Previous Unit 7 of 8 Next

200 XP

Exercise - Identity topology options

10 minutes

This exercise will demonstrate how to configure and implement an application that supports B2B.

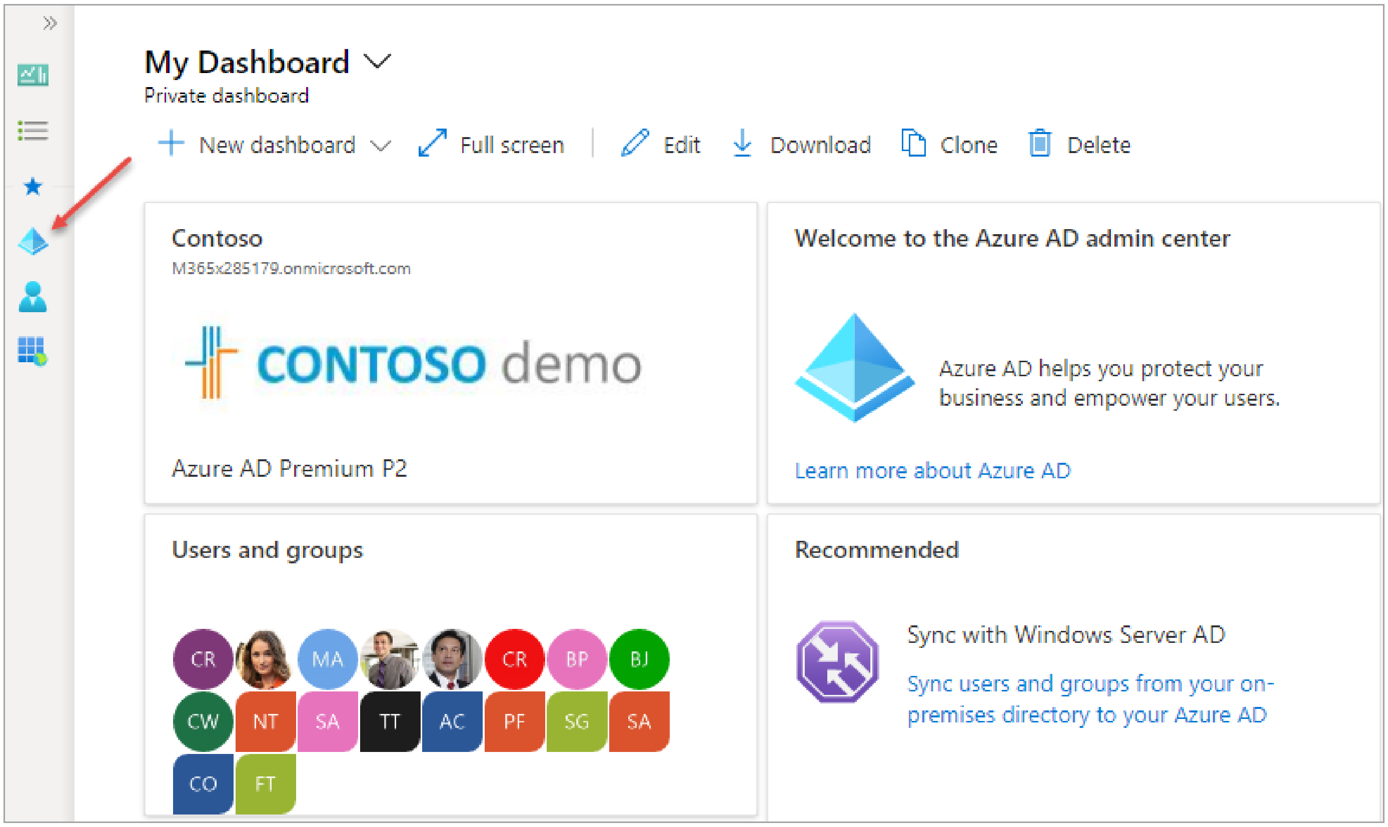
> **Note**
>
> This exercise demonstrates signing into a web application using three different accounts. These three accounts will come from two organizations, one of them being the organization where the Azure AD application is registered. Therefore, in order to complete the exercise, you'll need access to two user accounts in different Azure AD directories.

In this application, you'll create an an Azure AD application and ASP.NET Core web application that allow users from the current organization to sign in and display their information. You'll then invite a user from another organization as a guest to access the same resources in your organization

Create a single-tenant Azure AD application

Open a browser and navigate to the Azure Active Directory admin center (https://aad.portal.azure.com) . Sign in using a **Work or School Account** that has global administrator rights to the tenancy.

Select **Azure Active Directory** in the left-hand navigation.

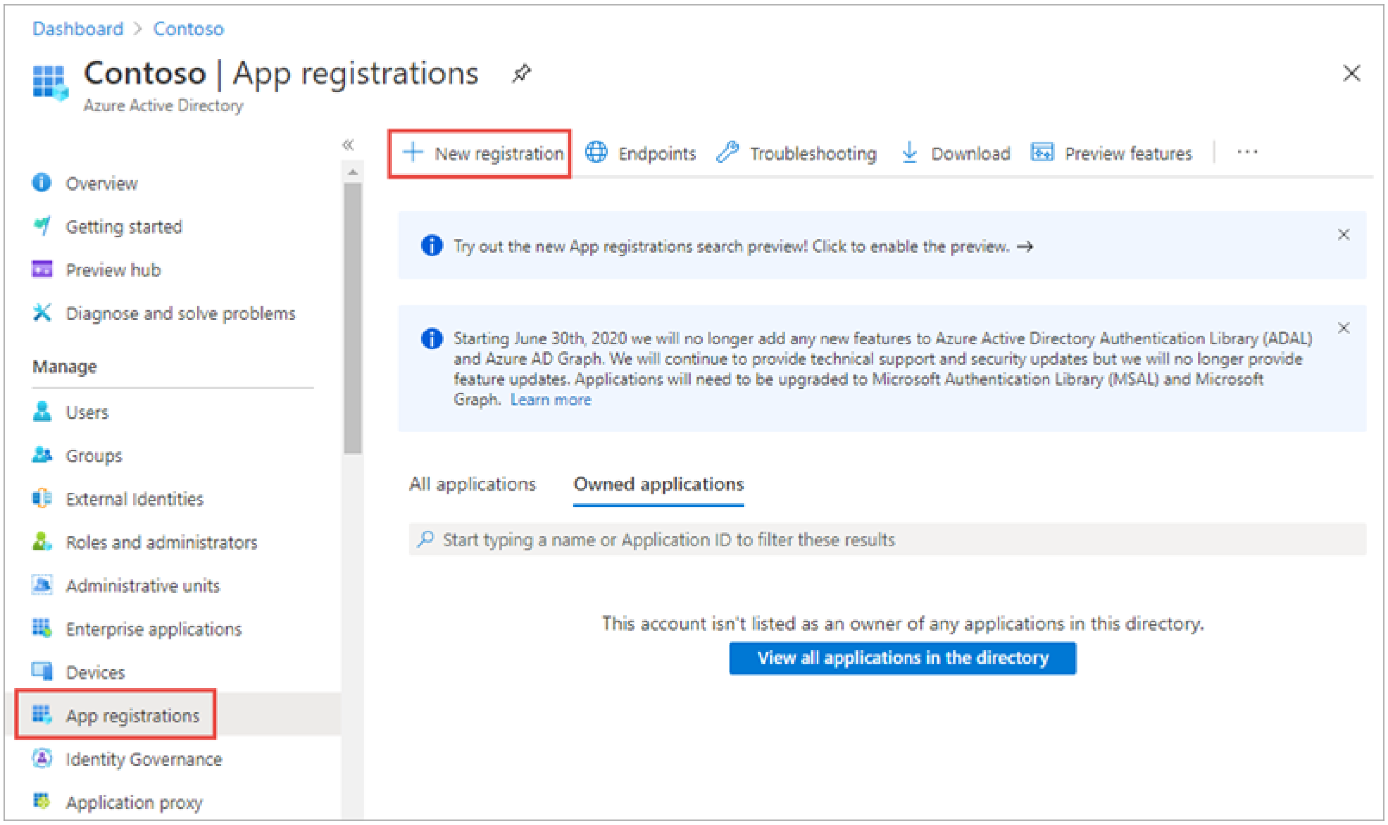


My Dashboard
Private dashboard
New dashboard
Full screen
Edit
Download
Clone
Delete
Contoso
M365x285179.onmicrosoft.com
CONTOSO demo
Azure AD Premium P2
Welcome to the Azure AD admin center
Learn more about Azure AD
Users and groups
CR MA CR BP BJ
CW NT SA TT AC PF SG SA
CO FT
Recommended
Sync with Windows Server AD
Sync users and groups from your on-premises directory to your Azure AD

Azure AD helps you protect your business and empower your users.

