Quest® On Demand

Group Management User Guide

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, 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.**

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

On Demand Group Management User Guide
Updated - 2021/03/17

Contents

1

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
- License Management
- Migration
- Recovery

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 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.

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.

2

Group Management overview

On Demand Group Management controls the chaos of managing Azure Active Directory (AD), Office 365, and on-premises 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.

The Group Management module is part of Quest On Demand. It consists of the following parts:

- Admin portal
- Self-service portal

Admin portal

Group Management allows you to manage all your groups from Azure AD and connected on-premises directories in one place. The admin portal serves as a control center where the Group Management administrator can manage groups, configure group policies, define approval process for self-services, and so on. It also provides a dashboard displaying various group statistics and operational data.

For more information about working with the admin portal, see Working with the admin portal.

Group Management administrator

The Group Management administrator is an administrative role in the Group Management module with the following permissions:

- Configure and manage the Group Management module
- Approve, reject, or cancel a request

The role can be assigned to one or more users by the Access Control interface on the On Demand Home site. For more information, refer to On Demand Global Settings User Guide.

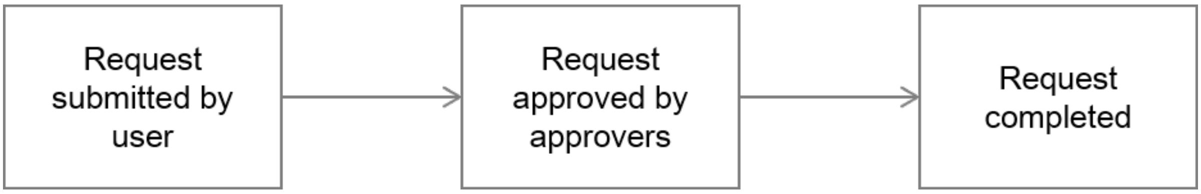
Self-service portal

Group Management enables users to manage groups on a self-service basis. Users can submit various requests in the self-service portal. This includes:

- Create, join, leave, attest, and delete groups
- Manage group owners and members

Group Management automatically completes a user request once the request is approved. The flow chart below shows the request handling process. For more information about working with the self-service portal, see Working with the self-service portal.

Figure 1: Request handling process



Concepts in Goup Management

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

- Group types
- Group roles
- Group attestations

Group types

Group Management supports the following types of groups:

- Office 365 group
- Security group and mail-enabled security group in Azure AD and on-premises AD
- Distribution list in Azure AD and on-premises AD
- Mail-enabled distribution list in on-premises AD

These groups are divided into the following types by their **AD Connect** attribute in Group Management:

Table 1: Group types in Group Management

AD Connect Attribute	Description
Cloud Only	Groups created in Azure tenant
Enabled	Groups synced from connected directory to Azure tenant
Disabled	Groups created in connected directory

The tables below show the supported operations for each group type in Group Management:

Table 2: Supported operations for 'Cloud Only' groups

Operation	Office 365	Mail-Enabled Security Group	Security Group	Distribution List
View group	Yes	Yes	Yes	Yes
Create group	Yes	Yes	Yes	Yes
Edit general information	Yes	Partial [1]	Yes	Partial [1]
Edit ownership	Yes	Yes	Yes	Yes
Edit membership	Yes	Yes	Yes	Yes
Auto-attestation	Yes	Yes	Yes	Yes
Delete group	Yes	Yes	Yes	Yes

[1]: Editing the Description field is not supported yet.

Table 3: Supported operations for 'Enabled' groups

Operation	Mail-Enabled Security Group	Security Group	Mail-Enabled Distribution List	Distribution List
View group	Yes	Yes	Yes	Yes
Create group	Yes	Yes	Yes	Yes
Edit general information	Partial [1]	Partial [1]	Partial [1]	Partial [1]
Edit ownership	Yes	Yes	Yes	Yes
Edit membership	Yes	Yes	Yes	Yes
Auto-attestation	Yes	Yes	Yes	Yes
Delete group	Yes	Yes	Yes	Yes

[1]: Editing the Description field is not supported yet.

Table 4: Supported operations for 'Disabled' groups

Operation	Mail-Enabled Security Group	Security Group	Mail-Enabled Distribution List	Distribution List
View group	Yes	Yes	Yes	Yes
Create group	Yes	Yes	Yes	Yes
Edit general information	Partial [1]	Partial [1]	Partial [1]	Partial [1]
Edit ownership	Yes	Yes	Yes	Yes
Edit membership	Yes	Yes	Yes	Yes
Auto-attestation	Yes	Yes	Yes	Yes
Delete group	Yes	Yes	Yes	Yes

[1]: Editing the Description field is not supported yet.

