**Microsoft**

# Take the guesswork out of secure and compliant access to SAP from Copilot and Power Platform with Entra ID

ROOM: 2202, 4/25/2024 11:15 AM CET
Martin Raepple, Martin Pankraz

# Agenda

- Scenario Overview

- Solution Architecture

- Hands-on instructions

- *Exercise 1*: Launch the SAP Product Search Copilot

- *Exercise 2*: Troubleshoot the SAP access in Power Automate

- *Exercise 3*: Fix the login error in SAP

- *Exercise 4*: Test SAP data access with the fixed flow

- *Exercise 5*: Change the user's authorizations in SAP

# Scenario Overview

# Build an AI-powered, secure & compliant copilot for searching products in an SAP system



Respond to unknown user intents* with generative answers

Only return data the user has access to in the SAP system. Authorizations in the backend may change at any time!
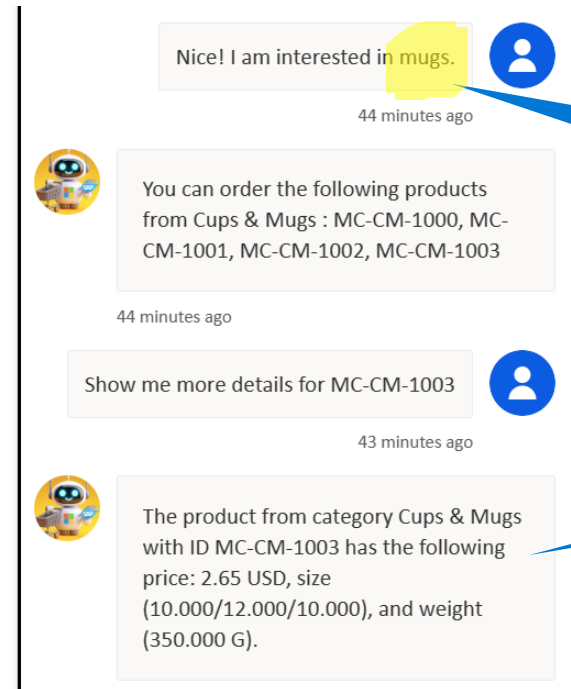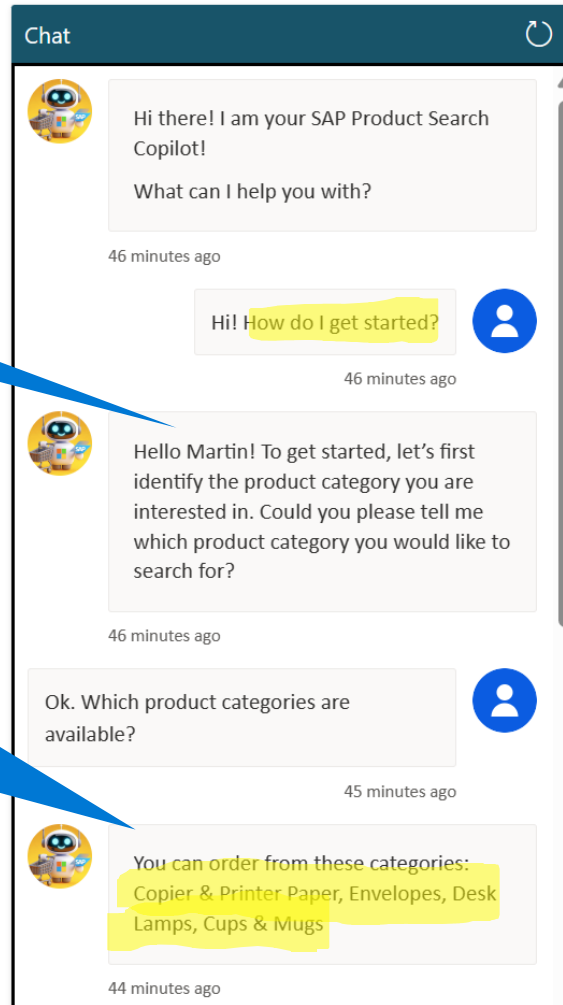
Understand incomplete or misspelled user input

Support Single Sign-On (SSO) from Entra to SAP

**Chat conversation:**

Hi there! I am your SAP Product Search Copilot!

What can I help you with?

46 minutes ago

Hi! How do I get started?

46 minutes ago

Hello Martin! To get started, let's first identify the product category you are interested in. Could you please tell me which product category you would like to search for?

46 minutes ago

Ok. Which product categories are available?

45 minutes ago

You can order from these categories: Copier & Printer Paper, Envelopes, Desk Lamps, Cups & Mugs

44 minutes ago

Nice! I am interested in mugs.

44 minutes ago

You can order the following products from Cups & Mugs : MC-CM-1000, MC-CM-1001, MC-CM-1002, MC-CM-1003

44 minutes ago

Show me more details for MC-CM-1003

43 minutes ago

The product from category Cups & Mugs with ID MC-CM-1003 has the following price: 2.65 USD, size (10.000/12.000/10.000), and weight (350.000 G).

✅ **Auditability**: Each data access from Copilot to SAP can be traced back to an individual.

✅ **Confidentiality**: Only data the user is allowed to see can be accessed in SAP from Copilot

* The goal or purpose that a user has within the context of a conversation with a customer service chatbot.

# High-level Solution Design

Entra ID Tenant

jdoe@bestruncorp.
onmicrosoft.com

Corporate Firewall

Azure OpenAI

**1** → John Doe (User)

**2** → SAP Product Search Copilot

**3** → Power Automate Flow

**4** ↑

**5** → On-Premise Data Gateway

✓ Authorizations for specific product categories

SAP

Product Catalog

JDOE

☑ Batteries
☐ Calendars
☑ Desk Lamps
☐ Files & Binders
☐ ...

👤 User account

1. User authenticates with Entra ID
2. User starts conversation with SAP Product Search Copilot
3. Copilot calls Power Automate Flow
4. Flow calls Azure OpenAI to determine the user's intended action
5. Flow calls the SAP system *on-behalf-of* the user via On-premise Data Gateway (OPDG)
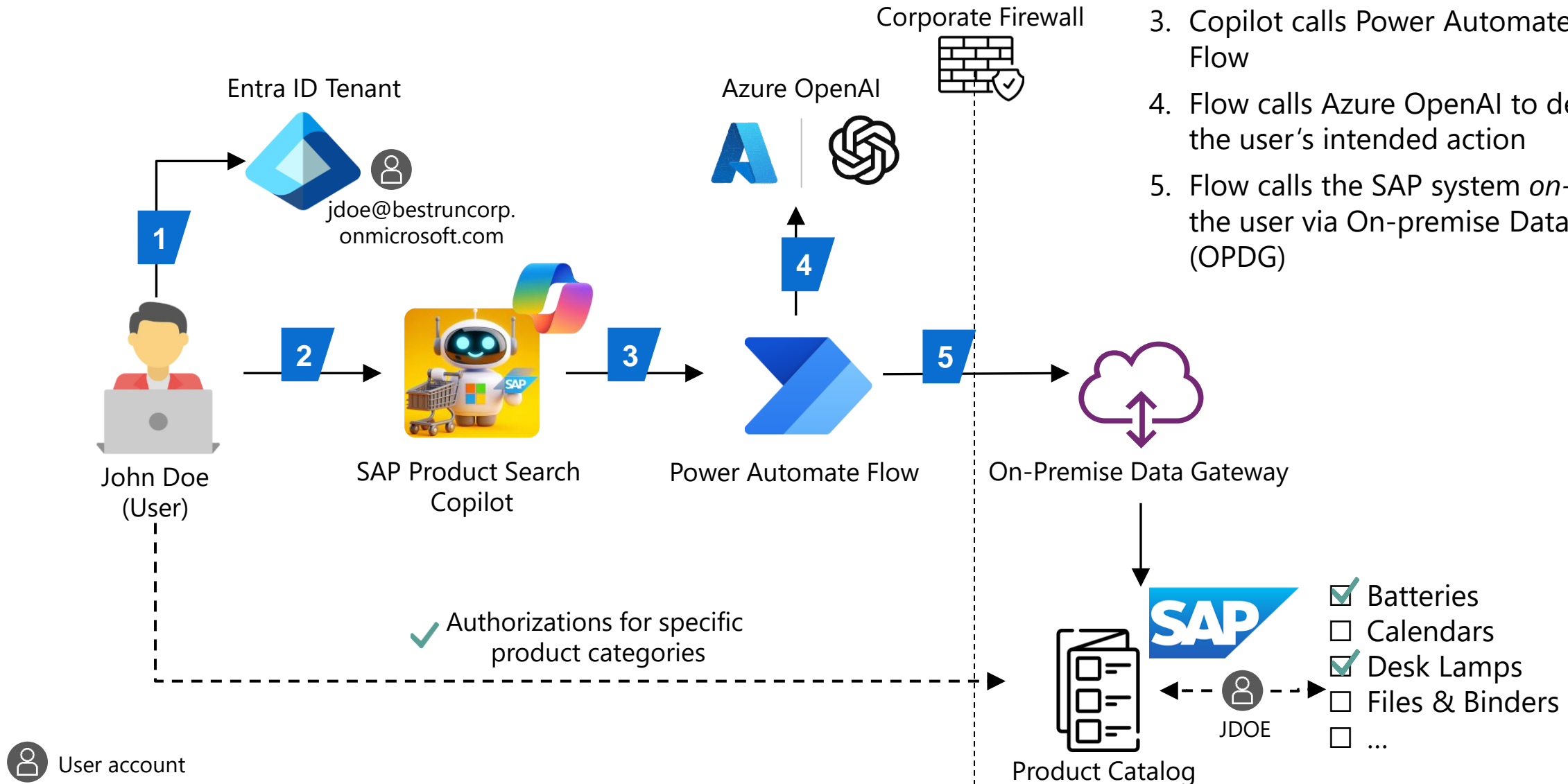
# Solution Architecture

