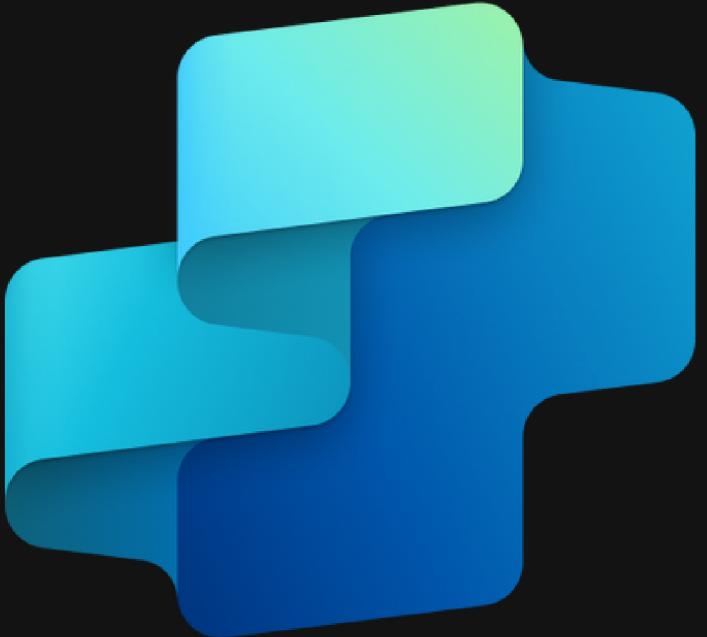


- 22 -

End-User Authentication in Copilot Studio



MONTHLY MASTERY

FEATURE-A-DAY

with Copilot Studio



Handcrafted Insights by
Katerina Chernevskaya

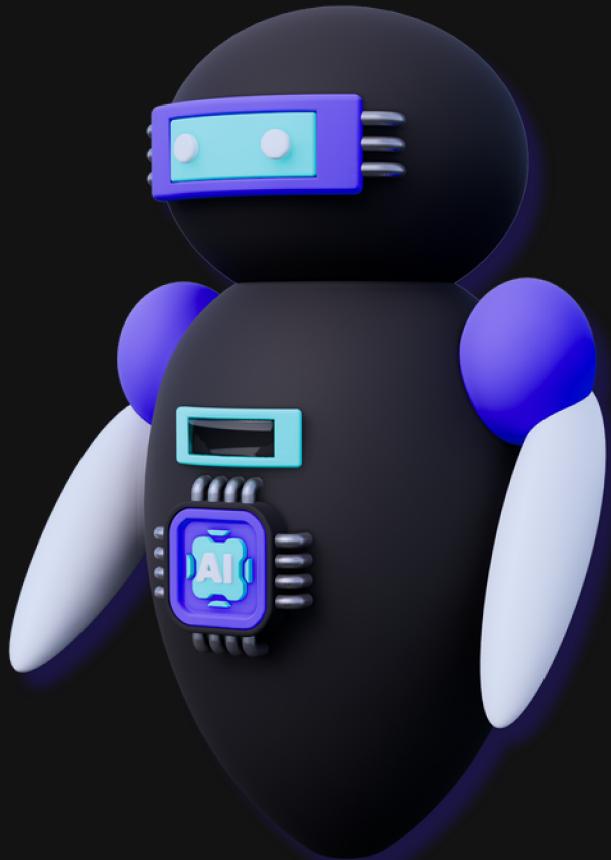


End-User Authentication

Introduction

User authentication within Microsoft Copilot Studio bot conversations adds a crucial layer of **security** and **personalization**.

It enables the bot to access **basic** user properties like **name** and **ID**, and more importantly, it allows for a sign-in process within the chat.



Handcrafted Insights by
Katerina Chernevskaya



End-User Authentication Configuration

Integrating user authentication into your Copilot Studio topics **enhances** customer interaction, enabling sign-in within the chat itself. Once authenticated, conversations can be **personalized** with user-specific **variables**, and the copilot can access **back-end systems** on behalf of the user. To utilize this feature, you first need to set up user **authentication with Microsoft Entra ID**, ensuring a secure and seamless experience.



