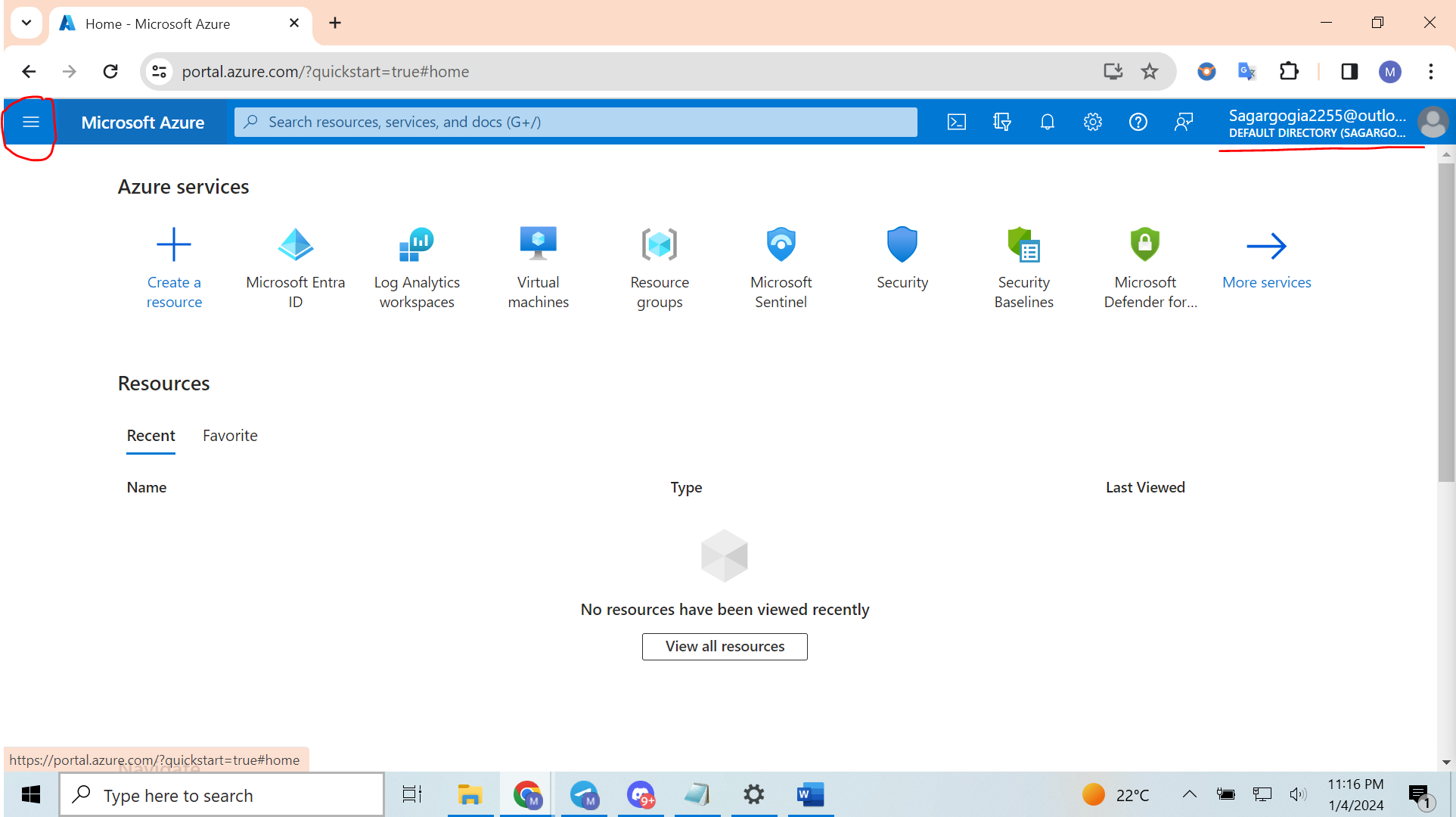
Azure Active Directory (Azure AD) is Microsoft's cloud-based identity and access management service, providing authentication and authorization services for applications and resources in the Azure cloud and other integrated services. For example, organizations use Azure AD to enable secure single sign-on for users across various Microsoft 365 applications like Outlook, Teams, and SharePoint. In this lab we will create/delete/manage users and implement password less authentication.   
  
Creating and managing users with Azure Active Directory

Sign in with your credentials on portal.azure.com and upon successful login you will be able to see your username on the top right. Click on hamburger menu on top left as shown in the screenshot below.