Select **Manage > App registrations** in the left-hand navigation.

On the **App registrations** page, select **New registration**.



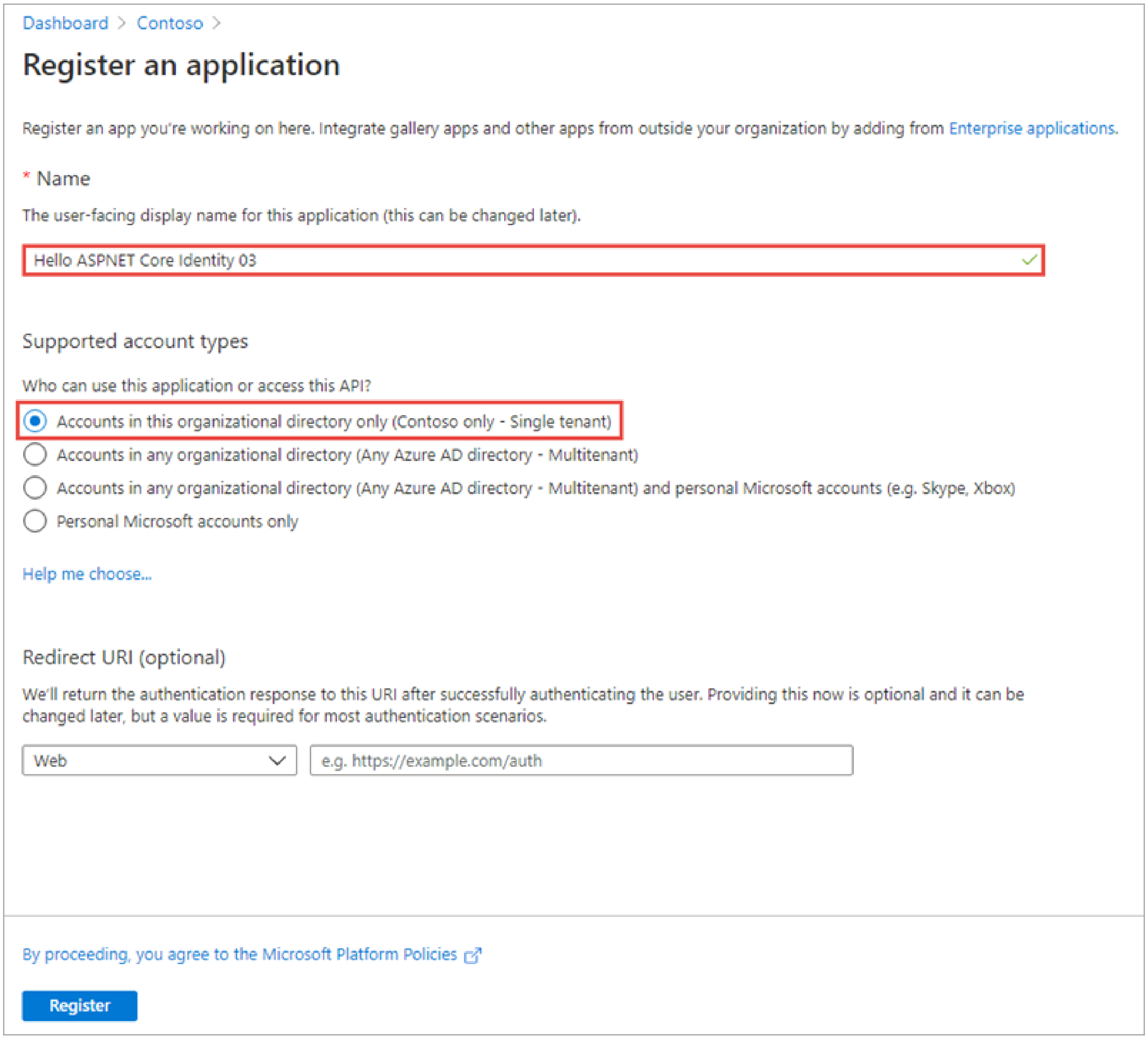
Try out the new App registrations search preview! Click to enable the preview. →

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more

This account isn't listed as an owner of any applications in this directory.

On the **Register an application** page, set the values as follows:

- **Name**: Hello ASPNET Core Identity 03
- **Supported account types**: Accounts in this organizational directory only (Single tenant)



Dashboard > Contoso >

Register an application

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from Enterprise applications.

* Name

The user-facing display name for this application (this can be changed later).

Hello ASPNET Core Identity 03 ✓

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (Contoso only - Single tenant)
○ Accounts in any organizational directory (Any Azure AD directory - Multitenant)
○ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
○ Personal Microsoft accounts only

Help me choose...

Redirect URI (optional)

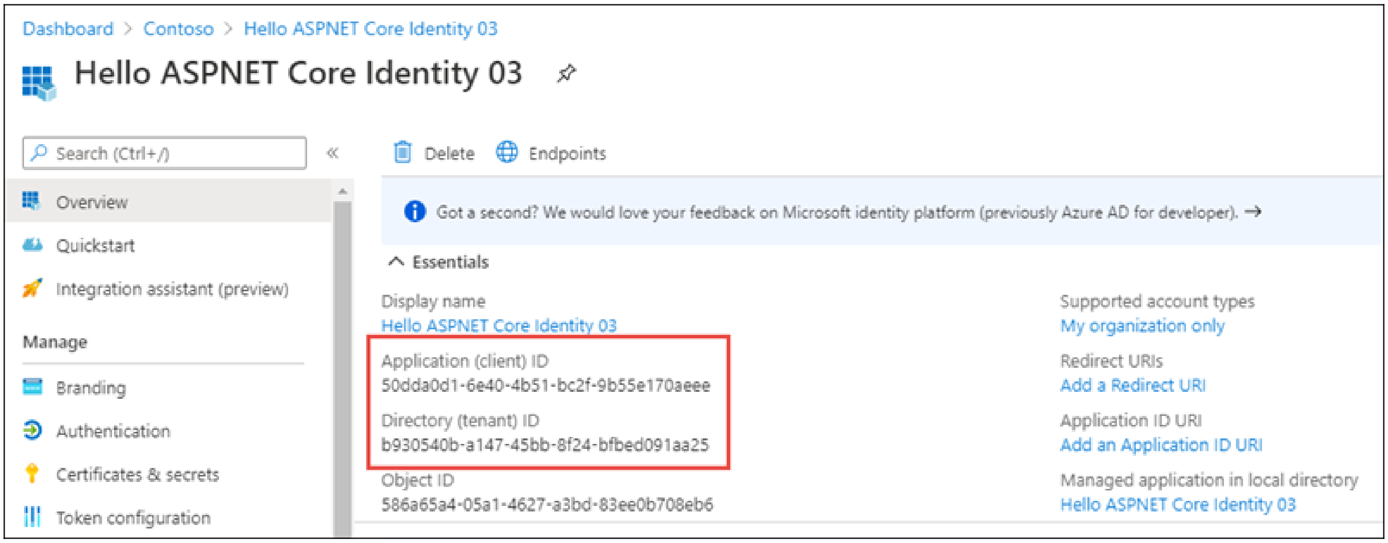
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web e.g. https://example.com/auth

By proceeding, you agree to the Microsoft Platform Policies

Select **Register** to create the application.

On the **Hello ASPNET Core Identity 03** page, copy the values **Application (client) ID** and **Directory (tenant) ID**; you'll need these values later in this exercise.



Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

Display name
Hello ASPNET Core Identity 03

Application (client) ID
50dda0d1-6e40-4b51-bc2f-9b55e170aeee

Directory (tenant) ID
b930540b-a147-45bb-8f24-bfbed091aa25

Object ID
586a65a4-05a1-4627-a3bd-83ee0b708eb6

Supported account types
My organization only

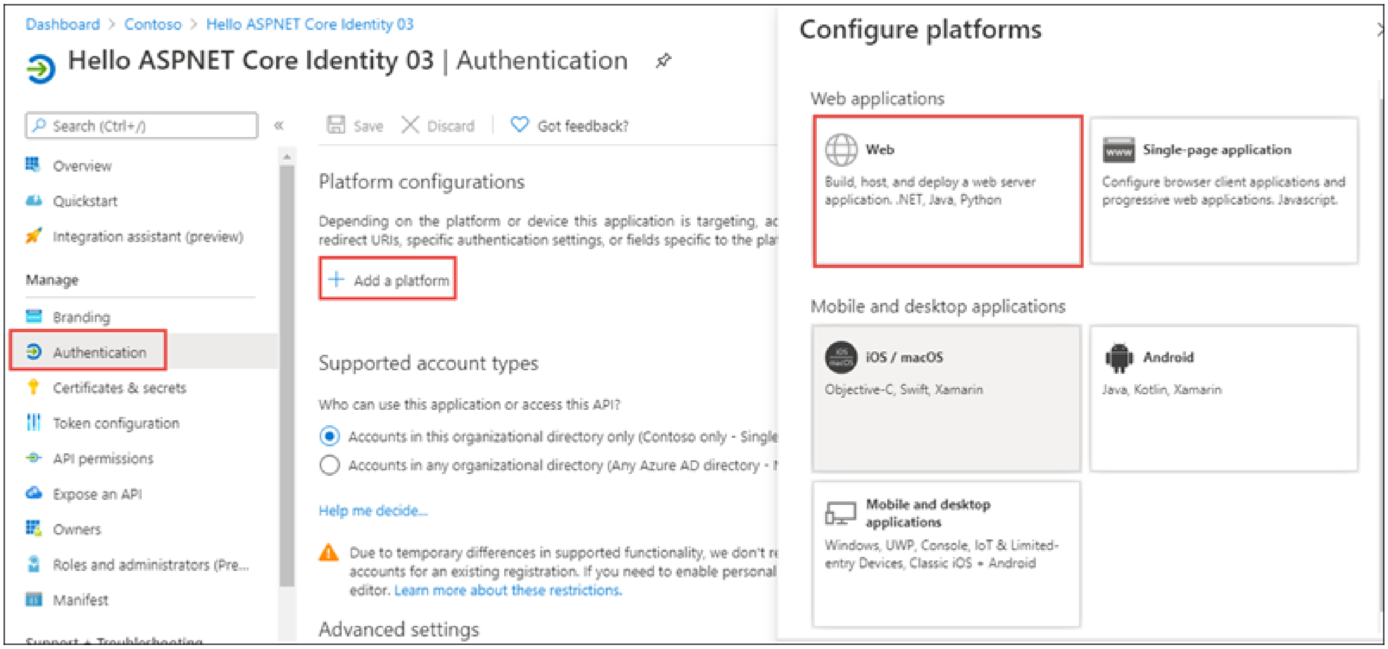
Redirect URIs
Add a Redirect URI

Application ID URI
Add an Application ID URI

Managed application in local directory
Hello ASPNET Core Identity 03

Select **Manage** > **Authentication** in the left-hand navigation.

In the **Authentication** page, select **Add a platform**. When the **Configure platform** panel appears, select **Web**.



Platform configurations

Depending on the platform or device this application is targeting, ac redirect URIs, specific authentication settings, or fields specific to the plat

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (Contoso only - Single

○ Accounts in any organizational directory (Any Azure AD directory - I

Due to temporary differences in supported functionality, we don't re accounts for an existing registration. If you need to enable personal editor. Learn more about these restrictions.

Advanced settings

Web: Build, host, and deploy a web server application. .NET, Java, Python

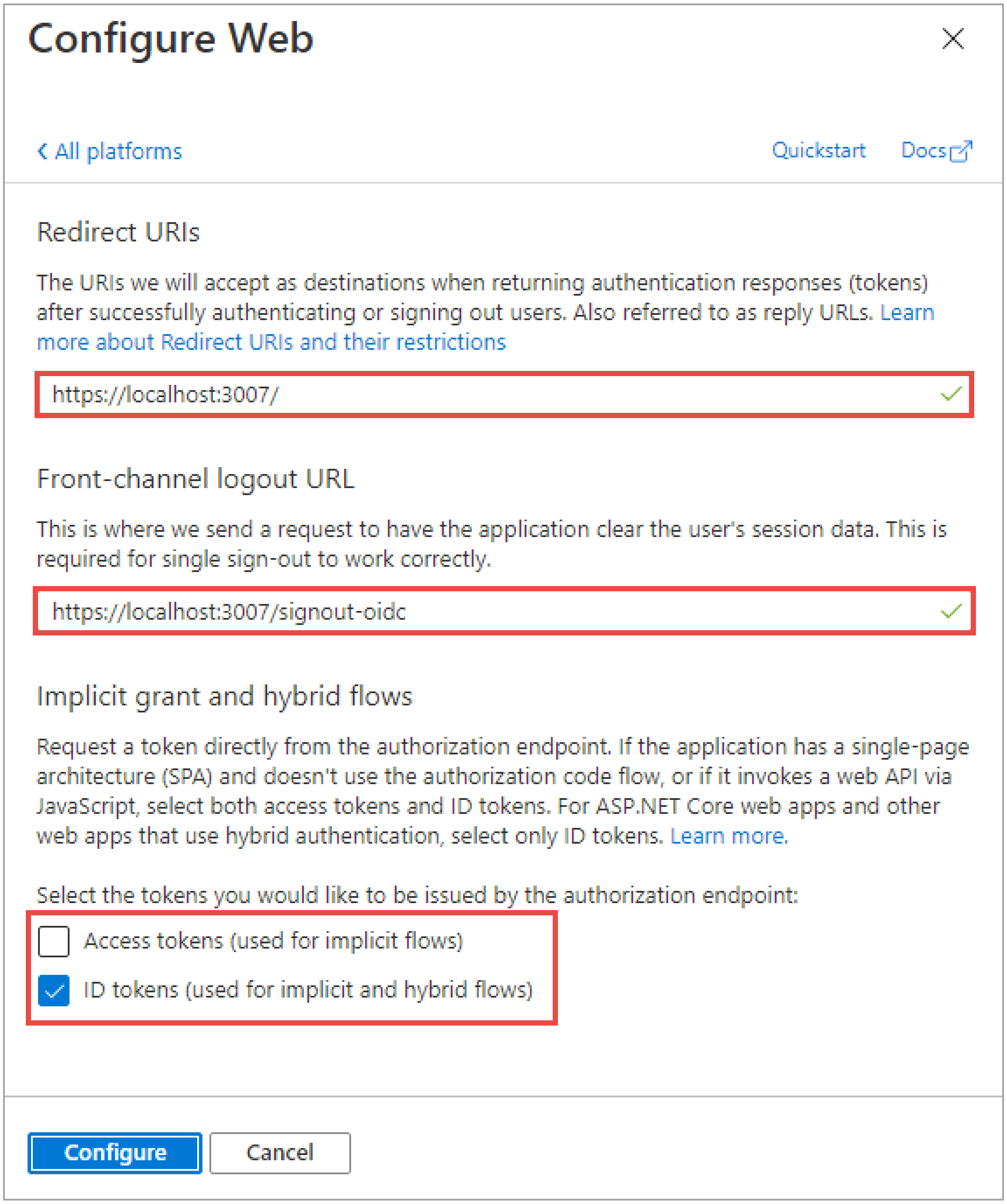
Single-page application: Configure browser client applications and progressive web applications. Javascript.

iOS / macOS: Objective-C, Swift, Xamarin

Android: Java, Kotlin, Xamarin

Mobile and desktop applications: Windows, UWP, Console, IoT & Limited-entry Devices, Classic iOS + Android

In the **Configure Web** panel, add **https://localhost:3007** under **Redirect URIs**, add **https://localhost:3007/signout-oidc** under **Logout URL**, select **ID tokens (used for implicit and hybrid flows)** under **Implicit grant and hybrid flows**, and select **Configure**.



