- 22 -

End-User Authentication
in Copilot Studio

MONTHLY MASTERY

FEATURE-A-DAY

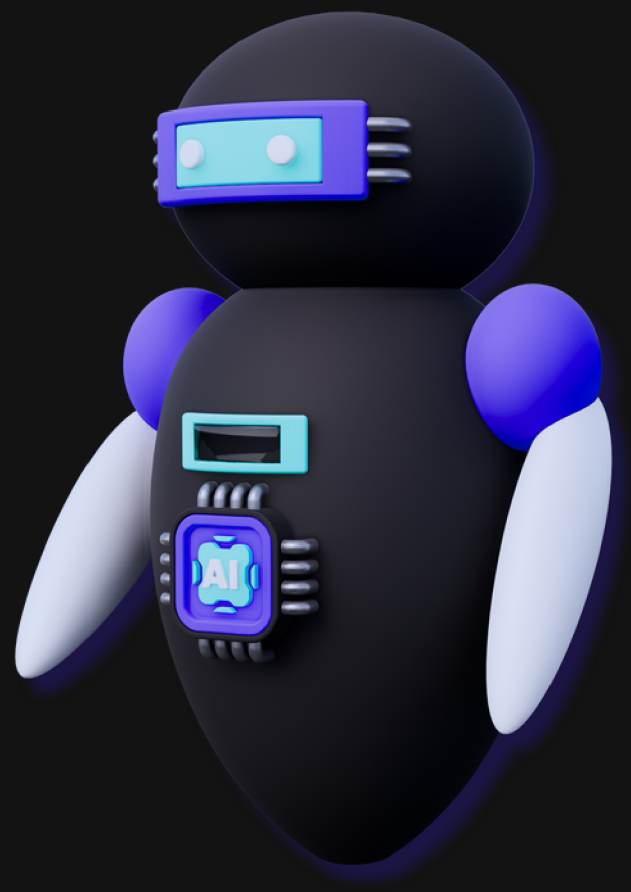
with Copilot Studio

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

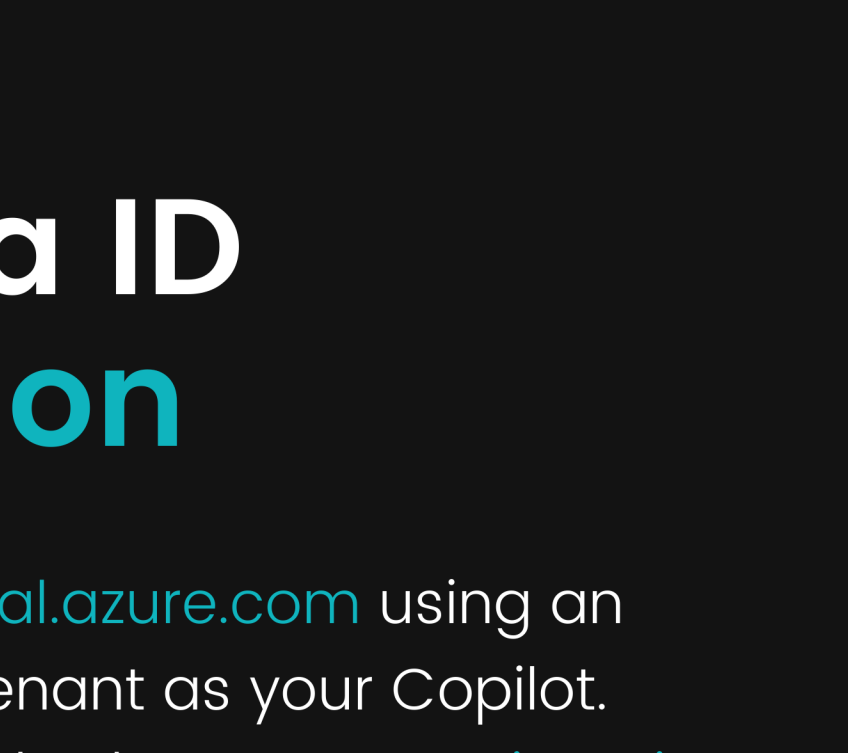
Integrating user authentication into your Copilot Studio topics enhances customer interaction, enabling sign-in within the chat itself. Once authenticated, conversations can be personalized with user-specific variables, and the copilot can access back-end systems on behalf of the user. To utilize this 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.

