be deleted.

Managing groups

To manage groups and their roles, select the directory under **DIRECTORY ADMINISTRATOR** in the side navigation panel, and select the **Groups** tab.

- Managing groups
- Managing role members for a group

Managing groups

Adding a group

Prerequisites

Before adding a group, complete the Group settings on **Settings** > **Polices** > **Group**.

To add a group

1. On the **Groups** tab, click **ADD**.
2. Edit the general information for the new group.
   NOTE: A group owner must be specified when adding a group. For more information about the group owner, see Understanding group.
3. Click **ADD**.

To add role members for the new group, see Managing role members for a group.

Editing a group

The following general information of a group can be edited after the group has been added to Group Management:

- Group category
- Description
- Expiration date

To edit general information of a group

1. On the **Groups** tab, select the group you want to edit.
2. Click **MORE** > **EDIT**.
3. Edit general information for the group.
4. Click **SAVE**.

To manage role members for the group, see Managing role members for a group.

Deleting a group

To delete a group

1. On the **Groups** tab, select the group you want to delete.
2. Click **MORE** > **DELETE**.
3. Click **YES**.

Managing role members for a group

For information about the group roles, see Understanding group.

- Assigning a group role
- Unassigning a group role

Assigning a group role

To assign a group role

1. On the **Role** sub page, select the role you want to assign.
2. On the tab, click **ADD**.
3. Search for and select the user you want to assign to on the **Users** tab, and set an expiration date.
   TIP: The option **Membership Expires** is not available when you assign the role **Owner**.
4. Click **SELECT**.
5. Repeat step 3 and 4 to assign the role to more users.
6. Click **SUBMIT**.

Unassigning a group role

To unassign a group role

1. On the **Roles** sub page, select the role you want to unassign.
2. Select the users you want to unassign from.
3. Click **REMOVE**.
4. Click **YES**.

Managing settings

To manage settings for a directory, select the directory under **DIRECTORY ADMINISTRATOR** in the side navigation panel, and select the **Settings** tab.

- Policies
- Roles
- Self-Services
- Value Sets
- Directory Administrators
- Synchronization

Policies

- Resource settings
- Group settings
- User settings

Resource settings

The following resource settings are available on the **Resource** tab:

- Resource Type
- Resource Security Level
- Resource Naming Rule
- Resource Category

Resource Type

Resource types are used to categorize the resources to facilitate management. A resource type must be specified when creating a resource.

Group Management provides the following built-in resource types:

- **Office 365 License**

This resource type is used to manage the Office 365 license assignment in the organization. Each Office 365 license is automatically associated with a role named the same as the license. Group Management automatically assigns a license to users when they are assigned the role of the license, or remove the license from them when the role is unassigned.

The **Office 365 License** resource type is available after enabled. To enable it, click **ENABLE OFFICE 365 LICENSE** on the **Resources** tab. After it's enabled, a resource named as **Office 365 Licenses** can be found in the resource list on the **Resources** tab.

- **Microsoft OneDrive**

This resource type is used to manage user access to the company-wide top-level OneDrive folders. Each OneDrive folder is associated with a resource of this type. Roles with different sets of permissions can be created for a resource to manage access to the company-wide top-level OneDrive folder.

- **GM**

This resource type is used to manage user access to the Group Management features by roles, see Roles for more information. A resource of this type named as **GM** can be found in the resource list on the **Resources** tab.

Resource Security Level

Resource automatic attestation can be scheduled by Resource Security Level to run attestations regularly. When enabling automatic attestation, define the attestation interval, scope and duration.

Resource Security Level also includes these settings:

- **Temp. resource lifetime**: The default days a temporary resource will expire in. This setting applies when selecting the expiration date for a resource.
- **Temp. membership valid**: The default days a temporary membership will expire in. This setting applies when selecting the expiration date for a user.

Resource Naming Rule

The resource naming rule defines the syntax to name a resource when Adding a resource. When editing a resource naming rule, the following data types are available for each field in the syntax:

- **Flexible Text**: Allows users to input flexible text in the field.
- **Fixed Text**: Specifies the field with fixed text.
- **Value Set**: Specifies the field with a value set. Users will need to select a value from the specified value set for the field. To manage value sets, see Value Sets.
- **User Attribute**
  - **Job title**: The **Job title** attribute of the current user automatically applies.
  - **Office**: The **Office** attribute of the current user automatically applies.