Configure Web

‹ All platforms

Redirect URIs

The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating or signing out users. Also referred to as reply URLs. Learn more about Redirect URIs and their restrictions

https://localhost:3007/ ✓

Front-channel logout URL

This is where we send a request to have the application clear the user's session data. This is required for single sign-out to work correctly.

https://localhost:3007/signout-oidc ✓

Implicit grant and hybrid flows

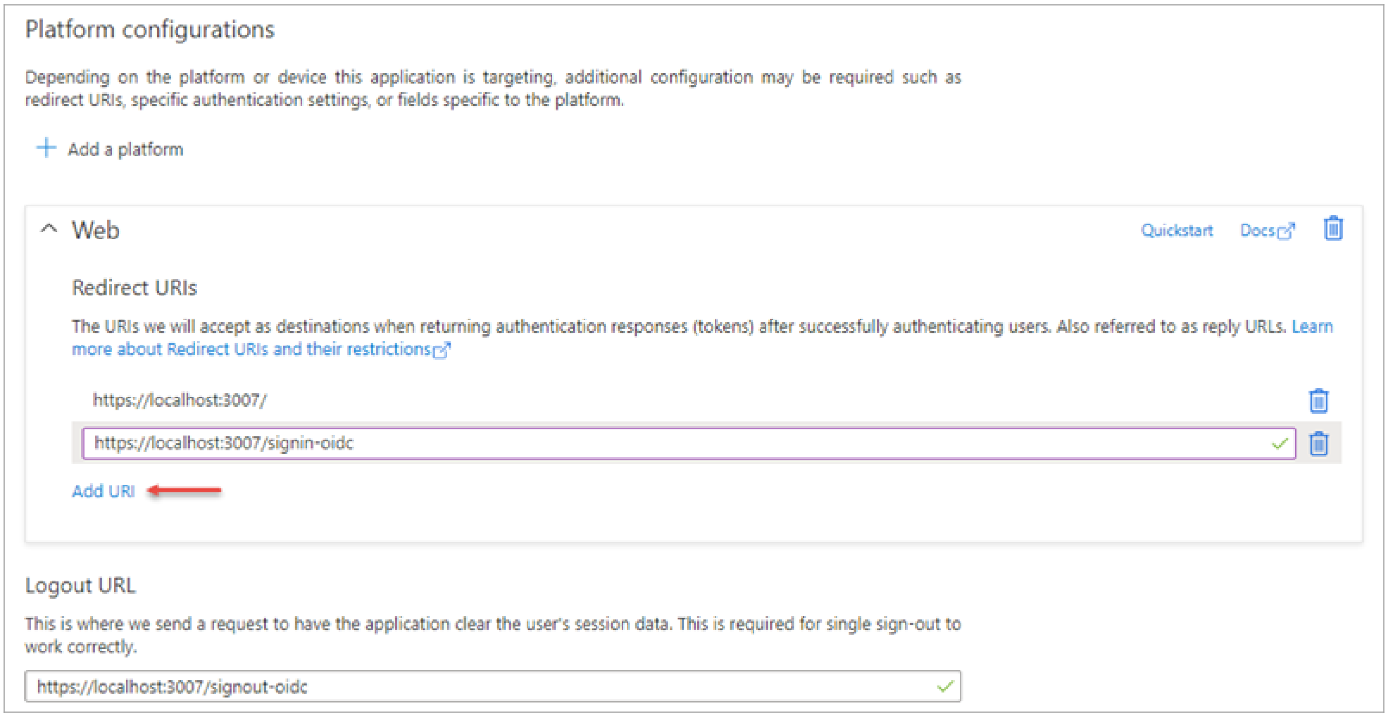
Request a token directly from the authorization endpoint. If the application has a single-page architecture (SPA) and doesn't use the authorization code flow, or if it invokes a web API via JavaScript, select both access tokens and ID tokens. For ASP.NET Core web apps and other web apps that use hybrid authentication, select only ID tokens. Learn more.

Select the tokens you would like to be issued by the authorization endpoint:

☐ Access tokens (used for implicit flows)

☑ ID tokens (used for implicit and hybrid flows)

When the **Authentication** page refreshes, select **Add URI**, add **https://localhost:3007/signin-oidc**, and select **Save** near the top of the page to save the changes.



Platform configurations

Depending on the platform or device this application is targeting, additional configuration may be required such as redirect URIs, specific authentication settings, or fields specific to the platform.

Redirect URIs

The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating users. Also referred to as reply URLs. Learn more about Redirect URIs and their restrictions

https://localhost:3007/

https://localhost:3007/signin-oidc

Logout URL

This is where we send a request to have the application clear the user's session data. This is required for single sign-out to work correctly.

https://localhost:3007/signout-oidc

Create a single organization ASP.NET core web application

> **Note**
>
> The instructions below assume you are using .NET 5. They were last tested using v5.0.202 of the .NET 5 SDK.

Open your command prompt, navigate to a directory where you want to save your work, create a new folder, and change directory into that folder.

Execute the following command to create a new ASP.NET Core MVC web application:

shell

```
dotnet new mvc --auth SingleOrg -o TopologyOptions
```

Open the application in Visual Studio Code using the following command:

Console

```
code .
```

If Visual Studio code displays a dialog box asking if you want to add required assets to the project, select **Yes**.

Configure the web application with the Azure AD application you created

Locate and open the **./appsettings.json** file in the ASP.NET Core project.

Set the **AzureAd.Domain** property to the domain of your Azure AD tenant where you created the Azure AD application (*for example: contoso.onmicrosoft.com*).

Set the **AzureAd.TenantId** property to the **Directory (tenant) ID** you copied when creating the Azure AD application in the previous step.

Set the **AzureAd.ClientId** property to the **Application (client) ID** you copied when creating the Azure AD application in the previous step.

Update the web application's launch configuration

Locate and open the **./Properties/launchSettings.json** file in the ASP.NET Core project.

Set the **iisSettings.iisExpress.applicationUrl** property to **https://localhost:3007**.

Set the **iisSettings.iisExpress.sslPort** property to **3007**.

Update the user experience

Finally, update the user experience of the web application to display all the claims in the OpenID Connect ID token.

Locate and open the **./Views/Home/Index.cshtml** file.

Add the following code to the end of the file:

HTML Copy

```html
@if (User.Identity.IsAuthenticated)
{
<div>
  <table cellpadding="2" cellspacing="2">
    <tr>
      <th>Claim</th>
      <th>Value</th>
    </tr>
    @foreach (var claim in User.Claims)
    {
      <tr>
        <td>@claim.Type</td>
        <td>@claim.Value</td>
      </tr>
    }
  </table>
</div>
}
```