# Secure & compliant access to SAP with Principal Propagation
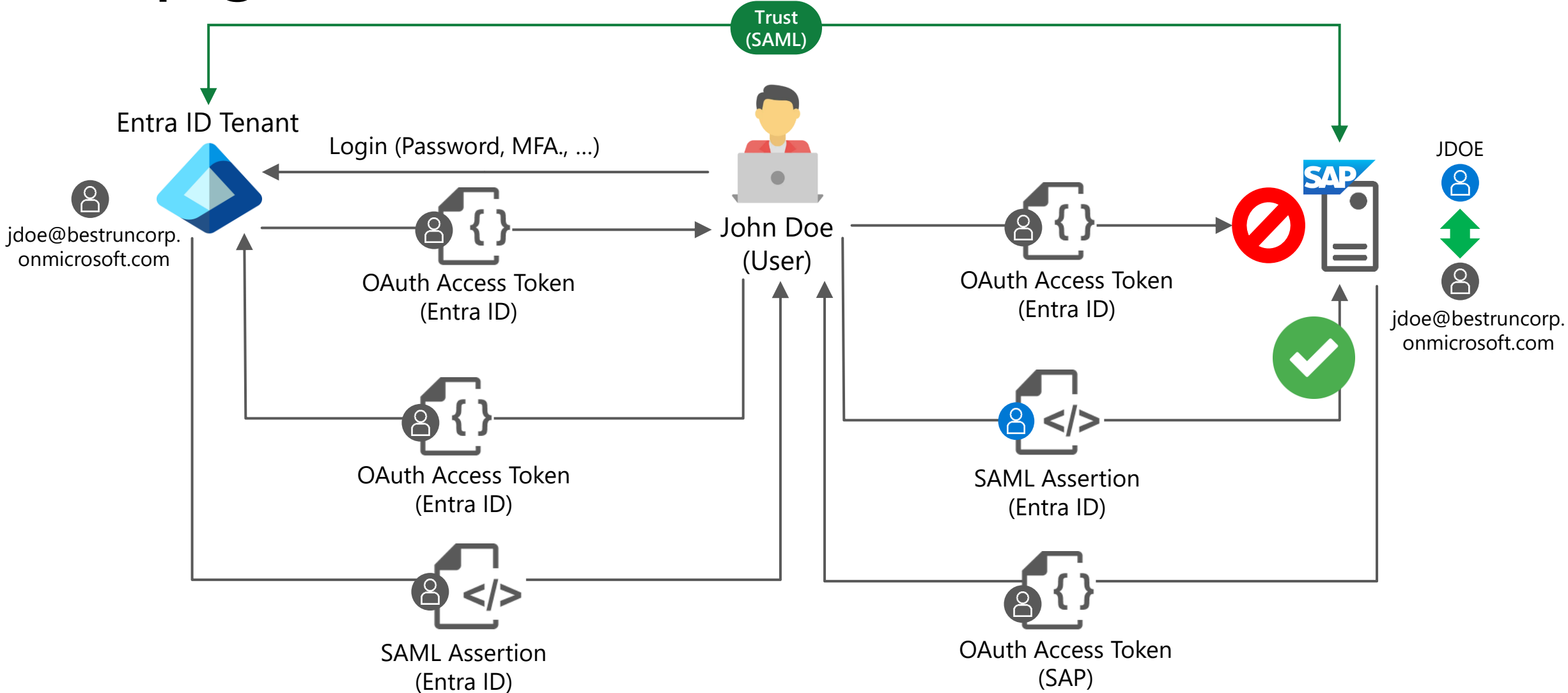
# A sample Entra ID OAuth Access Token in the scenario

```json
{
  "typ": "JWT",
  "alg": "RS256",
  "x5t": "q-23falevZhhD3hm9CQbkP5MQyU",
  "kid": "q-23falevZhhD3hm9CQbkP5MQyU"
}.{
  "aud": "api://66283309-24e0-419f-853f-79176d9d4d22",
  "iss": "https://sts.windows.net/85642982-0095-4777-a3e2-147c5c95af60/",
  "iat": 1713713948,
  "nbf": 1713713948,
  "exp": 1713718547,
  "acr": "1",
  "aio": "ATQAy/8WAAAAOqIhvezkxOYyMyn0s2I1FtWvLCgD+y00Yb/1fgGZr3uhMsEBb2x7LucDoPkzsBRf",
  "amr": [
    "pwd"
  ],
  "appid": "66283309-24e0-419f-853f-79176d9d4d22",
  "appidacr": "0",
  "given_name": "User25",
  "ipaddr": "213.232.102.10",
  "name": "User25",
  "oid": "6edcd404-091b-45c8-a85e-154008ee1d8f",
  "rh": "0.AYEAgilkhZUAd0ej4hR8XJWvYAkzKGbgJJ9BhT95F22dTSKBAL4.",
  "scp": "sap.access",
  "sub": "Sm1NIbu5dYnwGM8j2EFnV4jGGQ1j8V8BJWE6MIF0bmg",
  "tid": "85642982-0095-4777-a3e2-147c5c95af60",
  "unique_name": "user25@bestruncorp.onmicrosoft.com",
  "upn": "user25@bestruncorp.onmicrosoft.com",
  "uti": "xmyQJ9wwRku3WW_UuZwqAA",
  "ver": "1.0"
}.[Signature]
```

Application for which the token has been issued

Issuer of the access token (Entra ID tenant)

Context information (client IP, authentication method)

Identity information

Scope of access

# A sample Entra ID SAML Assertion in the scenario

```xml
<Assertion ID="_3a0dba09-266d-48c7-b287-86e5c3e02000" IssueInstant="2024-04-21T15:47:47.586Z"
    Version="2.0" xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
    <Issuer>https://sts.windows.net/85642982-0095-4777-a3e2-147c5c95af60/</Issuer>
    <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
        ...
        <SignatureValue>
            KVyhgqebPaYGj4Zbo1jfSEDaIeaJhldI7WqHyCCB4Ul3R3mxFxKjoHu3gYlsNXwu/wlic0kn8BnXOm0oAQr4dmb/5Br
    </Signature>
    <Subject>
        <NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress">
            user25@bestruncorp.onmicrosoft.com</NameID>
        <SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
            <SubjectConfirmationData NotOnOrAfter="2024-04-21T16:55:46.514Z"
                Recipient="https://vhcala4hci.bestrun.corp:50001/sap/bc/sec/oauth2/token" />
        </SubjectConfirmation>
    </Subject>
    <Conditions NotBefore="2024-04-21T15:42:47.514Z" NotOnOrAfter="2024-04-21T16:55:46.514Z">
        <AudienceRestriction>
            <Audience>https://vhcala4hci.bestrun.corp</Audience>
        </AudienceRestriction>
    </Conditions>
    <AttributeStatement>
        <Attribute Name="http://schemas.microsoft.com/identity/claims/tenantid">
            <AttributeValue>85642982-0095-4777-a3e2-147c5c95af60</AttributeValue>
        </Attribute>
        <Attribute Name="http://schemas.microsoft.com/identity/claims/displayname">
            <AttributeValue>User25</AttributeValue>
        </Attribute>
        <Attribute Name="http://schemas.microsoft.com/claims/authnmethodsreferences">
            <AttributeValue>
                http://schemas.microsoft.com/ws/2008/06/identity/authenticationmethod/password</Attribu
        </Attribute>
        <Attribute Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname">
            <AttributeValue>User25</AttributeValue>
        </Attribute>
        <Attribute Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress">
            <AttributeValue>user25@bestruncorp.onmicrosoft.com</AttributeValue>
        </Attribute>
        <Attribute Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name">
            <AttributeValue>user25@bestruncorp.onmicrosoft.com</AttributeValue>
        </Attribute>
    </AttributeStatement>
    <AuthnStatement AuthnInstant="2024-04-21T05:03:28.526Z">
        <AuthnContext>
            <AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:Password</AuthnContextClassRef>
        </AuthnContext>
    </AuthnStatement>
</Assertion>
```

Issuer of the access token (Entra ID tenant)

Application for which the token has been issued

Identity information

Context information (authentication method)

