

Quest® On Demand Global Settings
User Guide



© 2019 Quest Software Inc.

ALL RIGHTS RESERVED.

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

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

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

Quest Software Inc.
Attn: LEGAL Dept.
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our website (<https://www.quest.com>) for regional and international office information.

Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at <https://www.quest.com/legal>.

Trademarks

Quest and the Quest logo are trademarks and registered trademarks of Quest Software Inc. 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.

[To determine what trademarks to add, review your document for any of the trademarks listed on https://www.quest.com/legal/trademark-information.aspx. Any references should be listed in the trademark paragraph.](https://www.quest.com/legal/trademark-information.aspx)

Legend

- **WARNING:** A WARNING icon indicates a potential for property damage, personal injury, or death.

- ⚠ **CAUTION:** A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

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

Contents

Working with On Demand	6
Overview of On Demand	7
Organizations	7
Azure Active Directory tenants	7
Signing up for On Demand	9
Organizations and regions	9
Multi-factor Authentication	10
On Demand trials and subscriptions	10
Signing up and creating an organization	10
Signing in to On Demand with your existing Quest account	12
Signing up for a new Quest account and signing in to On Demand	12
Trying On Demand as a Guest User	13
Managing organizations and regions	14
Geographic regions	14
Multiple organizations	15
Displaying the current organization ID	16
Creating a new organization	16
Switching organizations	16
Renaming organizations	16
Displaying the organization ID	17
Adding users to an organization	18
Users and roles	18
Default roles	18
On Demand administrator	18
Module administrator	18
Default role permissions	19
Adding a user and assigning a role	19
Access Control: Roles	21
Viewing role permissions	21
Creating a custom role	21
Editing a custom role	22
Adding a user to a role	22
Deleting a custom role	22
Access Control: Users	23
Adding a user to your organization and assigning a role	23
Editing user roles	23
Removing a user from the organization	24
Inviting new users	24
Creating a Quest account and joining an existing On Demand organization	25
Joining an existing On Demand organization	25

Joining an existing On Demand organization with an Azure AD account	26
Managing tenants	27
Tenant overview	27
Number of users in the tenant	27
Azure AD tenant	27
Azure Global administrator	28
Admin consent permission levels	28
Adding a tenant	28
Managing admin consent	29
Admin consent status	29
Granting consent	30
Revoking admin consent	30
Removing a tenant	31
On Demand Home page	32
Masthead	32
Masthead drop-down menu	32
Information window	33
On Demand Status page	33
Side navigation panel	34
Dashboard	34
Tenant filter	35
Tenant summary	35
Needs your attention!	35
Module tiles	36
Settings	37
Activity trail	37
Agents	38
Notifications	38
Configuring notification recipients	38
Subscriptions	38
Subscription details	39
Managing subscriptions	39
Subscription expiry	40
Documentation roadmap	42
Global settings	42
Modules	42
Documentation	42
User Guides	42
Release Notes	43
More resources	43
Technical Support	44
Current operational status	44
Contact support	44

Module product support pages	44
Information and discussion: Quest community forums	44

Working with On Demand

Welcome to On Demand. For an overview of the application, see [Overview of On Demand](#). Use the links below for information on using On Demand.

Signing up for On Demand	<p>On Demand software is hosted in the cloud by Quest Software and made available to users through the internet. This section contains information regarding signing up for the On Demand service.</p> <p>On Demand management is based on the concept of organizations. An On Demand organization can subscribe to modules. Organization administrators can use the tools provided by the modules to perform administrative actions on Azure AD tenants.</p> <p>IMPORTANT: To use the features of a module after you sign up, you must have a subscription.</p> <p>Trial licenses are available. See "Product Licensing" in the Global Settings Release Notes.</p>
Managing tenants	<p>A tenant houses the users in a company and the information about them. You must add a tenant to manage the tenant properties using an On Demand module. For the U.S. region, in addition to commercial tenants, you can add GCC and GCC High tenants if needed,</p>
Adding users to an organization	<p>Once you have created an organization, you can add additional users and determine what tasks each user can perform.</p>
On Demand Home page	<p>After signing in, users see the Dashboard. In addition to a tile for each module, the Dashboard displays statistics and operational data for your tenant.</p>
Settings	<p>Configure On Demand for your organization.</p>
Documentation roadmap	<p>Links to the User Guide and Release Notes for each module.</p>
Technical Support	<p>Resources for On Demand technical support.</p>

Overview of On Demand

On Demand is a cloud based management platform that provides access to multiple Quest Software tools for Microsoft product management through a unified 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 activity trail 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](#).

Signing up for On Demand

On Demand is a Software as a Service (SaaS) application. SaaS is a software licensing and delivery model in which application software is licensed on a subscription basis. The On Demand software is hosted in the cloud by Quest Software and made available to users through the internet. This section contains information regarding signing up for the On Demand service.

Organizations and regions	This section provides an overview of organizations and regions. You can configure organizations and regions after you sign up.
Multi-factor Authentication	Information on how to enable multi-factor authentication.
On Demand trials and subscriptions	You must start a trial or purchase a subscription to begin using On Demand services.
Signing up and creating an organization	A task flow of the sign up process with links to step by step procedures.

Organizations and regions

On Demand management is based on the concepts of organizations. When you sign up for the On Demand service, you create an organization and you become the organization administrator. The organization can subscribe to modules. Organization administrators can use the tools provided by the modules to perform administrative actions on Azure AD tenants. You can add additional organization administrators and module administrators that have access to specific modules.

For most On Demand use cases, a customer creates a single organization. Multiple administrators and multiple tenants can be added to the organization.

CAUTION: Adding a tenant to multiple organizations.

Adding the same tenant to multiple organizations can result in conflicting application of policies and settings. When using multiple organizations to manage a tenant, the organization administrators must coordinate their management activities.

A Microsoft Azure region is a set of data centers deployed within a geographic area. Selecting the correct region for your organization enables you to achieve higher performance and supports your requirements and preferences regarding data location. Specifying the region for your organization determines the geographical region where your data is stored.

During sign up, you can choose the region where your On Demand data will be hosted. The following regions are currently supported:

- Australia
- Canada
- Europe
- United Kingdom
- United State

For more information, see [Geographic regions](#).

Multi-factor Authentication

Multi-factor authentication (MFA) increases the security of the sign in process. With MFA, a user is granted access only after presenting two or more pieces of evidence (or factors) to an authentication mechanism.