Build and test the web app

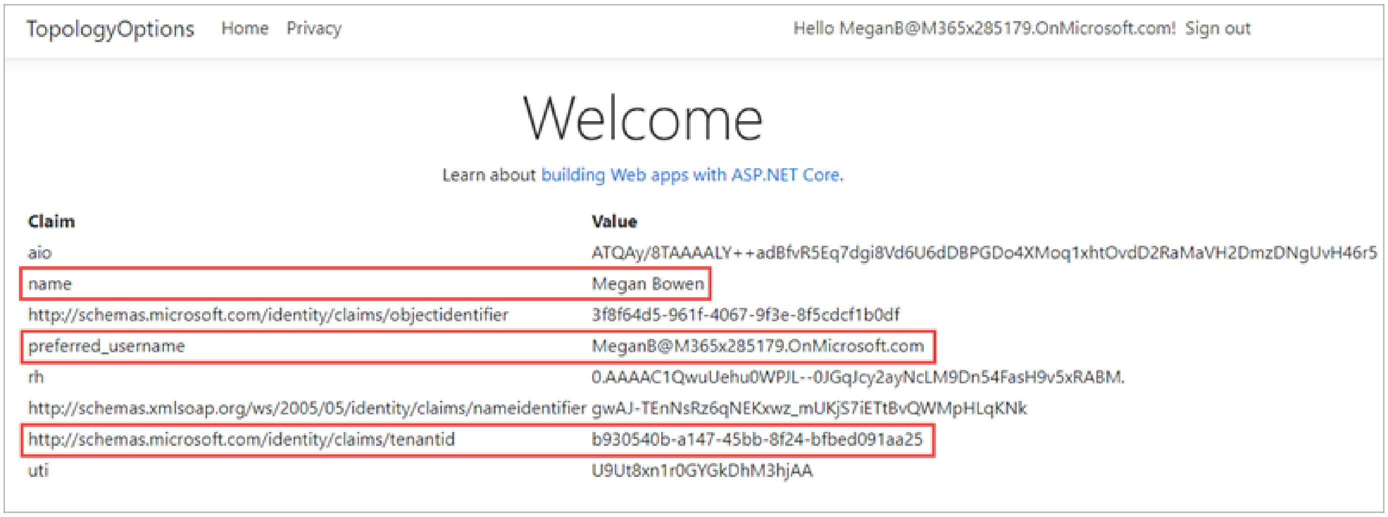
Run the following commands in a command prompt to compile and run the application:

shell Copy

```
dotnet build
dotnet run
```

Open a browser and navigate to the url **https://localhost:5001**. The web application will redirect you to the Azure AD sign in page.

Sign in using a Work and School account from your Azure AD directory. Azure AD will redirect you back to the web application.



Welcome

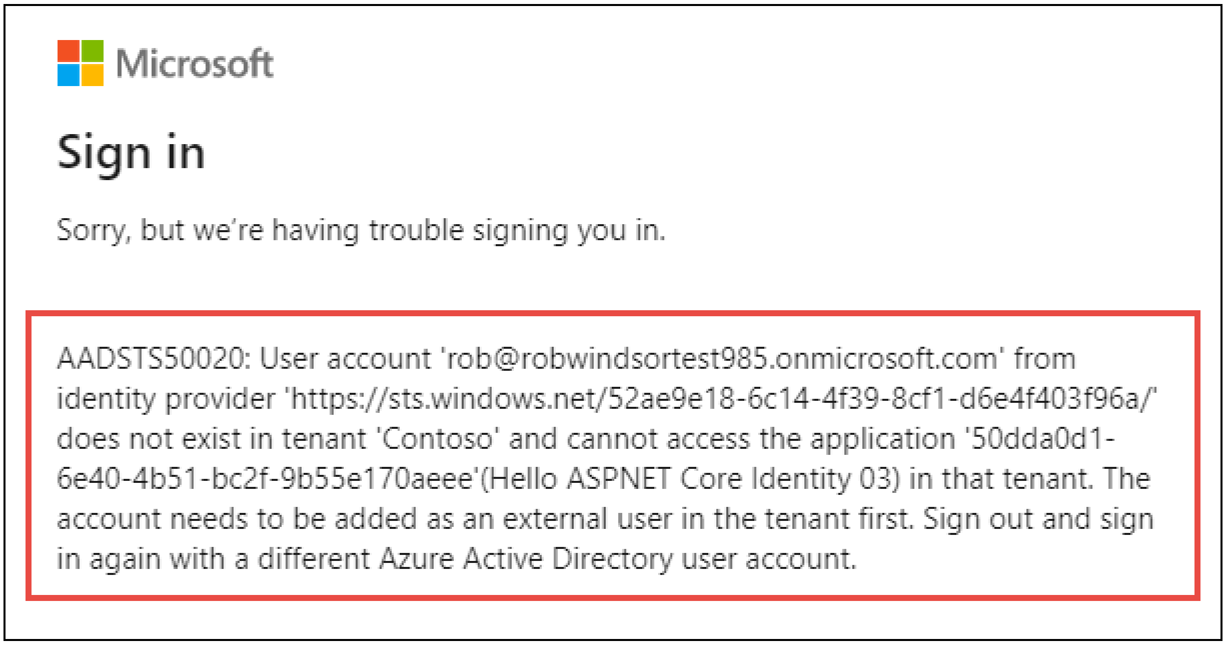
Learn about building Web apps with ASP.NET Core.

Claim	Value
aio	ATQAy/8TAAAALY++adBfvR5Eq7dgi8Vd6U6dDBPGDo4XMoq1xhtOvdD2RaMaVH2DmzDNgUvH46r5
name	Megan Bowen
http://schemas.microsoft.com/identity/claims/objectidentifier	3f8f64d5-961f-4067-9f3e-8f5cdcf1b0df
preferred_username	MeganB@M365x285179.OnMicrosoft.com
rh	0.AAAAC1QwuUehu0WPJL--0JGqJcy2ayNcLM9Dn54FasH9v5xRABM.
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier	gwAJ-TEnNsRz6qNEKxwz_mUKjS7iETtBvQWMpHLqKNk
http://schemas.microsoft.com/identity/claims/tenantid	b930540b-a147-45bb-8f24-bfbed091aa25
uti	U9Ut8xn1r0GYGkDhM3hjAA

Notice some of the details from the claims included in the ID token. Take special note of the **preferred_username** and **tenantid** claim. These claims indicate the ID of the Azure AD directory and ID of the user that signed in. Make a note of these values to compare them to the values displayed later in this exercise.

Now try logging in as a user from a different organization. Select the **Sign out** link in the top left. Wait for Azure AD and the web application signs out the current user. When the web application reloads, repeat the sign in process, except this time try signing in as a user from a different organization or use a Microsoft Account.

Notice Azure AD will reject the user's sign in, explaining that the user's account doesn't exist in the current tenant.



Microsoft

Sign in

Sorry, but we're having trouble signing you in.

AADSTS50020: User account 'rob@robwindsortest985.onmicrosoft.com' from identity provider 'https://sts.windows.net/52ae9e18-6c14-4f39-8cf1-d6e4f403f96a/' does not exist in tenant 'Contoso' and cannot access the application '50dda0d1-6e40-4b51-bc2f-9b55e170aeee'(Hello ASPNET Core Identity 03) in that tenant. The account needs to be added as an external user in the tenant first. Sign out and sign in again with a different Azure Active Directory user account.

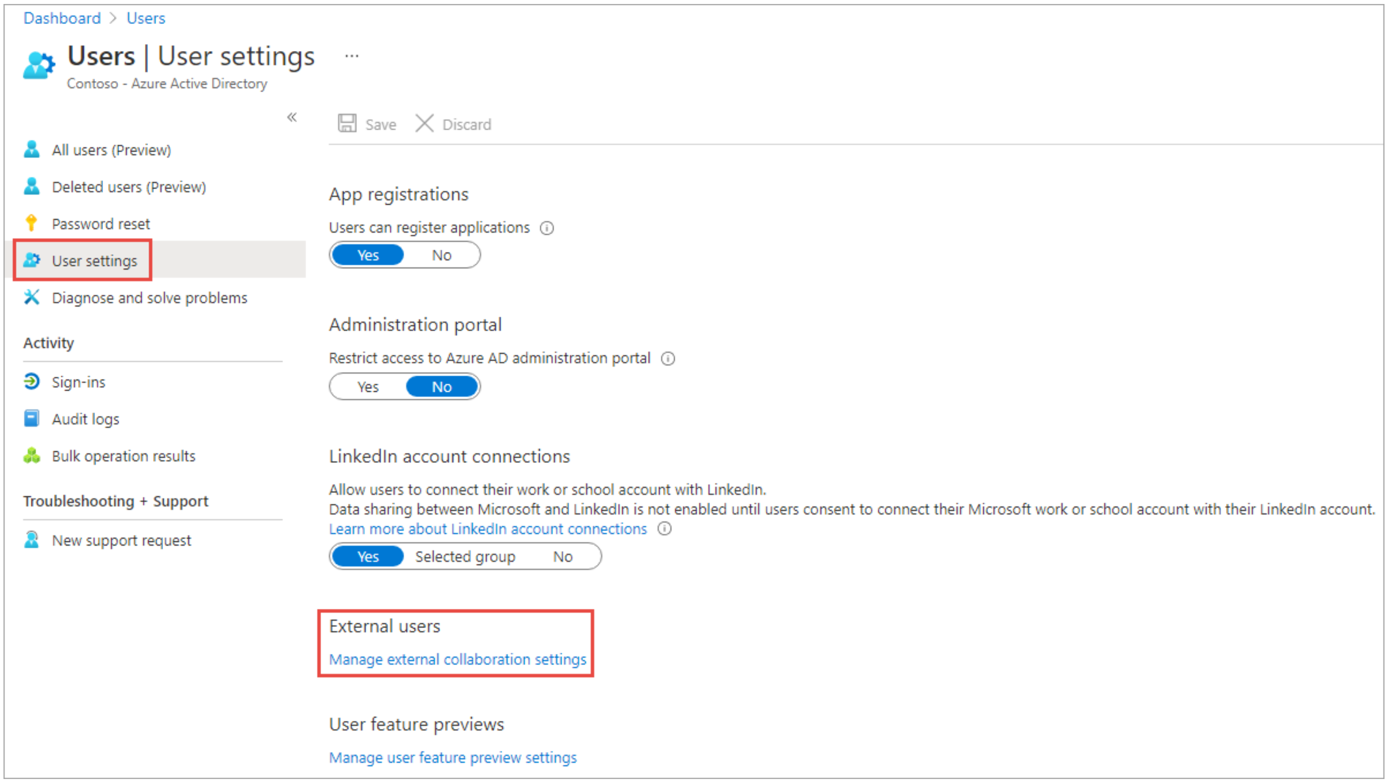
Before this user can access this application, they need to be added as a guest into the Azure AD directory where the application was registered.