# Solution Architecture
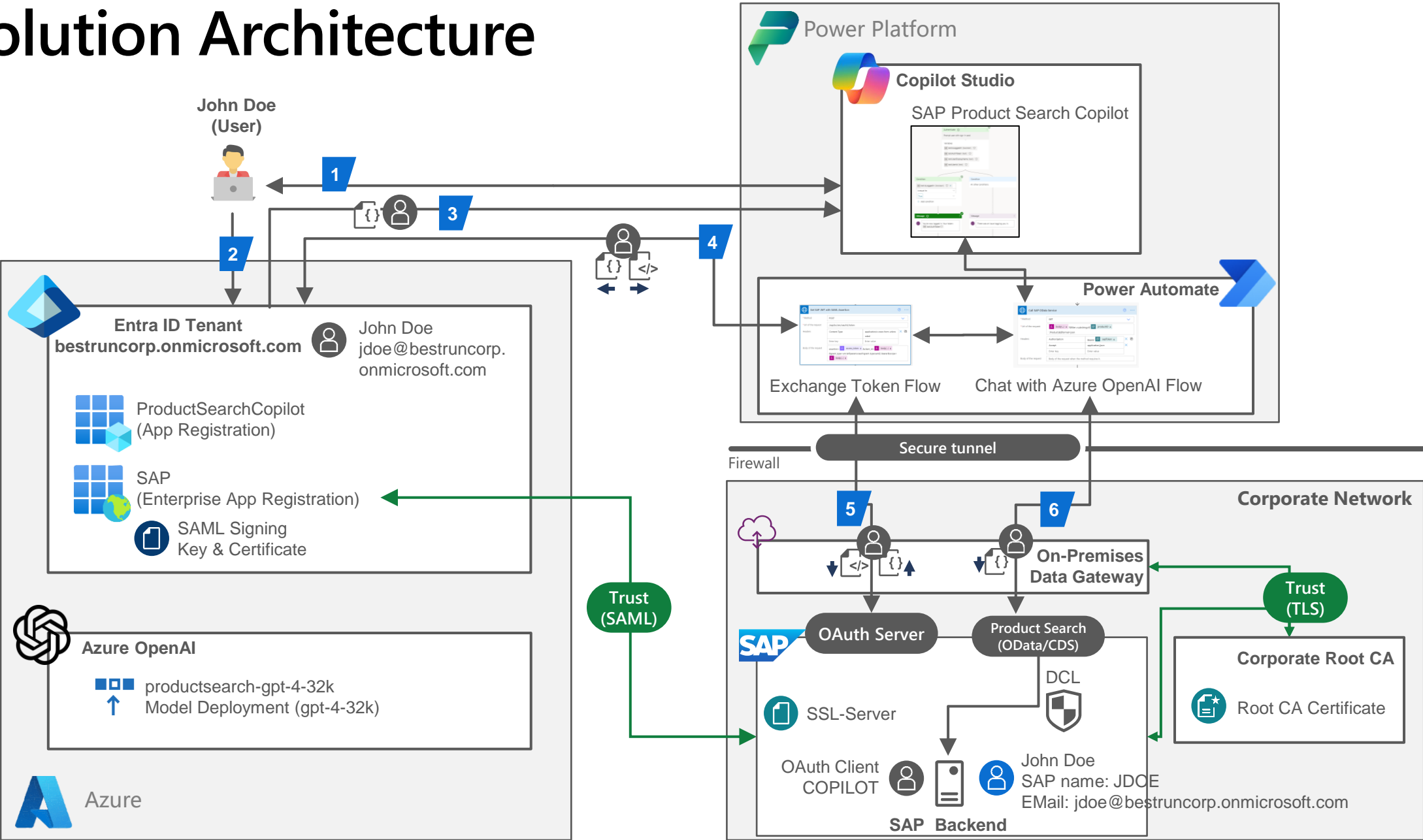
# Hands-on instructions
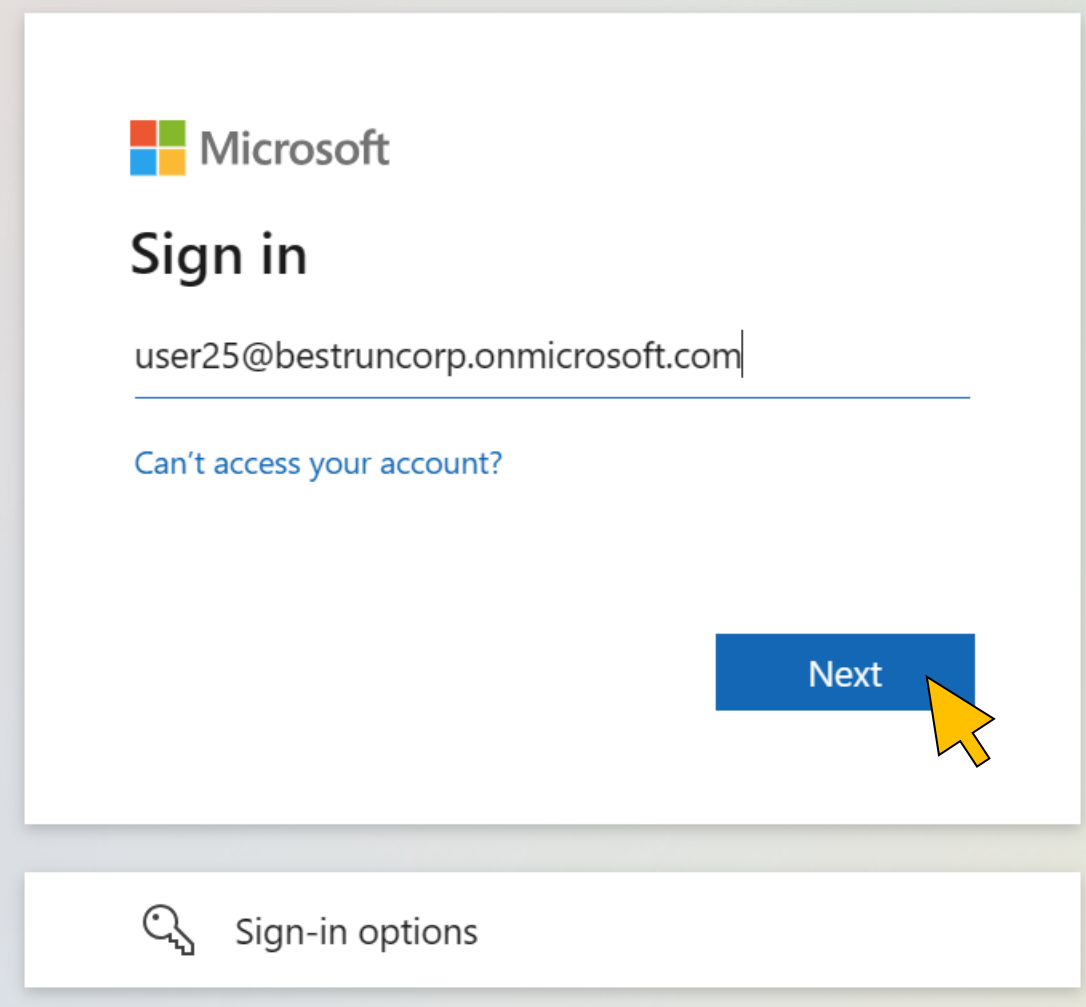
# Hands-on instructions

- Take a user:
  - user1@bestruncorp.onmicrosoft.com
  - user2@bestruncorp.onmicrosoft.com
  - …
  - user20@bestruncorp.onmicrosoft.com
- Password: Welcome24#1234

- *Optional*:
  - Add the following line to your `C:\Windows\System32\drivers\etc\hosts` file
    ```
    172.190.56.1 vhcala4hci.bestrun.corp vhcala4hci
    ```
  - Clone the hands-on repository from https://github.com/raepple/SAPProductSearchCopilot.git
  - Import the file trustedca.crt into your computer's local trusted certificate store with `certmgr.msc`

# Exercise 1

Launch the SAP Product Search Copilot

# 1.1 Sign in to [Copilot Studio](#) as user<N>@bestruncorp.onmicrosoft.com, password Welcome24#1234

# 1.2 Switch to your user's environment bestruncorp_user<N>
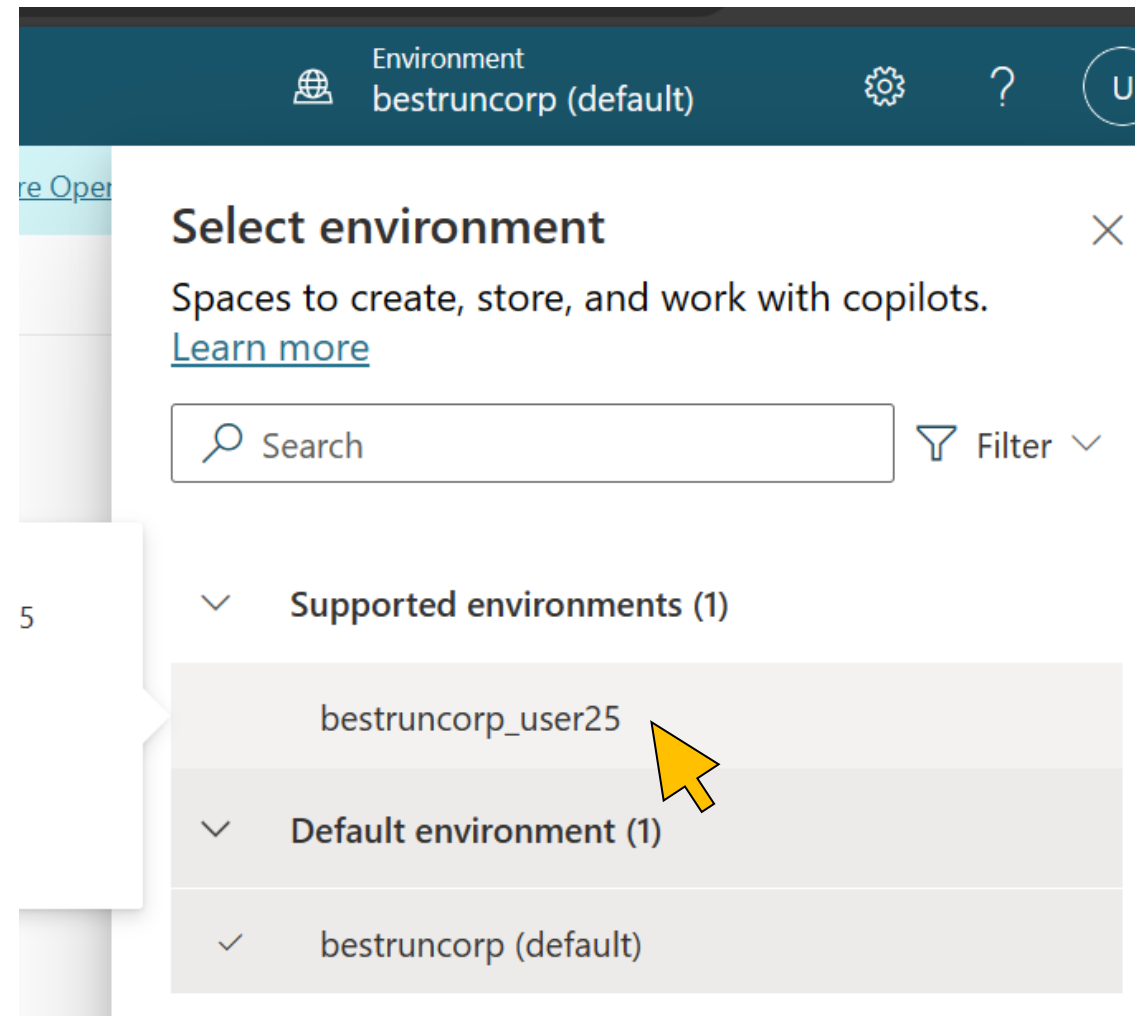
# 1.3 Open the Product Search Copilot