Group roles

Group roles in Group Management include **Owner** and **Member**. Group owners can manage their group via Self-Services in the self-service portal. This includes:

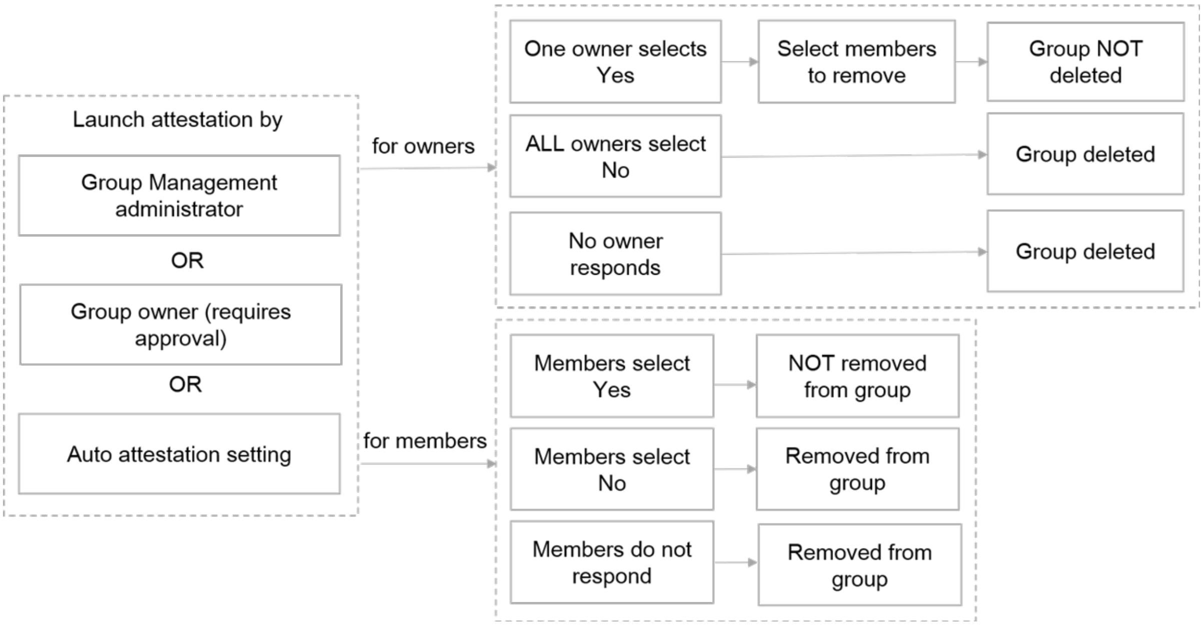
- Manage group owners and members
- Create group attestations
- Delete group

NOTE: Only one owner is allowed for groups of some types. For more information, see Group types.

Group attestations

The flow chart below shows the group attestation processes in Group Management.

Figure 2: Group attestation processes



Group Management provides the following group attestations that enable group owners and members to review and confirm their membership:

- Attestation for group owners: Each group owner receives a request to confirm if they still want to keep the group.
  - The attestation process completes as long as one owner selects to keep the group and confirms the membership.
  - If all the owners select to delete the group, the group will be automatically deleted.
  - If no owner responds to the request before the due date, the group will be automatically deleted.

- Attestation for group members: Each group member receives a request to confirm if they still want to stay in the group.
  - The members who select to stay in the group will not be removed.
  - The members who select to leave the group will be automatically removed.
  - The members who do not respond to the request before the due date will be automatically removed.

A group attestation process can be launched by the following methods:

- A Group Management administrator can create a group attestation in the admin portal.
- A group owner can submit a request to attest the group in the self-service portal. This needs approval before the attestation is launched.
- The group setting **Automatic Attestation** triggers the process periodically.

Getting started

Prerequisites

The following prerequisites must be met before you enter the Group Management module:

1. Your tenant must have been added to On Demand.
2. The tenant admin consent must have been granted to the Group Management module.

For more information about adding a tenant and granting admin consent, refer to On Demand Global Settings User Guide.

Opening Group Management

To open the Group Management module, click **Group Management** in the side navigation panel.

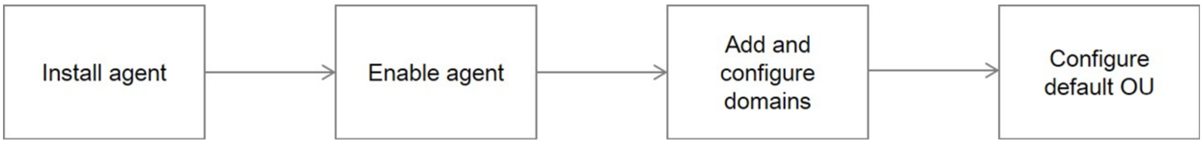
The Group Management dashboard page is displayed on the right. For more information about the dashboard, see Viewing the dashboard.