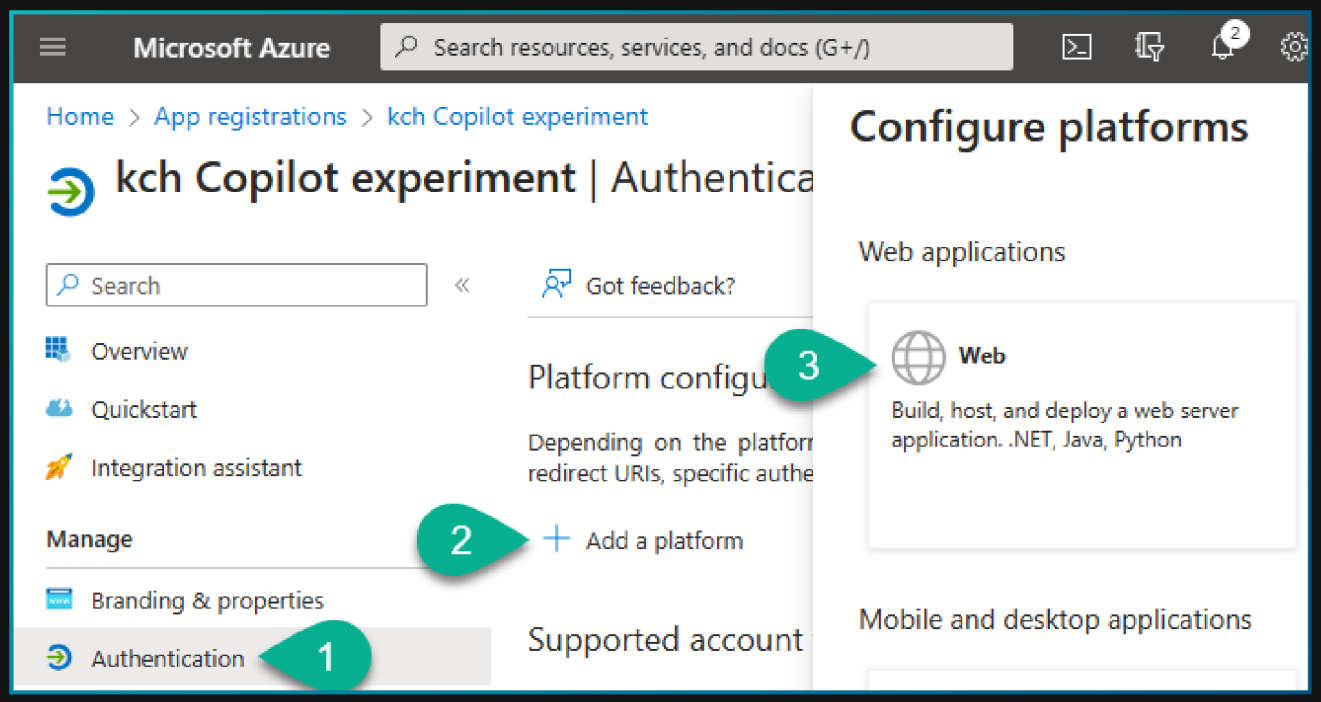
1. Name your App registration.
2. Select the all-encompassing Accounts in any organizational directory option.
3. Leave the Redirect URI as a cliffhanger for now.
4. Hit Register.



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.