# 1.4 Select Settings → Channels
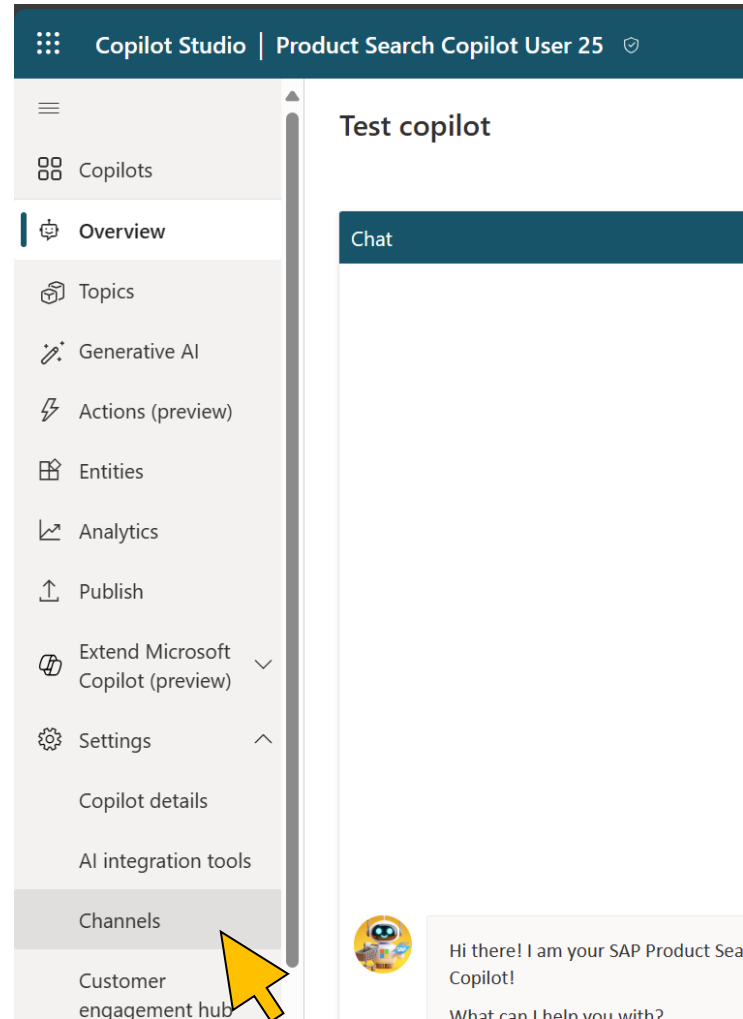
# 1.5: Select Demo website

# 1.6 Copy the URL

Share your website

To invite team members to see your copilot in action, copy the link below.

https://copilotstudio.microsoft.com/environments/6acdd581-5ba2-e39e-82b1-ba1
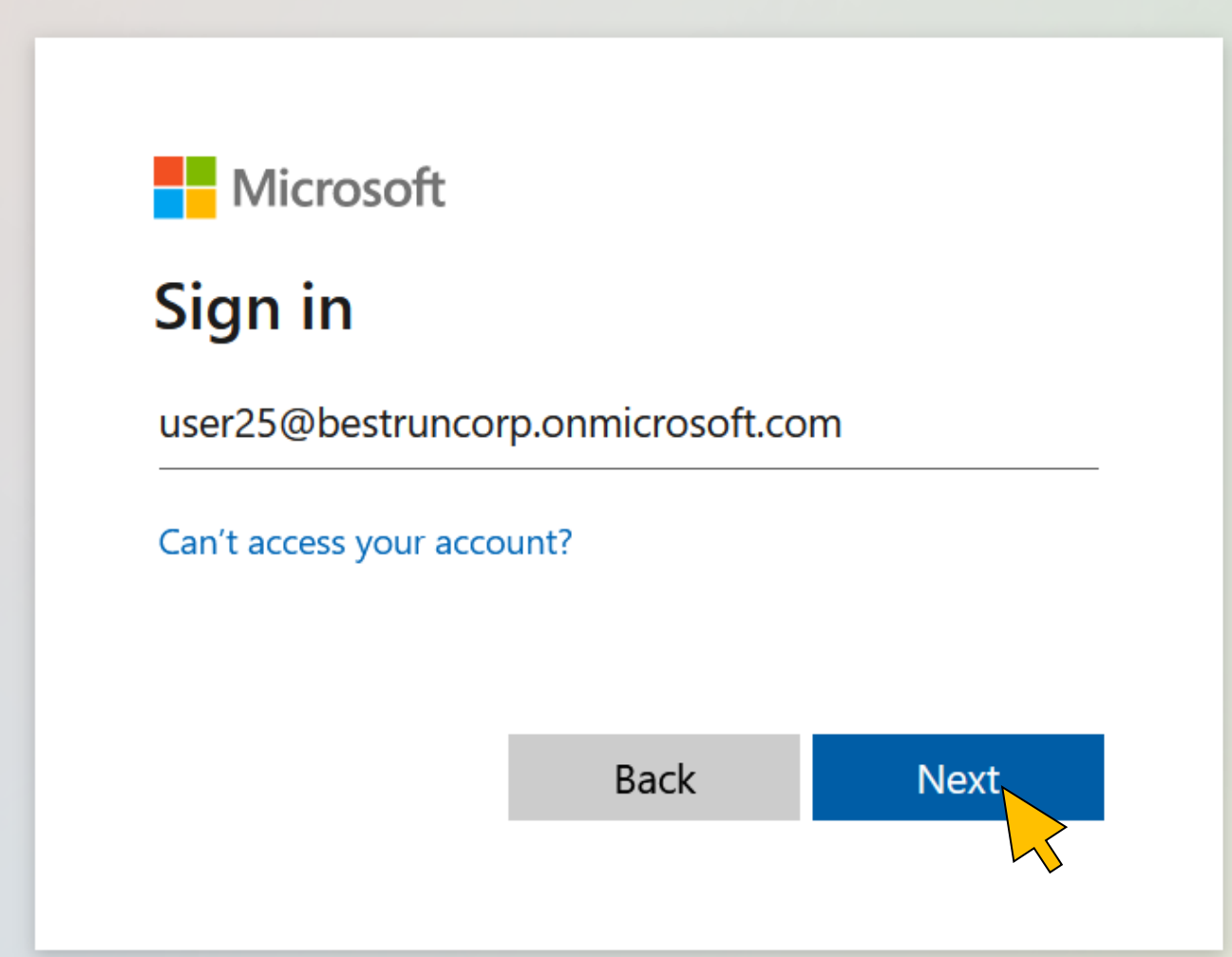
Copy

# 1.7 Open the demo website in a private browser window. Click Login
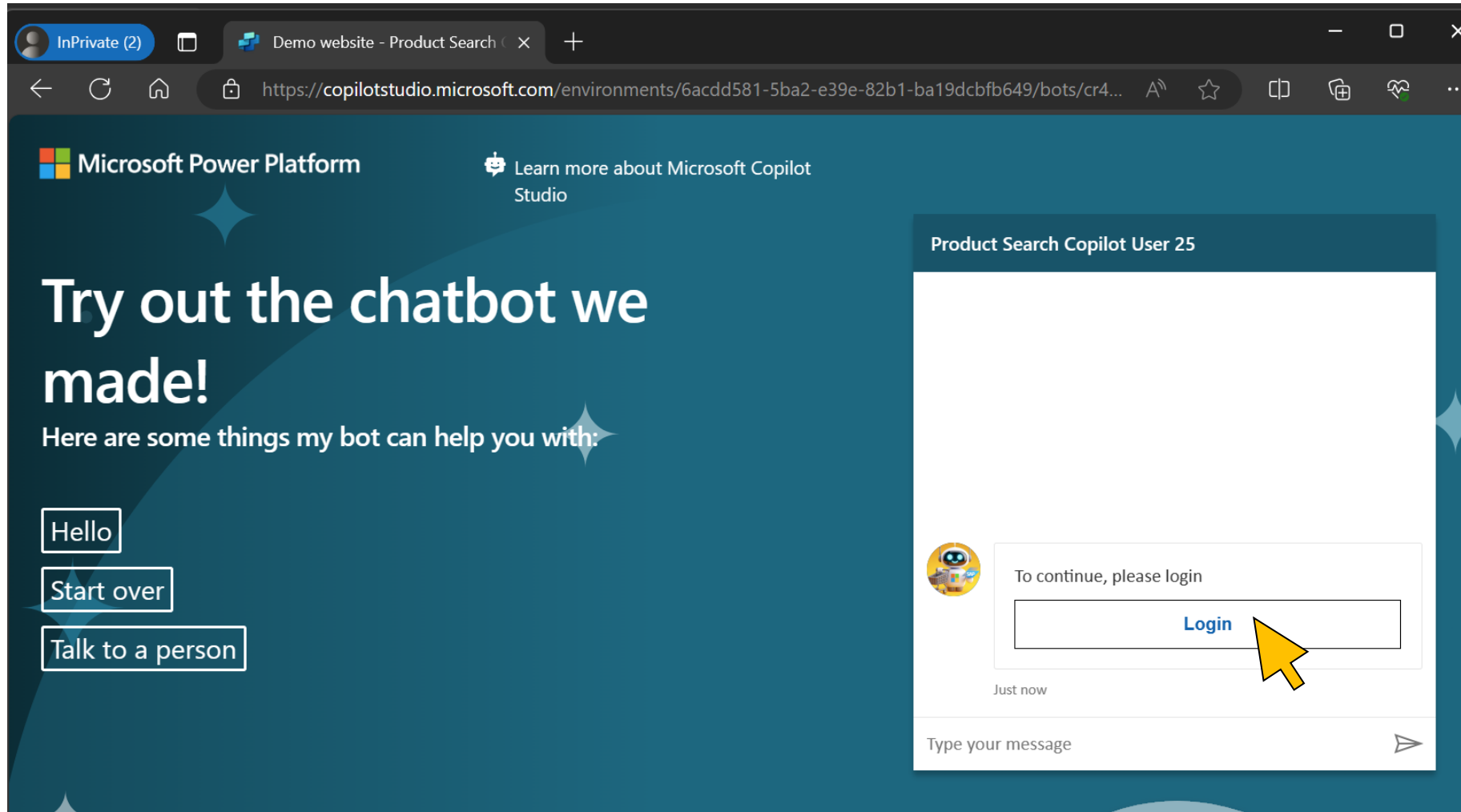
# 1.8 Login to the Copilot as user<N>@bestruncorp.onmicrosoft.com