> ℹ **TIP:** If you have multiple tenants managed by Group Management, you can click the filter icon at the top right of the page to switch tenants.

Supporting hybrid mode

Group Management supports tenants in hybrid mode to manage your on-premises groups. The flow chart below shows the process of enabling hybrid mode in Group Management.

Figure 3: Enabling hybrid mode



A local agent is required to query and perform management actions on on-premises groups. Agents run as a service on a machine in the local network. The machine must have sufficient privileges to perform the actions required. You must install the agent on the local machine.

This section contains information on installing and configuring an agent. For information about configuring default OU, see Organizational Units.

- Installing an agent
- Enabling and disabling the agent
- Adding and configuring domains
- Uninstalling the agent
- Additional agent commands

Installing an agent

1. On your local machine, create a folder to store the agent install file and installation key.
2. In the On Demand navigation panel, click **Settings**.
3. In the main panel menu bar, click **AGENTS**.
4. Under **Download Agent**, click **Download** and save the file in the folder you created.
   If your browser automatically saves the file in a default folder, locate the file and copy it into the folder you created.
5. Go to the folder you created and extract the contents of the zip file into the folder. An Agent folder is created.

   NOTE: The installer must be extracted to a folder before you launch it.

6. Return to the On Demand **Settings > AGENTS** page and under **Generate Installation Key**, click **Generate** and save the generated file in the Agent folder. If your browser automatically saves the file in a default folder, locate the installation key file and copy it into the Agent folder.

   NOTE: If you do not copy the key file into the Agent folder, you will be prompted for the path to the file during the installation.

7. In the Agent folder, double click `Setup.exe`.
   A console window opens.

   NOTE: Before the installation, make sure the file `bin\OPGMService.exe` in the Agent folder is unblocked (File Properties > General > Security > Unblock), otherwise the installation will fail.

8. In the console window, you are prompted to confirm the installation. Type `y` and press **Enter**.
9. In the console window, you are prompted to confirm the installation. Type **y** and press **Enter**.
10. You are prompted to enter the **Agent name**. Press **Enter** to accept the default or type a name and press **Enter**.
    The agent is installed and the console window closes.

11. Return to the On Demand **Settings > AGENTS** page and click **Refresh**.
    In the **Modules** pane, the agent name is listed under the **Group Management** module.
12. Click on the agent name to display the **Agent Information**.

Enabling and disabling the agent

If an agent is enabled, it is returned in a request for available agents within the organization. For example, a service may request an agent for domain `xyz.corp` in organization A. The agent management service looks for all enabled agents that support domain `xyz.corp` for organization A. Any agents that have been disabled are ignored. If the agent has been disabled, it is not used.

To enable or disable an agent

1. In the On Demand navigation panel, click **Settings**.
2. In the main panel menu bar, click **AGENTS**.
3. In the **Modules** panel, select the agent under the **Group Management** module.
4. The Enabled / Disabled toggle is at the top right of the **Agent Information** fields.
5. Click on the toggle to change the state of the agent.

> **NOTE:** You can start and stop the agent from a console window. See Additional agent commands.

Adding and configuring domains

You must add your on-premises Active Directory domains to the domain list of the agent, and provide required authentication information. The agent validates the domain name when it is added. For example, if you add domain `xyz.corp` and it does not exist or cannot be connected to, you receive an error.

The agent must be enabled and online to add a domain name to the list. Check the **Enabled** and **Online** icons at the top right of the **Agent Information** fields.

To add and configure a domain

1. In the On Demand navigation panel, click **Settings**.
2. In the main panel menu bar, click **AGENTS**.
3. In the **Modules** panel, select the tenant under the **Group Management** module.
4. The **Domains** field is below the **Agent Information**. Enter the domain name in the text box and click **Add Domain**.
   If the operation is successful, the domain is added to the domain list.
5. Click **CONFIGURE** on the domain you added.
6. In the **Domain Authentication** section, provide an account with the following permissions:
   - Read users
   - Read/Edit groups, group owners, and group members
   - Delete groups

7. (Optional) In the **Exchange Authentication** section, provide the on-premises Exchange server URL (in the format: `http://<ExchangeServer>/powershell`) and Exchange admin credentials.
   If the account you provided in step 6 is also an Exchange admin, select the check box **Use Domain Authentication Credentials** instead of entering the credentials.

   > **NOTE:** This step is only required for managing on-premises mail-enabled security groups and distribution lists.