Resource Category

A resource category is a combination of Resource Security Level and Resource Naming Rule. A resource category must be specified when creating a resource.

Group settings

The following group settings are available on the **Group** tab:

- Group Security Level
- Group Naming Rule
- Group Category

Group Security Level

Group automatic attestation can be scheduled by Group Security Level to run attestations regularly. When enabling automatic attestation, define the attestation interval, scope and duration.

Group Security Level also includes these settings:

- **Temp. group lifetime**: The default days a temporary group will expire in. This setting applies when selecting the expiration date for a group.
- **Temp. membership valid**: The default days a temporary membership will expire in. This setting applies when selecting the expiration date for a user.

Group Naming Rule

The group naming rule defines the syntax to name a group when Adding a group. When editing a group naming rule, the following data types are available for each field in the syntax:

- **Flexible Text**: Allows users to input flexible text in the field.
- **Fixed Text**: Specifies the field with fixed text.
- **Value Set**: Specifies the field with a value set. Users will need to select a value from the specified value set for the field. To manage value sets, see Value Sets.
- **User Attribute**
  - **Job title**: The **Job title** attribute of the current user automatically applies.
  - **Office**: The **Office** attribute of the current user automatically applies.

Group Category

A group category is a combination of Group Security Level and Group Naming Rule. A group category must be specified when creating a group.

User settings

The following user settings are available on the **User** tab:

- User ID Naming Rule
- Built-in Value Sets

User ID Naming Rule

The **User ID Naming Rule** defines the user ID (the part before @) syntax of a user which applies to the **User ID** field for On-boarding a user. When editing a user ID naming rule, the following data types are available for each field in the syntax:

- **User Attribute**
  - **First Name**: Uses the input value of the **First name** field when on-boarding the user.
  - **Last Name**: Uses the input value of the **Last name** field when on-boarding the user.

Built-in Value Sets

The following are the available built-in value sets for user management:

- **Office**: Applies to the **Office** field when On-boarding a user and Editing a user.
- **Employee type**: Applies to the **Employee type** field when On-boarding a user and Editing a user.
- **Job title**: Applies to the **Job title** field when On-boarding a user and Editing a user.
- **Business unit**: Applies to the **Business unit** field when On-boarding a user and Editing a user.

Roles

The **Roles** page allows Directory Administrator to create custom roles in Group Management, and assign each role a set of permissions to access to the Group Management features. Each role can be assigned to one or more users. The roles on this page are created for the resource **GM**, see Resource settings for more information about the resource **GM**.

The following roles are automatically created by Group Management:

- Owner
- HR
- IT

NOTE: The role **Owner** cannot be deleted.

Self-Services

Group Management self-services provide users access to the directory resources and functional features via approval processes, for example, a user submits a request for an Office 365 license, and once the request is approved, the license will be automatically assigned to the user.

The **Self-Services** page allows Directory Administrator to view all the available self-services, and associate an approval process for each of them.

- Services
- Approval Processes

Services

The **Services** tab lists all the self-services provided by Group Management. Each self-service must be associated with an approval process defined on the Approval Processes tab.

NOTE: If no approval is required for a self-service, associate the self-service with an approval process without any approval steps.

Approval Processes

The **Approval Processes** tab lists the available approval processes for self-services. An approval process contains a general workflow, and optional BU-specific workflows. The approval process will use the BU-specific workflow when a specific workflow has been created for the requester's BU, otherwise, the general workflow will apply.

When an approval process requires a level-N manager who does not exist for the requester (for example, the approval process requires a level-3 manager, but the requester does not have a level-3 manager at all by the organization structure), the approval process will go to the requester's direct manager (the person that the requester reports to) instead.

TIP: Group Management provides an organization chart based on the relationships between managers and their subordinates within a directory. Directory Administrators, and users with at least one permission (in the **Edit Permissions** list when editing a role) assigned can see the chart by clicking the organization-chart icon on the **Users** tab.

Generally, a user cannot approve a request submitted by himself or herself. When the approver of a step is supposed to be the same person as the requester, and according to the approval process,

- The approver is the specific user: The approval process cannot move on any further.
- The approver is a resource or group owner: The requester himself or herself cannot approve the request (but other owners of the resource or group can do).