# 1.9 Copy the login validation code

Please enter this validation code into the chat window to complete the sign-in:

102811

Copy
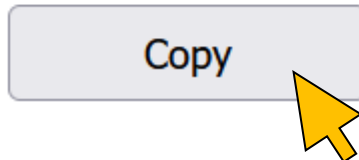
# 1.10 Send the code
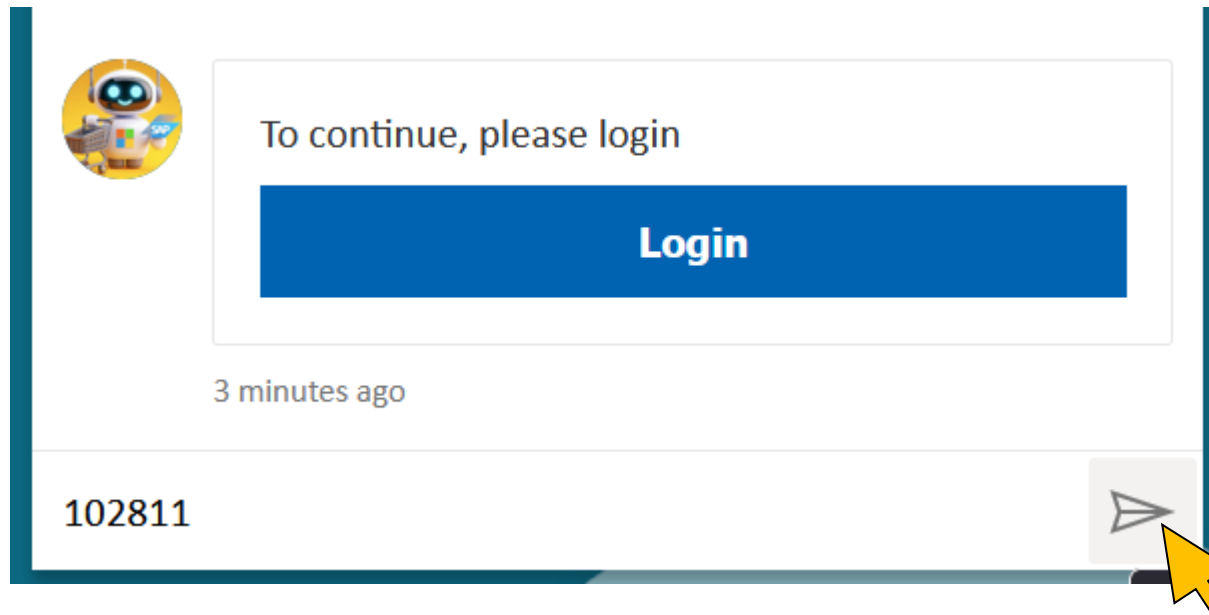
# 1.11 Start the conversation e.g. by typing „Hi! How do I get started?" until you run into an error
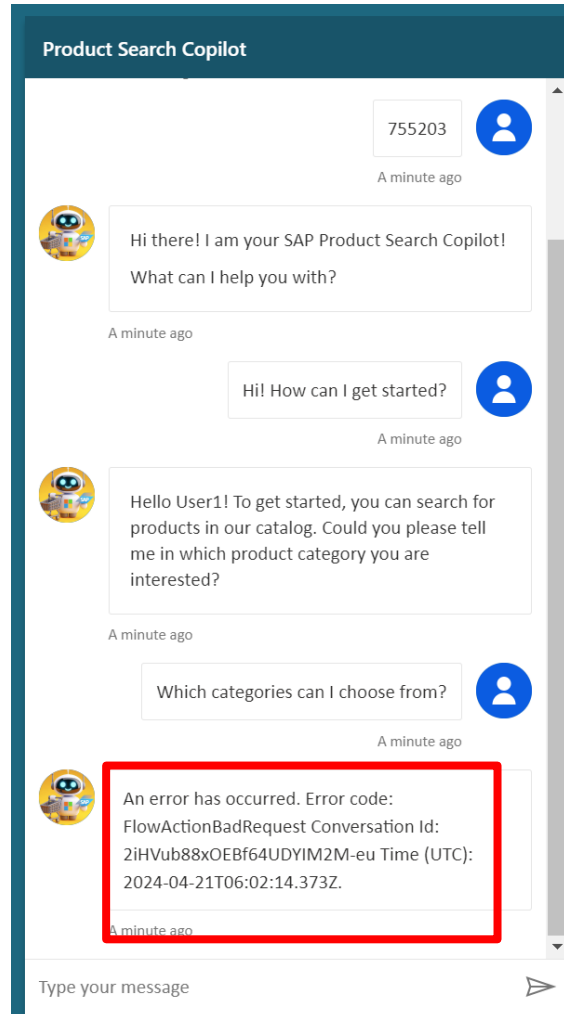
# Exercise 2

Troubleshoot the SAP access in Power Automate

# 2.1 Open [Power Automate](#) in a new browser tab
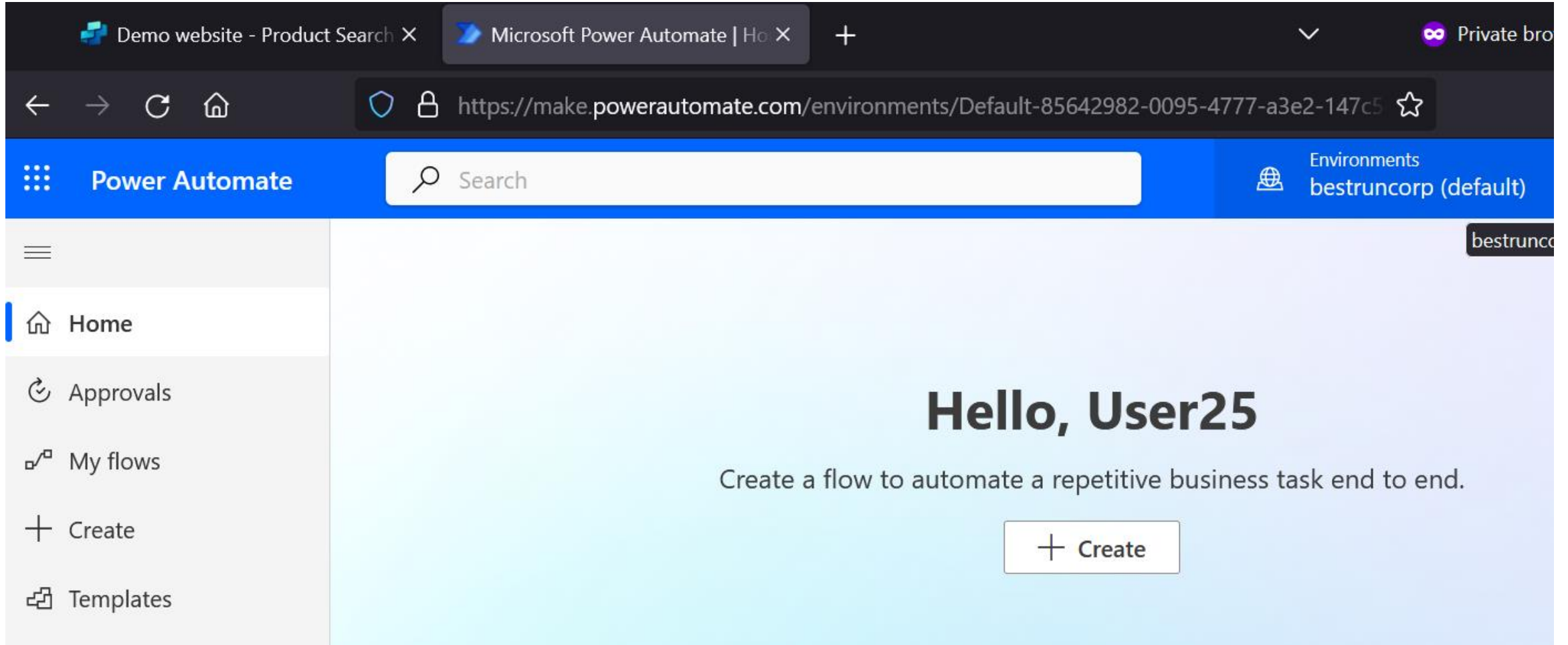
# 2.2 Switch to your user's enviornment bestruncorp_user<N>

# 2.3 Select Solutions → SAP Product Search Copilot

# 2.4 Select Cloud Flows → Chat with Azure OpenAI

# 2.3 Select the last failed instance from the run history

# 2.4 Browse to the failed action in the instance trace

# 2.5 Check the „innerError" message

- "innerError": "<html><head><meta http-equiv=\"content-type\" content=\"text/html; charset=windows-1252\"><title>Logon failed</title><style>body { background: #ffffff; text-align: center; width:100%; height:100%; overflow:hidden; }.content