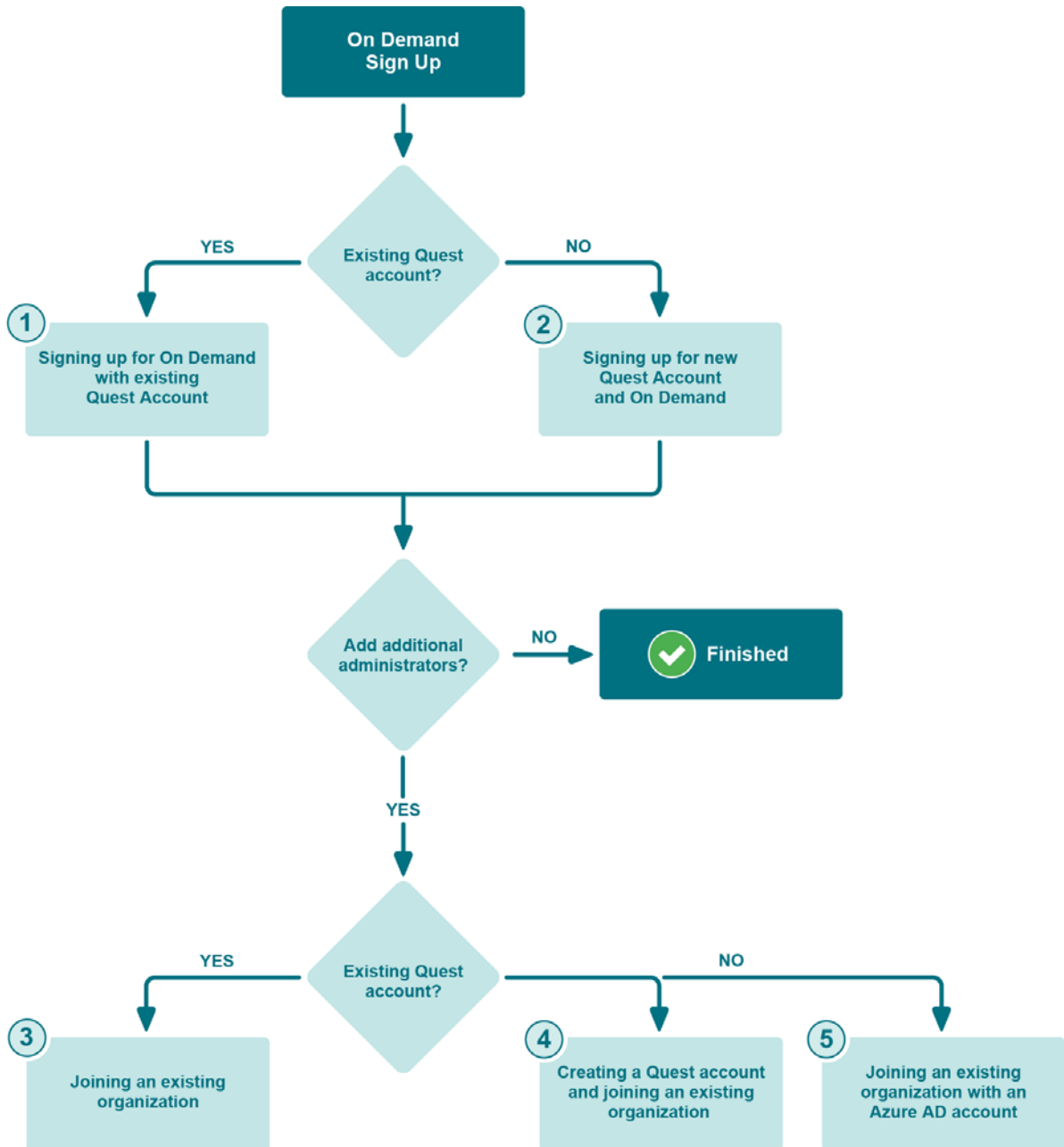
Microsoft accounts can be MFA-enabled. To enable multi-factor authentication (MFA) when signing in to OnDemand, select **Sign in with Microsoft** on the Sign In page and login with your Microsoft MFA-enabled account.

On Demand trials and subscriptions

Once you have signed in to and created an organization, you have the option to begin a trial or purchase a subscription for modules. In the side navigation panel, click Services to open a page with module information and Learn More links that take you to the appropriate Quest web sites.

Signing up and creating an organization

The flow chart that follows shows the sign up process.



Signing in to On Demand with your existing Quest account

1

Signing up for a new Quest account and signing in to On Demand

2

Trying On Demand as a Guest User

3

Adding users to an organization

4

Signing in to On Demand with your existing Quest account

You may already have a Quest account if you currently use other Quest products. Use this procedure to sign in to with your Quest account and create a new On Demand organization.

i | **NOTE:** To enable multi-factor authentication (MFA) when signing in to OnDemand, select **Sign in with Microsoft** on the Sign In page and login with your Microsoft MFA-enabled account.

To sign in to On Demand using your Quest account:

- 1 Go to the web page quest-on-demand.com.
The "Welcome to On Demand" page opens.
- 2 Under **Already have an account**, click **Sign In**.
The "Sign in" page opens.
- 3 Enter your Quest account credentials.
- 4 Click **Sign In**
A page opens that states, "We are unable to locate any organizations for your account". Click the link **Click here**.
The "Subscribe" page opens.
- 5 Complete the required fields. Use your Quest credentials for the email and password.
- 6 Click **Subscribe**.
The Welcome to On Demand page opens.
- 7 In the **Add organization** name field, enter a name for your On Demand organization.
- 8 In the **Select Region** field, select the region where you want your data to reside.
- 9 Click **Create New Organization**.

You are signed in to your organization. You are an On Demand administrator for the organization.

Signing up for a new Quest account and signing in to On Demand

Prerequisites

To perform this procedure, you must have a valid email account where you can receive a verification email from support.quest.com.

i | **NOTE:** To enable multi-factor authentication (MFA) when signing in to OnDemand, select **Sign in with Microsoft** on the Sign In page and login with your Microsoft MFA-enabled account.

Use this procedure to create a Quest account and create a new On Demand organization.

To sign up for a new Quest account:

- 1 Go to the web page quest-on-demand.com.
The "Welcome to On Demand" page opens.
- 2 Under **Create a Quest account** click **Sign Up**.
The "Create a Account" page opens.
- 3 Enter your credentials for your new Quest account.
Note that the email and password entered here will be the credentials you use to sign in to On Demand.

- 4 Click the check box to agree to Quest's privacy policy and terms of use.
- 5 Click **Sign Up**.
The "We've sent you an email" page opens.
- 6 Go to your email account and open the email from `support.quest.com`.
- 7 Click on the **Verify email address** link.
The "Welcome to On Demand" page opens.
- 8 In the **Add organization name** field, enter a name for your On Demand organization.
- 9 In the **Select Region** field, select the region where you want your data to reside.
- 10 Click **Create Organization**.

You are signed in to your organization. You are an On Demand administrator for the organization.

Trying On Demand as a Guest User

You can try On Demand by signing in with an email address and scanning your environment. This process provides a dashboard view based on your data.

When you sign in as a guest user, a Quest account is associated with your email address and an On Demand organization is created for you.

Prerequisites

In order to scan your environment and provide a dashboard view based on your data, you must add a tenant. Admin consent is required to add a tenant to On Demand. Since only an Azure Global administrator can grant admin consent, you must be able to provide Azure Global administrator credentials for the tenant you are adding.

To sign in as a guest user

- 1 Go to the web page quest-on-demand.com.
The "Welcome to On Demand" page opens.
- 2 Under **Explore On Demand** click **Continue as Guest**.
The Guest User Demo Dashboard opens.
- 3 In the top right of the screen, click **Scan My Environment** and follow the steps to add your Azure AD tenant.

Managing organizations and regions

On Demand management is based on the concept of organizations. An organization can subscribe to modules. Organization administrators can use the tools provided by the modules to perform administrative actions on Azure AD tenants.

When a user signs up for On Demand, an organization is created and the user becomes an administrator for the organization. For most On Demand use cases, a customer creates a single organization. Multiple administrators and multiple tenants can be added to the organization. See [Signing up for On Demand](#).

Use the links below for more information on managing organizations and regions.

- [Geographic regions](#)
- [Multiple organizations](#)
- [Displaying the current organization ID](#)
- [Creating a new organization](#)
- [Switching organizations](#)
- [Renaming organizations](#)
- [Displaying the organization ID](#)

i | **NOTE:** To delete an organization, contact [Technical Support](#).