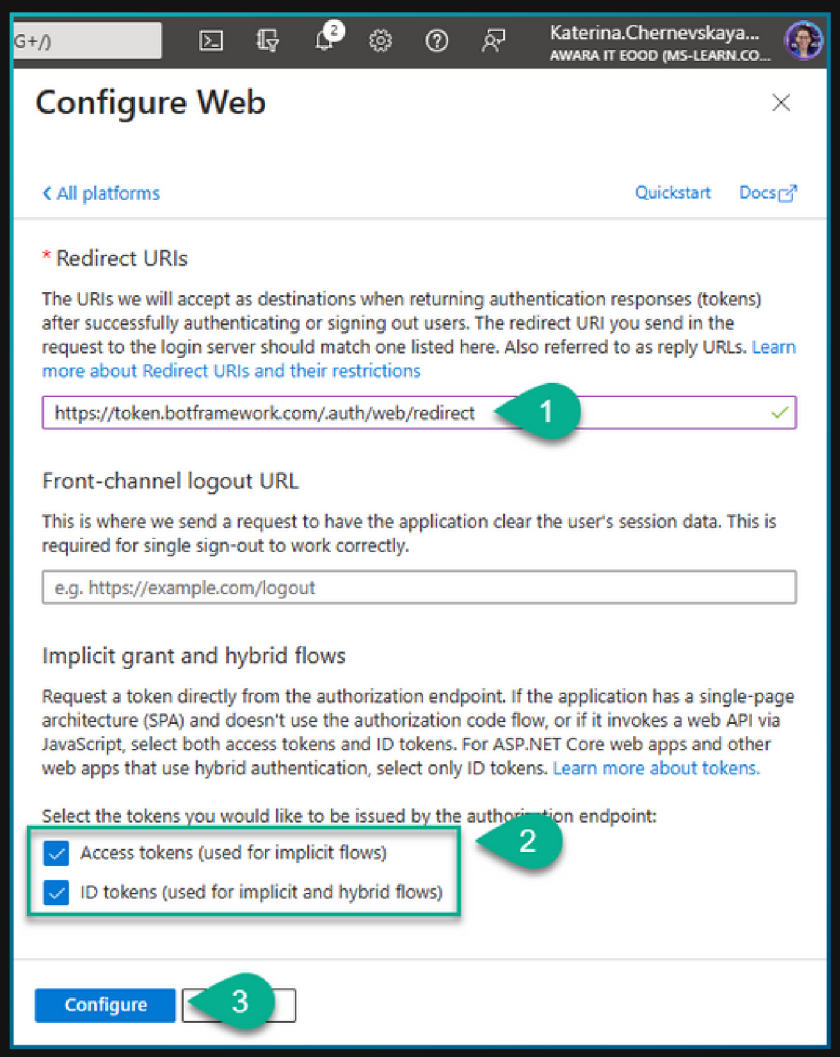


Handcrafted Insights by
Katerina Chernevskaya

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.