Invite a guest user from another organization

Within a browser, navigate to the Azure Active Directory admin center (https://aad.portal.azure.com) and sign in using the **Work or School Account** that has global administrator rights to your tenant where you registered the Azure AD application.

In the left-hand navigation, select **Users**.

Examine the external user settings available to administrators by selecting **User Settings** and then **Manage external collaboration settings**.



Dashboard > Users

Users | User settings ···

Contoso - Azure Active Directory

App registrations

Users can register applications ⓘ

[✓ Yes] No

Administration portal

Restrict access to Azure AD administration portal ⓘ

Yes [✓ No]

LinkedIn account connections

Allow users to connect their work or school account with LinkedIn.
Data sharing between Microsoft and LinkedIn is not enabled until users consent to connect their Microsoft work or school account with their LinkedIn account.
Learn more about LinkedIn account connections ⓘ

[✓ Yes] Selected group No

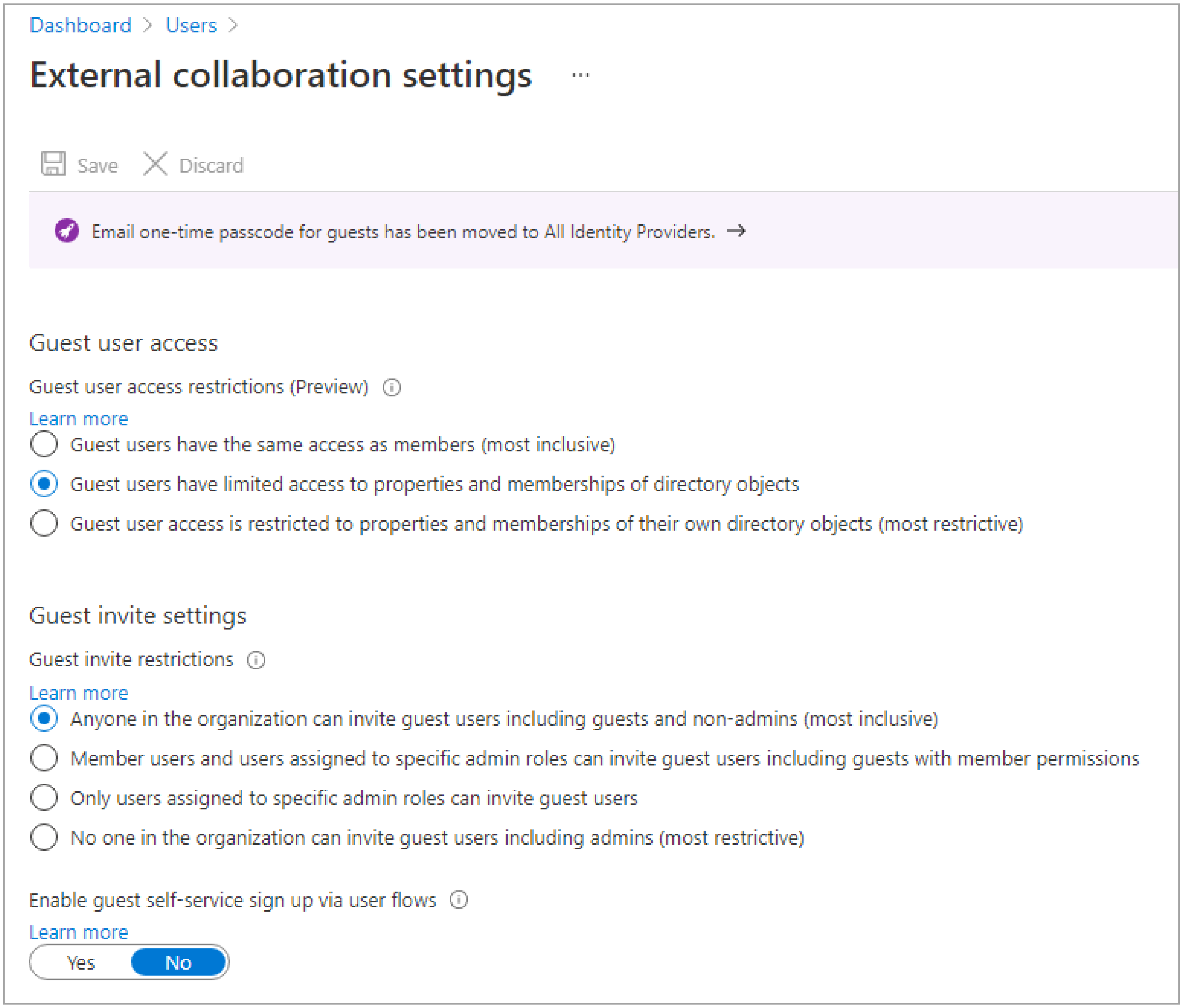
External users

Manage external collaboration settings

User feature previews

Manage user feature preview settings

Notice that administrators can configure the Azure AD directory so guest users have limited rights compared to other users, and who can invite guest users.



External collaboration settings ...

Email one-time passcode for guests has been moved to All Identity Providers. →

Guest user access

Guest user access restrictions (Preview)

Learn more

○ Guest users have the same access as members (most inclusive)

● Guest users have limited access to properties and memberships of directory objects

○ Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)

Guest invite settings

Guest invite restrictions

Learn more

● Anyone in the organization can invite guest users including guests and non-admins (most inclusive)

○ Member users and users assigned to specific admin roles can invite guest users including guests with member permissions