Geographic regions

A Microsoft Azure region is a set of data centers deployed within a geographic area. Selecting the correct region for your On Demand organization enables you to achieve higher performance and supports your requirements and preferences regarding data location. Specifying the region for your organization determines the geographical region where your data is stored. For more information, see [Azure regions](#).

During sign up, you can choose the region where your On Demand data will be hosted. The following regions are currently supported:

- United States
- Europe
- United Kingdom
- Canada
- Australia

Regional availability of modules

Microsoft continues to deploy services across Azure regions. However, at this time, not all services are available in all regions. As a result, not all On Demand modules are available in all regions. The table below lists current module availability by region. When you create an organization in a region, only the available module tiles are displayed on your home page.

Region	Available Modules
U.S.	<ul style="list-style-type: none"> • Audit • Group Management • License Management • Migration • Recovery
Europe	<ul style="list-style-type: none"> • Audit • Group Management • License Management • Migration • Recovery
U.K.	<ul style="list-style-type: none"> • Audit • Group Management • License Management • Migration • Recovery
Canada	<ul style="list-style-type: none"> • Audit • Group Management • License Management • Migration • Recovery
Australia	<ul style="list-style-type: none"> • Audit • Group Management • License Management • Migration

For the most up-to-date information, see <https://regions.quest-on-demand.com/>.

Multiple organizations

Some customers may want to create multiple organizations. For example:

- A managed service provider (MSP) can create an organization for each client.
- A global company can create separate organizations for employees by geographic region.

When you sign up for On Demand, you are prompted to name your organization. Users with multiple organizations associated with their email address are prompted to select an organization during sign in.

CAUTION: Adding a tenant to multiple organizations.

Adding the same tenant to multiple organizations can result in conflicting application of policies and settings. When using multiple organizations to manage a tenant, the organization administrators must coordinate their management activities.

Displaying the current organization ID

You can display the organization to which you are currently signed in and its region by clicking on your email address in the top menu bar.

In the menu list, if you have only one tenant, the organization is shown under the Organization Name title. Click the organization to display the Edit Organization page which shows the Organization ID.

If you have more than one tenant, the Manage Tenants option is shown under Organization Name. Click **Manage Tenants** to see the list of your tenants with the tenant to which you are connected indicated. The organization ID is displayed on the tile for each tenant.

Creating a new organization

As an On Demand user, there may be no organizations associated with your account. This can happen if you have been removed from all organizations. In this case, after you sign in, the Welcome to On Demand page opens where you can create a new organization. Use the following steps to create an organization.

If you are currently signed in, you can create a new organization by clicking your email address in the menu bar at the top of the page and selecting **Create Organization**. Follow the steps that follow to create an organization.

i | **TIP:** On the Create Organization page, if you decide not to create a new organization, click on your browser back button to return to your original organization.

To create a new organization:

- 1 Enter an organization name.
- 2 Select a region.
- 3 Click **Create Organization**.

i | **NOTE:** To delete an organization, contact [Technical Support](#).

Switching organizations

If you have multiple organizations associated with your email address, you are prompted to select an organization when you sign in. Once you are signed in, you can switch to another organization.

To switch to another organization:

- 1 In the top menu bar, on the right hand side, click on your user email address.
- 2 Select **Switch Organization**.
The Choose an Organizations page opens.
- 3 locate the row that contains the organization to which you want to switch.
- 4 Click **Select**.

Renaming organizations

You can rename the organization to which you are currently signed in.

Prerequisites

You must be an On Demand organization administrator to rename an organization.

To rename an organization:

- 1 Sign in to the organization that you want to change.
- 2 In the top menu bar, on the right hand side, click on your user email address.
- 3 Click **Organization Name**.
The Edit Organization page opens.
- 4 In the **Organization Name** field, enter the new name.
- 5 Click **UPDATE ORGANIZATION NAME**.
The organization name is updated.

Displaying the organization ID

Each organization has a unique organization ID. This ID may be required by technical support to troubleshoot issues. The Organization ID is displayed on the Manage Tenants page.

To display the organization ID:

- 1 In the top menu bar, on the right hand side, click on your user email address.
- 2 Click **Organization Name**.
The Edit Organization page opens.
Make note of the organization ID.
- 3 Click the browser back arrow to return to the Home page.

In the menu list, if you have only one tenant, the organization is shown under the Organization Name title. Click the organization to display the Edit Organization page which shows the organization ID.

If you have more than one tenant, the Manage Tenants option is shown under Organization Name. Click **Manage Tenants** to see the list of your tenants with the tenant to which you are connected indicated. The organization ID is displayed for each tenant.

Adding users to an organization

Once you have created an organization, you can add additional users and determine what tasks each user can perform.

For a list of access control procedures, see the task flow [Adding a user and assigning a role](#).

Users and roles

When you add a user to an organization, you also assign one or more roles. The role assignment determines what permission level a user has and ultimately, what tasks the user can perform. Assigning roles and setting user permissions is referred to as access control.

Access control is a process by which users are granted access and certain privileges to systems, resources, or information. In On Demand, you can grant authenticated users access to specific resources based on your company policies and the permission level assigned to the user.

On Demand comes configured with a number of default roles. The default role permissions settings cannot be changed, but you can create custom roles with specific permission settings to align with your company policies. You can assign multiple roles to each user in order to combine permission sets.

NOTE: Every user must be assigned to at least one role. You cannot remove all roles from a user.

Default roles and their permission settings are described below.

The On Demand access control interface is comprised of two pages.

- For information specific to configuring roles, see [Access Control: Roles](#)
- For information specific to managing users, see [Access Control: Users](#)

Default roles

On Demand is configured with default roles that cannot be edited or deleted. You can duplicate default roles to create custom roles. The default roles are listed below.

On Demand administrator

On Demand administrators have full access to global settings and all modules. The user who signed up for On Demand and created the organization is automatically assigned the On Demand Administrator role.

Module administrator

Module administrators only have access to the specific module where they have been added as an administrator. Module administrators do not have access to global settings or tenants.