8. Click **SAVE**.

Uninstalling the agent

Prerequisites

You must know the location of the agent `setup.exe` file. See Installing an agent

To uninstall an agent

1. Open a console window and navigate to the folder where the agent `setup.exe` file is located.
2. Type `setup.exe uninstall` and press **Enter**.
3. You are prompted to confirm the uninstall. Type `y` and press **Enter**.

Additional agent commands

The following commands and switches can be used from the Windows console command line. To use a command or switch, you must first navigate to the folder where the agent `setup.exe` file is located or provide the path to the file as part of the command syntax.

Prefix each command or switch with `setup.exe`. For example `setup.exe install`.

Table 5: Agent commands

Type	Syntax	Description

Command	`install`
	or
	`i`
		Installs the agent.

Command	`uninstall`
	or
	`u`
		Uninstalls the agent.

Switch	-q	Do not ask for install or uninstall confirmation.

Switch	`-keyfile`
	or
	`-kf`
		The full path to the agent installation key file.

Switch	`-key`	A string representation of the installation key.
Switch	`-name`	The name of the agent.

Type	Syntax	Description
	or `-n`	
Switch	`-user`	The username to run the Windows service under.
Switch	`-password`	The password for the username of the Windows service account.
Command	`start`	Starts the agent.
Command	`stop`	Stops the agent.
Command	`restart`	Restarts the agent.
Command	`status`	Gets the status of the agent. Status can be Running or Stopped.

Switch	`-h`
	or
	`-?`
		Displays the help screen.

4

Working with the admin portal

Viewing the dashboard

Group Management provides a dashboard to display various group statistics and operational data. The dashboard contains the following components:

- **Groups**: The total number of groups.
- **Pending admin approvals**: The total number of self-service requests pending approval by a Group Management administrator.
- **Pending admin approvals**: The total number of self-service requests pending approval by a Group Management Administrator.
- **Self-service requests**: The total number of self-service requests being processed, including requests in an "In-progress" state and "Attesting" state.
- **Needs your attention!**: A summary of alerts and cautions that require your action.
- **Top 5 group membership**: Top five groups with the largest number of members. Nested group members are not taken into consideration.

Searching in the admin portal

In the admin portal, on the **Groups** tab, you can perform the following searches:

ℹ NOTE: Any search performed in the admin portal is not case-sensitive.

- Type the name of the group that you are looking for in the **Group name** field.
- Click the filter icon to perform a more detailed search for a group.
- When viewing group details, in the **Display name** field, type the name of an owner or member that you are looking for.
- When viewing group details, in the **Service name** field, type the service name that you want to view change history for.

On the **Activities** tab, you can perform the following searches:

- Type the name of the group that you are looking for in the **Group name** field.
- Click the filter icon to perform a more detailed search for the group.

Managing groups

ℹ NOTE: Before managing mail-enabled security groups or distribution lists, you must configure a service account on **Settings** > **Service Accounts**.

- Adding a group
- Editing group general information
- Viewing group change history
- Adding group owners or members
- Removing group owners or members
- Attesting a group
- Deleting a group

Adding a group

Prerequisites

Before creating an on-premises group for a local domain, you must configure the default Organizational Unit for the domain on **Group Management** > **Settings** > **Organizational Units**.

To add a group

1. On the **Groups** tab, click **ADD**.
2. Edit the general information for the new group.

   ℹ NOTE: **Multiple domains exist in a tenant**. You are allowed to select one from the existing domains for the **Domain** field when adding a mail-enabled security group or a distribution list. For Office 365 group, the default domain is automatically applied to the **Domain** field, and you cannot change it.

3. Edit the general information for the new group.
   NOTE: **Multiple domains exist in a tenant**. You are allowed to select one from the existing domains for the **Domain** field when adding a mail-enabled security group or a distribution list. For Office 365 group, the default domain is automatically applied to the **Domain** field, and you cannot change it.
4. Click **ADD**.

Editing group general information

The following general information of a group can be edited in Group Management:

- Group category
- Description
- Expiration date

NOTE: Editing the Description filed is not supported yet for groups of some types. For more information, see Group types.

To edit general information for a group

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

Viewing group change history

The group change history refers to the group membership changes made via self-service, admin service, and group attestation.

To view the change history of a group

1. On the **Groups** tab, search for and select the group you want to view.
2. Click **VIEW** to open the group details page.
   The **Change History** section shows at the bottom of the group details page.

Adding group owners or members

NOTE: Only one owner is allowed for groups of some types. For more information, see Group types.

To add owners or members to a group

1. On the **Groups** tab, search for and select the group you want to add owners or members to.
2. Click the group name to view the group details page.
3. In the **Membership** section of the group details page, select the **Owner** or **Member** tab.

4. On the **Owner** or **Member** tab, click **ADD**.
5. Search for and select the user you want to add on the **Users** tab, and set an expiration date for the membership.