  
  
Navigate to **Microsoft Entra ID** > **Users**

A screenshot of a computer

Description automatically generated

Enter the required user details such as Name, password, domain and so on.

“On the New User page, provide the new user's information:

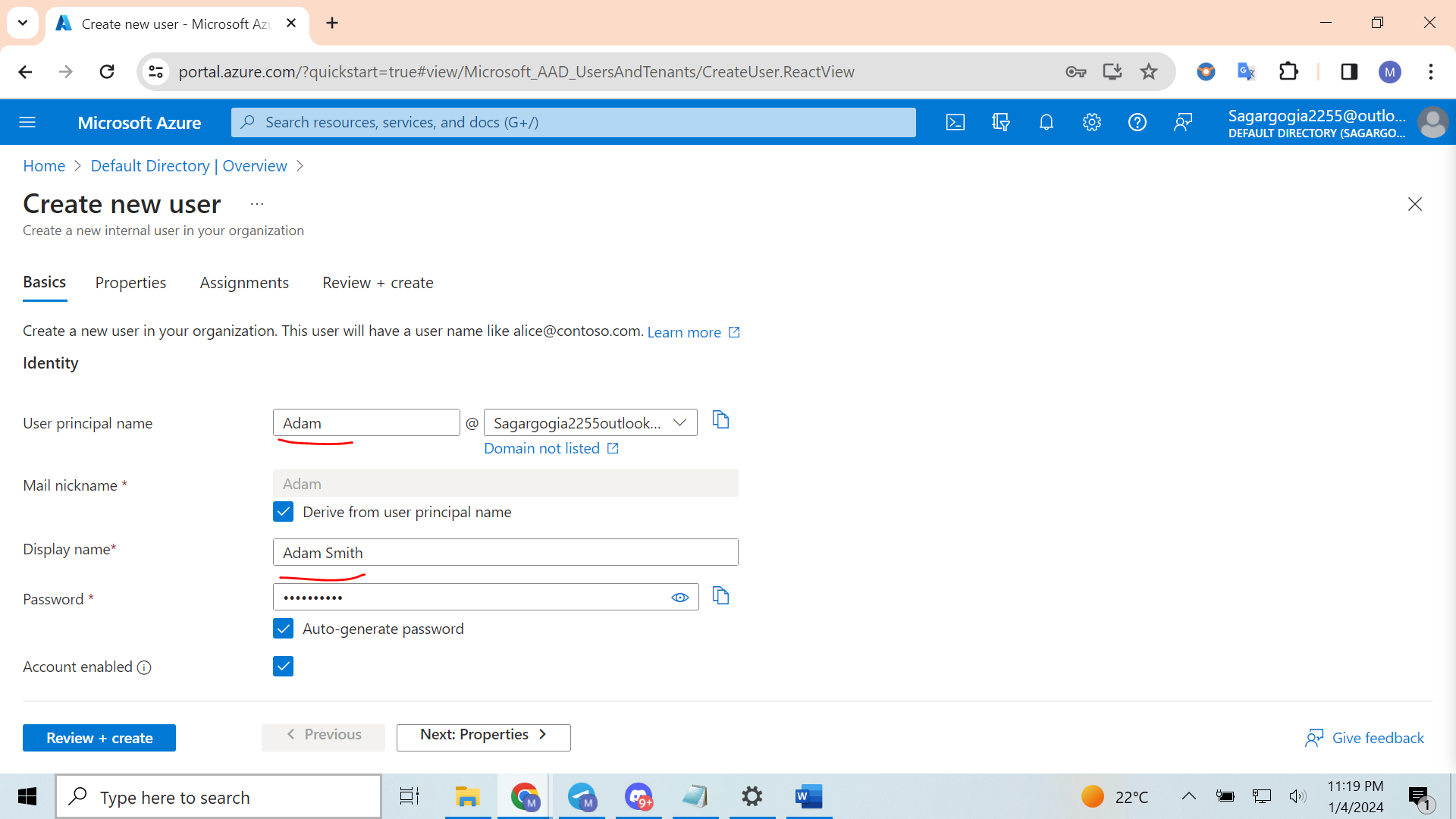
**Identity**: Add a user name and display name for the user. User name and Name are required and can't contain accent characters. You can also add a first and last name.

The domain part of the user name must use either the initial default domain name, <yourdomainname>.onmicrosoft.com, or a custom domain name, such as contoso.com.