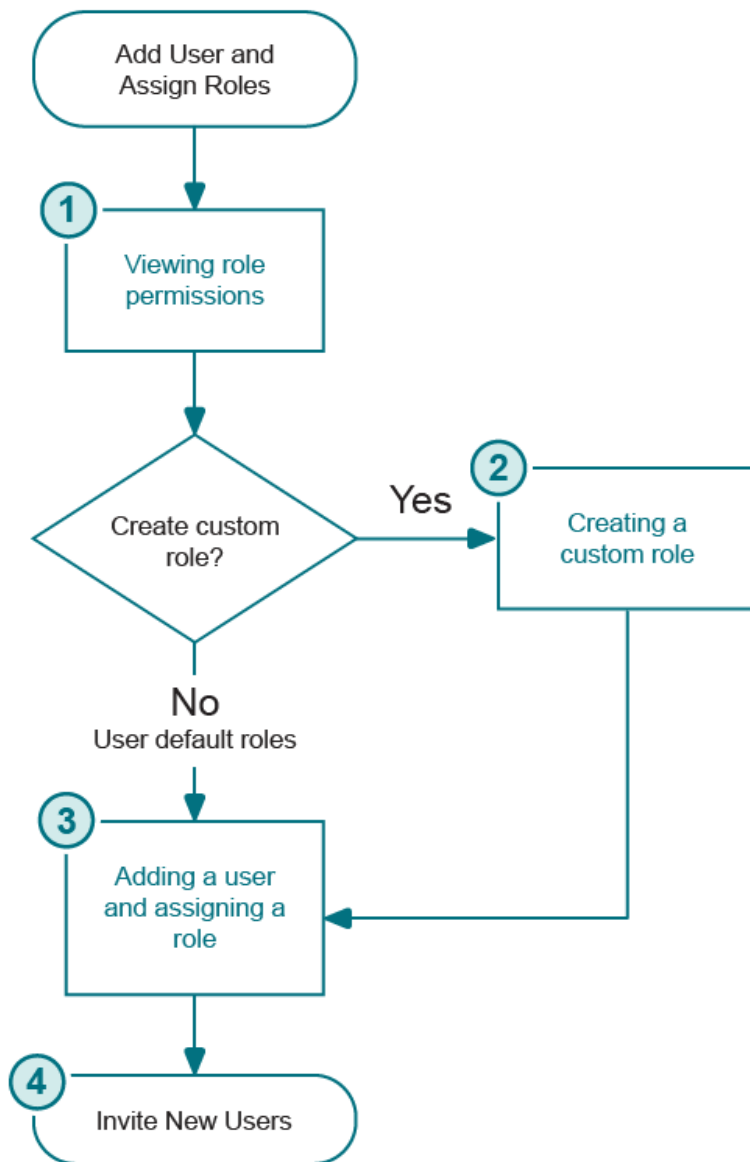
Default role permissions

Role	Permissions
On Demand Administrator (also has all module permissions)	<ul style="list-style-type: none">• Can rename the organization• Can read access control roles• Can create, delete, and assign access control roles• Can add and remove tenants• Can read Activity Trail Specific services can be selected for this permission.
Recovery Administrator	<ul style="list-style-type: none">• Can manage backup settings• Can download hybrid credentials• Can run backup manually• Can unpack backups• Can run difference Report• Can restore from objects• Can restore from differences• Can read backup history• Can read unpacked objects• Can read differences• Can read task history• Can read events• Can read restore attributes• Can read UI projects• Can read UI collections• Can manage events• Can manage project settings
Audit Administrator	Can configure auditing and manage searches Specific services can be selected for this permission.
Group Management Administrator	<ul style="list-style-type: none">• Can configure and manage group management• Can approve ,reject, or cancel a request
Migration Administrator	Can configure and run migrations
License Management Administrator	<ul style="list-style-type: none">• Can read licenses• Can manage licenses

Adding a user and assigning a role

The flow chart that follows shows the process for adding users and assigning a role. The first step is to view the default role permissions settings. If required, you can create custom roles with specific permission settings to align with your company policies.

Once you have added a user, you must invite the user to sign in to the organization.



Viewing role permissions

1

Creating a custom role

2

Adding a user to your organization and assigning a role

3

Inviting new users

4

Access Control: Roles

Each access control role has a specific set of permissions that determines what tasks a user assigned to the role can perform. Your On Demand organization comes configured with a number of default roles. The default role permissions settings cannot be changed, but you can create custom roles with specific permission settings to align with your company policies.

i | **NOTE:** To manage access control roles, you must have the permission "Can create, delete, and assign access control roles".

Perform the following tasks from the access control Roles page:

- [Viewing role permissions](#)
- [Creating a custom role](#)
- [Editing a custom role](#)
- [Adding a user to a role](#)
- [Deleting a custom role](#)

Viewing role permissions

Use the Roles page to view the list of roles defined for your organization. You can also view the users assigned to each role.

To view roles and permissions:

- 1 In the side navigation panel, expand the **Access Control** item and select **Roles**.
- 2 Click on a role name to open a read only page that displays the **Role Permissions**. The panel on the right is a list of users assigned to the role.
- 3 To add users to the role, see [Access Control: Users](#).

Creating a custom role

You can create roles with a custom set of permissions. Default roles cannot be edited. You must create a custom role to enable editing.

To create a role:

- 1 In the side navigation panel, expand the **Access Control** item and select **Roles**.
- 2 At the top right of the Roles page, click **Create Role**.
NOTE: You can define a role based on an existing role. In the Roles list, click on the **Action** menu for a role and select **Duplicate**.
- 3 On the Create Role page, enter a **Role Name** and **Description**.
- 4 Under Role Permissions, select the check boxes for the permissions you want to assign to the role.
Some role permissions are partitioned into services. If available, you can configure access to a service using the **Selected Services** field.
- 5 At the top right of the page, click **Create Role**.
You are returned to the Roles page and there is a prompt to **Assign Users**.
- 6 To add a user to the role, click **Assign Users**.
- 7 In the **Add User to <custom_role>** field, enter the email address of the user you want to add.

- 8 Click **Add User**.

If the user is not currently a member, they are added to the organization.

Editing a custom role

Note that you cannot edit a default role. You can duplicate a default role and edit it to create a custom role.

To edit a role:

- 1 In the side navigation panel, expand the **Access Control** item and select **Roles**.
- 2 In the **Roles** list, click on the **Action** menu for a role and select **Edit**.
- 3 On the Edit Role page, you can edit:

Name

Description

Role Permissions.

Some role permissions are partitioned into services. If available, you can configure access to a service using the **Selected Services** field.

- 4 Click **Save**.

You are returned to the Roles page and there is a prompt to **Assign Users**.

- 5 To add a user to the role, click **Assign Users**.
- 6 In the **Add User to <custom_role>** field, enter the email address of the user you want to add.
- 7 Click **Add User**.

If the user is not currently a member, they are added to the organization.

Adding a user to a role



NOTE: Email notification

When a user is added to a role, the user receives an email informing them of the action.

To add a user to a role:

- 1 In the side navigation panel, expand the **Access Control** item and select **Roles**.
- 2 In the **Roles** list, click on the **Action** menu for a role and select **Assign Users**.
The Assign Role page opens.
- 3 In the **Add a user to this role** field, enter the email address of the user you want to add.
The user name must use the email address format <local_part>@<domain>.
- 4 Click **Add User**.

The user is assigned to the role and has the permission set defined by the role.

Deleting a custom role

You cannot delete a default role.

Before deleting a role, you must remove all users from the role and either assign them a new role or remove them from the organization.

To delete a role:

- 1 In the side navigation panel, expand the **Access Control** item and select **Roles**.
- 2 In the **Roles** list, click on the **Action** menu for a role and select **Delete**.
- 3 In the confirmation window, click **Delete**.

You are returned to the Roles page.

Access Control: Users

Organization user credentials are based on email addresses. To log in to On Demand using the email address, the user must create a On Demand account with the email address. To create an On Demand account, see [Signing up and creating an organization](#).

Perform the following tasks on the access control Users page:

- [Adding a user to your organization and assigning a role](#)
- [Editing user roles](#)
- [Removing a user from the organization](#)

Once you have added a user, inform them that they have been added to an organization and specify the email address or Azure AD account used. Direct the new users to sign in to the organization using the procedures under [Inviting new users](#).

Adding a user to your organization and assigning a role

On Demand is configured with default roles. To create a custom role, see [Access Control: Roles](#).



NOTE: Email notification

When a user is added to a role, the user receives an email informing them of the action.

To add a user:

- 1 In the side navigation panel, expand the **Access Control** item and select **Users**.
- 2 In the **User Name** field, enter the email address of the user you want to add.
The user name must use the email address format <local_part>@<domain>.
- 3 In the **Assigned Role** field, enter the role name. An auto-complete list offers suggestions based on your input.
- 4 Select a role to enable the **Add** button.
- 5 Click **Add**.

Editing user roles

On Demand is configured with default roles. To create a custom role, see [Access Control: Roles](#).



