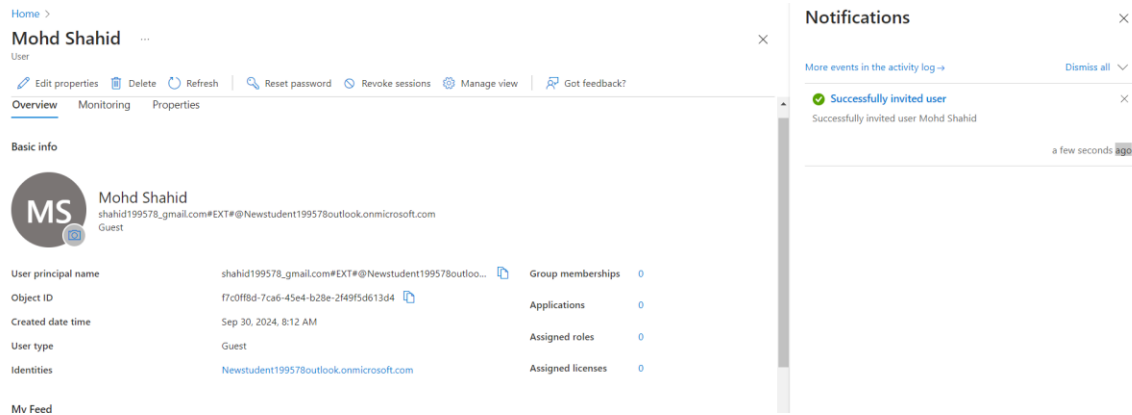


Task 1: Add External Partners as Users in Azure Active Directory and Grant Read-Only Access to Azure Blob

1. Log in to the [Azure Portal](#).
2. In the left-hand menu, select **Azure Active Directory**.
3. Click on **Users** and then **+ New guest user**.
4. Enter the email address of the external partner and add a personal message if needed. Click **Invite**.



5. After the user accepts the invitation, go to the **Subscriptions** or **Resource Groups** where the Azure Blob Storage resides.
6. Click on **Access control (IAM)**.
7. Click on **+ Add**, then select **Add role assignment**.
8. In the **Role** dropdown, select **Storage Blob Data Reader** (this role provides read-only access to Blob storage).

[Home](#) > [Subscriptions](#) > [Free Trial | Access control \(IAM\)](#) >

Create a custom role

[Basics](#) [Permissions](#) [Assignable scopes](#) [JSON](#) [Review + create](#)

To create a custom role for Azure resources, fill out some basic information. [Learn more](#)

Custom role name *



Description







Baseline permissions ☐ Clone a role ☒ Start from scratch ☐ Start from JSON

Create a custom role ...

Basics **Permissions** Assignable scopes JSON Review + create

+ Add permissions + Exclude permissions

Click Add permissions to select the permissions you want to add to this custom role.
To add a wildcard (*) permission, you must manually add the permission on the JSON tab. [Learn more](#) 
To exclude specific permissions from a wildcard permission, click Exclude permissions. [Learn more](#) 

Permission	↑↓	Description	↑↓	Permission type	↑↓
Microsoft.Storage/storageAccounts/blobServices/containers/read		Returns list of containers		Action	
Microsoft.Storage/storageAccounts/blobServices/generateUserDelegationKey/action		Returns a user delegation key for the ...		Action	
Microsoft.Storage/storageAccounts/blobServices/containers/blobs/read		Returns a blob or a list of blobs		DataAction	
Microsoft.Storage/storageAccounts/blobServices/containers/blobs/delete		Returns the result of deleting a blob		NotDataAction	
Microsoft.Storage/storageAccounts/blobServices/containers/blobs/write		Returns the result of writing a blob		NotDataAction	
Microsoft.Storage/storageAccounts/blobServices/containers/blobs/tags/read		Returns the result of reading blob tags		NotDataAction	

9. In the **Assign access to** dropdown, select **User, group, or service principal**.

Add role assignment ...