   > TIP: The option **Membership Expires** is not available when you add an owner.

6. Click **SELECT**.
7. Repeat step 3 and 4 to add more users.
8. Click **SUBMIT**.

Removing group owners or members

To remove owners or members from a group

1. On the **Groups** tab, search for and select the group you want to remove owners or members from.
2. Click the group name to view the group details page.
3. In the **Membership** section of the group details page, select the **Owner** or **Member** tab.
4. On the **Owner** or **Member** tab, select the users you want to remove.
5. Click **REMOVE**.
6. In the confirmation window, click **YES**.

Attesting a group

For information about the available group attestations, see Group attestations.

To attest a group

1. On the **Groups** tab, search for and select the group you want to attest.
2. Click **MORE** > **ATTEST**.
3. Select the attestation scope by the **Role** field.
4. Set the maximum duration by the **Must complete in** field.
5. Click **SUBMIT**.

Deleting a group

To delete a group

1. On the **Groups** tab, search for and select the group you want to delete.
2. Click **MORE** > **DELETE**.
3. In the confirmation window, click **YES**.

Managing activities

The **Activities** tab includes the following sub tabs:

- **Admin Approvals**: Lists all the requests pending approval by a Group Management administrator.
- **Self-Services**: Lists all the requests submitted by users in the directory via self-service, including approved, pending, rejected, and canceled requests.
- **Admin Attestations**: Lists all the group attestations launched by a Group Management administrator.
- **Auto Attestations**: Lists all the group attestations triggered by the group setting **Automatic Attestation**.

A Group Management administrator can perform the following tasks on the **Activities** tab:

- Approving/Rejecting request on behalf of approver
- Canceling request on behalf of requester

Approving/Rejecting request on behalf of approver

A Group Management administrator can approve or reject a request on behalf of the current approver.

To approve or reject a request on behalf of the current approver

1. On the **Self-Services** sub tab, search for and select the request you want to approve or reject.
2. Click the ellipsis (...) on the request and select **APPROVE** or **REJECT**.
3. In the confirmation window, click **YES**.

Canceling request on behalf of requester

A Group Management administrator can cancel a request on behalf of the requester.

To cancel a request on behalf of the requester

1. On the **Self-Services** sub tab, search for and select the request you want to cancel.
2. Click the ellipsis (...) on the request and select **CANCEL**.
3. In the confirmation window, click **YES**.

Managing settings

Click **SETTINGS** at the top right of the page to manage the following settings for your tenant:

- Lookup Values
- Policies
- Self-Services

- Service Accounts
- Organizational Units

> **NOTE:** These settings apply to all your tenants added to Group Management.

Lookup Values

Lookup values are predefined values for group names. It allows you to fill the fields in a group name with your predefined values when you create a group.

To create a group with lookup values

1. Define a lookup value list on **Settings** > **Lookup Values**.
2. Add or edit a group naming rule on **Settings** > **Policies** > **Group** > **Group Naming Rule**.
3. Add a **Lookup Value** field in the syntax as needed, and select the lookup value list you defined from the drop-down list for the value.
4. When you create a group, select the group category associated with the group naming rule you edited. The **Lookup Value** field in the group name shows a drop-down list on the page.
5. Select a value from the drop-down list for the group name.

Policies

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

- Group Security Level
- Group Naming Rule
- Group Creation Template for Self-Service
- Group Privacy Rule
- Group Category

Group Security Level

The group security level is a part of Group Category. Group automatic attestation can be enabled in the Group Security Level setting to run group attestation regularly. When you enable the automatic attestation, you are allowed to define the attestation interval, scope, and duration. For information about the available group attestations, see Group attestations.

> TIP: **Enabling automatic attestation for the "Default" group category is not recommended**. The "Default" group category will be automatically assigned to a group without a specified group category, for example, the groups synchronized from an on-premises AD. Such groups might have members who do not have an Azure account to log in to the self-service portal to respond to an attestation request.

Group Naming Rule

The group naming rule is a part of Group Category, and defines the syntax to name a group when Adding a group. When you edit 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.
- **Lookup Values**: Specifies the field with a value set. Users will need to select a value from the specified value set for the field. To manage lookup values, see Lookup Values.
- **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 Creation Template for Self-Service

The group creation template is a part of Group Category, and defines the following attributes for groups created via self-service. A group category can include one or multiple group creation templates. When creating a group in the self-service portal, users must select one to apply the configured attributes to the new group.

- **Group Location**: Specifies where the new group will be created, in the Azure or local domain.
- **Group Type**: Specifies the group type.
- **Group Scope**: Specifies the group scope for the new on-premises group.
- **Domain**: Specifies the domain for the new on-premises group.