# Exercise 3

Fix the login error in SAP

# 3.1 Click Edit

# 3.2 Scroll down and click on „+" → „Add an action" below the action „Parse response message for action"
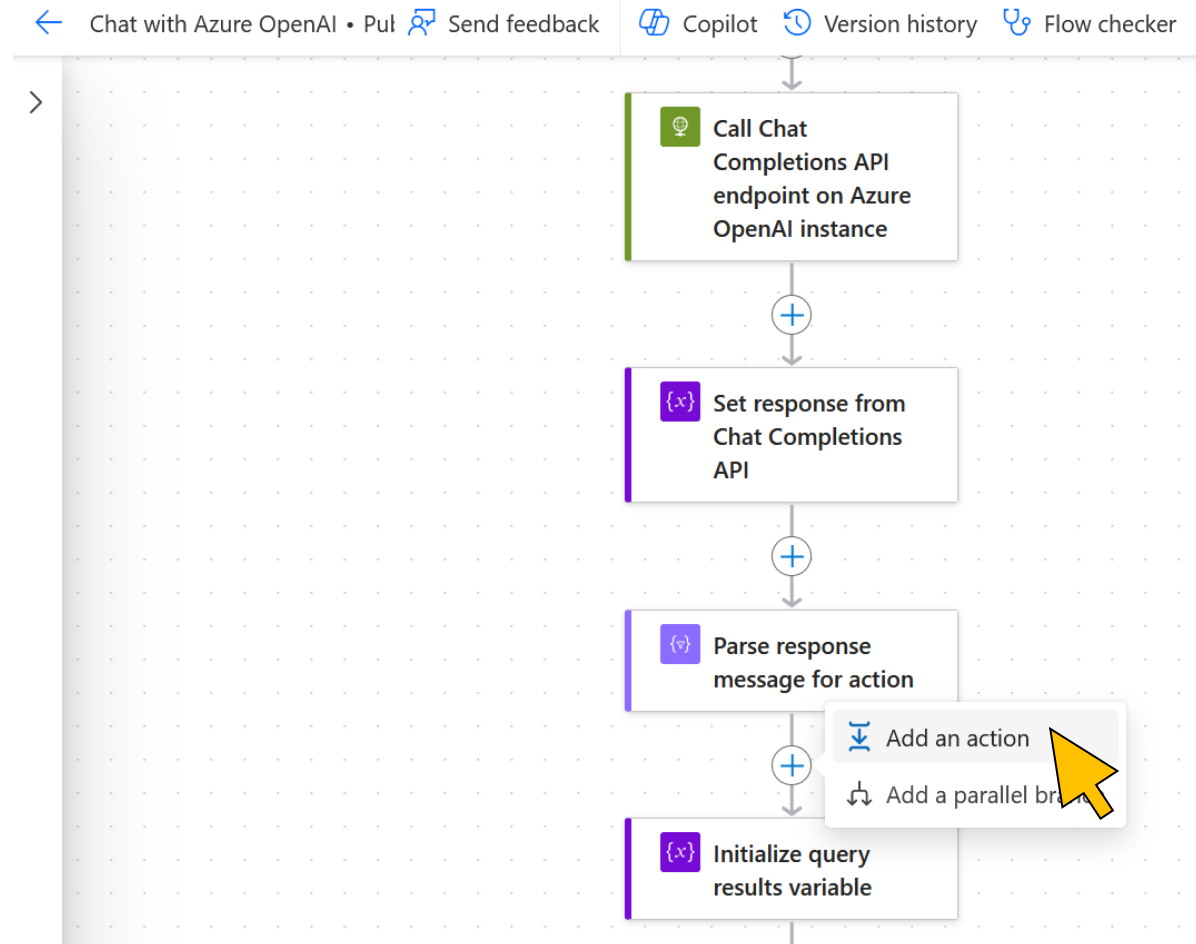
# 3.3 Select Control → Condition

## Add an action                                          ✕

Search

Runtime

Select a runtime                                      ⌄

| | |
|---|---|
| ⬡ **AI Builder** <br> In App                    ⓘ | ✓ Approvals                              ⓘ |
| ⬛ **Azure DevOps**                              ⓘ | ▥ Control <br> In App |

## Add an action                                          ✕

← Return to search

⬛ **Control**

| | |
|---|---|
| Condition | In App  ⓘ |
| Apply to each | In App  ⓘ |

# 3.4 Click on the Flash icon

# 3.5 Select Body action from the Parse response message for action

Provide the values to compare and select the operator to use.

AND ⌄

☐ Choose a value

＋ New item ⌄

ⓘ

Search

{x} Variables

messages

System prompt

{∇} Parse response message for action

Body

Body action

Body productID

# 3.6 Select „is not equal to"

# 3.7 Enter *none* in the last field
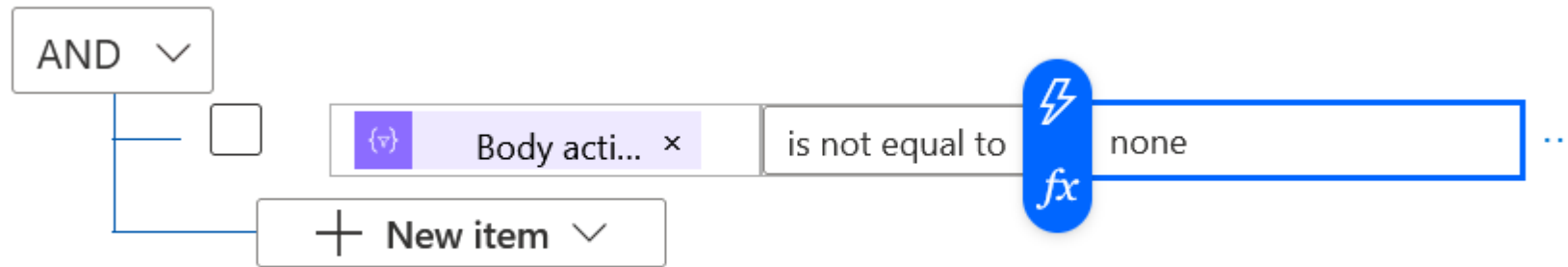
# 3.8 Click Collapse
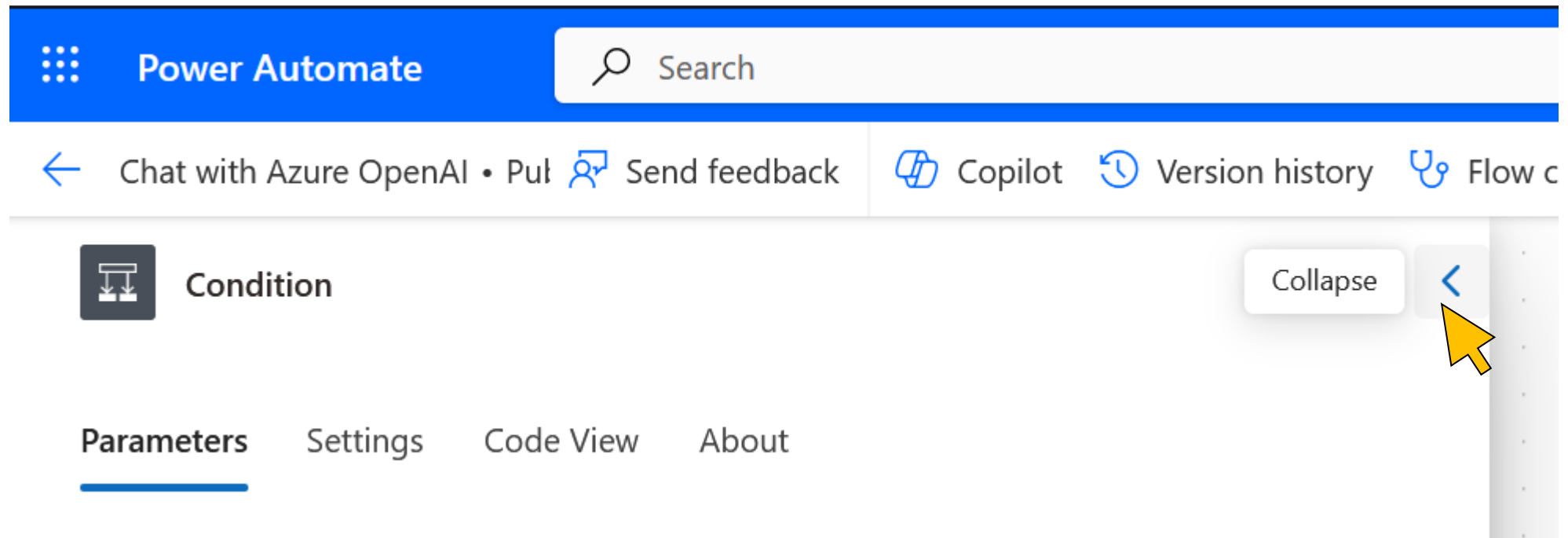
# 3.9 Click on „+" → „Add an action" in the *True* path
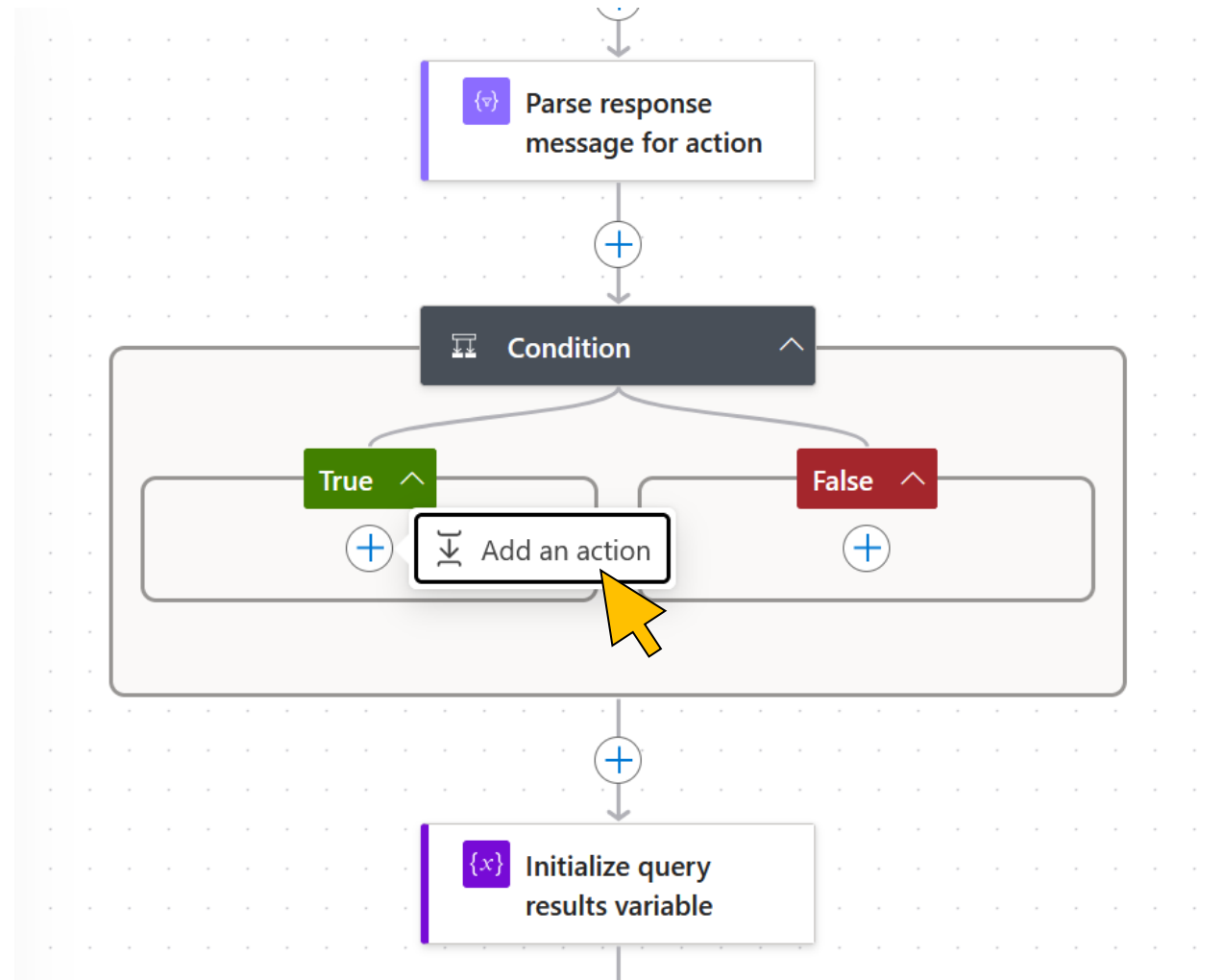
# 3.10 Enter „Run a child" in the search bar and select „Run a Child Flow" from the list