○ Only users assigned to specific admin roles can invite guest users

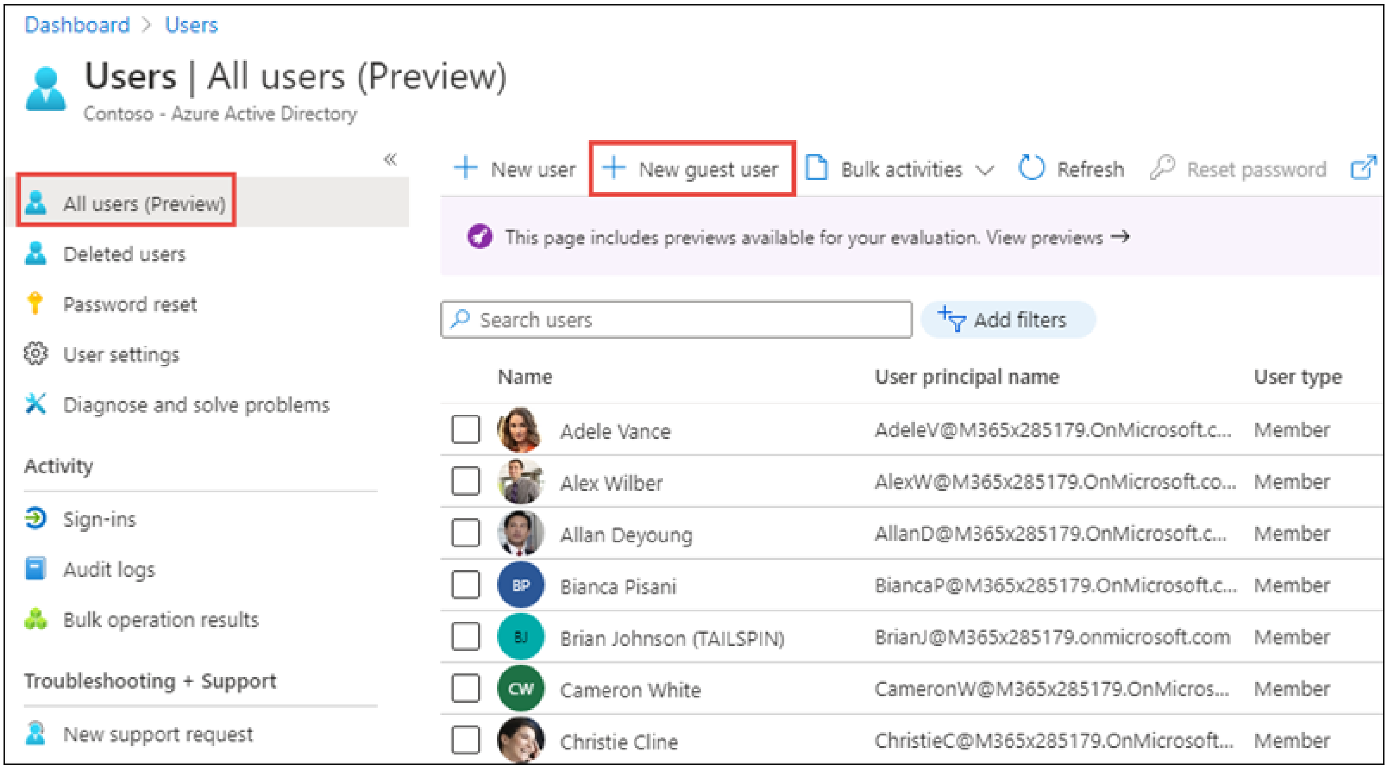
○ No one in the organization can invite guest users including admins (most restrictive)

Enable guest self-service sign up via user flows

Learn more

Yes [✓ No]

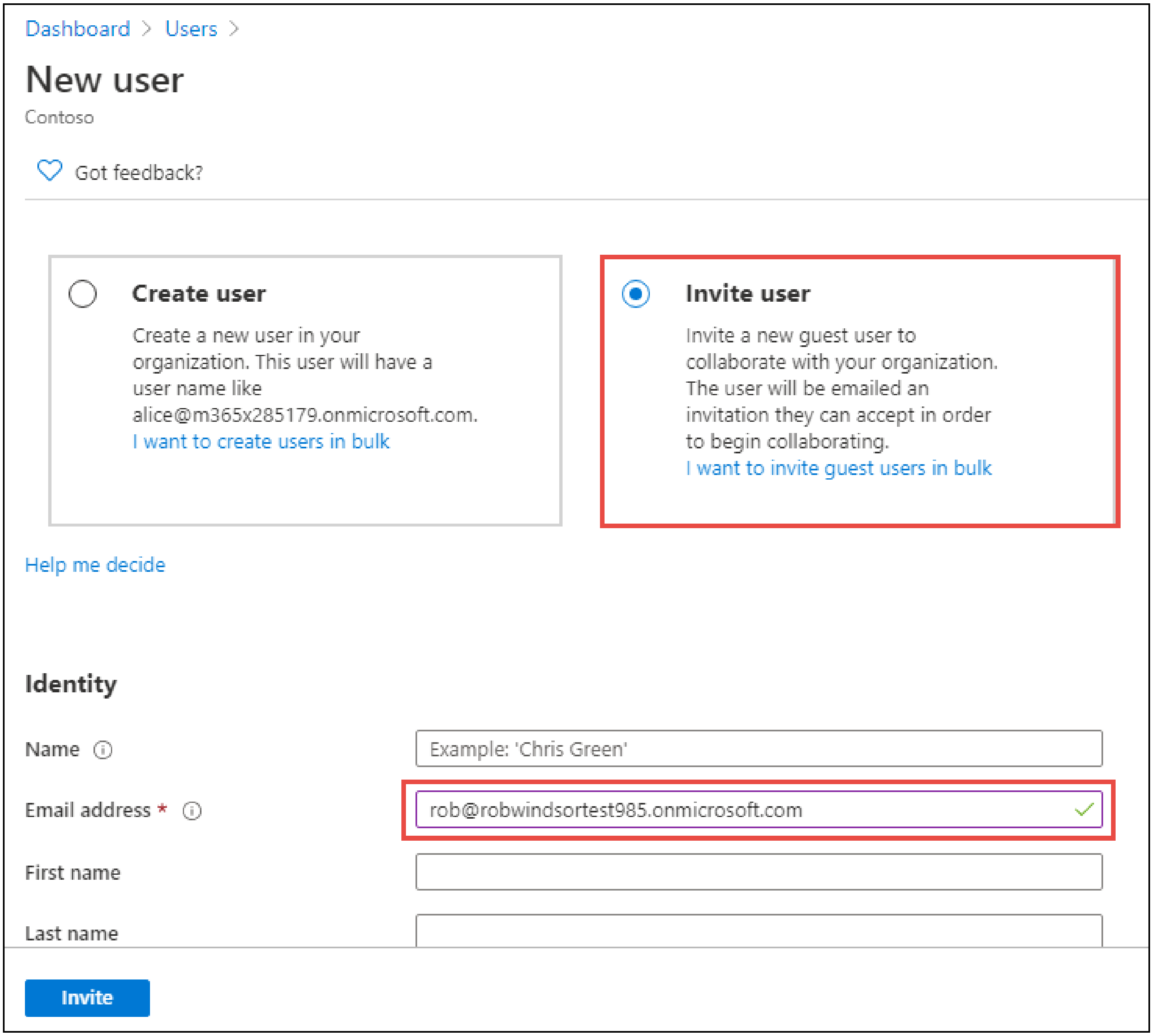
Now let's invite a guest user. Select **All users** in the left-hand navigation, and then select **New guest user**:



This page includes previews available for your evaluation. View previews →

	Name	User principal name	User type
☐	Adele Vance	AdeleV@M365x285179.OnMicrosoft.c...	Member
☐	Alex Wilber	AlexW@M365x285179.OnMicrosoft.co...	Member
☐	Allan Deyoung	AllanD@M365x285179.OnMicrosoft.c...	Member
☐	Bianca Pisani	BiancaP@M365x285179.OnMicrosoft.c...	Member
☐	Brian Johnson (TAILSPIN)	BrianJ@M365x285179.onmicrosoft.com	Member
☐	Cameron White	CameronW@M365x285179.OnMicros...	Member
☐	Christie Cline	ChristieC@M365x285179.OnMicrosoft...	Member

On the **New user** page, select **Invite user**, enter the email address of a user in another Azure AD directory that you want to invite and select **Invite**. In this scenario displayed in the following screenshot, we are inviting the user we previously tried to sign in with.



New user

Contoso

○ **Create user**

Create a new user in your organization. This user will have a user name like alice@m365x285179.onmicrosoft.com.