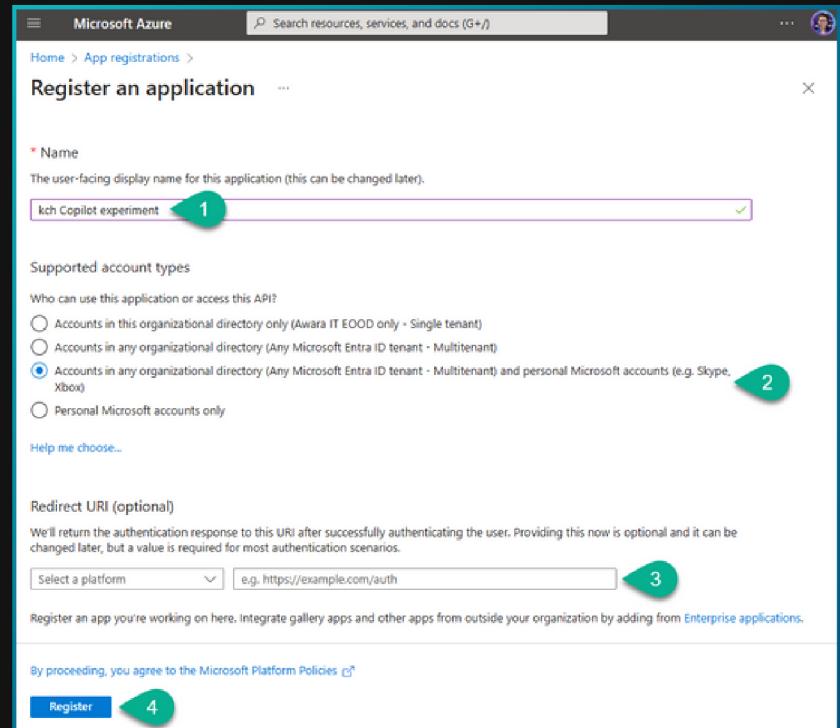
Handcrafted Insights by
Katerina Chernevskaya



Microsoft Entra ID App Registration

Start by logging into <https://portal.azure.com> using an admin account from the same tenant as your Copilot. Navigate to [App registrations](#) and select [+New registration](#).

1. Name your App registration.
2. Select the all-encompassing [Accounts in any organizational directory](#) option.
3. Leave the [Redirect URI](#) as a cliffhanger for now.
4. Hit [Register](#).



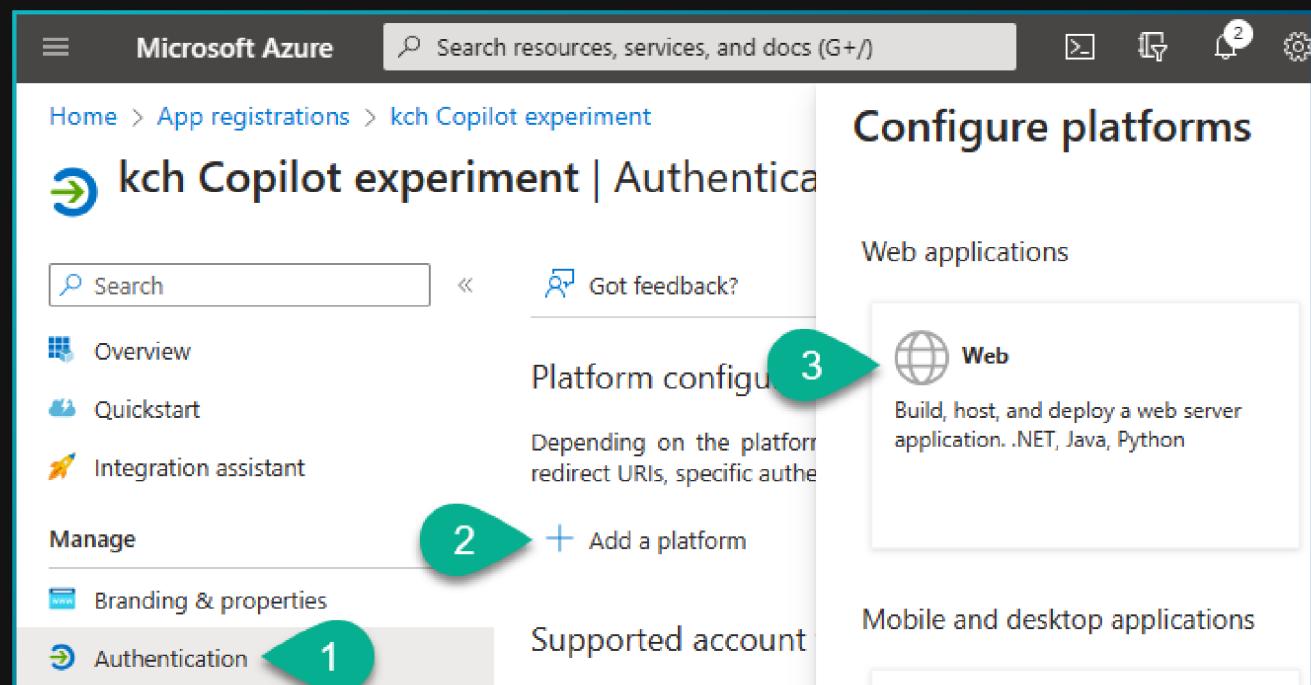
Handcrafted Insights by
Katerina Chernevskaya