NOTE: A group creation template will not be available to a user in the self-service portal if the domain specified in the template is not connected to the tenant the user belongs to.

Group Privacy Rule

The group privacy rule is a part of Group Category and allows you to define whether groups are visible to non-group members in the self-service portal. By default, when a user signs in to the self-service portal, all the groups associated with the tenant are visible. This rule also defines which groups users can view, and request to join, via the **New Request** > **Join Group** feature in the self-service portal. You can manage the visibility of groups by adding group privacy rules and choosing one of the following options:

- **Public**: A group assigned a category with a privacy rule set to public is visible to all users in the self-service portal.
- **Private**: A group assigned a category with a privacy rule set to private is only visible to owners and members of that group.

NOTE: The privacy setting of a group privacy rule cannot be changed after the rule is saved.

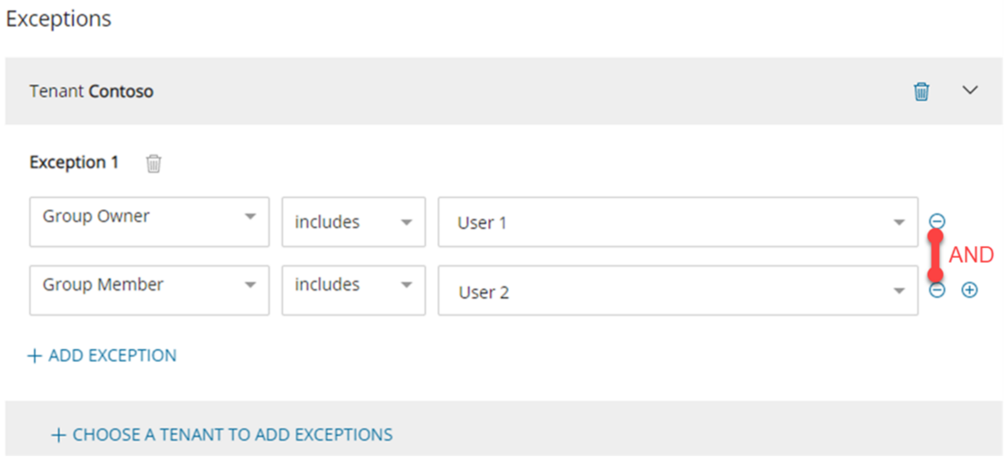
Adding exceptions to group privacy rules

For each group privacy rule, you can create one or more exceptions. An exception defines the groups in a tenant in an organization that are exempt from the group privacy rule setting. Exceptions can be made by group name, group owner, or group member.

For example, Tenant 1 contains some groups, including Group A, which is owned by User 1 and has User 2 as a member. Group A is created using Category A, which is assigned a group privacy rule that is set to private. But, the group privacy rule contains an exception for groups with User 1 as the group owner and User 2 as a group member. This means that Group A is an exception to the private group privacy rule and is visible in the self-service portal. The other groups created using Category A are not visible in the self-service portal.

You can add exceptions for groups in different tenants to one group privacy rule. So, if multiple tenants exist in your organization, you can use one privacy rule to specify exceptions for all tenants.

You can add multiple rules within one exception. The default operator between rules within one exception is "AND". For example, you can add an exception for groups owned by User 1 ***and*** also have User 2 as a group member.



Exceptions

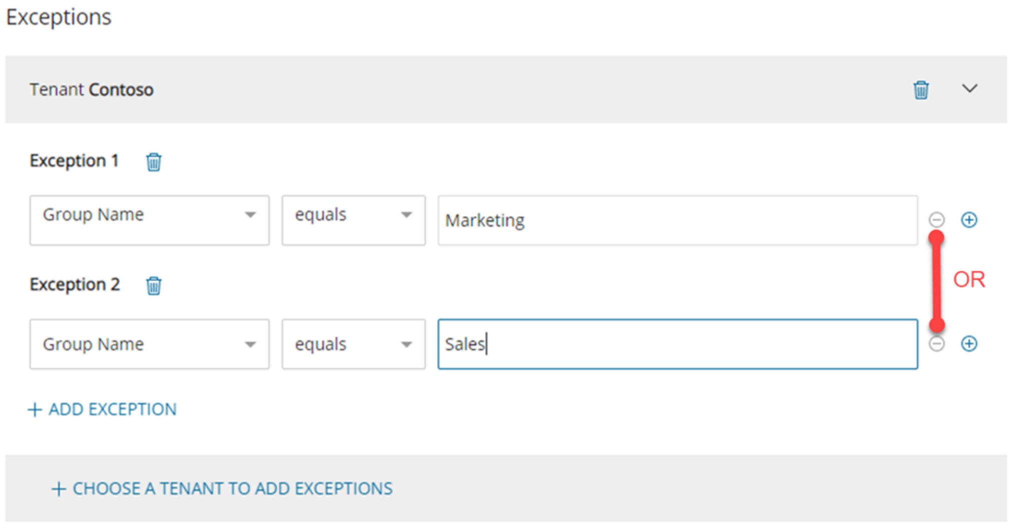
Tenant Contoso

Exception 1

Group Owner includes User 1

Group Member includes User 2

If you add multiple exceptions, the default operator between exceptions is "OR". For example, you can add two exceptions that include groups named "Marketing" ***or*** groups named "Sales".