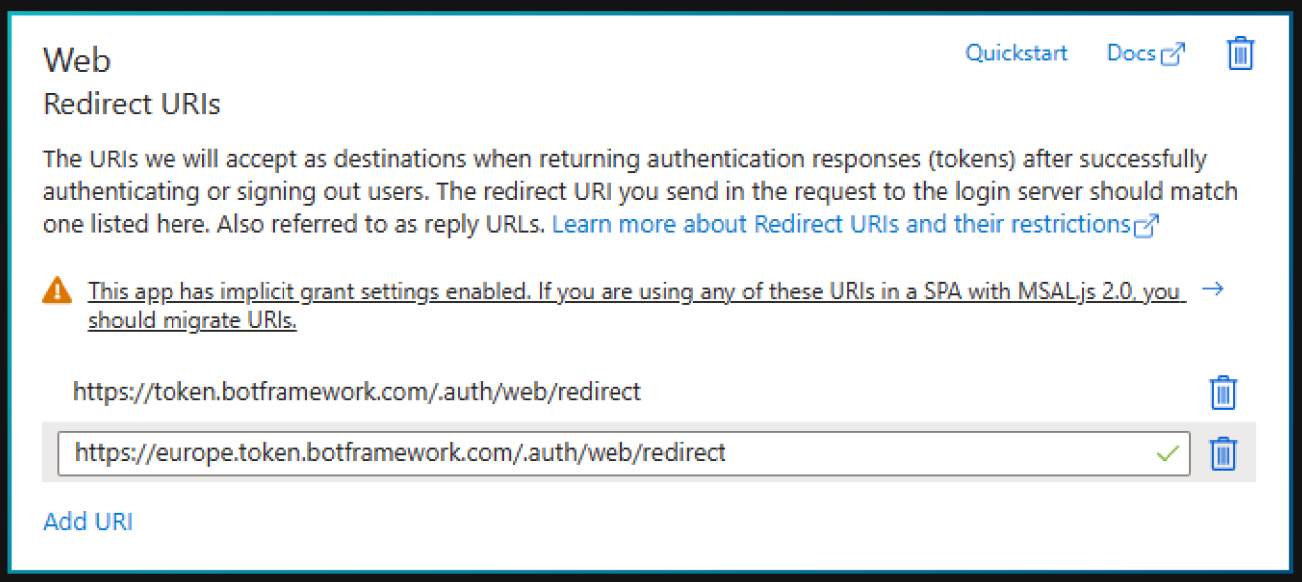


Handcrafted Insights by
Katerina Chernevskaya

Microsoft Entra ID
Redirect URL

On the Authentication page select Add URI to add:

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

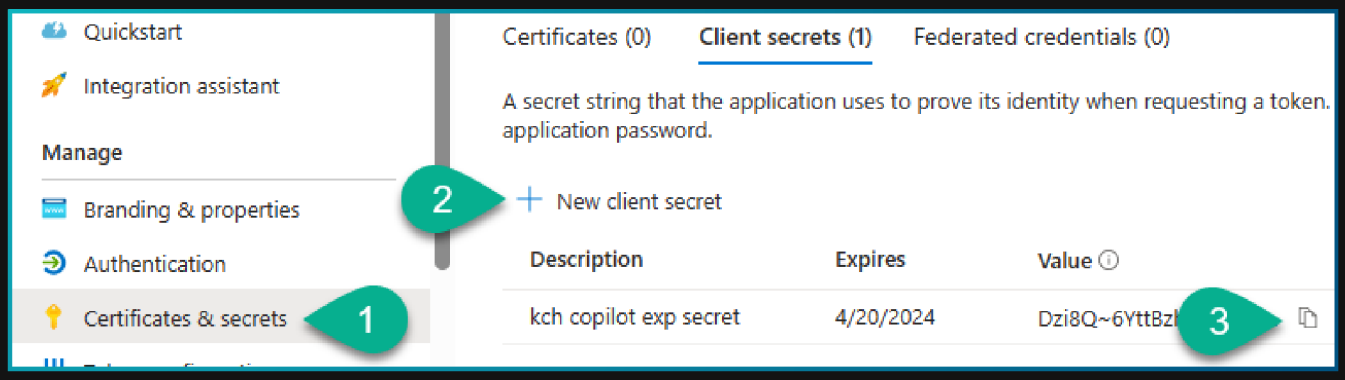


Handcrafted Insights by
Katerina Chernevskaya

Microsoft Entra ID
Client Secret

To create a client secret for your bot in Azure:

