



Step by Step Guide for Partners who need to create an Azure Active Directory



Topics covered

- ❑ AAD Options Overview
- ❑ AAD Options – Detailed
- ❑ Steps to set up a new AAD
- ❑ Resources to support you

AAD Options - Overview

The first step is for the Partner to choose which version of AAD is suitable for their company

Pricing details for AAD

- AAD comes in four editions—Free, Office 365 apps, Premium P1, and Premium P2.
- The Free edition is included with a subscription of a commercial online service, such as Azure, Dynamics 365, Intune, and Power Platform.
- Office 365 subscriptions include the Free edition, but Office 365 E1, E3, E5, and F1 subscriptions also include the features listed under the Office 365 apps column on the next slide.
- The Premium editions are available through your Microsoft representative, the Open Volume License Program, and the Cloud Solution Provider program.
- Azure and Office 365 subscribers can also buy Azure Active Directory Premium P1 and P2 online.

AAD Options - Detailed

There are 4 different AAD options which are detailed below

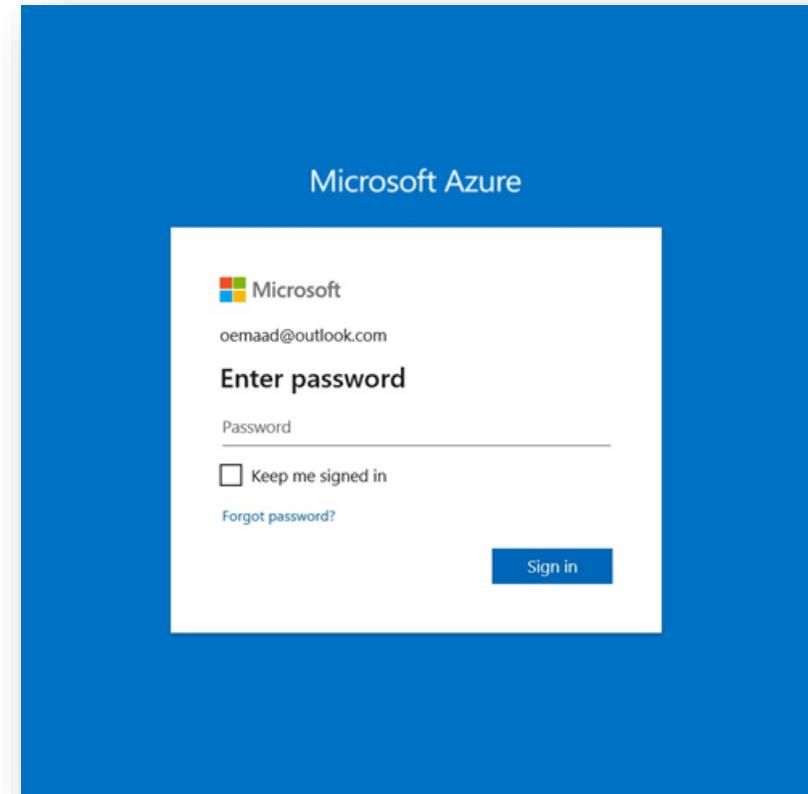
	FREE	OFFICE 365 APPS	PREMIUM P1	PREMIUM P2
Core Identity and Access Management				
Directory Objects	500,000 Object Limit	No Object Limit	No Object Limit	No Object Limit
Single Sign-On (SSO)	up to 10 apps	up to 10 apps	unlimited	unlimited
User provisioning	✓	✓	✓	✓
Federated Authentication (ADFS or 3rd party IDP)	✓	✓	✓	✓
User and group management (add/update/delete)	✓	✓	✓	✓
Device registration	✓	✓	✓	✓
Cloud Authentication (Pass-Through Auth, Password Hash sync, Seamless SSO)	✓	✓	✓	✓
Azure AD Connect sync (extend on-premises directories to Azure AD)	✓	✓	✓	✓
Self-Service Password Change for cloud users	✓	✓	✓	✓
Azure AD Join: desktop SSO & administrator bitlocker recovery	✓	✓	✓	✓
Password Protection (global banned password)	✓	✓	✓	✓
Multi-Factor Authentication	✓	✓	✓	✓
Basic security and usage reports	✓	✓	✓	✓

	FREE	OFFICE 365 APPS	PREMIUM P1	PREMIUM P2
Business to Business Collaboration				
Azure AD features for guest users	✓	✓	✓	✓
Identity & Access Management for Office 365 apps				
Company branding (customization of logon & logout pages, access panel)		✓	✓	✓
Self-service password reset for cloud users		✓	✓	✓
Service Level Agreement (SLA)		✓	✓	✓
Device write-back (device objects two-way synchronization between on-premises directories and Azure)		✓	✓	✓

Visit [this page](#) for more details on Premium AAD editions.