Exceptions

Tenant Contoso

Exception 1

Group Name equals Marketing

Exception 2

Group Name equals Sales

To add exceptions to group privacy rules

1. On the **Group** tab of the **Policies** page, click **ADD** next to the **Group Privacy Rule** heading.
2. Give your group privacy rule a name and select the privacy setting.
3. In the **Exceptions** section, click **CHOOSE A TENANT TO ADD EXCEPTIONS**.

4. From the **Tenant** drop-down list, select the tenant that contains the groups you want to add as exceptions to the rule and click the check mark.
5. From the first drop-down list, select one of the following options:
    - **Group Name** - allows you to define an exception for a group by name or by text contained in the group name.
    - **Group Owner** - allows you to define an exception for a group owned by a specified user.
    - **Group Member** - allows you to define an exception for a group containing a specified member.
6. From the last drop-down list, type the name of the group or select the user.
7. Click the plus sign (+) to add the exception.

Group Category

A group category includes a Group Security Level, a Group Naming Rule, one or multiple Group Creation Template for Self-Service, and a Group Privacy Rule. You must specify a group category when you create a group.

Self-Services

The **Self-Services** page allows you to manage approval processes for Group Management self-services.

- Approval Processes
- Services

Approval Processes

Group Management provides the following default approval processes on the **Approval Processes** tab:

- **First manager**: Requires approval from the user's manager.
- **Second manager**: Requires approval from the manager of the user's manager.
- **Owner**: Requires approval from one of the group owners.
- **Directory administrator**: Requires approval from one of the Group Management administrators.
- **No approval required**: No approval is required.

> TIP: Users who are assigned the permission **Group Management** > **Can Approve, Reject or Cancel a Request** by the Access Control interface on the On Demand Home site can also approve a request as a Group Management administrator.

Group Management checks the availability of the approvers in the approval process when a user submits a request. If an approver is not available for the user (for example, a request needs approval by the user's manager, but the user does not have a manager in Active Directory), the user gets an error when submitting the request.

You can edit or delete the default approval processes if necessary, or create your own approval processes by clicking **ADD** at the top right of the page.

> NOTE: You cannot delete an approval process that is currently associated with a self-service.

Services

The **Services** tab lists all the Group Management self-services, and each of them comes with a default approval process. You can change the approval process for a self-service by associating the service with another approval process defined on the Approval Processes tab.

> ℹ NOTE: For self-services that do not need any approvals, associate them with the default approval process "No approval required".

Service Accounts

Group Management requires a service account to manage mail-enabled security groups and distribution lists from your tenants.

Prerequisites

The role group Organization Management in Exchange must be assigned the roles “Distribution Groups” and "Security Group Creation and Membership".

To configure the service account for a tenant

1. Navigate to the **Group Management** > **Settings** > **Service Accounts** page, and click the edit button in the **Action** column on the tenant.
2. Provide the Exchange admin credentials in the **Service account** column.
3. Click the check mark.

Organizational Units

The **Organizational Units** page allows you to configure the default organizational unit (OU) for your on-premises domains. The default OU applies to on-premises groups created in Group Management. You must configure the default OU before creating groups for an on-premises domain.

To configure the default OU for an on-premises domain

1. Navigate to the **Group Management** > **Settings** > **Organizational Units** page, click the edit button in the **Action** column on the domain.
2. Enter the default OU in the **Default OU** column.

   > ℹ NOTE: Make sure the default OU has been synchronized to Group Management. It takes about 10 minutes to synchronize a newly-added OU from your local domain to Group Management.

3. Click the check mark.

Downloading activity trail logs

An activity trail is a set of records that provide documentary evidence of the sequence of activities that have affected at any time a specific operation, procedure, or event. Group Management retains the complete successful and failed activity trail history for the events listed in the table below.