Value Sets

When on-boarding a user, or define a naming rule syntax, each of the following fields provides a value list for users to select one:

- Business unit
- Office
- Employee type
- Job title

These values are managed as **Built-in Value Sets** on the **Value Sets** page. Besides these built-in ones, Directory Administrator can also create **Custom Value Sets** on the page for defining naming rule syntax.

Directory Administrators

A Directory Administrator can assign or unassign the Directory Administrator role to one or more users on the **Directory Administrators** page. For more information about the Directory Administrator permissions, see Roles and permissions.

Synchronization

A regular full synchronization is established between Group Management and the directory to keep your data consistent. The following synchronization settings are available on the page:

- Sync direction for users: Can be from Azure AD to GM, or from GM to Azure AD.
- Sync direction for groups: Can be from Azure AD to GM, or from GM to Azure AD.
- Sync interval: Defines how often synchronization occurs. The default value is 12 hours.

Each row in the **Sync Results** table indicates the results of a synchronization , including:

- Sync time
- Sync direction
- The number of users and groups on the source before sync
- The number of users and groups on the target that were synced from the source

See also: Appendix: Attribute mappings between Azure AD and Group Management

Managing users

To manage users, select the directory under **DIRECTORY ADMINISTRATOR** in the side navigation panel, and select the **Users** tab.

- On-boarding a user
- Editing a user
- Off-boarding a user

On-boarding a user

Prerequisites

Before on-boarding a user, complete the User settings on **Settings** > **Polices** > **User**.

To on-board a user

1. On the **Users** tab, click **ON BOARD** on the page.
2. Edit information for the new user.
3. Click **ON BOARD**.

Editing a user

To edit a user

1. On the **Users** tab, select the user you want to edit.
2. Click **MORE** > **EDIT**.
3. Edit the user's information.
4. Click **SAVE**.

Off-boarding a user

To off-board a user

1. On the **Users** tab, select the user you want to off-board.
2. Click **MORE** > **OFF BOARD**.
3. Click **OK**.

TIP: If the user to be off-boarded is a manager, you will be prompted to assign a new manager before off-boarding.

Working as General User

When a user logs in to Group Management, the following menu is available under **GENERAL USER** in the side navigation panel:

- My Profile
- My Activities
- Gallery
- New Request

My Profile

The following tabs are available on the **My Profile** page:

- Basic
- My Resources
- My Groups

Basic

This tab shows general information of the user, and a list of users who share the same manager.

My Resources

This tab lists all the resources that the user has joined as an owner on the **Owner** sub tab, and as other roles on the **Others** sub tab. The user can click a resource in the list to perform the following actions:

- View the resource's general information
- View the roles assigned to the current user

- View the available roles for the resource
- Submit requests of various types for the resource

My Groups

This tab lists all the groups that the user has joined as an owner on the **Owner** sub tab, and as a member on the **Member** sub tab. The user can click a group in the list to perform the following actions:

- View the group's general information
- View the roles assigned to the current user
- Submit requests of various types for the group

My Activities

The following tabs are available on the **My Activities** page:

- My Requests
- My Approvals
- My Attestations

My Requests

The **My Requests** tab lists all the requests submitted by the user, including the requests that have been approved or rejected, and the ones that are still awaiting approval. Clicking on each request will open a page showing the current approval progress, and other detailed information about the request.

The user can cancel a request that is still awaiting approval (the request status shows **In progress**) on this tab.

To cancel an In Progress request:

1. On the **My Requests** tab, search for and select the request you want to cancel.
2. Click the … icon and select **CANCEL**.
3. Input the reason you cancel the request.
4. Click **SUBMIT**.

My Approvals

The **My Approvals** tab lists all the requests that require approval from the user, including the requests that have been approved or rejected by the user, and the ones that are still awaiting approval. Clicking on a request opens a page showing the detailed information on the request.

The user can approve or reject a request by clicking the … icon on the request and selecting **APPROVE** or **REJECT**.

My Attestations

The **My Attestations** tab lists all the attestation requests that require the user to respond.

Each attestation request comes with a due date, the user needs to handle them before they expire. Once the user has selected **YES** or **NO** for an attestation request, it cannot be changed any more even when it is still before the due date.