Microsoft Entra ID

Redirect URL

1. In your App registration, navigate to [Authentication](#).
2. Click on [Add a platform](#).
3. Under [Configure platforms](#), choose [Web](#).



Handcrafted Insights by
Katerina Chernevskaya



Microsoft Entra ID

Redirect URL

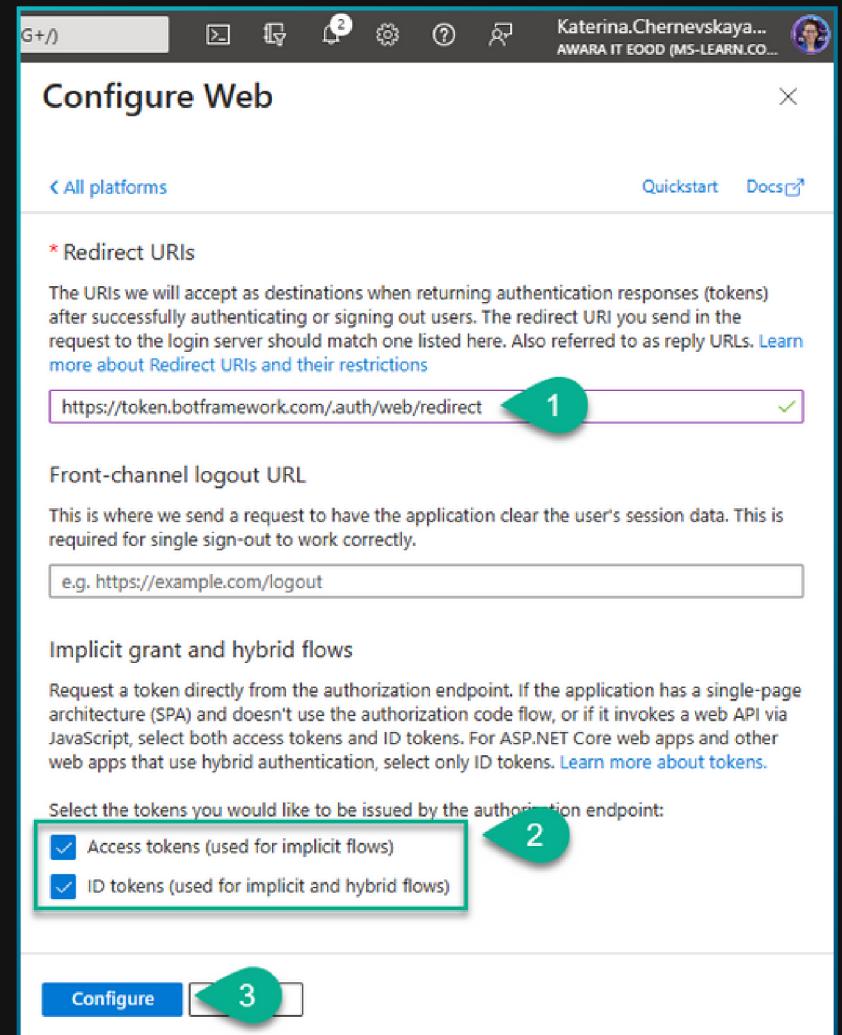
Configure Redirect URL:

1. Enter the provided Bot Framework token URLs in the **Redirect URIs** section:

<https://token.botframework.com/.auth/web/redirect>

2. In the **Implicit grant and hybrid flows** section, make sure to activate both **Access tokens** and **ID tokens**.

3. Hit **Configure**.



Handcrafted Insights by
Katerina Chernevskaya



Microsoft Entra ID Redirect URL

On the Authentication page select [Add URI](#) to add:

<https://europe.token.botframework.com/.auth/web/redirect>

The screenshot shows the 'Web' section of the Microsoft Entra ID configuration. Under 'Redirect URIs', it lists two entries: 'https://token.botframework.com/.auth/web/redirect' and 'https://europe.token.botframework.com/.auth/web/redirect'. The second entry is highlighted with a green checkmark and a trash can icon. A warning message at the top states: '⚠ This app has implicit grant settings enabled. If you are using any of these URLs in a SPA with MSAL.js 2.0, you should migrate URLs.' Below the list is a button labeled 'Add URI'.



Handcrafted Insights by
Katerina Chernevskaya



Microsoft Entra ID

Client Secret

To create a client secret for your bot in Azure:

1. Navigate to [Certificates & secrets](#).
2. Click [New client secret](#) in the Client secrets area.
3. Name your secret.
4. Choose an appropriate expiry period for the secret, ideally the shortest that suits your copilot's lifespan.
5. Select [Add](#) to generate the secret.
6. Safely store the secret's Value, as it's crucial for later configuring your bot's authentication.

The screenshot shows the Microsoft Entra ID portal interface. On the left, there is a sidebar with various options: Quickstart, Integration assistant, Manage, Branding & properties, Authentication, and Certificates & secrets (which is highlighted with a green circle labeled '1'). The main content area has tabs for Certificates (0), Client secrets (1) (which is underlined and highlighted with a green circle labeled '2'), and Federated credentials (0). Below the tabs, there is a description: 'A secret string that the application uses to prove its identity when requesting a token.' Under the 'Client secrets' tab, there is a table with columns for Description, Expires, and Value. A new row is being added, with the 'Description' field containing 'kch copilot exp secret', the 'Expires' field showing '4/20/2024', and the 'Value' field showing 'Dzi8Q~6YttBzl'. A green circle labeled '3' points to the 'Value' column.