NOTE: Email notification

When a user is added to a role, the user receives an email informing them of the action.

To assign a new role:

- 1 In the side navigation panel, expand the **Access Control** item and select **Users**.

- 2 In the list of users, locate the user you want to edit in the **User Name** column.
- 3 On the right side of the **Role** field for the user, click the edit icon to make the **Role** field editable.
- 4 Click inside the editable **Role** field and begin typing the name of the role you want to add. An auto-complete list offers suggestions based on your input.
- 5 Enter the role name you want to add. An auto-complete list offers suggestions based on your input.
- 6 Select the role from the list.
- 7 Add additional roles or remove assigned roles as required.
- 8 Click the check mark to confirm the role assignment.

Removing a user from the organization

To remove a user:



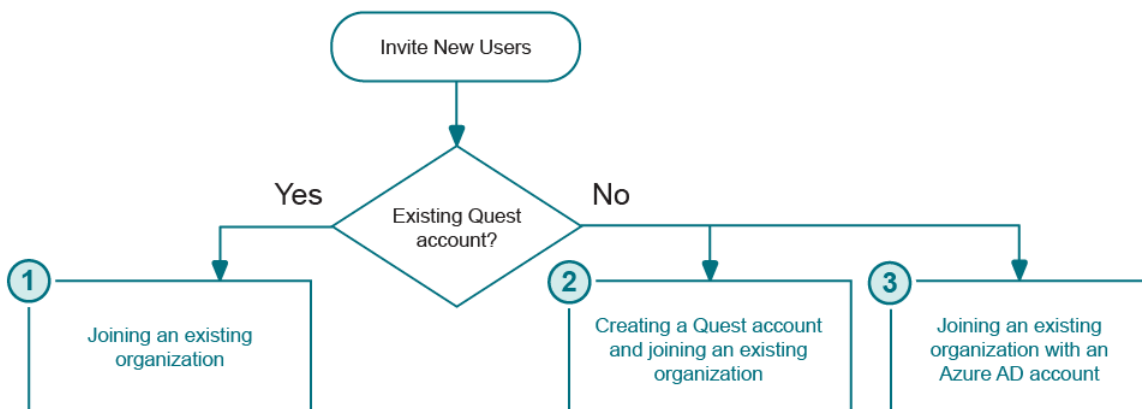
NOTE: Email notification

When a user is removed from the organization, they receive an email informing them that they no longer have access to the organization.

- 1 In the side navigation panel, expand the **Access Control** item and select **Users**.
- 2 In the list of users, locate the user you want to delete in the **User Name** column.
- 3 In the **Action** field for the user, click the delete icon.
- 4 In the confirmation window, click **Remove**.

Inviting new users

Once you have added a user, inform them that they have been added to an organization and specify the email address or Azure AD account used. Direct the new users to the following procedures to sign in to the organization.



1 Creating a Quest account and joining an existing On Demand organization



Creating a Quest account and joining an existing On Demand organization

This procedure is for new On Demand users. You do not need to create a Quest account to join an existing On Demand organization. However, creating a Quest account allows you to access On Demand resources such as the support site.

If do not want to create a Quest account or you already have an On Demand account and an administrator has added you to their organization, see [Joining an existing On Demand organization](#).

Prerequisites

The following prerequisites must be met:

- You must have a valid email account where you can receive a verification email from *support.quest.com*.
- An administrator for the organization must have added you to the organization.

To join an organization:

- 1 Go to the On Demand web page quest-on-demand.com and under Create a Quest account, click **Sign Up**.
The Create a Quest Account page opens.
- 2 Enter your credentials for your new account.
The email and password you enter will be the credentials you use to sign in to On Demand.
- 3 Click the check box to agree to Quest's privacy policy and terms of use.
- 4 Click **Sign Up**.
The We've sent you an email page opens.
- 5 Open your email account and open the email from Support.quest.com.
- 6 Click the **Verify email address** link.
The On Demand home page opens. You are signed in to the organization to which you were added.

Joining an existing On Demand organization

This procedure is for users that want to join an existing organization.

Prerequisites

- An administrator for the organization must have added you to the organization.

i | **NOTE:** An administrator can add you to an organization by specifying your Azure AD account. See [Joining an existing On Demand organization with an Azure AD account](#).

- If multiple On Demand organizations are associated with your email account, you must know the name of the organization you want to sign in to. After sign in, the "Select Organization" page is displayed where you must select the organization that you want to sign in to.

To join an organization:

- 1 Go to the web page quest-on-demand.com.
The Welcome to On Demand page opens.
- 2 Under Already have an account, click **Sign In**.
- 3 Enter your email account credentials.
- 4 Click **Sign In**.
 - If only one organization is associated with your email account, the On Demand home page opens. You are signed in to the organization to which you were added.
 - If there are multiple organizations associated with your email account, the Multiple Organizations Found page opens with a list of organizations. Click the organization you want and click **Select Organization**.

Joining an existing On Demand organization with an Azure AD account

You can use your Azure AD account to join an existing On Demand organization. Using your Azure AD account is referred to as federated identity management.

Federated identity management can increase security and lower risk by enabling an organization to identify and authenticate a user once, and then use that identity information across multiple systems, including external partner websites such as On Demand.

Prerequisites

- An administrator for the organization must have added you to the organization.
- If multiple On Demand organizations are associated with your email account, you must know the name of the organization you want to sign in to. After sign in, the Select Organization page is displayed where you must select the organization that you want to sign in to.

To join an organization with an Azure AD account:

- 1 Go to the web page quest-on-demand.com.
The Welcome to On Demand page opens.
- 2 Under Already have an account, click **Sign In**.
- 3 At the bottom of the page, click **Sign in with Microsoft**.
 - If only one organization is associated with your email account, the On Demand home page opens. You are signed in to the organization that your were added to.
 - If there are multiple organizations associated with your email account, the Multiple Organizations Found page opens with a list of organizations. Click the organization you want and click **Select Organization**.

Managing tenants

A tenant is a dedicated instance of Azure Active Directory (Azure AD) that your Microsoft organization receives and owns when it signs up for a Microsoft cloud service such as Azure or Office 365. For more information, see [this Microsoft help page](#).

This section contains information on adding and removing tenants.

- [Tenant overview](#)
- [Adding a tenant](#)
- [Managing admin consent](#)
- [Removing a tenant](#)

Tenant overview

The Tenants page provides an overview of all your tenants. It shows the number of users, consent status, and provides access to admin consent for the different On Demand modules.

Number of users in the tenant

On the Tenants page, each tenant tile lists the number of Users in the tenant. The user count is divided into **Cloud only** and **Hybrid** users. Hybrid users are Microsoft identities that can access both on-premises and cloud-based resources.

Azure AD tenant

A tenant houses the users in a company and the information about them. You must add a tenant to manage the tenant properties using an On Demand module.

Applications used to manage Azure AD tenant properties must participate in the consent flow provided by Azure AD. This means an Azure Global Administrator must provide admin consent when adding a tenant to On Demand. Admin consent is granted on behalf of the Microsoft Azure organization.

B2C tenants

In addition to the standard Azure AD tenant, you can also add an Azure AD B2C tenant. On the Tenant page, Azure AD B2C tenants can be distinguished by the following icon next to the tenant name:



For more information on B2C tenants, see this [Microsoft help page](#).

Azure Global administrator

The Azure Global Administrator role is the top level administrator role and has access to all features. By default, the person who signs up for an Azure subscription is assigned the Global Administrator role for the tenant. Additional users can be assigned to the Global administrator role.