I want to create users in bulk

● **Invite user**

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

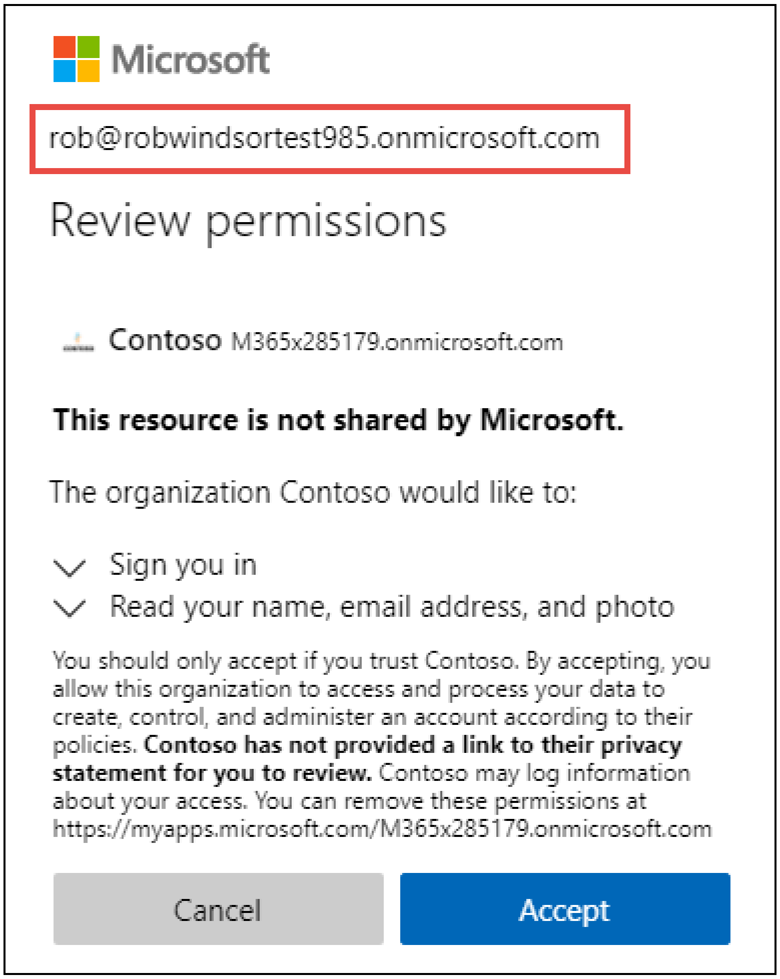
Help me decide

Identity

Name	Example: 'Chris Green'
Email address *	rob@robwindsortest985.onmicrosoft.com ✓
First name	
Last name	

Now let's try to sign in with the user. In the browser, navigate to **https://localhost:5001**.

This time, after successfully logging in, the user's Azure AD directory will prompt the them to grant the application's Azure AD directory permissions. That is to sign in as the user and obtain basic information about them.



rob@robwindsortest985.onmicrosoft.com

Review permissions

Contoso M365x285179.onmicrosoft.com

This resource is not shared by Microsoft.

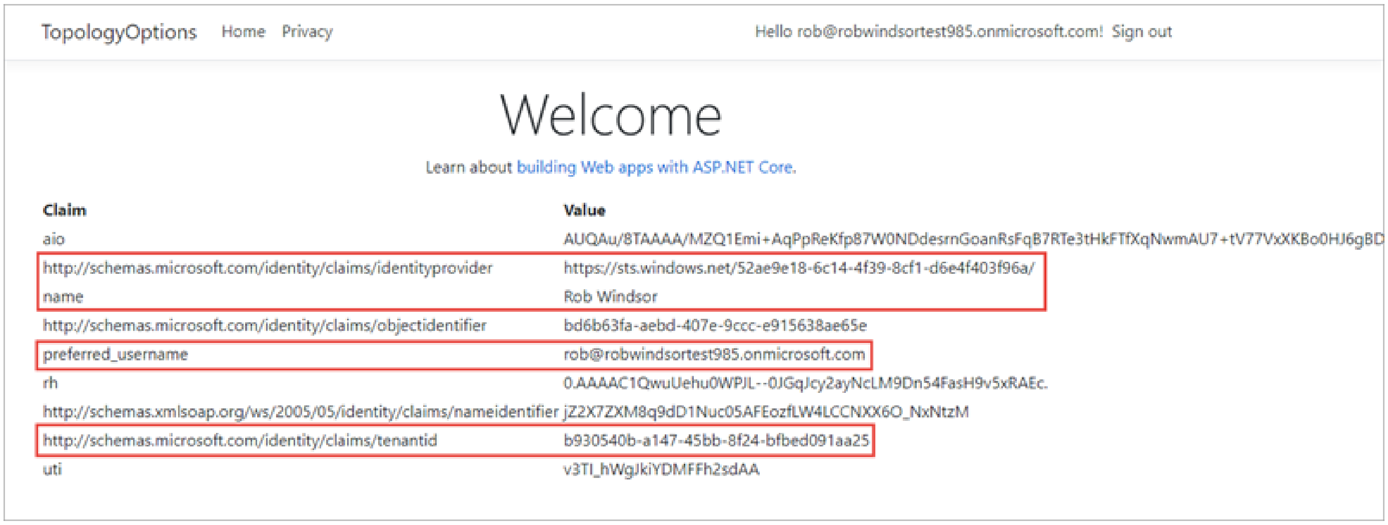
The organization Contoso would like to:

- Sign you in
- Read your name, email address, and photo

You should only accept if you trust Contoso. By accepting, you allow this organization to access and process your data to create, control, and administer an account according to their policies. **Contoso has not provided a link to their privacy statement for you to review.** Contoso may log information about your access. You can remove these permissions at https://myapps.microsoft.com/M365x285179.onmicrosoft.com

Take note of what is happening at this point. The application's Azure AD directory is not signing in the user, rather the user has been redirected to sign in with their Azure AD directory. Once they sign in, their Azure AD directory will provide a token to the application's directory. That token is used to verify the user is authenticated and that they have authorized the application to obtain their basic profile information. The application's Azure AD then created a new access token that can be used by our ASP.NET Core web application.

After selecting **Accept**, the user is taken to our ASP.NET application. Notice the difference in some of the claims.



Welcome

Learn about building Web apps with ASP.NET Core.

Claim	Value
aio	AUQAu/8TAAAA/MZQ1Emi+AqPpReKfp87W0NDdesrnGoanRsFqB7RTe3tHkFTfXqNwmAU7+tV77VxXKBo0HJ6gBD
http://schemas.microsoft.com/identity/claims/identityprovider	https://sts.windows.net/52ae9e18-6c14-4f39-8cf1-d6e4f403f96a/
name	Rob Windsor
http://schemas.microsoft.com/identity/claims/objectidentifier	bd6b63fa-aebd-407e-9ccc-e915638ae65e
preferred_username	rob@robwindsortest985.onmicrosoft.com
rh	0.AAAAC1QwuUehu0WPJL--0JGqJcy2ayNcLM9Dn54FasH9v5xRAEc.
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier	jZ2X7ZXM8q9dD1Nuc05AFEozfLW4LCCNXX6O_NxNtzM
http://schemas.microsoft.com/identity/claims/tenantid	b930540b-a147-45bb-8f24-bfbed091aa25
uti	v3TI_hWgJkiYDMFFh2sdAA

- The **identityprovider** claim is the ID of the Azure AD directory that authenticated the user. This claim is the user's Azure AD directory
- The **tenantid** claim is the ID of the Azure AD directory our application is registered in. Notice this value is not the same as the **identityprovider** claim, indicating the user's identity is in one directory while they have been added as a guest user to another Azure AD directory.

Stop the web server by pressing CTRL+C in the command prompt.

Summary

In this exercise, you created an ASP.NET Core web application and an Azure AD application that allows guest users from partner Azure AD directories to sign in and access the application. You then invited a guest user to the directory and signed into the application with this user.

Test your knowledge

1. Microsoft Identity supports multiple topology options. Which of the following options does not support using Microsoft Accounts for user sign-in?

○ Consumer

○ Azure AD Business to Business (B2B)

○ Azure AD Business to Customer (B2C)

2. How do Azure AD B2B and B2C differ?

○ Azure AD B2B refers to users who are already paid customers while B2C

○ refers to leads, or potential customers who haven't yet purchased a product.

○ Azure AD B2B refers to the collaboration of users in two organizations who have entered into formal partnership while B2C is more of a loose partnership between organizations.

○ Azure AD B2B refers to users sharing or collaborating between two organizations, while B2C is more about businesses implementing an application for their customers.

Check your answers