**Groups and roles**: Optional. Add the user to one or more existing groups. Group membership can be set at any time.

**Settings**: Optional. Toggle the option to block sign-in for the user or set the user's default location.

**Job info**: Optional. Add the user's job title, department, company name, and manager. These details can be updated at any time” (Source- Microsoft.com)

  
  
  
Upon successful creation of user, you will be able to see a popup saying “successfully created user”

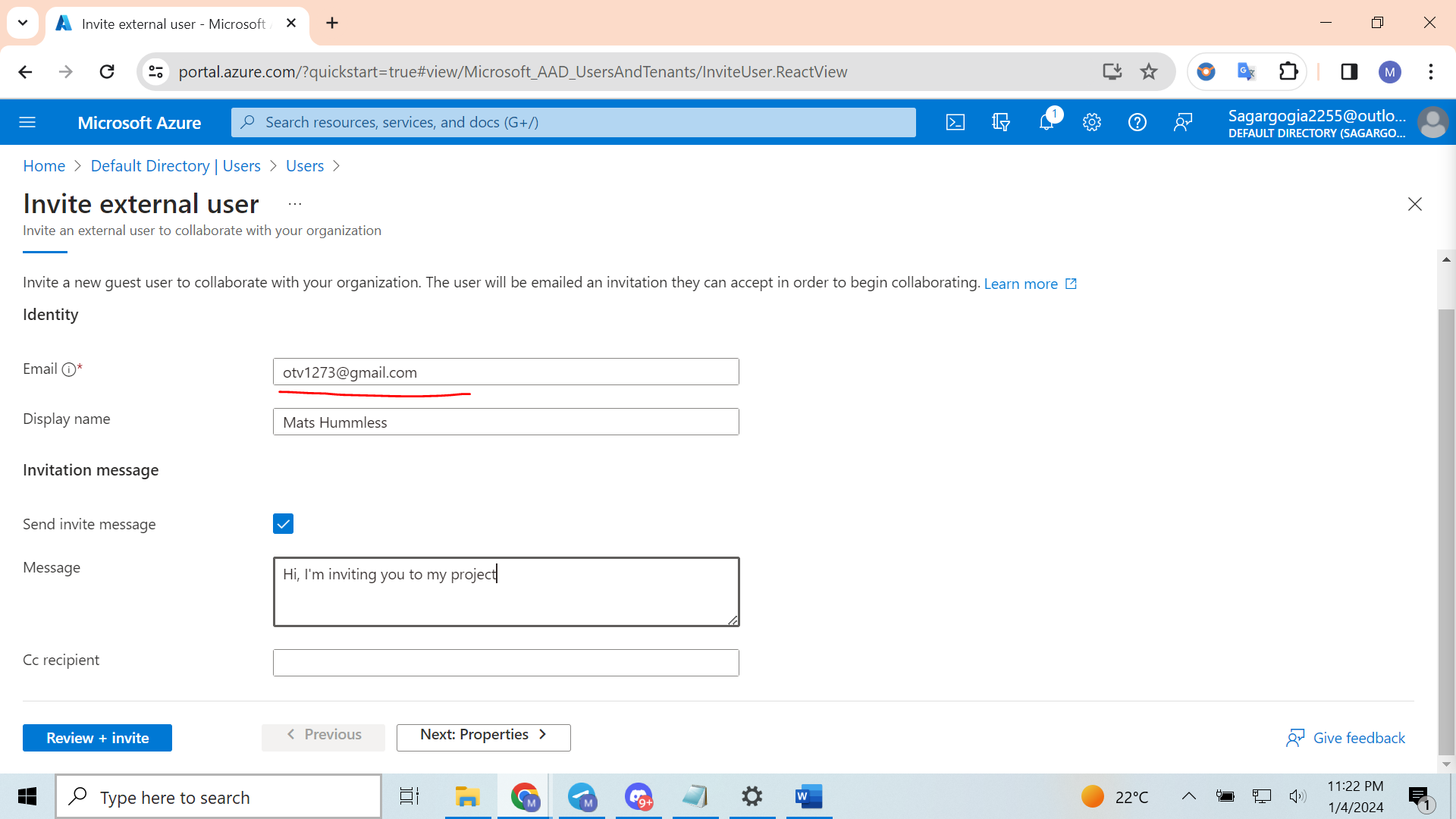
A screenshot of a computer

Description automatically generated

You also have the option to welcome the recent guest user into your organization by choosing the "Invite user" option on the New user page. In case your organization's external collaboration settings permit guest access, the user will receive an invitation via email, which they need to accept to initiate the collaboration process.