About adding tenants

If you are in the U.S. region, once you select **Tenants**, you must select the type of tenant you are adding, whether commercial, GCC, or GCC High. When you click **Add Commercial or GCC Tenant** (or **Add GCC High Tenant**) you are redirected to the Microsoft tenant administration login page where you must log in with the Global Administrator credentials for the tenant.

If you are in any other region, you select **Add Tenant** and are immediately redirected to the Microsoft tenant administration login page where you must log in with the Global Administrator credentials for the tenant

About GCC and GCC High tenants

GCC or a GCC High tenants are available only for deployments in the U.S. region. Currently, only the On Demand Migration module supports GCC and GCC High tenants.

GCC Office 365 tenants are typically used by US public sector organizations and the contractor organizations that service them. GCC High tenants provide Office 365 services that adhere to additional US Department of Defense security requirements. Customer eligibility to GCC High tenants is restricted.

Admin consent permission levels

Once you add a tenant, you are redirected to a page that lists the permissions that will be granted. You must click **Accept** and provide admin consent for the On Demand application. Once the Global Administrator adds a tenant to On Demand, an application record is created in the tenant indicating that admin consent has been provided.

i | **NOTE:** Global Admin credentials are only required to grant admin consent for the minimal list of permissions required by On Demand. Global Admin credentials are not stored, share, or used for any other purpose.

For security, when you first add a tenant, only the minimum permission settings are granted. Some modules require additional permissions. Once a tenant has been added to On Demand, you can grant additional permissions on the [Admin consent status](#) page.

Adding a tenant

When you add a tenant, you must have Global Administrator credentials in Microsoft Azure since part of the process of adding a tenant is done in the Microsoft Azure portal.

Prerequisites

Admin consent is required to add a tenant to On Demand. Since only an Azure Global Administrator can grant admin consent, you must be able to provide Azure Global administrator credentials for the tenant you are adding.

To add a tenant

- 1 Log in to On Demand using the credentials you used to sign up for On Demand.
- 2 In the navigation panel on the left, click **Tenants**.
- 3 Click **Add Tenant**.

If you are in any region other than the U.S region, such as Europe, United Kingdom, Canada, or Australia, you are immediately redirected to the Microsoft login page.

4 If you are in the U.S. region, you must select the type of tenant that you are adding:

- Click **Add Commercial or GCC Tenant**

- OR -

Click **Add GCC High Tenant**

i | **NOTE:** Currently, only the On Demand Migration module supports GCC and GCC High tenants.

You are redirected to the Microsoft login page.

5 Enter your Azure AD Global Administrator credentials and click **Next**.

A page opens with the list of permissions that you are granting.

6 Click **Accept**.

The On Demand Tenants page is displayed.

7 On the Tenants page, at the bottom of the tile for the newly added tenant, click **EDIT CONSENTS**.

The Admin Consent status page opens.

8 If the minimum permission settings granted when the tenant was added are sufficient for a module, the Status for the module is **Uses Base**. If the module requires additional permissions, the **Status is Not Granted**.

If you need to have additional permissions for a module, click **Grant Consent**. You are redirected to the Microsoft login page.

9 Enter the Azure AD Global Administrator credentials and click **Next**.

A page opens with the list of permissions settings you are granting.

10 Click **Accept**.

The On Demand Tenants page is displayed. GCC or GCC High tenants are identified with a GCC or GCC High tag in the right corner of the tenant tile.

Managing admin consent

- [Admin consent status](#)
- [Granting consent](#)
- [Revoking admin consent](#)

Admin consent status

To open the Admin Consent status page, click **Tenants** in the navigation page and click **EDIT CONSENTS** on the tenant tile.

On the Admin Consent status page, you can view the module admin consent status for each tenant you have added. 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. A 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.

To edit admin consent

- 1 Click **Tenants** in the navigation panel on the left.
- 2 At the bottom of a tenant tile, click **EDIT CONSENTS**.

The Admin Consent edit page for the tenant opens.

The **Status** information on the tenant tile indicates if admin consent has been granted for a module. If the current status is **Not Granted**, you can enable a module for this tenant by clicking **Grant Consent** in the **Actions** column.

i | **NOTE:** If additional admin consent permission is required to perform specific tasks within a module, these items are listed beneath the main admin consent item for the module.

Granting consent

For the following scenarios, click **Grant Consent** in the **Actions** column.

- Admin consent has been revoked in the Azure AD portal, resulting in a status of **Revoked**.
- The admin consent token for the module has expired, resulting in a status of **Token Expired**. This can occur if the Azure Global Administrator account used to grant consent has changed (deleted, role change, password change). Note that a **Token Expired** status is not serious and has a limited impact on On Demand operation.

Prerequisite for Self Service License Reporting access

For the License Management module, to use Self Server License Reporting, you must grant permissions above Base permissions.

Sometimes, when you grant consent for Self Service License Reporting, you might see an error that indicates that the app requires access to a service that your organization has not subscribed to or enabled. This error occurs if the Microsoft M365 License Manager API, required to gather self-service policy data, is not enabled in the tenant by default. You can resolve the error by enabling the M365 License Manager API in the tenant.

You must grant admin consent per On Demand tenant. For example, if you grant access for MyCompany tenant in organization A, and add the MyCompany tenant to organization B, organization B will still require the access grant.

To enable the M365 License Manager API

- 1 Install the [Azure PowerShell Az](#) module if it is not already installed.
- 2 Run the `Connect-AzAccount` cmdlet to log into your tenant using an account that has Azure AD administrative rights.
- 3 Run the following command:

```
New-AzADServicePrincipal -ApplicationId aeb86249-8ea3-49e2-900b-54cc8e308f85
```

After you complete these steps, you can complete the Grant Consent for Self Service License Reporting without errors.

Revoking admin consent

Completely revoking admin consent removes all permissions granted for the On Demand application. This action is usually performed as part of the process of removing a tenant. Revoking admin consent is a manual process that must be performed in the Microsoft Azure portal.

Revoking admin consent in the Azure Portal

Revoking admin consent removes all permissions granted for the On Demand application.

To revoke admin consent:

- 1 Log in to the Azure Resource Manager with the credentials for the tenant Active Directory.
- 2 Click on the **Azure Active Directory** icon in the left menu.
- 3 In the Active Directory panel, select **Enterprise applications**.
- 4 In the Enterprise applications panel, select **All applications**.
- 5 Select the Quest On Demand application.
The On Demand application Overview displays in the main panel.
- 6 At the top of the main panel, click **Delete**.

Removing a tenant

You can remove a tenant from On Demand. Removing a tenant disables all module functions related to the tenant. Active backups and provisioning actions are canceled.

i | **NOTE:** To restore a tenant and all the associated On Demand configuration, contact [Technical Support](#).
Tenant restore is possible for up to 30 days after it has been removed. You must provide the tenant name and your organization ID. See [Displaying the organization ID](#).

To remove a tenant:

- 1 Click **Tenants** in the navigation panel on the left.
- 2 On the tenant tile for the tenant you want to remove, click **Remove**.

Once you add a tenant to On Demand, an application record is created in your tenant indicating that you have agreed to admin consent. When you remove a tenant from On Demand, this record is not removed and admin consent access remains. You must log in to Azure and manage access to the application.

On Demand Home page

The Home page contains the following components.

Masthead	The masthead displays your current user ID and provides information about your organization.
Side navigation panel	The side navigation panel is always available as you move through the On Demand site.
Dashboard	In addition to a tile for each module, the Dashboard displays statistics and operational data for your tenant.