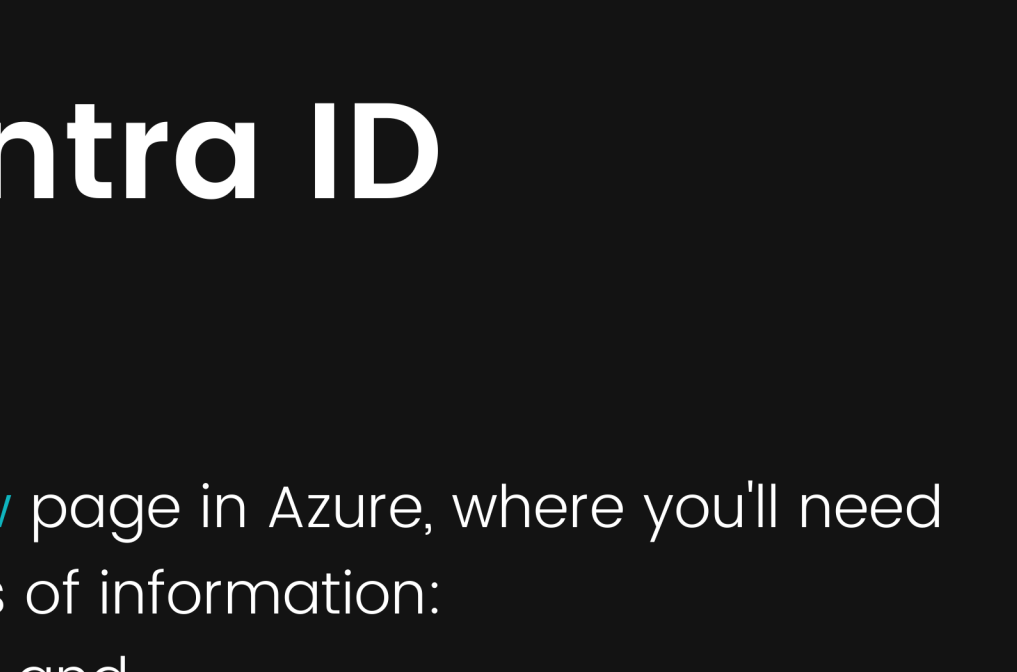
1. Navigate to Certificates & secrets.
2. Click New client secret in the Client secrets area.
3. Name your secret.
4. Choose an appropriate expiry period for the secret, ideally the shortest that suits your copilot's lifespan.
5. Select Add to generate the secret.
6. Safely store the secret's Value,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



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.

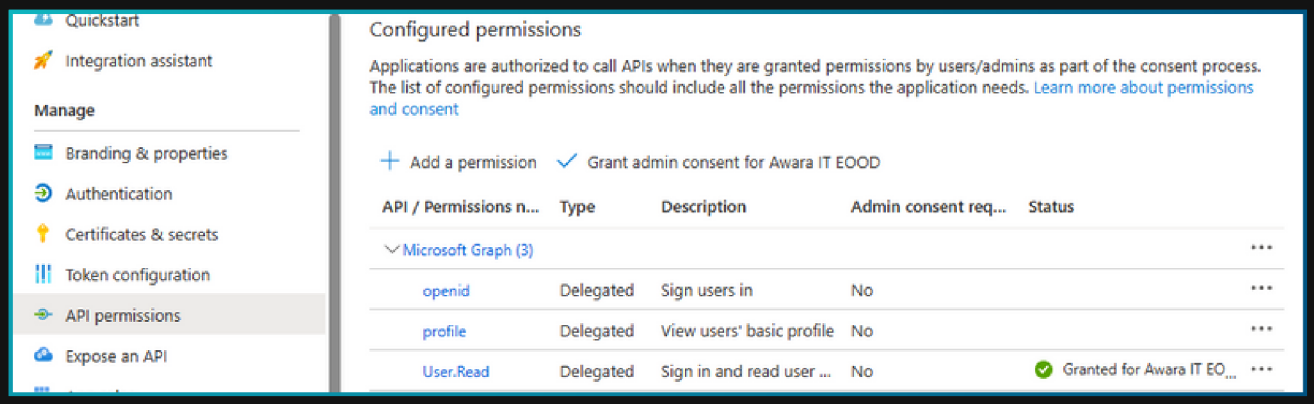


Handcrafted Insights by
Katerina Chernevskaya

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.