Description	Expires	Value
kch copilot exp secret	4/20/2024	Dzi8Q~6YttBzl



Handcrafted Insights by
Katerina Chernevskaya

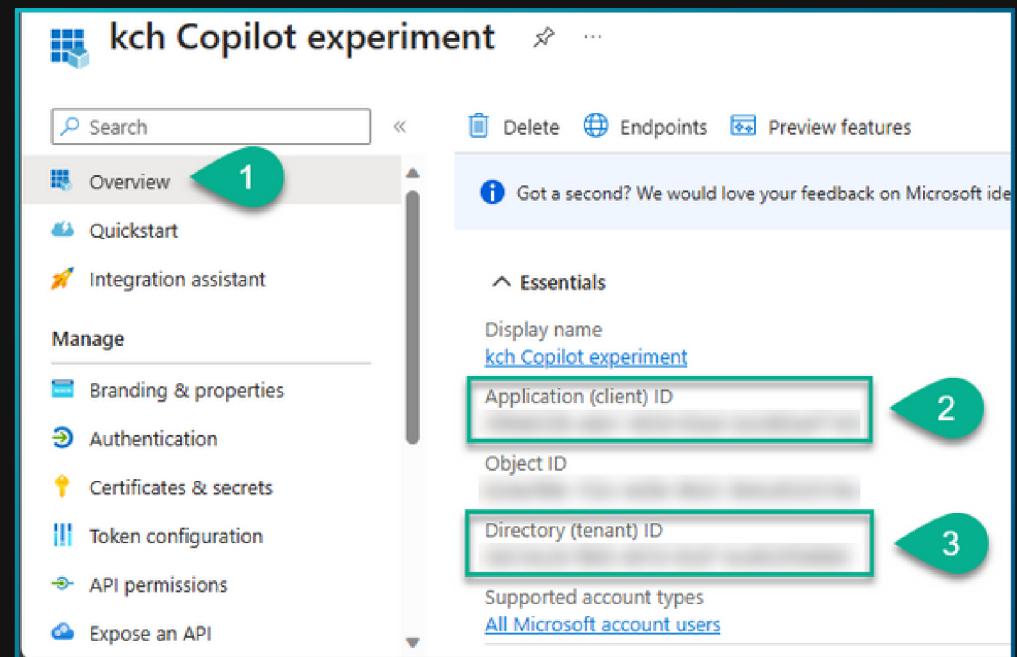


Microsoft Entra ID

ID Values

Head over to the [Overview](#) page in Azure, where you'll need to copy two critical pieces of information: the [Application \(client\) ID](#) and the [Directory \(tenant\) ID](#) values.

Keep these values safe along with the secret you created earlier. They are essential for the next step in configuring your bot's authentication setup.



Handcrafted Insights by
Katerina Chernevskaya



Microsoft Entra ID API Permissions

Let's set up API permissions for your copilot in Azure:

1. Go to [API permissions](#) in your Azure portal.
2. Click on [Grant admin consent for \[\]](#) and confirm with [Yes](#). If the option isn't available, a tenant administrator will need to grant this consent.
3. Then, add a new permission by selecting [Microsoft Graph](#).
4. Choose [Delegated permissions](#), and under [OpenId permissions](#), enable [openid](#) and [profile](#).
5. Finally, click [Add permissions](#) to finalize.

The screenshot shows the 'Configured permissions' section of the Microsoft Entra ID API permissions page. It includes a sidebar with options like 'Integration assistant', 'Manage', 'Branding & properties', 'Authentication', 'Certificates & secrets', 'Token configuration', 'API permissions' (which is selected), and 'Expose an API'. The main area displays a table of permissions:

API / Permissions n...	Type	Description	Admin consent req...	Status
openid	Delegated	Sign users in	No	...
profile	Delegated	View users' basic profile	No	...
User.Read	Delegated	Sign in and read user ...	No	Granted for Awara IT EO... Grant Admin Consent Edit



Handcrafted Insights by
Katerina Chernevskaya



Microsoft Entra ID

Custom Scope

These steps will help us to define a custom scope for your copilot, which is key for setting user and admin roles and access:

1. Head over to [Expose an API](#) and click on [Add a scope](#).
2. Fill in the details, giving the scope a relevant name (like [Test.Read](#)), choosing [Admins and users](#) for consent, and providing a clear admin consent name and description.
3. Ensure the [State](#) is [Enabled](#).
4. Finally, click [Add scope](#) to complete the process.

Add a scope

Scope name * ⓘ
 ✓

Who can consent? ⓘ
 Admins and users Admins only

Admin consent display name * ⓘ
 ✓

Admin consent description * ⓘ

User consent display name ⓘ

User consent description ⓘ

State ⓘ
 Enabled Disabled

[Add scope](#) [Cancel](#)