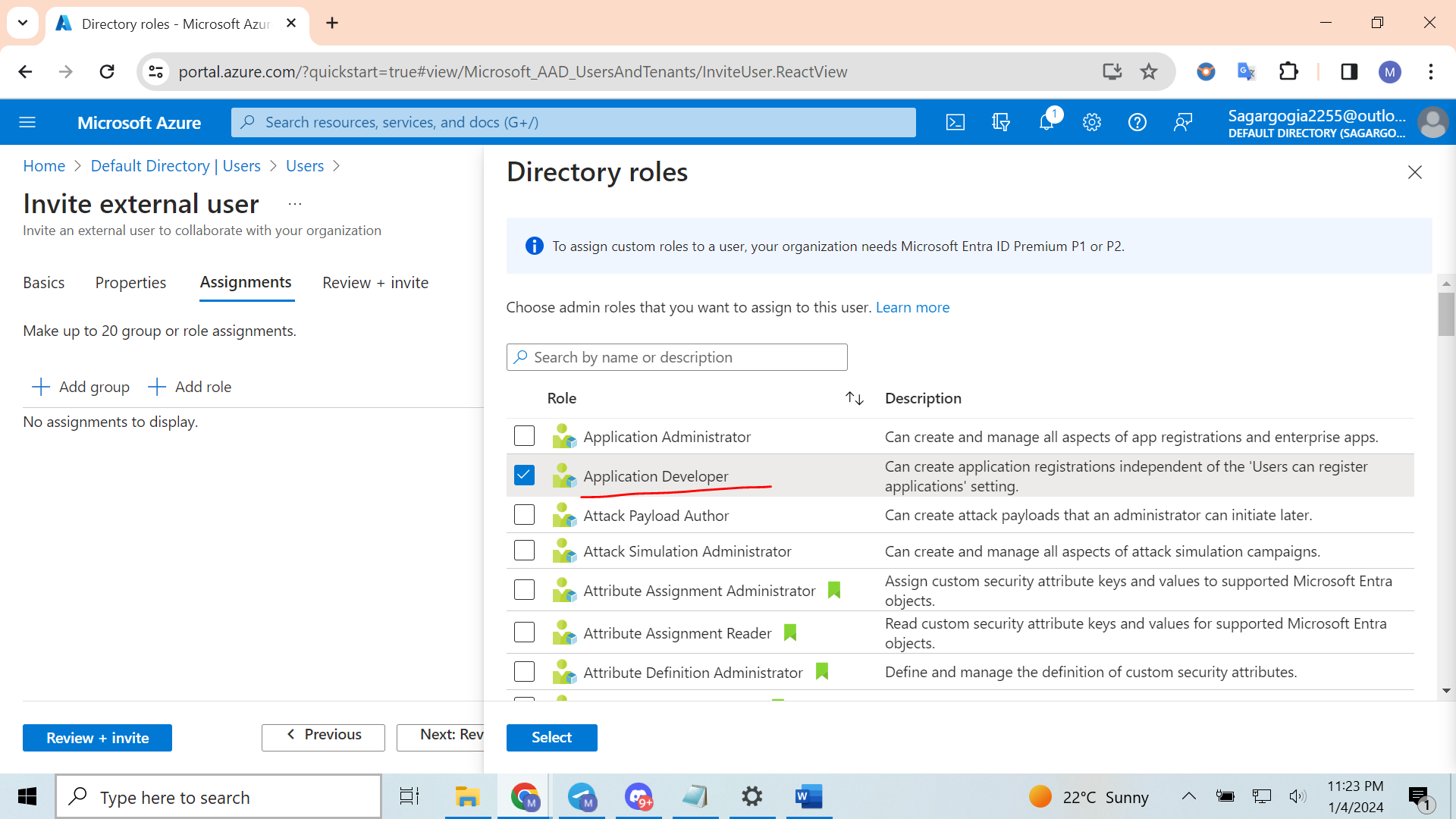
A computer screen with a message box

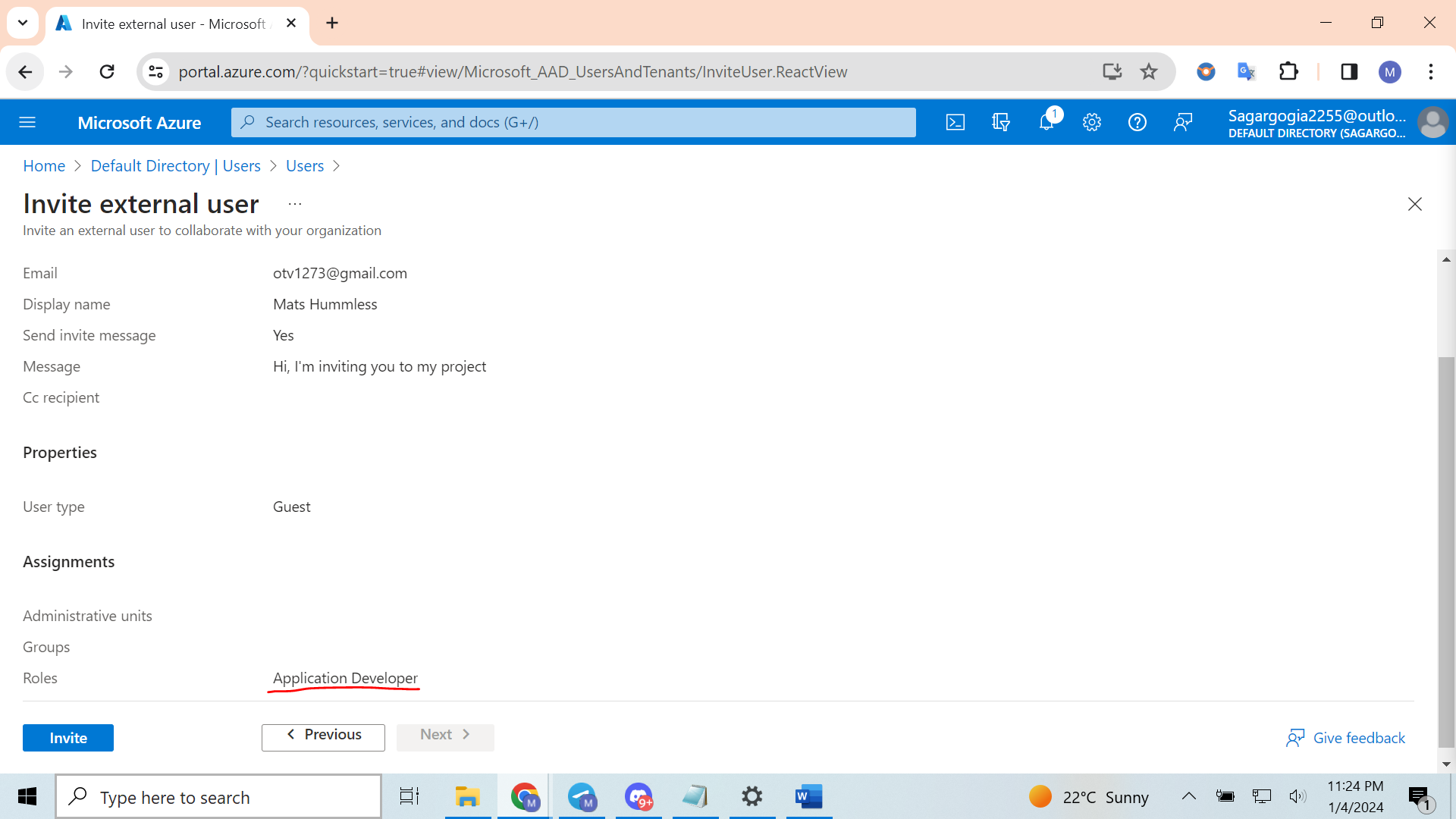
Description automatically generated  
  
Enter the email address of the person whom you want to send an invite.