Masthead

The masthead displays the On Demand name on the left and on the right side shows the following:

- Your user ID with a drop down menu arrow.
- An information icon (i) that opens the On Demand information window.
- A status icon and a message that indicates the system status for the modules in your organization. You can expand the status to view the individual modules that might be affected. You can click the **Status Overview** link to view the On Demand Status page.
 - If all your modules (such as Auditing, License Management, and Recovery) are operational, the icon is green and displays **All Systems Operational**. If you click the status text, you can see the individual modules with green icons indicating systems are operational.
 - If one or more modules has a status of degraded performance or partial outage, the icon is yellow and displays **Partial System Outage**. When you click the status text, yellow icons appear beside the affected modules.
 - If one or more modules has a status of major outage the icon is red and the text link displays **Major Service Outage** in red. When you click the status text, red icons appear beside the affected modules .

You can click the **Status Overview** link to display details about outages, past incidents, and all planned maintenance in the near future in the [On Demand Status page](#).

If there is scheduled maintenance planned that will include system downtime, a blue banner is displayed at the top of the masthead that includes information about the scheduled outage. You can click **Read more** to view the maintenance details on the [On Demand Status page](#).

Masthead drop-down menu

Clicking anywhere on your user ID opens the drop-down menu to perform the following tasks:

- View your current **Region Name** and **Organization Name**.
- Perform organization management [Managing organizations and regions](#).
- Configure your user settings by clicking My Account.

- **Use of Cookies:** You can enable or disable the use of a cookie for session monitoring. The initial state of this setting is determined by your response to the cookie notice when you join an organization. Note that this setting is by region. If you join an organization in a different region, you receive the cookie notice again.
- **Sign Out** from your current session. Note that you are automatically logged out after 30 minutes of inactivity.

Information window

The On Demand information window contains the following tabs:

- **About:** Version numbers and copyright information.
- **Third Party:** The list of third party components used in the product. This information is also contained in the Release Notes.
- **Contact:** Information on how to contact [Technical Support](#).

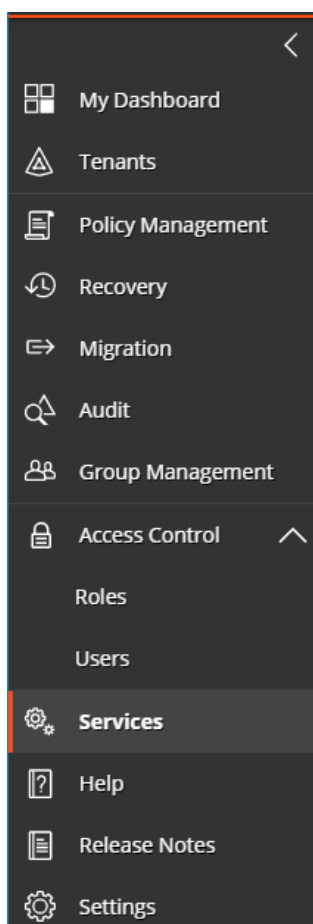
On Demand Status page

When expand the system status on the masthead and click the **Status Overview** link, you can view the On Demand Status page. The page provides detailed information about outages, past incidents, and planned maintenance. If there are partial outages or degraded performance for some modules, you can view an expanded list that indicates which geographic locations are affected.

If a blue banner displays at the top of the masthead, you can click **Read more** to see the scheduled maintenance list in the On Demand Status page. The list provides the date for each scheduled maintenance activity and indicates whether downtime is expected during the maintenance activity.

You have the option to subscribe to updates through email notifications whenever Quest On Demand creates, updates or resolves an incident.

Side navigation panel



Minimize the panel

Click on the arrow at the top to minimize the side navigation panel.

My Dashboard

Click to return to the Home page.

Tenants

Opens the Tenants page. For information, see [Managing tenants](#).

Module links

Use the module links to quickly open a module page.

Access Control

Manage users and their assigned roles. See [Adding users to an organization](#).

Services

Provides information on all available modules and provides a link to the Quest product page for the module.

Help and Release Notes

Help opens a User Guide

Release Notes opens a document with information on the currently deployed software version and technical support information.

When you are on the On Demand Home page, the Global Settings documents open. When you are on a module page, these links open the documentation for the module.

Settings

Activity trail

Agents

Notifications

Subscriptions

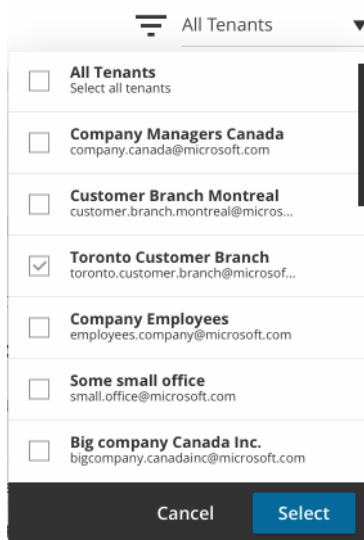
Dashboard

The dashboard contains the following components:

- [Tenant filter](#)
- [Tenant summary](#)
- [Needs your attention!](#)
- [Module tiles](#)

Tenant filter

Located in the top right of the dashboard, the tenant filter determines what data is displayed on the dashboard. You can choose to display all tenants, a subset, or a single tenant.



Tenant summary






The tenant summary indicates which tenants are currently selected and provides a summary of licenses, users and groups in the selected tenant.

Tenant	Office 365 Licences		Users		Groups	
All Tenants Selected	Assigned	Unassigned	Cloud only	Hybrid	Cloud only	Hybrid
SHOW DETAILS	1,234	150	1,200	3,100	200	300

Needs your attention!

The Needs your attention! tile displays a summary of alerts and cautions from all of the modules you are currently subscribed to. It also displays information on the status of your subscription or trial if it is close to expiry.

Needs your attention!

	Group modifications by Admin	21	VIEW
	Failed backups	5	VIEW
	Groups without owners	4,568	ASSIGN
	Something to warn you about	2	VIEW
	Something strange happened	3	VIEW

Module tiles

If you have a subscription to a module, the module tile displays status information for your tenant.

Recovery
PROTECTION STATUS

 4 of your 6 tenants are protected.

PROTECTED TENANTS	Last backup
Quest Managers	1 hour ago
Quest Employees	31 minutes ago
Some small company	2 days ago

[VIEW ALL](#)

NOTE: GCC High and GCC tenants are supported only by the On Demand Migration module. Totals shown for other On Demand modules do not include GCC High or GCC tenants.

Settings

- [Activity trail](#)
- [Agents](#)
- [Notifications](#)
- [Subscriptions](#)

Activity trail

An activity trail is a set of records that provide documentary evidence of the sequence of activities that have affected a specific operation, procedure, or event at any time. The recorded information includes date and time, actor, a description and customized fields of the event. On Demand retains the complete activity trail history for an organization.

The following activity trail logs are available:

Global Settings: Records the information for:

- adding and removing tenant events
- granting of admin consent for a tenant
- assigning and unassigning a user to be On Demand access control roles
- notification events

Recovery: Records information about backup enable and disable events.

Migration: Records information about migration process events.

Group Management: Records information about group management and user activity events.

Filtering and exporting activity trail logs

You can filter for the events that you want to see using the **FILTERS** option. You can also use the **EDIT COLUMNS** option to add and remove columns. When you are displaying the activities that you want, you can export the results to a .csv file.

NOTE: To see the detailed information for the event, click on a specific event.