Handcrafted Insights by
Katerina Chernevskaya

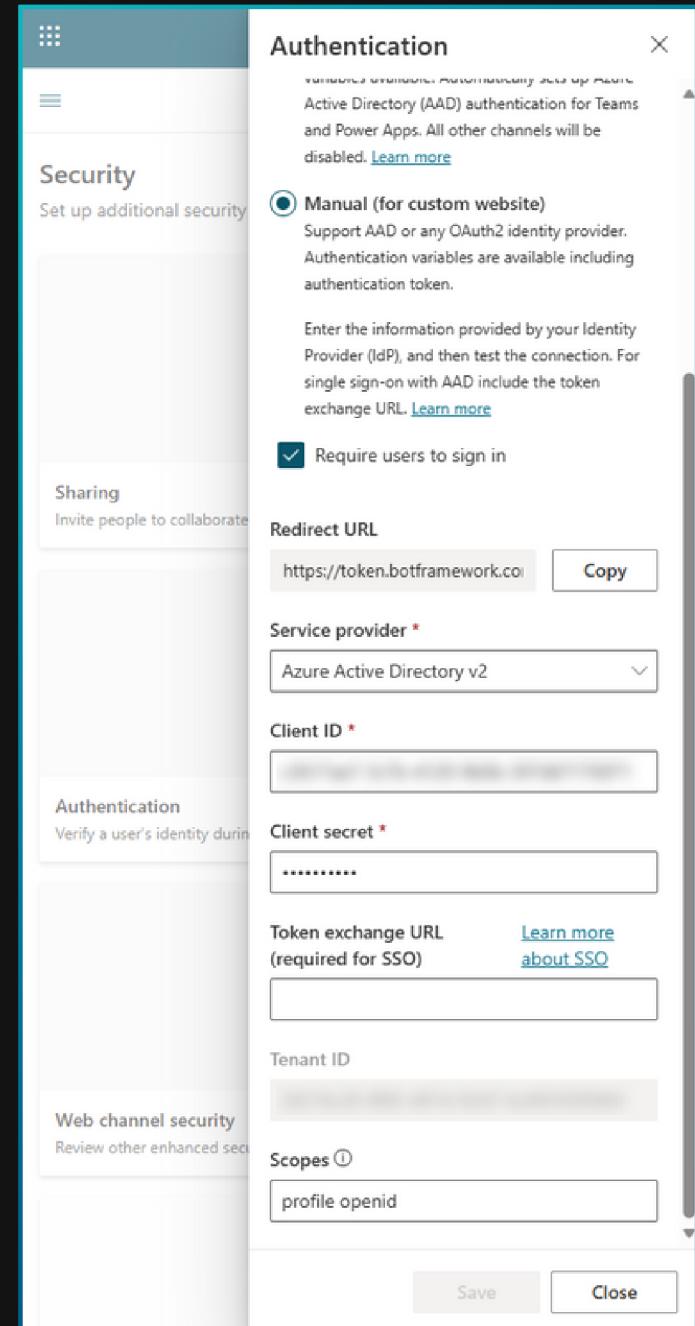


Microsoft Copilot Studio

Configure Authentication

In Microsoft Copilot Studio, here's how to set up authentication:

1. Navigate to [Settings](#), then [Security](#), and select [Authentication](#).
2. Choose [Manual Authentication \(for custom website\)](#).
3. Turn on the [Require users to sign in](#).
4. Select [Azure Active Directory v2](#) as the service provider, and add the [Client ID](#) and [Client Secret](#) from Azure. For scopes, use [profile openid](#).
5. Don't forget to hit [Save](#) to apply these changes.