  
  
  
Keep the user type as “Guest” and assign a role (from a list of roles available)s to the user

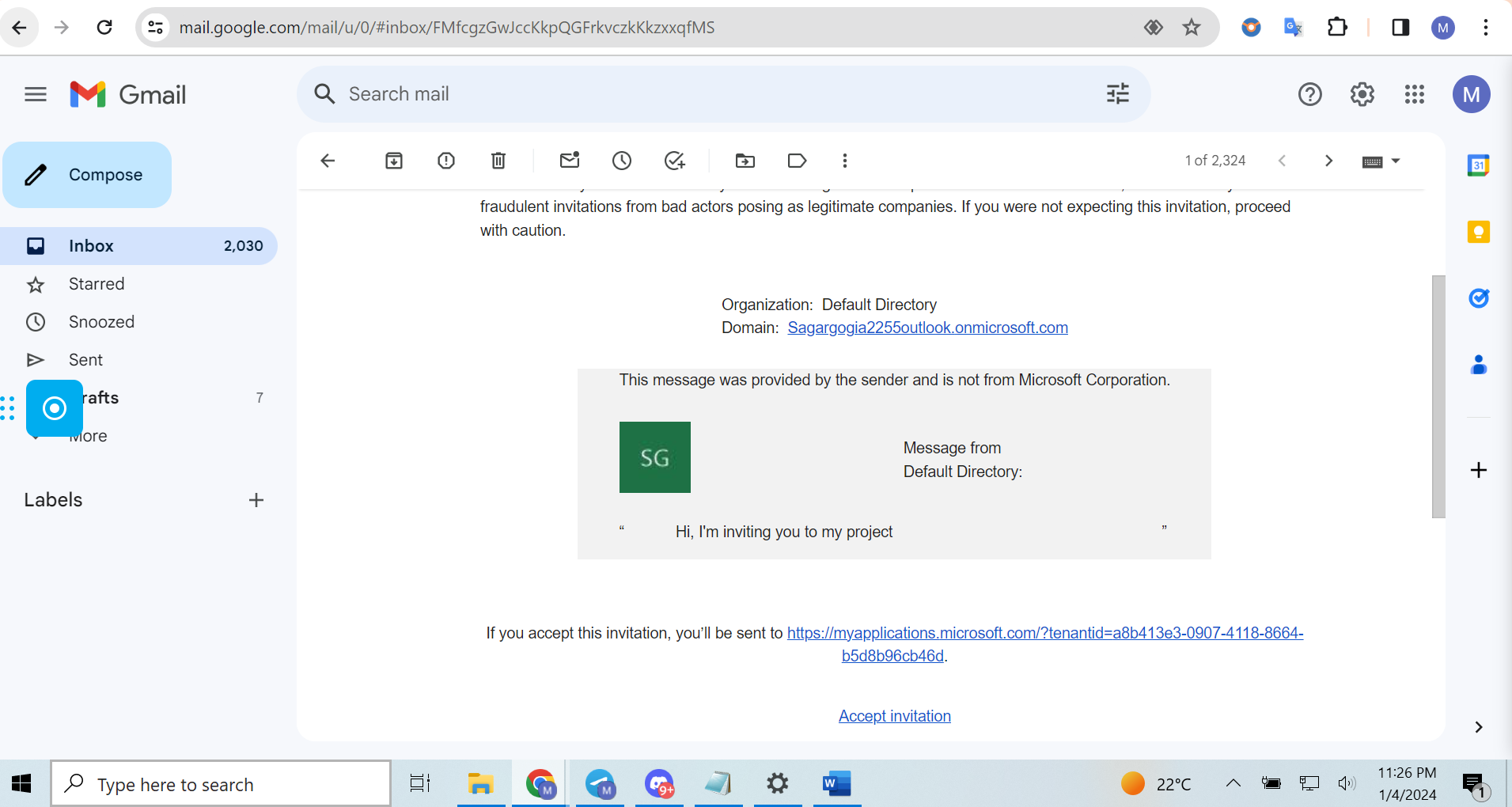
A screenshot of a computer

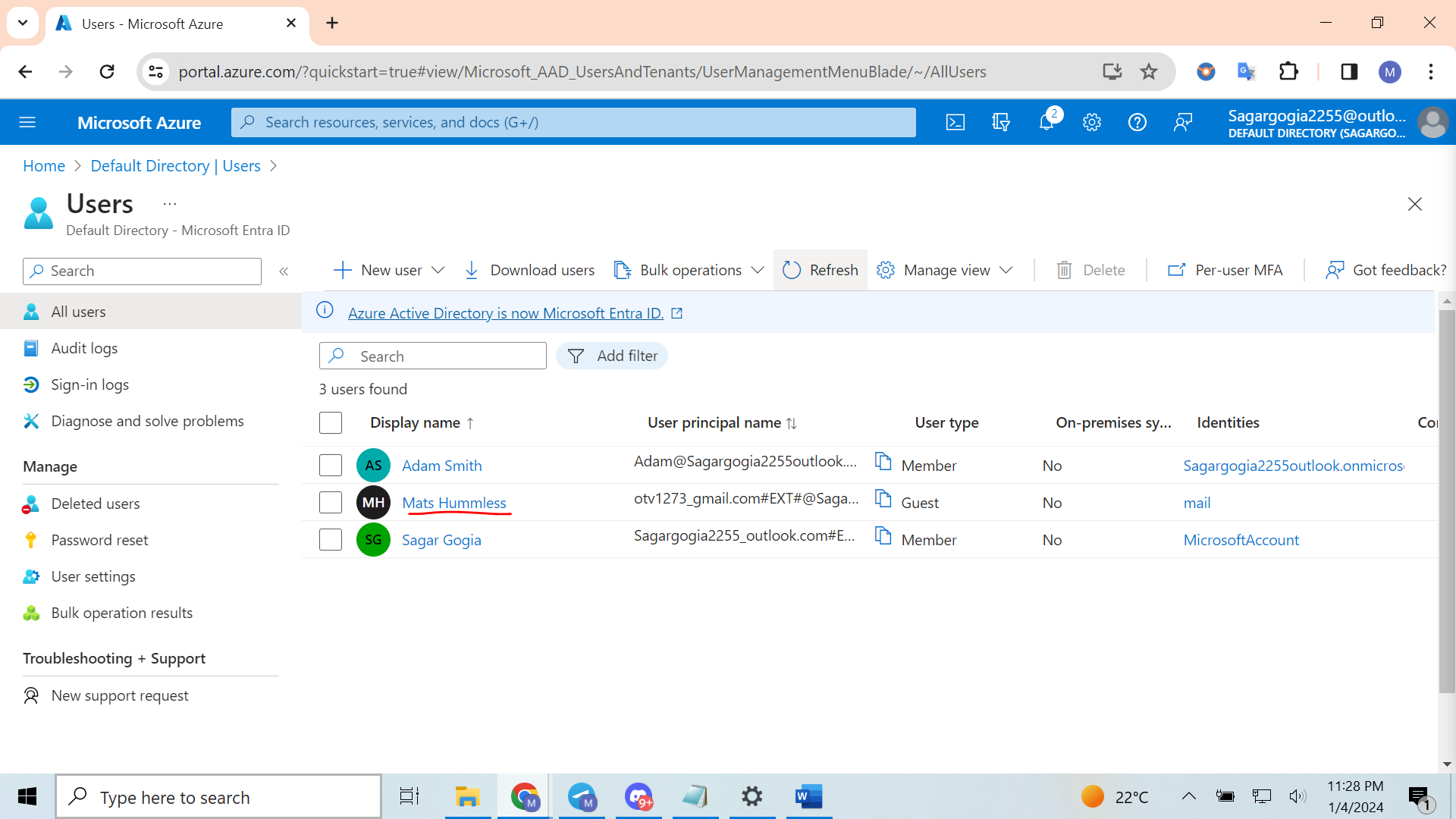
Description automatically generated





User should get an invite email that says to accept the invition in order to collaborate with the tenant’s project. Screenshot below shows the invite email that was sent to the user we invited externally

  
  
  
Once user accepts the invite email, it reflects in the “All users” tab of navigation pane

  
  
For the users that are no longer required on the project, we can always select the username from the user list and click delete. Note- The user is deleted and no longer appears on the Users - All users page. The user can be seen on the Deleted users page for the next 30 days and can be restored during that time.

When a user is deleted, any licenses consumed by the user are made available for other users.

A screenshot of a computer

Description automatically generated

A computer screen with a message

Description automatically generated  
  
  
Password less authentication

- **Enable MFA for a user:**

- Access the Portal and locate Microsoft Entra ID.

- Under "Manage," select "Security."

- Under "Manage," choose "MFA."

- In the central pane, under "Configure," select "Additional cloud-based MFA settings."

- Go to the "Users" tab.

- **Select and note user details:**

- Choose the user AZ500User1.

- Make a note of their username in the format user@domain.com.

- **Initiate MFA activation:**

- On the far right, click "Enable."

- Review information about enabling multi-factor authentication in Azure.

- Click "Enable multi-factor auth."

- **Await the update:**

- Wait for the system to update.

- AZ500User1 will now be required to provide two-factor authentication.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated  
  
Note- Because of restricted access through the student account, I am unable to proceed and demonstrate the complete implementation of passwordless sign-in.