Create the Tenant – step 1

1. Sign into the Azure [portal](#).

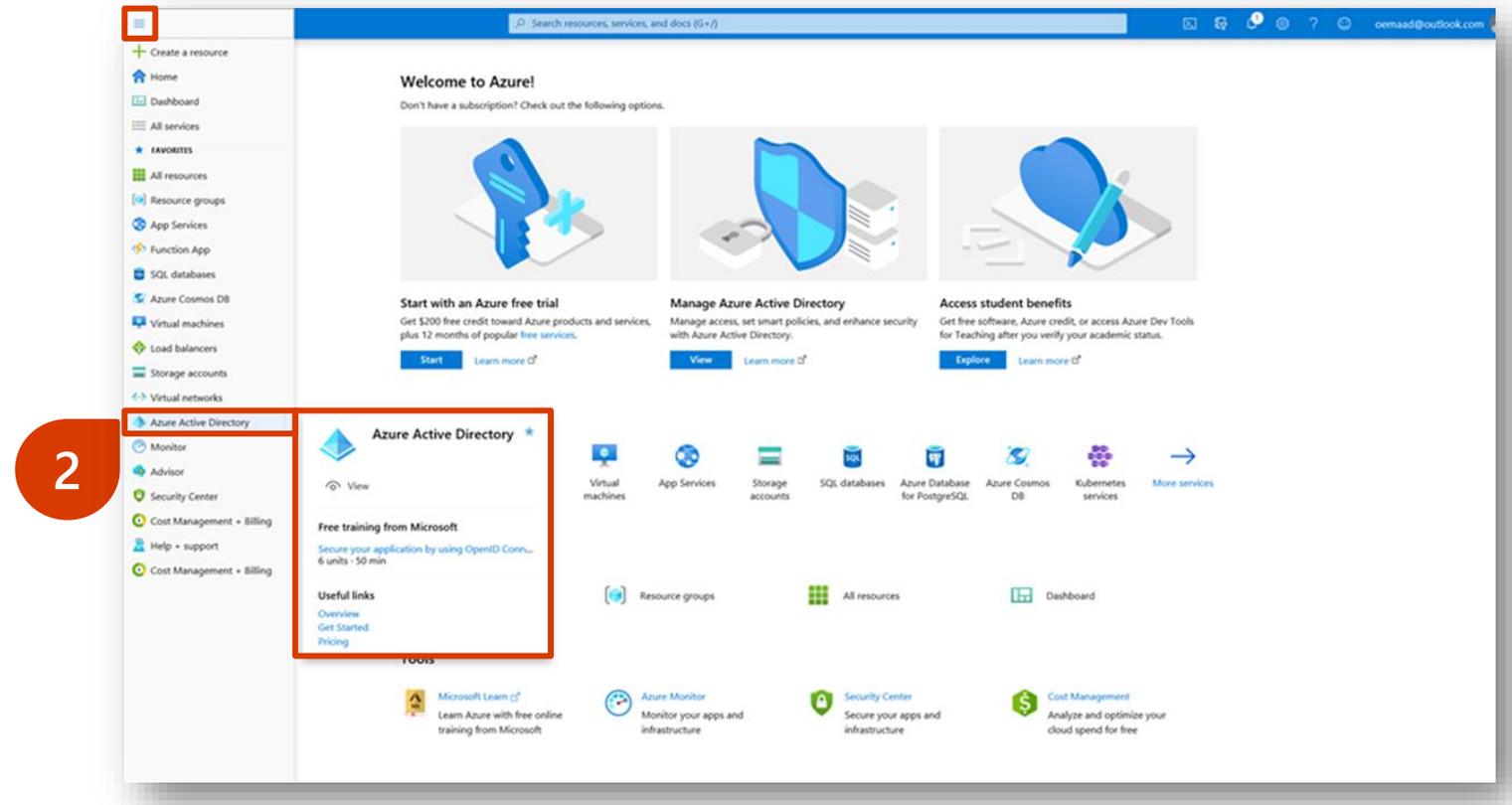


Steps to set up a new AAD

When you have decided which version of AAD is right for your company, please follow the step by step guide in the following slides to set up.