Handcrafted Insights by
Katerina Chernevskaya

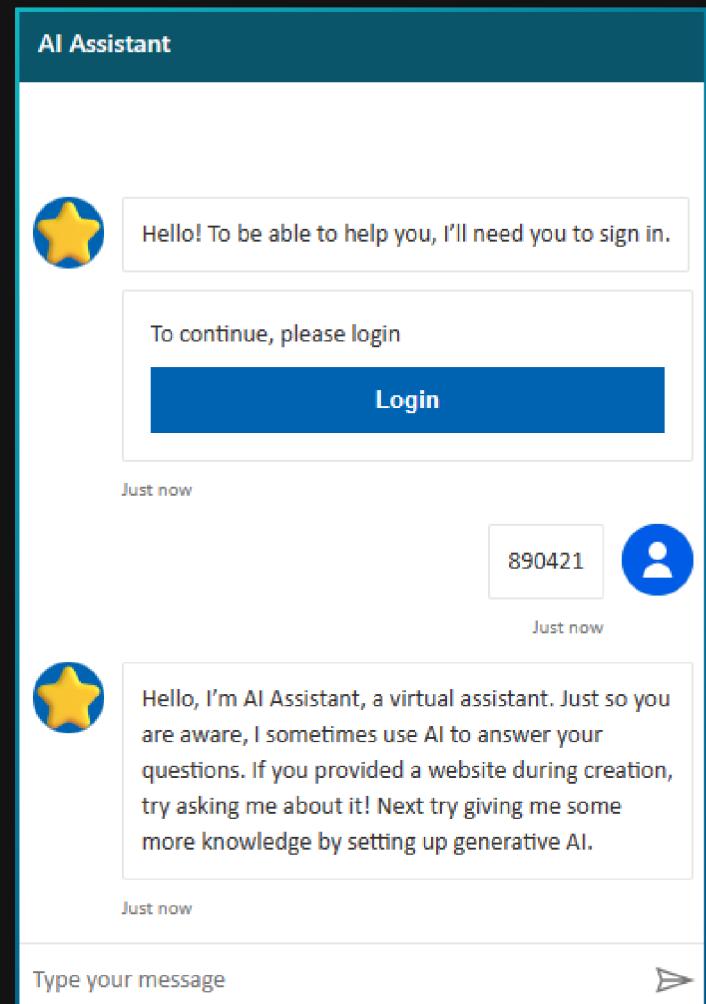


Microsoft Copilot Studio

Test Your Copilot

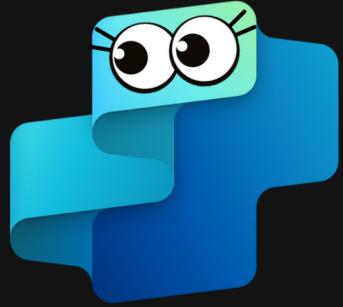
To test your copilot with authentication:

1. Publish Your Copilot.
2. In the Test bot pane or on the Demo website, start the interaction.
3. The copilot should respond with a login prompt. Click [Login](#).
4. A browser tab will open for [signing in](#). Follow the sign-in process.
5. After signing in, copy the [validation code](#) shown.
6. Paste this code back in the copilot chat to finalize the sign-in process.



Handcrafted Insights by
Katerina Chernevskaya





Today's Task: Implementing and Testing Authentication

1. Configure Authentication in Azure

Set up user authentication for your copilot in the Azure portal, including app registration, API permissions, and defining custom scopes.

2. Update Copilot Studio Settings

In Microsoft Copilot Studio, adjust the Security settings to enable and configure authentication with the details from Azure.

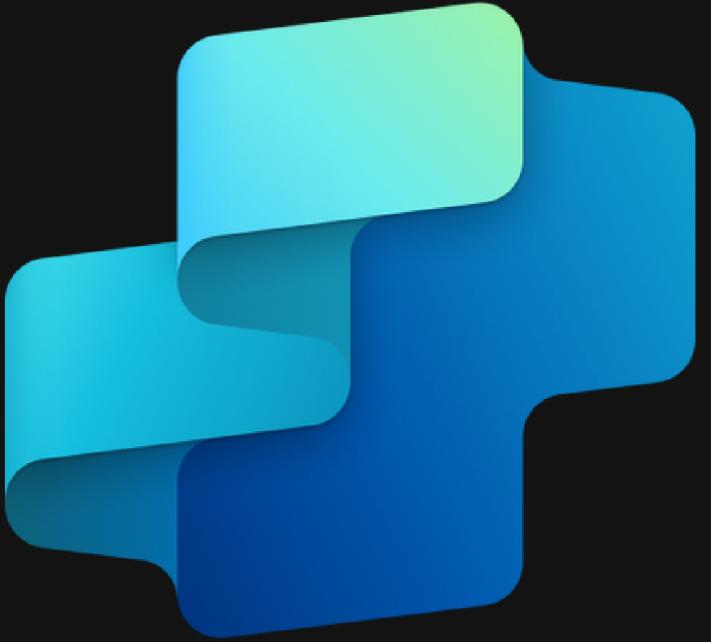
3. Test the Authentication Process

Publish your copilot and conduct a test run, ensuring the sign-in process and validation code work as intended.



Handcrafted Insights by
Katerina Chernevskaya





MONTHLY MASTERY

FEATURE-A-DAY

with Copilot Studio



Handcrafted Insights by
Katerina Chernevskaya

Follow for more!