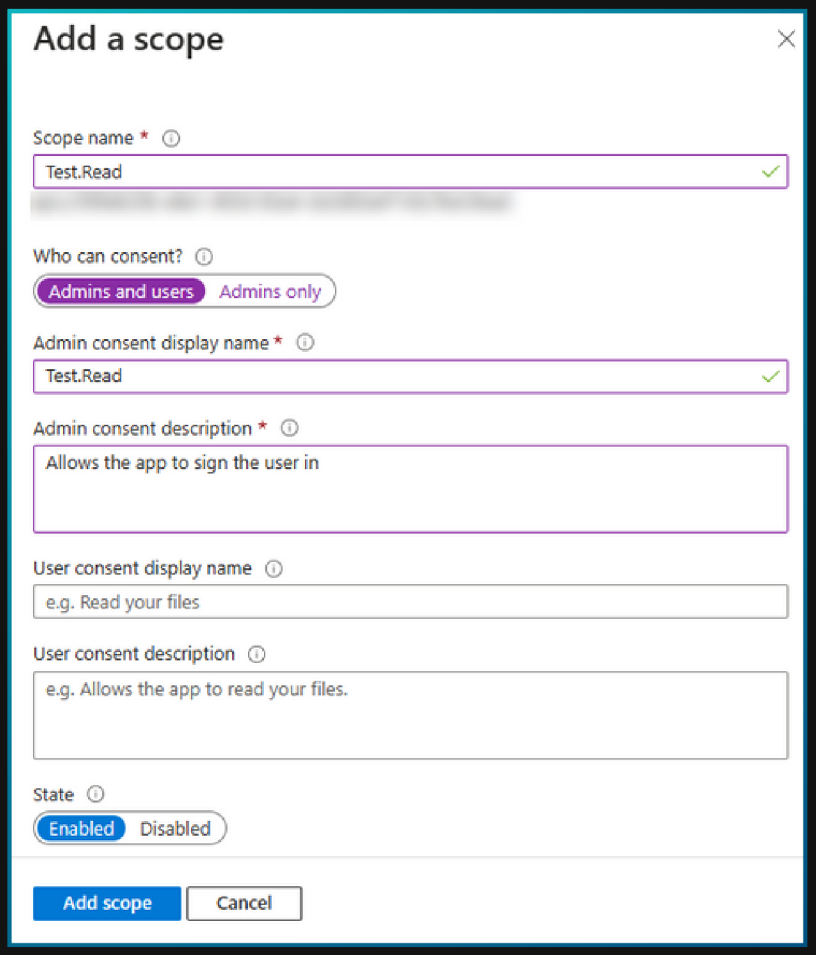


Handcrafted Insights by
Katerina Chernevskaya

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.