When a user does not respond to an attestation request before the due date, and

- The user is the resource or group owner: It will be considered as that the user does not want to keep the resource or group any more.
- The user is NOT the resource or group owner: It will be considered as that the user does not want to be a member of the resource or group any more.

Gallery

The **Gallery** page lists all the users, resources, and groups in the directory on each tab.

On the **Resources** tab, the user can request to add a resource by clicking **ADD A RESOURCE** on the page, and can also apply for a role of a resource by clicking the … icon for the resource in the list and selecting the role.

On the **Groups** tab, the user can request to add a group by clicking **ADD A GROUP** on the page, and can also apply for the Owner or Member role of a group by clicking the … icon for the group in the list and selecting the role.

New Request

The **New Request** page allows the user to submit various requests for groups and resources on the **Group** or **Resource** tab.

Custom Attestation

The custom attestation can be used as a tool to launch a survey. The user can make one question for the survey, and define the scope with specified users.

> **TIP: Make a Yes/No question**: Customizing answer choices is not supported yet, recipients can only select **Yes** or **No** to answer your question.

To request to launch a survey

1. On the **Others** tab, click the **Custom Attestation** tile.
2. Search for and select the user to define the survey scope.
3. Click **SELECT**.
4. Repeat step 2 and 3 to add more users.
5. Click **NEXT**.

6. Fill the form.
7. Click **SUBMIT**.

Appendix: Attribute mappings between Azure AD and Group Management

Table 1: Attribute mappings between Azure AD and Group Management

Azure AD User	Group Management User
givenName	First name
surname	Last name
displayName	Display name
userPrincipalName	User id
jobTitle	Job title
officeLocation	Office
businessPhones	Work phone
manager *	Manager
usageLocation	Country
Azure AD Group	**Group Management Group**
displayName	Name
description	Description
mailNickname *	Name
The part after @ in email address **	Domain
mail	Mail
owners	Owners
members	Members

* Mapping from Group Management to Azure AD only.

** Mapping from Azure AD to Group Management only.

About us

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.

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

Glossary

A

Active Directory

Microsoft Azure Active Directory (AD) is a multi-tenant, cloud based, directory and identity management service. For more information, see https://docs.microsoft.com/en-us/azure/active-directory/active-directory-whatis

Admin consent

The process of approving the use of an application for the whole Microsoft Azure AD organization by the Microsoft Global administrator is referred to as admin consent. The Microsoft Global administrator must provide admin consent when adding a tenant to On Demand. When a tenant is first added, On Demand requests base admin consent permissions. Some modules can function using the base permission set while other require a higher level of admin consent permissions.

Administrator: Microsoft Azure AD Global Administrator

The Microsoft Azure AD Global administrator is the top level administrator role and has access to all features. The person who signs up for Azure becomes the Global Administrator.

Administrator: Module Administrator

Module administrators have permission to perform tasks in a specific module. You can add multiple module administrators to your On Demand organization.

Administrator: Office 365 Global Administrator

The Office 365 Global administrator has access to all Office 365 administrative features, including Skype for Business Online and Exchange Online

Administrator: On Demand Organization Administrator

The On Demand organization administrator role is the top level administrator role and has access to all features. By default, the user that completes the On Demand Sign Up process is assigned to the On Demand organization administrator role for the organization.

M

Microsoft Azure

A cloud computing service created by Microsoft. It is used by developers and IT professionals for building, deploying, and managing applications and services through a global network of Microsoft-managed data centers. Quest On Demand is hosted in Microsoft Azure.

O

Organization

On Demand administration is based on organizations. When a user signs up for On Demand, an organization is created. Administrators perform management tasks on Microsoft Active Directory tenants that have been added to the organization.

Organizational account: Microsoft

When you subscribe to Microsoft Azure, you create an organizational account. The subscription process prompts you to provide details about your organization and your organization's internet domain name registration. The organization information is used to create a new Azure Active Directory instance for the organization. Microsoft documentation sometimes refers to Organizational Accounts as Work or school Accounts to distinguish them from Microsoft Accounts.

T

Tenant

In Azure Active Directory (Azure AD), a tenant is representative of a Microsoft Azure AD organization. It is a dedicated instance of the Azure AD service that an organization receives and owns when it signs up for a Microsoft cloud service such as Azure, Microsoft Intune, or Office 365. Each Azure AD tenant is distinct and separate from other Azure AD tenants.