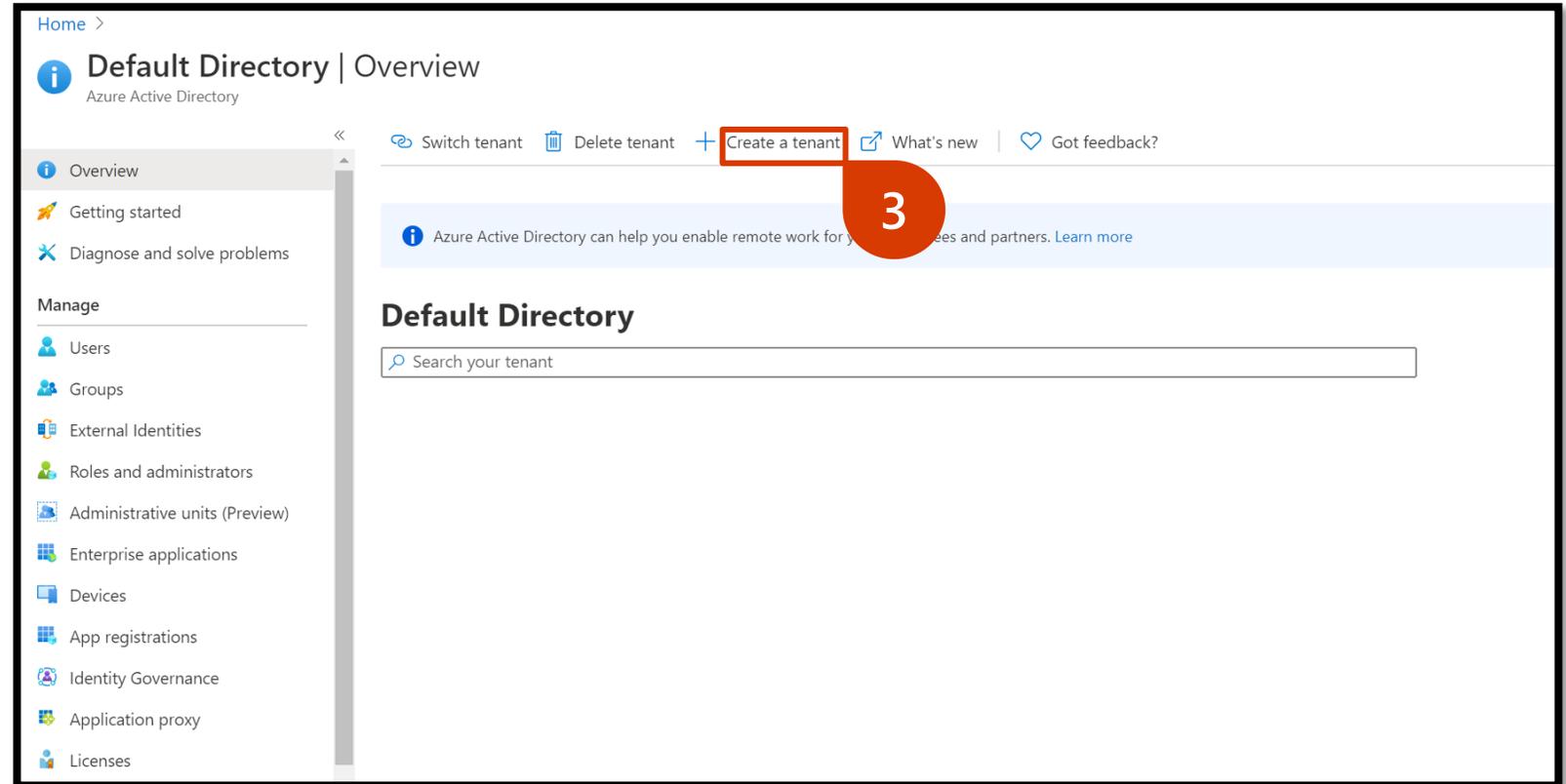
Create the Tenant – step 2

2. Select [Azure Active Directory](#) on the home page.



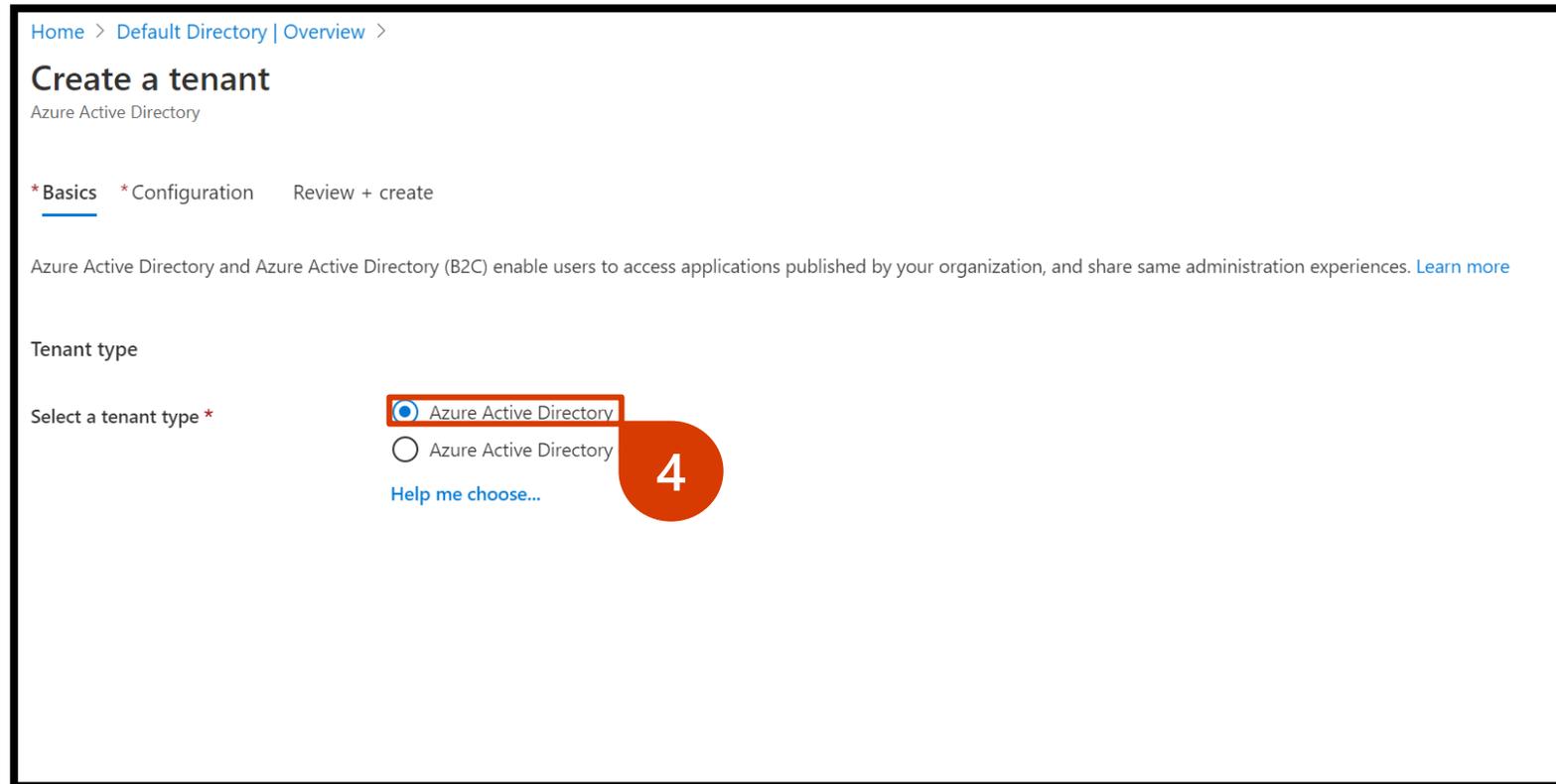
Create the Tenant– step 3

3. Select [Create a tenant](#).



Create the Tenant – step 4

4. Next to [Select a tenant type](#), select the radio button for [Azure Active Directory](#). (No subscription is required for this option.)



Home > Default Directory | Overview >

Create a tenant

Azure Active Directory

* Basics * Configuration Review + create

Azure Active Directory and Azure Active Directory (B2C) enable users to access applications published by your organization, and share same administration experiences. [Learn more](#)

Tenant type

Select a tenant type *

Azure Active Directory

Azure Active Directory

[Help me choose...](#)

4

Create the Tenant – steps 5 & 6

5. Enter your [Organization name](#), [Initial Domain name](#), and [country of incorporation](#).
6. Select [Next: Review + Create >](#). The initial domain will be set up as [domainname.onmicrosoft.com](#).

The screenshot shows the 'Create a tenant' page in the Azure Active Directory portal, specifically the 'Configuration' tab. The page is titled 'Create a tenant' and 'Azure Active Directory'. It has three tabs: 'Basics', 'Configuration', and 'Review + create'. The 'Configuration' tab is active. Under 'Directory details', there are three input fields: 'Organization name' with the value 'OEM AAD Test', 'Initial domain name' with the value 'oemaadtestone', and 'Country/Region' with the value 'United States'. The 'Initial domain name' field has a checkmark and the text 'oemaadtestone.onmicrosoft.com' next to it. Below these fields, there is a green checkmark and the text 'Datacenter location - United States' and 'Datacenter location is based on the country/region selected above.' At the bottom of the page, there are three buttons: 'Review + create' (blue), '< Previous' (grey), and 'Next: Review + create >' (grey). The 'Next: Review + create >' button is highlighted with a red box. A red circle with the number '6' is overlaid on the bottom right corner of the screenshot.

Create the Tenant – steps 7 & 8

7. A message stating **Validation passed** will be displayed. Select **Create**.
8. The tenant has now been created.

Home > Default Directory | Overview >

Create a tenant

Azure Active Directory

✓ Validation passed.