Role **Members** Conditions Assignment type (Preview) Review + assign

Selected role blob view

Assign access to
☒ User, group, or service principal
☐ Managed identity

Members + Select members

Name	Object ID	Type
No members selected		

Description Optional

MS Mohd Shahid(Guest) technantramantra9911@gmail.com


NS New Student admin@Newstudent199578outlook.onmicrosoft.com

TE test@Newstudent199578outlook.onmicrosoft.com

VM VM@Newstudent199578outlook.onmicrosoft.com

VO VM Operators Group VM Operators Group they can read, start and stop

Selected members:

MS Mohd Shahid(Guest) technantramantra9911@gmail.com 

10. Search for and select the external partner's user account, then click **Save**.

Task 2: Create Users for Internal Employees in Custom Azure Active Directory Domain

1. **Log in to the Azure Portal.**
2. **Navigate to Azure Active Directory.**
3. **Click on Users and then + New user.**
4. **Fill in the details for the internal employee:**
 - **User name:** Choose a username in the format of your custom domain (VM).
 - **Name:** Enter the full name of the employee.
 - **Password:** Generate or set a password for the user.

5. Click **Create** to create the user.

The image shows two screenshots from the Azure portal. The top screenshot displays the 'Users' page under 'Default Directory | Users'. It includes a search bar, a list of users, and a sidebar with navigation options like 'All users', 'Audit logs', 'Sign-in logs', 'Diagnose and solve problems', 'Manage', 'Deleted users', 'Password reset', 'User settings', 'Bulk operation results', 'Troubleshooting', and 'Support'. The user list shows four users: 'Mohd Shahid' (Guest), 'New Student' (Member), 'test' (Member), and 'VM' (Member). The bottom screenshot shows the 'VM | Azure role assignments' page. It includes a search bar, a 'Subscription' dropdown set to 'Free Trial', and a table of role assignments. The table has columns for 'Role', 'Resource Name', 'Resource Type', 'Assigned To', and 'Condition'. One role assignment is shown: 'view access' for the 'Free Trial' resource, assigned to the 'VM Operators Group' with no conditions.

Display name	User principal name	User type	On-premises sy...	Identities	Company name	Creation type
Mohd Shahid	shahid199578@gmail.com...	Guest	No	MicrosoftAccount		Invitation
New Student	admin@Newstudent1995...	Member	No	MicrosoftAccount		
test	test@Newstudent199578...	Member	No	Newstudent199578outlook.onmic		
VM	VM@Newstudent199578...	Member	No	Newstudent199578outlook.onmic		

Role	Resource Name	Resource Type	Assigned To	Condition
view access	Free Trial	Subscription	VM Operators Group	None

Task 3: Set Up Password Reset for Users Without Help Desk Support

1. **Log in to the Azure Portal.**
2. Navigate to **Microsoft Entra ID**.
3. Select **Users** and then click on **User settings**.
4. Under **Password reset**, enable the option for **All users** or specific groups as required.
5. Choose the **Authentication methods** you want to allow for password resets, such as **Email** or **Mobile app verification**.
6. Set up the **Registration** for users to ensure they provide the necessary information for password resets.
7. Click **Save** to apply the settings.

Home > Default Directory | Users > Users > VM

VM | Authentication methods

User

Search

Save Discard Reset password Require re-register multifactor authentication Revoke multifactor authentication sessions Got feedback?

Switch to the new user authentication methods experience! Click here to use it now. →

Authentication methods are the ways your users sign into Microsoft Entra ID. Here, you can set the phone numbers and email addresses that users use to perform multifactor authentication and self-service password reset, and reset a user's password.

Authentication contact info

Phone

Alternate phone

Email newstudent199578@outlook.com ✓

Alternate email is now managed on the Profile page

Overview Audit logs Sign-in logs Diagnose and solve problems Manage Custom security attributes Assigned roles Administrative units Groups Applications Licenses Devices Azure role assignments Authentication methods

Home > Default Directory | Users > Users | Password reset > Password reset

Password reset | Properties

Default Directory

Save Discard

Diagnose and solve problems

Manage

Properties

- Authentication methods
- Registration
- Notifications
- Customization
- On-premises integration
- Administrator Policy

> Activity

> Troubleshooting + Support

Self service password reset enabled ⓘ

None Selected All

Select group ⓘ

VM Operators Group

These settings only apply to end users in your organization. Admins are always enabled for self-service password reset and are required to use two authentication methods to reset their password. Click here to learn more about administrator password policies.