**Add an action**  ✕

Run a chi  ✕

Runtime

Select a runtime  ▾

Action Type

Actions  ▾

☑ Group by Connector

---

**Excel Online (Business)**  ⓘ

See more

| Run script | ⓘ |

| Run script from SharePoint library | ⓘ |

---

**Desktop flows**  ⓘ

See more

| Run a flow built with Power Automate for desktop | ⓘ |

---

**Flows**  ⓘ
In App

See more

| Run a Child Flow | In App  ⓘ |

# 3.11 Select „Exchange Token" from the list in Child Flow

# 3.12 Click on the Flash icon in the EntraIDToken field

# 3.13 Select the EntraIDToken data element from the Run a flow from Copilot Trigger

# 3.14 Rename the action to „Exchange Entra ID Access Token for SAP Access Token" and click Collapse

# 3.15 Scroll down and select the SAP data access action „Get all products the user has access to from SAP" from the switch „List categories" case
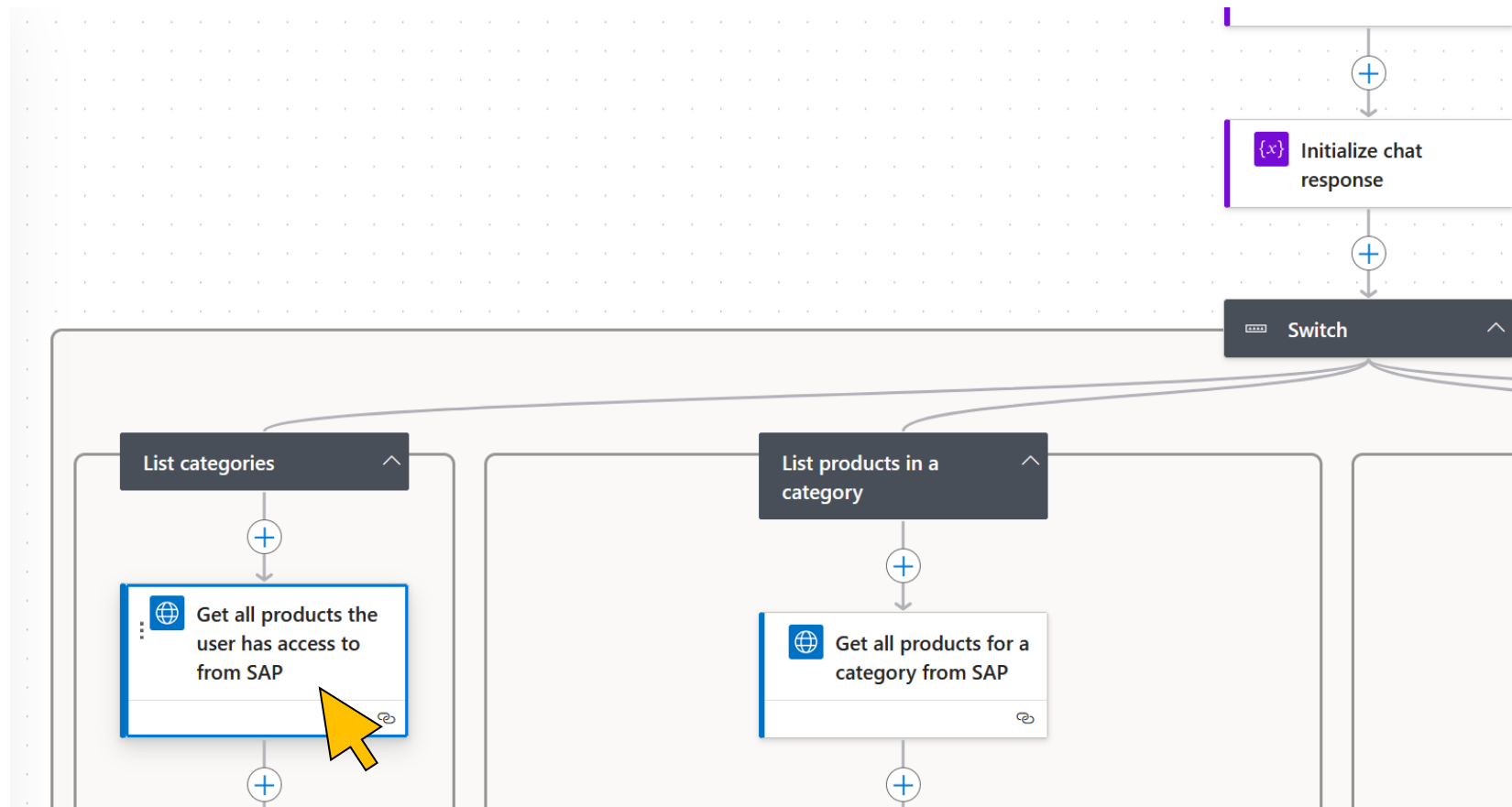
# 3.16 Delete the placeholder text „<fix missing token here>" in the Authorization Headers field. Type in „Bearer<Space>" and click on the Flash icon

Get all products the user has access to from SAP

Parameters    Settings    Code View    Testing    About

Method *

GET

Url Of The Request *

[@]    SAPODat... ×    ?$select=ProductCategory

Advanced parameters

Showing 1 of 2    Show all    Clear all

Headers

| Accept | application/json |
| Authorization | Bearer |
| Enter key | Enter value |

Enter the data from previous step. You can also add data by ty

Connected to HTTP With Microsoft Entra ID.    Change connection reference

# 3.17 Scroll down and select the SAPToken data element from the Exchange EntraID Access Token for SAP Access Token action

# 3.18 Click Collapse

Chat with Azure OpenAI • Published

🌐 **Get all products the user has access to from SAP**

Collapse ‹

**Parameters**   Settings   Code View   Testing   About

Method *

GET ⌄

Url Of The Request *

[@] SAPODat... × ?$select=ProductCategory

Advanced parameters

Showing 1 of 2 ⌄    Show all    Clear all

Headers

| Accept | application/json |
| Authorization | Bearer 🔑 SAPToken × |
| Enter key | Enter value |

🔗 Connected to HTTP With Microsoft Entra ID.   Change connection reference

# 3.19 Repeat the steps 3.15 to 3.18 for the two remaining actions „Get all products for a category from SAP" and „Get product details from SAP"