* Basics * Configuration Review + create

Summary

Basics

Tenant type Azure Active Directory

Configuration

Organization name OEM AAD Test

Initial domain name oemaadtestone.onmicrosoft.com

Country/Region United States

Datacenter location United States

Create < Previous Next >

7

Tenant is created

8. Click on the link to go to the home page where you can add users.

[Home](#) > [osdrdv](#) >

Create a tenant

Azure Active Directory

✔ Tenant creation was successful. [Click here to navigate to your new tenant:](#)

Configuration



Organization name

Initial domain name

.onmicrosoft.com

Country/Region

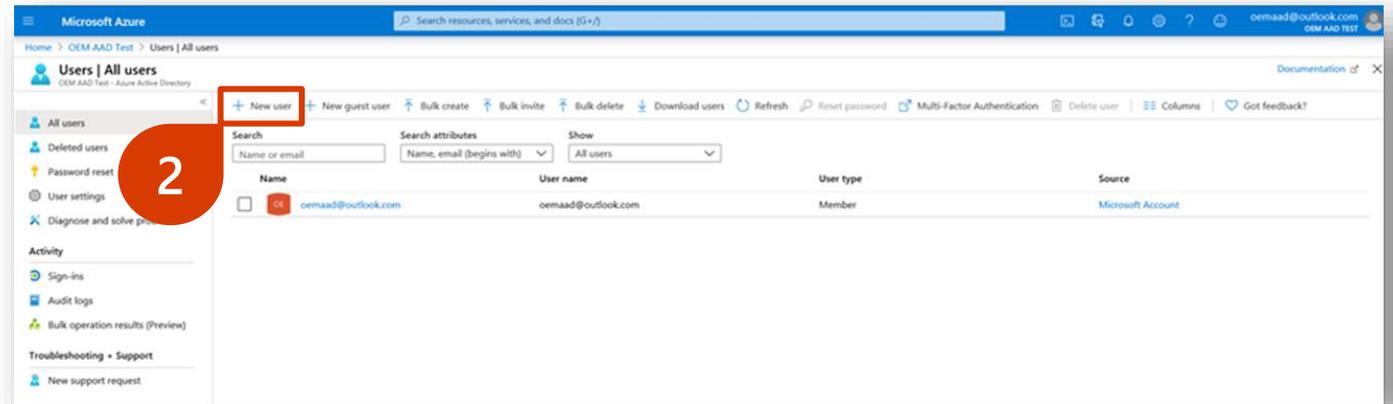
United States

Datacenter location

United States

Add Users to the Directory – steps 1 & 2

1. On the [Azure Active Directory](#) page, select [All Users](#) to view all the users in the directory.
2. Select [+ New user](#) to create a new user account.



Add Users to the Directory – steps 3 & 4

3. Select the **Create user** option.
4. Fill in the details for the new user.

The screenshot shows the Microsoft Azure portal interface for adding a new user. The page title is "New user" and the breadcrumb is "Home > OEM AAD Test > Users | All users > New user". There are two main options: "Create user" (selected and highlighted with a red box) and "Invite user". The "Create user" option is described as "Create a new user in your organization. This user will have a user name like alice@oemaadtest.onmicrosoft.com. I want to create users in bulk". The "Invite user" option is described as "Invite a new guest user to collaborate with your organization. The user will be emailed an invitation they can accept in order to begin collaborating. I want to invite guest users in bulk". Below the options is a "Help me decide" link. The "Identity" section contains fields for "User name" (with an example "chris@oemaadtest.onmicrosoft.com" and a domain dropdown), "Name" (with an example "Chris Green"), "First name", and "Last name". The "Groups and roles" section shows "0 groups selected" and "User" role. The "Settings" section has a "Block sign in" toggle set to "No" and a "Usage location" dropdown. A "Create" button is at the bottom.

Add Users to the Directory – step 5

5. Select **Create**.

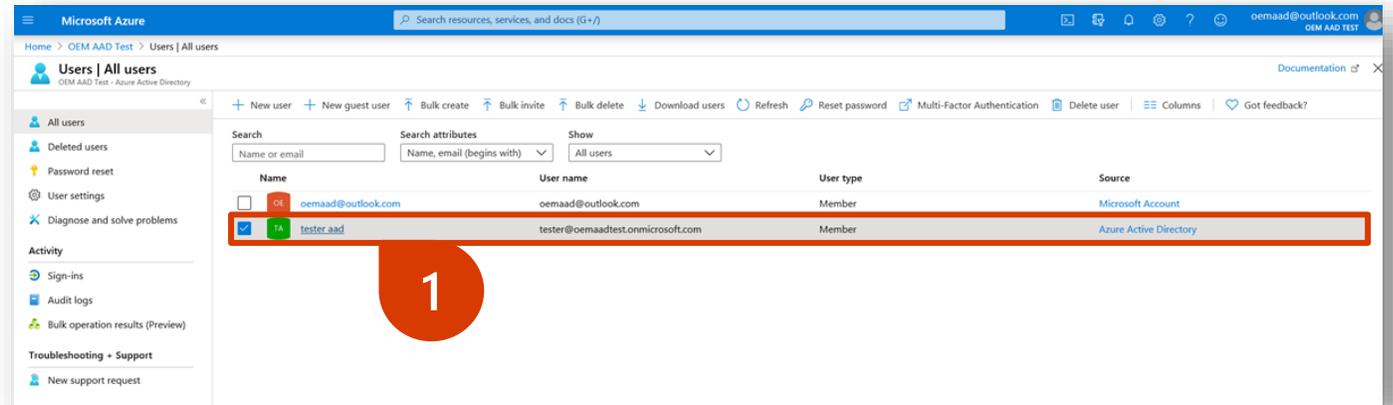
Note: For Free version of AAD, the user account will be set up as username@domain.onmicrosoft.com