Microsoft Azure



← vm@newstudent199578outlook.onmicrosoft.co...

Enter password

Password

[Forgot my password](#)

Sign in



Get back into your account

verification step 1 > choose a new password

Please choose the contact method we should use for verification:

☒ Email my alternate email

You will receive an email containing a verification code at your alternate email address (ne*****@outlook.com).

Email

[Cancel](#)



Get back into your account

verification step 1 ✓ > **choose a new password**

* Enter new password:

.....

strong

* Confirm new password:

.....

Finish

[Cancel](#)

Your Default Directory password has been reset

lo: VM@Newstudent199578outlook.onmicrosoft.com

Mon 9/30/2024 9:29 AM

Cc: newstudent199578@outlook.com

Password reset notification

The password on your account has recently been reset. If you performed this password reset, then this message is for your information only.

- **User ID: VM@Newstudent199578outlook.onmicrosoft.com**

If you are not sure you or your administrator performed this password reset, then you should contact your administrator immediately.

Remember: Make sure you update all of your devices (phones, tablets, and PCs) with your new password!

Sincerely,

Task 4: Set Up MFA for External Partners

1. **Log in to the Azure Portal.**
2. Navigate to **Azure Active Directory**.
3. Click on **Users**, then select **Multi-Factor Authentication**.
4. On the MFA settings page, find the external partner's user account.
5. Enable Multi-Factor Authentication for that user. You can set up various verification methods such as:
 - **SMS**
6. Inform the external partner to complete the MFA setup by following the instructions they receive.

Conditional Access | Policies

Microsoft Entra ID

Overview

Policies

Insights and reporting

Diagnose and solve problems

Manage

Named locations

Custom controls (Preview)

Terms of use

VPN connectivity

Authentication contexts

Authentication strengths

Cherlin nashirae

+ New policy

+ New policy from template

Upload policy file

What if

Refresh

Preview features

Got feedback?

Microsoft Entra Conditional Access policies are used to apply access controls to keep your organization secure. [Learn more](#)

All policies

1

Total

Microsoft-managed policies

0

out of 1

Search

Add filter

1 out of 1 policy found

Policy name	State	Creation date	Modified date
Require multifactor authentication for guest access	Report-only	9/30/2024, 9:41:10 AM	

Home > Default Directory | Users > Users > Mohd Shahid

Mohd Shahid

Authentication methods

Search

Save

Discard

Reset password

Require re-register multifactor authentication

Revoke multifactor authentication sessions

Got feedback?

Switch to the new user authentication methods experience! Click here to use it now. →

Authentication methods are the ways your users sign into Microsoft Entra ID. Here, you can set the phone numbers and email addresses that users use to perform multifactor authentication and self-service password reset, and reset a user's password.

Authentication contact info

✓ = SMS sign-in ready

Phone ✓

+91 9717710218

Alternate phone

Email

Alternate email is now managed on the [Profile](#) page

Mohd Shahid

Authentication methods

Search

+ Add authentication method

Reset password

Require re-register multifactor authentication

Revoke multifactor authentication sessions

View authentication methods policy

Want to switch back to the old user authentication methods experience? Click here to go back. →

Authentication methods are the ways users sign into Microsoft Entra ID and perform self-service password reset (SSPR). The user's "default sign-in method" is the first one shown to the user when they are required to authenticate with a second factor - the user always can choose another registered, enabled authentication method to authenticate with. [Learn more](#)

Default sign-in method (Preview)

SMS (primary mobile)

Usable authentication methods

Authentication method	Detail
Phone number	Primary mobile: +91 9717710218 (Ready for SMS sign-in) ...

Non-usable authentication methods

Authentication method	Detail
No non-usable methods.	

System preferred multifactor authentication method

Feature status	System preferred MFA method
Enabled	Sms