To modify columns and filter activity trail logs

- 1 In the side navigation panel, click **Settings**.
- 2 In the Activity Trail tab, click **FILTERS** to expand and specify your filter criteria.
By default, the filter setting shows logs for the last 7 days (**Date | during last | 7 | days**).
- 3 To change filter criteria, you can select attributes, operators, and values from the dropdown list.
 - To add more filter criteria, click **AND**.
 - To see all available logs for current organization, click **CLEAR ALL**.

- 4 To customize the displayed columns, click **EDIT COLUMNS**, select or clear the columns, and click **SELECT**.

Once you are displaying the activity trail information that you want, you can click **EXPORT TO .CSV** to download the information in a .csv (comma separated value) format file.

Agents

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

Currently, agents are installed and configured for the Group Management module. For information on using agents, see the *On Demand Group Management User Guide*.

Notifications

An On Demand notification is an email sent to one or more recipients following an event. For example, after a backup failure event, specified recipients receive a notification email.

Configuring notification recipients

To add notification recipients for an event:

- 1 In the side navigation panel, click **Settings**.
- 2 In the main panel, click **Notifications** in the menu bar.
- 3 Under Modules, select a module type and an event type.
- 4 In the **Set the recipients** text box, enter the email address for a recipient and click **Add**.
The recipient is listed below the text box.
- 5 Repeat step 4 to add more recipients.
- 6 Click **Save**.

The next time the event occurs, all the listed recipients receive a notification email.

Subscriptions

This section contains the following topics.

Subscription details

The **Subscriptions** page contains the details of your current subscriptions.

Managing subscriptions

On Demand subscriptions are associated with an email address. To activate a subscription, you must add the email address of the subscription owner to the **Subscription Owner** list.

Subscription expiry

To prevent loss of data, subscription expiry takes place in stages.

Subscription details

Click the module name to see information about product subscription details and pricing as well as links to Quest sales support.

The On Demand subscription information is grouped by modules such as Audit, Group Management, License Management, Migration, and Recovery. Modules can offer separate licenses for specific features.

Table 1. Subscription field descriptions

Field	Value	Description
Features	Feature name	A feature is the smallest subscription unit. Features can be bundled into Standard, Professional, and Advanced offerings.
Subscription Type	Standard, Professional, or Advanced	The organization has purchased a subscription to features offered by this module. The specific subscription type depends on the number of features purchased.
	Trial	The organization has subscribed to a trial license. Module features may be limited. Note: When moving from Trial to Paid, the user associated with the paid subscription must be an organization administrator. See Subscription Owner when Moving from a Trial to a Paid subscription .
	Technical Preview	The organization has subscribed to a technical preview license. Module features may be limited.
	Not subscribed	The organization is not subscribed to this module.
Status	Current status	Shows whether the subscription is active, inactive, expired, expiring soon, and so on.
Expiry Date	mm/dd/yyyy	The date on which the subscription will expire. See Subscription expiry .
Rate Plan	Prepaid	A set number of licenses have been purchased.
	Overage	The organization is billed for licenses as they are consumed.
Licenses	####	The number of licenses purchased (∞ if the Rate Plan is Overage).
Used	####	The number of licenses currently consumed.

Managing subscriptions

On Demand subscriptions are associated with the email address that was used to purchase the subscription. All valid email address formats are supported. The email address does not need to be associated with a Quest account to activate a subscription; the email address of the subscription owner must be added to the Subscription Owners list on the **Settings | Subscriptions | Shared Subscriptions** page. A subscription owner can share subscriptions with multiple organizations.

Adding a subscription owner to the Subscription Owners list does not add the user to the organization. A subscription owner does not have sign-in capability or any other permission settings. To add a user to an organization, see [Adding users to an organization](#).

Sharing a subscription

To share a subscription with the organization, request permission from the subscription owner to add their email address to the Subscription Owners list. If the request is accepted, all subscriptions associated with the email address are assigned to the organization. A subscription owner can share subscriptions with multiple organizations.

Note that a **Subscription sharing** status of **Active** indicates that the user has consented to share subscriptions. It does not indicate that a valid subscription is associated with the email address.

- 1 In the side navigation panel, click **Settings**.
- 2 On the Settings page, click **SUBSCRIPTIONS** in the top menu.
- 3 At the top right, click **SHARED SUBSCRIPTIONS**.
- 4 On the Shared Subscriptions page, enter the email address of the subscription owner and click **Request**.
The email address is added to the Subscription Owners lists with a **Subscription sharing** status of **Pending**.
- 5 The subscription owner receives an email with a request to share the subscriptions associated with the email address.
If the subscription owner accepts the request, the **Subscription sharing** status changes to **Active** and any subscriptions associated with the email address are added to the Subscriptions page.
- 6 If **Subscription sharing** remains in the **Pending** state, you can choose to select **Cancel Request** from the Action menu.

Stop using a subscription

You can stop subscription sharing by removing the subscription owner's email address from the Subscription Owners list.

- 1 In the side navigation panel, click **Settings**.
- 2 On the Settings page, click **SUBSCRIPTIONS** in the top menu.
- 3 At the top left, click **SHARED SUBSCRIPTIONS**.
- 4 In the Subscription Owners list, locate the email address of the subscription owner that will no longer share subscriptions with the organization.
- 5 In the Action column for the subscription, select **Stop Using Subscription**.
- 6 The confirmation window lists the subscriptions that will be removed from the organization. Click **Stop Using Subscription**. The subscription owner receives an email informing them that the subscription is no longer assigned to the organization. All subscriptions associated with the email address are removed from the Subscriptions page.

Subscription Owner when Moving from a Trial to a Paid subscription

The user that signed up for a trial subscription is automatically an administrator for the organization. If a different user email address is used for purchasing a paid subscription, this user address must be added to the Subscription Owners list before the subscription status displays as **Paid**.

If you need assistance determining the email address used to purchase the subscription or, if you want to change the address associated with the subscription, contact [Technical Support](#).

Subscription expiry

To prevent loss of data, subscription expiry takes place in stages.

Stage 1: Your subscription expires in X days

Thirty days prior to expiry, the On Demand organization administrator receives an email notification. From this time on, the module tile on the On Demand home page displays the number of days before the subscription expires.

Stage 2: Subscription expired. Access denied.

Once the subscription expires, members of the organization can no longer access the On Demand module. The configuration settings have been preserved and module services continue for the next 30 days.

Stage 3: Subscription expired. Service disabled.

After 30 days, module services are no longer operational for the tenants in the organization. Data is preserved for 30 days and then, it is permanently deleted.

Stage 4: Subscription expired. Data deleted.

Your data has been deleted and cannot be restored.

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 activity trail 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 discuss the On Demand products.

Technical Support

Quest provides numerous resources to support you with our products.

Current operational status

[On Demand status](#)

On Demand relies on Microsoft Azure and Amazon Web Services (AWS) infrastructure and as such, is subject to the possible disruption of these services. You can view the following status pages:

- [Microsoft Azure status](#)
- [AWS status](#)

Contact support

The [Contact Support](#) page allows you to submit a Technical Service Request. It also provides the phone numbers to use when contacting the Quest support team.

Module product support pages

Each On Demand module has a dedicated support page with "getting started", troubleshooting, and other useful information.

- [Product Support - Audit](#)
- [Product Support - Group Management](#)
- [Product Support - Migration](#)
- [Product Support - Recovery](#)

Information and discussion: Quest community forums

Visit the [On Demand community forum](#) to read current information or to post a forum topic.

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 data centers, 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.