Table 6: Supported audit events

Portal	Audit Events
Admin portal	Adding or removing a group owner or member Adding, updating, or deleting a group Attesting or auto-attesting membership or ownership of a group Auto-deleting an expired group Auto-removing an expired member from group Adding, updating, or deleting a group category Adding, updating, or deleting a group naming rule Adding, updating, or deleting a group security level
Self-service portal	Adding or removing a group owner or member Joining or leaving a group as owner or member Adding, updating, or deleting a group Attesting or auto-attesting membership or ownership of a group

To download activity trail logs

1. In the side navigation panel, click **Settings**.
2. In the main panel, under **ACTIVITY TRAIL**, select **Group Management**.
   By default, the date fields are configured to download logs from the last seven days.
3. To change the start or end dates, click on the date fields and select a date from the calendar window.
4. Click **Download**.
   A zip file containing a comma separated values (.csv) file is downloaded.

Working with the self-service portal

Signing in to the self-service portal

Group Management users can sign in to the self-service portal at https://quest-on-demand.com/groups/management.

To sign in to the self-service portal

1. Go to the web page https://quest-on-demand.com/groups/management.
2. Enter your Azure account.
3. Click **Accept** to grant permissions requested by the self-service portal.
   The **My Approvals** page opens. You are signed in to the self-service portal.

Searching in the self-service portal

In the self-service portal, on the **My Activities** page, you can perform the following search for a group that you want to manage:

> **NOTE:** Any search performed in the self-service portal is not case-sensitive.

- On the **My Approvals** tab, **My Requests** tab, and **My Attestations** tab, type the name of the group that you are looking for in the **Group name** field.

On the **My Profile** page, you can perform the following search for a group that you have joined:

- Type the name of the group that you are looking for in the **Group name** field.

On the **Gallery** page, you can perform the following searches for a group:

- Type the name of the group that you are looking for in the **Group name** field.
- Click the filter icon to perform a more detailed search.

When making a new request, you can perform the following search for a group:

> NOTE: You cannot search for groups when making a request to add a group.

- Type the name of the group that you are looking for in the **Group name** field.

My Activities

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

- My Approvals
- My Requests
- My Attestations

My Approvals

The **My Approvals** tab lists all the requests that require approval from the user. This includes:

- The requests that are awaiting approval from the user.
- The requests that the user has approved or rejected.

To approve or reject a request in the list, click the ellipsis (...) on the request and select **APPROVE** or **REJECT**.

My Requests

The **My Requests** tab lists all the requests submitted by the user. This includes:

- The requests that are awaiting approval.
- The requests that have been approved or rejected.

The user can cancel a request if the request has not been approved or rejected yet (the request status shows **In progress**).

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 ellipsis (...) on the request and select **CANCEL**.

3. Input the reason you canceled the request.
4. Click **SUBMIT**.

My Attestations

The **My Attestations** tab lists all the attestation requests that require a response from the user.

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

My Profile

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

- My Groups

My Groups

The **My Groups** tab lists all the groups that the user has joined:

- The **Owner** sub tab lists the groups that the user has joined as an owner.
- The **Member** sub tab lists the groups that the user has joined as a member.

The user can click a group in the list to perform the following actions:

- View the group general information
- View the group roles assigned to the user: either owner or member, or both
- Submit various requests:
  - (For group owners only) Manage group owners and members
  - (For group owners only) Attest the group
  - (For group owners only) Delete the group
  - Leave the group

Gallery

The following tabs are available on the **Gallery** page:

- Groups

Groups

On the **Groups** tab, users can see all the groups in the tenant that they own, are a member of, or are granted permission to view. The user can perform the following actions:

- View the general information, ownership, and membership of a group
- Submit various requests:
  - Join a group as an owner or member
  - Add a group

New Request

The following tabs are available on the **New Request** page:

- Group

Group

The user can submit various requests on the **Group** tab. This includes:

- Add group
- Join group
- Leave group
- Attest group
- Add group owners
- Remove group owners
- Add group members
- Remove group members
- Delete group

6

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
- License Management
- Migration
- Recovery

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
- License Management
- Migration
- Recovery

Release Notes

- Global Settings
- Audit
- Group Management
- License Management
- Migration
- Recovery

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.

Appendix A: Attribute mappings between Azure AD and GM

Table 7: Attribute mappings between Azure AD and GM

Azure AD Group	Group Management Group
displayName	Name
description	Description
The part after @ in email address [1]	Domain
mail	Mail
owners	Owners
members	Members

[1]: Mapping from Azure AD to Group Management only.

Appendix B: Attribute mappings between on-premises AD and GM

Table 8: Attribute mappings between on-premises AD and GM

On-Premises AD Group	Group Management User
displayName [1]	Name
description [1]	Description
mail [1]	Email address
The domain name of the on-premises AD [1]	Domain
managedBy + msExchCoManagedByLink	Owner
member	Member

[1]: Mapping from on-premises 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.