Now, the user can add this login to DOC user profile.

The screenshot shows the Microsoft Azure portal interface for creating a new user. The page title is "New user" and the breadcrumb is "Home > OEM AAD Test > Users | All users > New user". There are two main options: "Create user" (selected) and "Invite user". The "Create user" option is described as "Create a new user in your organization. This user will have a user name like alice@oemadtest.onmicrosoft.com. I want to create users in bulk." The "Invite user" option is described as "Invite a new guest user to collaborate with your organization. The user will be emailed an invitation they can accept in order to begin collaborating. I want to invite guest users in bulk." Below these options is a "Help me decide" link. The "Identity" section contains the following fields: "User name" (tester) with a dropdown for the domain (oemadtest.onmicrosoft.com), "Name" (tester aad), "First name" (empty), and "Last name" (empty). The "Password" section has two radio buttons: "Auto-generate password" (selected) and "Let me create the password" (unselected). Below this is an "Initial password" field with a masked password (*****). The "Groups and roles" section shows "0 groups selected". At the bottom left, there is a blue "Create" button highlighted with a red box. A red circle with the number "5" is overlaid on the bottom center of the page.

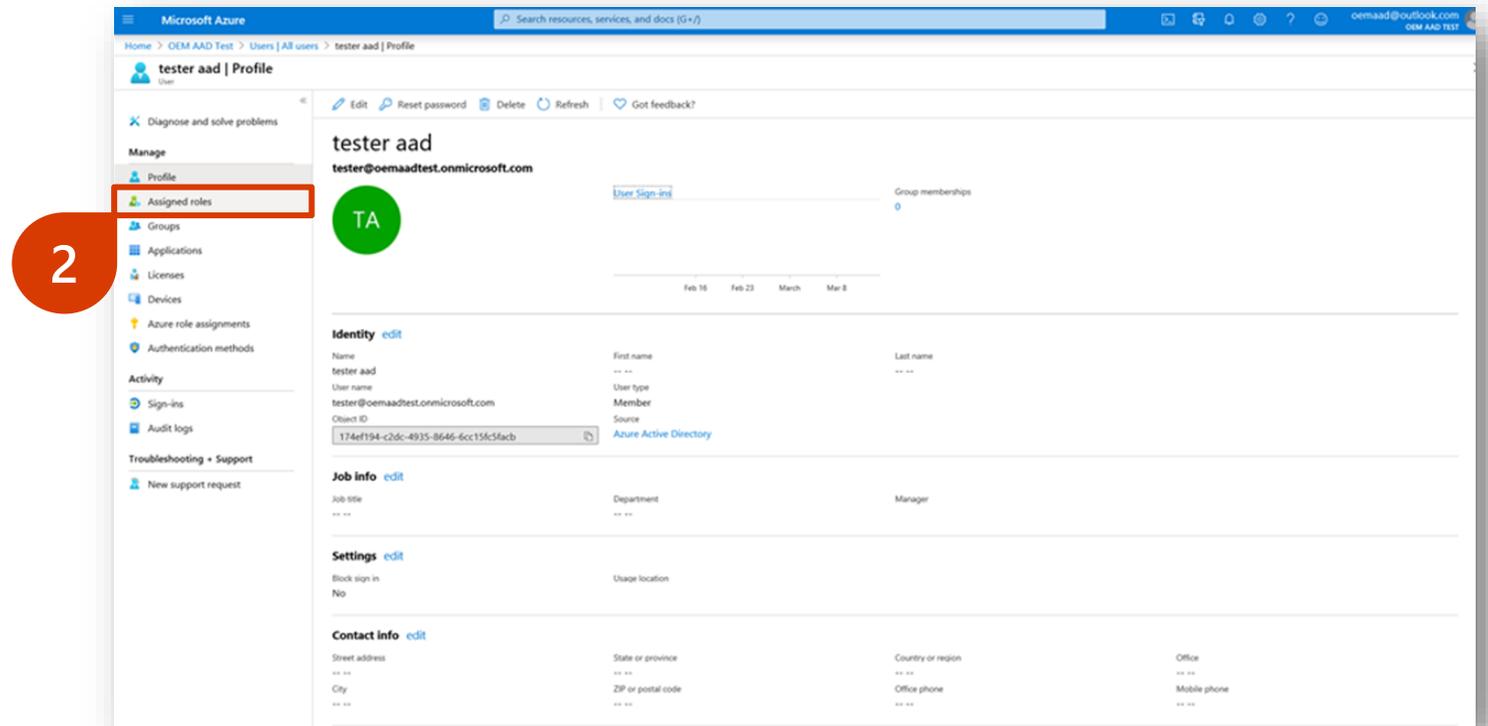
Set up the Azure Global Admin – step 1

1. On the [All users](#) page, select the user you'd like to assign as the global admin.



Set up the Azure Global Admin – step 2

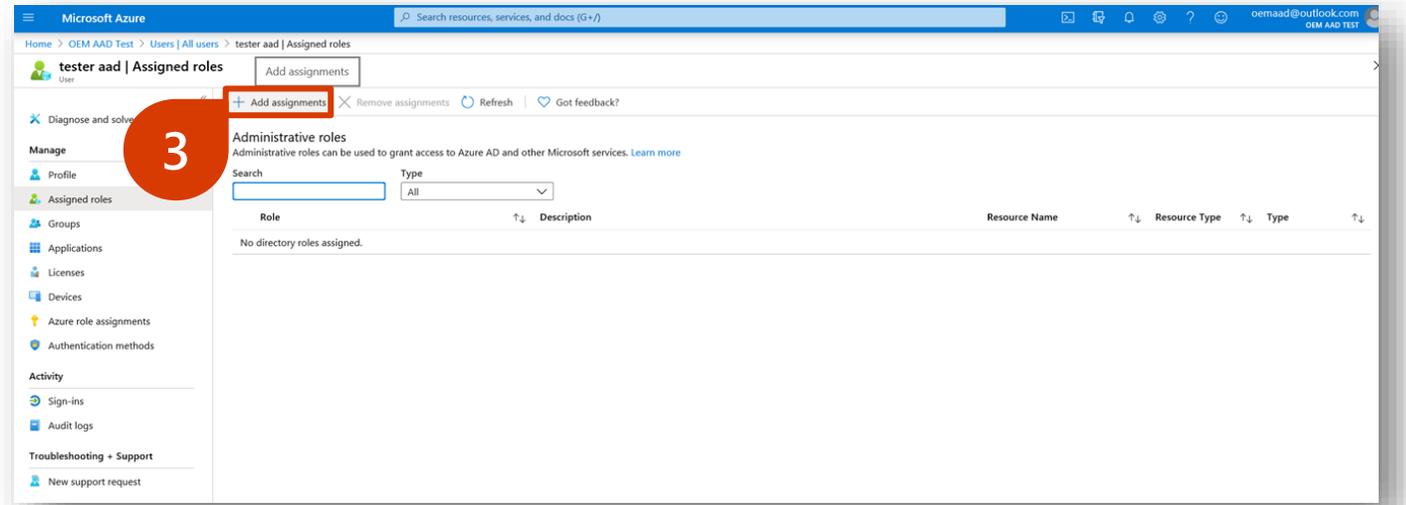
2. Select **Assigned roles** on the left panel.



The screenshot displays the Microsoft Azure portal interface for the user 'tester aad'. The left-hand navigation pane is visible, with the 'Assigned roles' option highlighted by a red rectangular box. A red circle containing the number '2' is positioned to the left of the navigation pane. The main content area shows the user's profile details, including their name 'tester aad', email 'tester@oemaadtest.onmicrosoft.com', and a green circular profile picture with the initials 'TA'. Below the profile picture, there are sections for 'Identity', 'Job info', 'Settings', and 'Contact info', each with an 'edit' link. The 'Identity' section shows the user's name, user name, user type (Member), and source (Azure Active Directory). The 'Job info' section shows the job title and department. The 'Settings' section shows the block sign-in status (No) and usage location. The 'Contact info' section shows fields for street address, city, state or province, ZIP or postal code, country or region, office, and mobile phone.