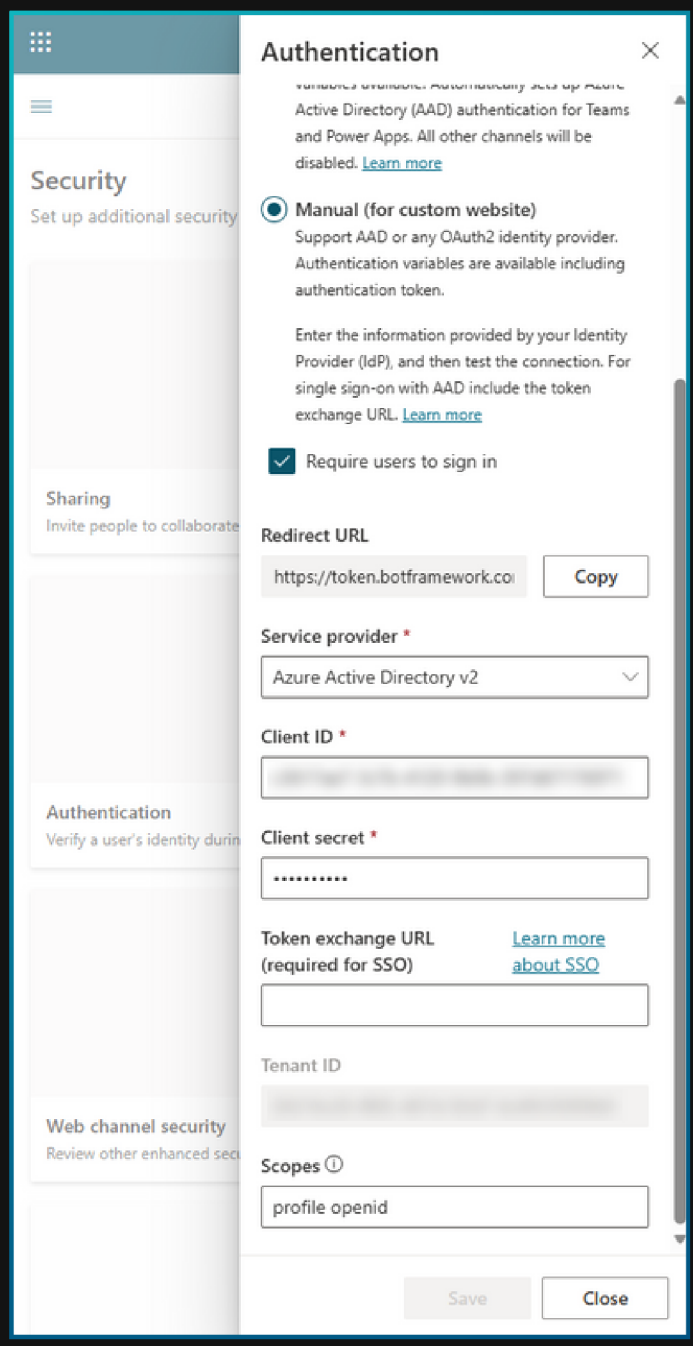


Handcrafted Insights by
Katerina Chernevskaya

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.

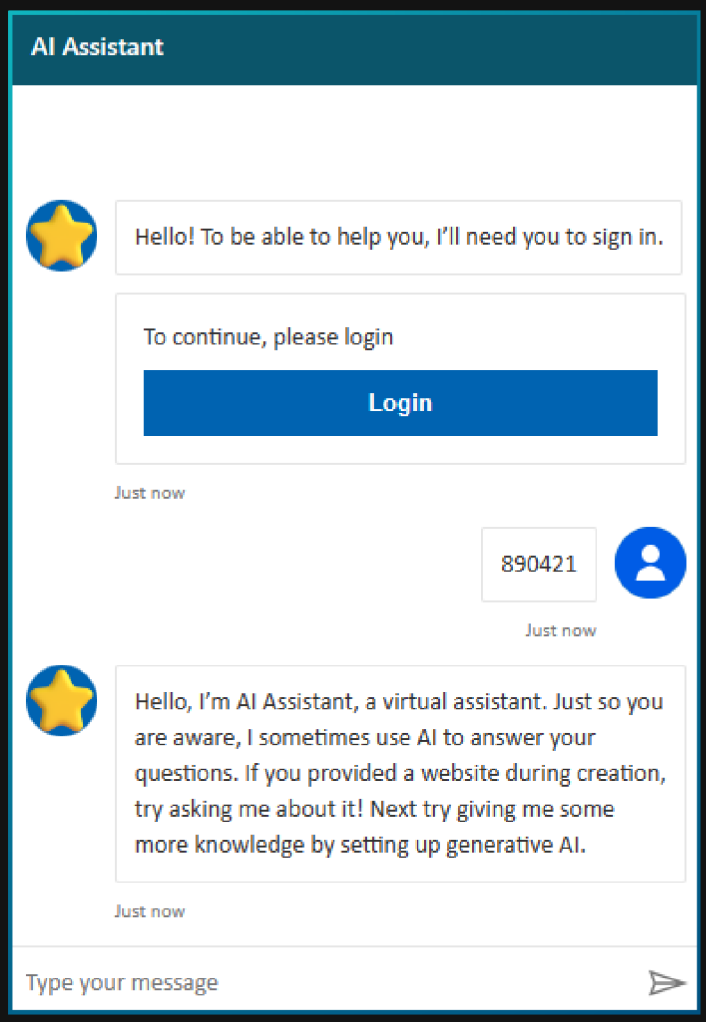


Handcrafted Insights by
Katerina Chernevskaya

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!