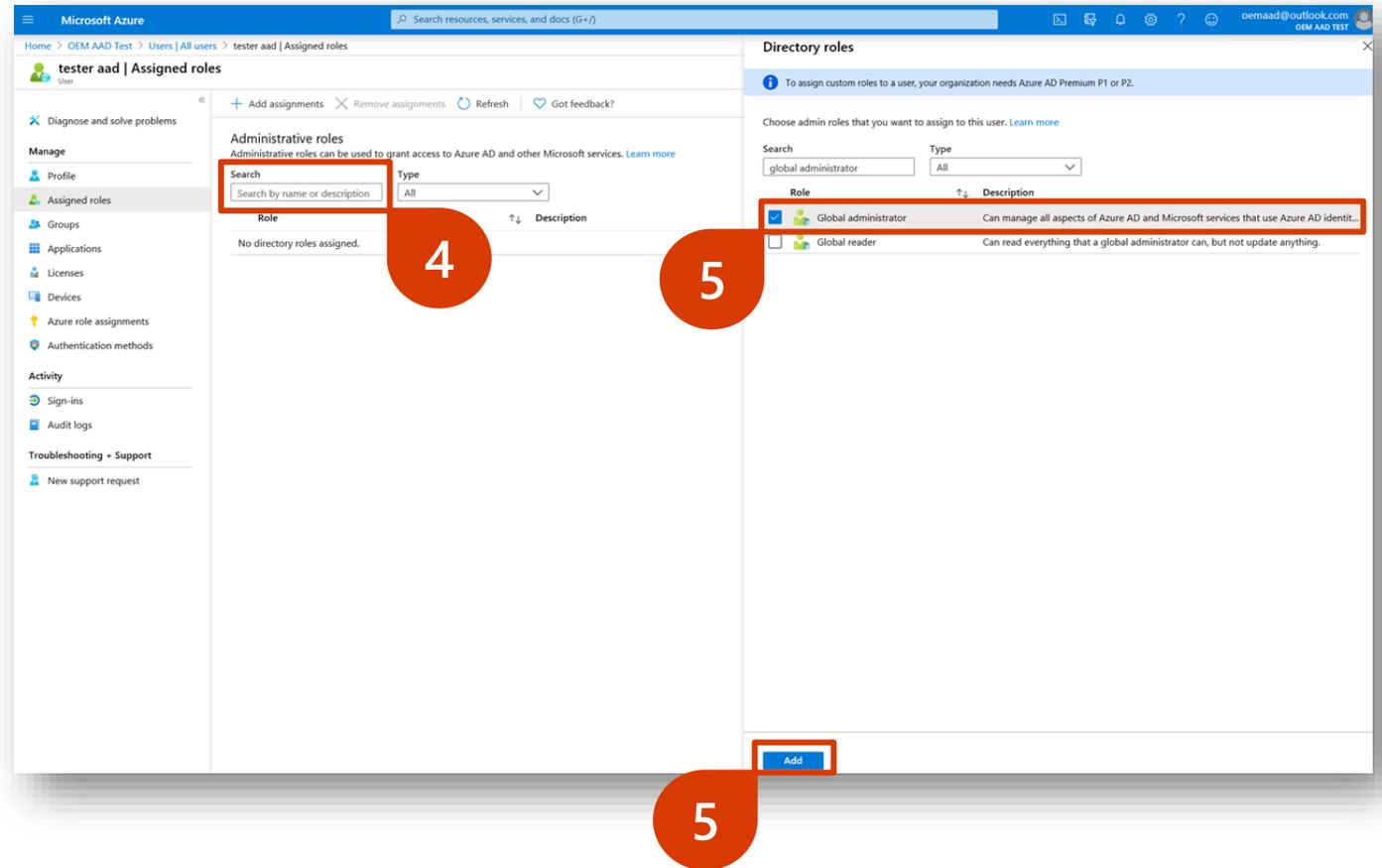
Set up the Azure Global Admin – step 3

3. Select + Add assignments.



Set up the Azure Global Admin – steps 4 - 6

4. Enter "Global administrator" in the [Search](#) box.
5. Select this role in the search results, then select [Add](#).
6. The global admin role will now be assigned to the user.



Adding your AAD Login to OEM Storefront

- You will now need to add your AAD email address to the DOC / MDOS Login page
- Please refer to the relevant step by step Guide available on DPC at the link below
- <https://devicepartner.microsoft.com/assets/collection/azure-active-directory-onboarding-oem-applications-user-management>

DOC and MDOS Support

For questions about DOC or MDOS please contact

msoemops@microsoft.com

AAD Support

For Questions about your AAD Tenant, support options are below

Raise a ticket on the Azure Portal

https://portal.azure.com/#blade/Microsoft_Azure_Support/HelpAndSupportBlade/newsupportrequest

Telephone Support

<https://support.microsoft.com/en-us/help/4051701/global-customer-service-phone-numbers?ocid=IA-4027136-AdminCU>

Live chat:

<https://support.microsoft.com/en-us/contactus/?ocid=IA-4027136-CU>

The M365 Data Protection team can help admins who need support with password reset.

Partners can [Self Serve](#) or can at Call (800) 865-9408 (toll-free, US only). If you are outside the United States, see the [Global Support Phone Numbers](#).