# 3.20 Click Save draft

Power Automate    🔍 Search    🌐 Environments bestruncorp_user25
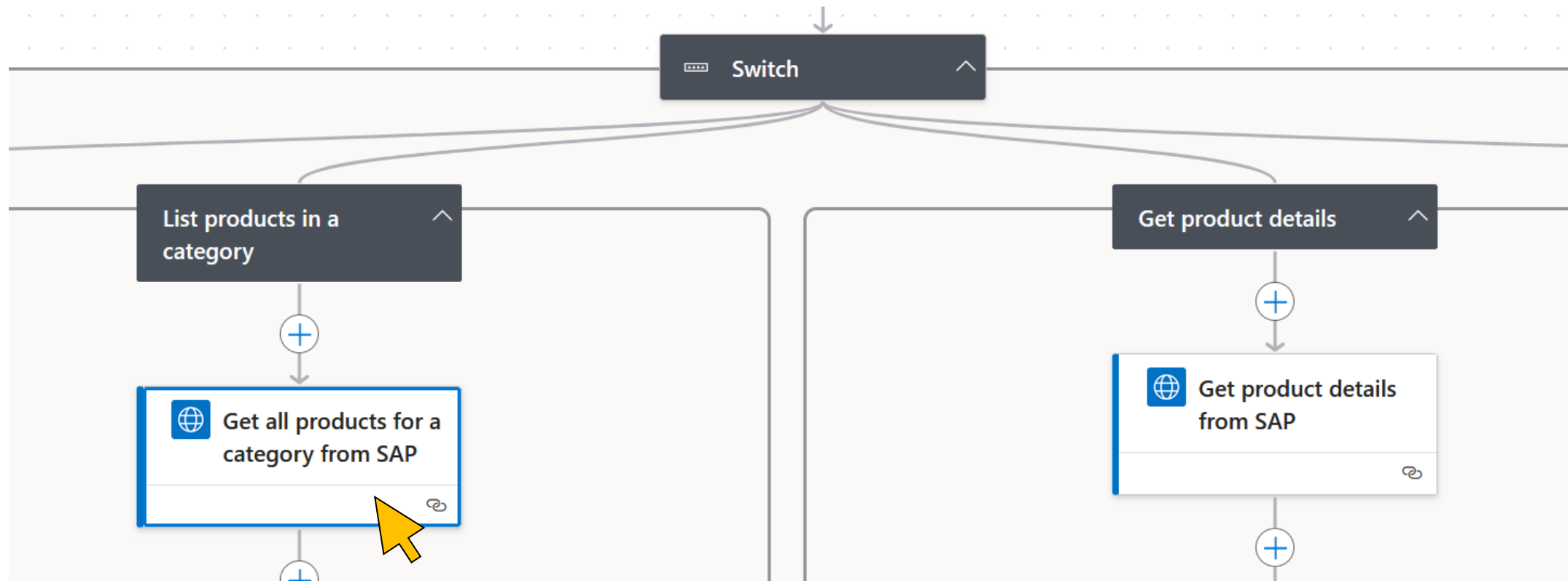
← Chat with Azure OpenAI   Send feedback   Copilot   Version history   Flow checker   💾 Save draft   Test
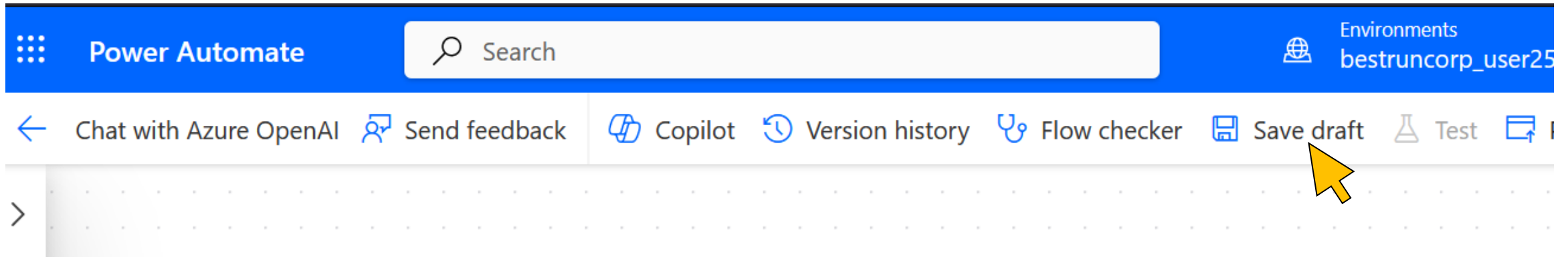
# 3.21 Wait for the save operation to complete, then click Publish



Power Automate

Search

Environments
bestruncorp_user25

← Chat with Azure OpenAI   Send feedback   Copilot   Version history   Flow checker   Save draft   Test   Publish

✓ We saved your draft flow. You can test and run it after you publish.

Publish

>
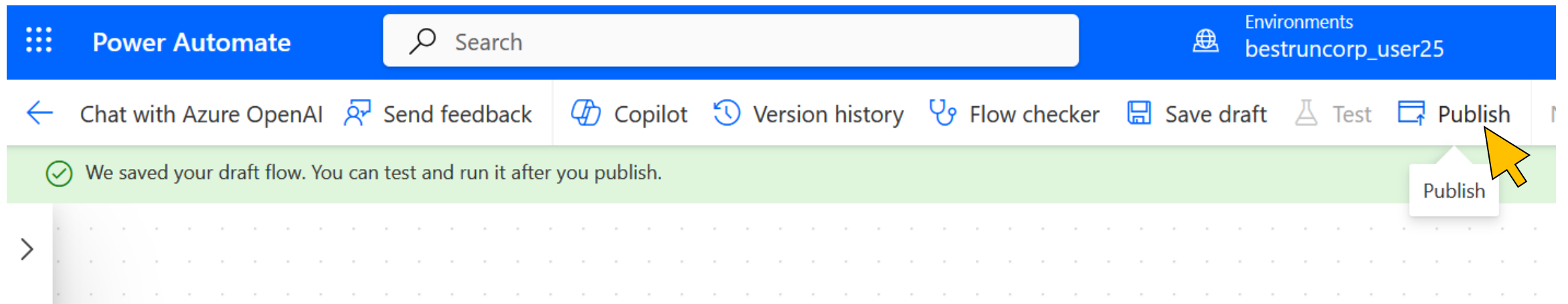
# 3.22 In Copilot Studio, go to Topics → System, and select the „Fallback" topic

# 3.23 Scroll down to the Action where the Chat with Azure OpenAI flow is called. Click „Select Variable" on the EntraIDToken input field

# 3.24 Select the System tab and select User.AccessToken from the list

# 3.25 Click Save

# 3.26 Go to Publish and click Publish

# Exercise 4

Test SAP data access with the fixed flow

# 4.1 Reload the demo website
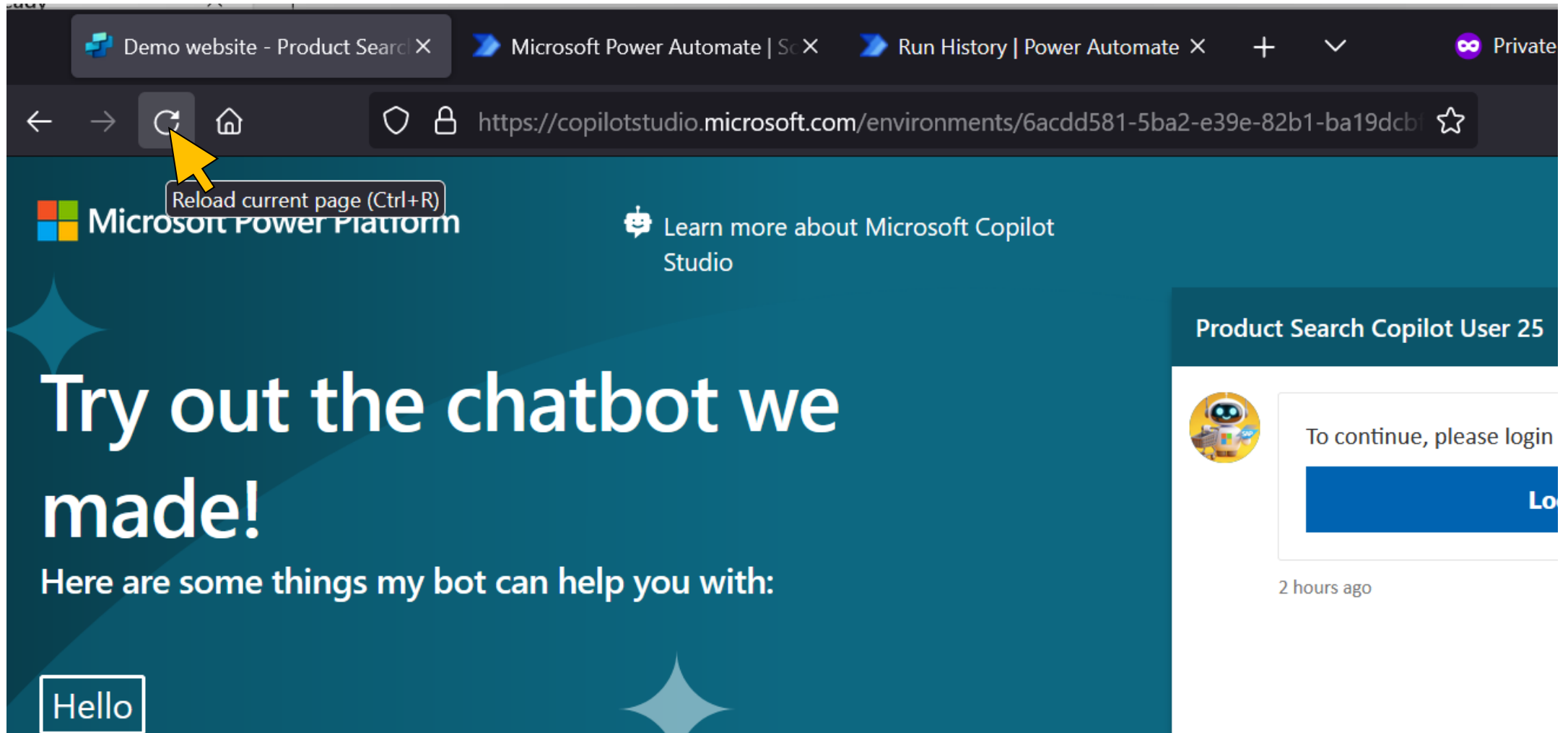
# 4.2 You may need to re-login to the copilot
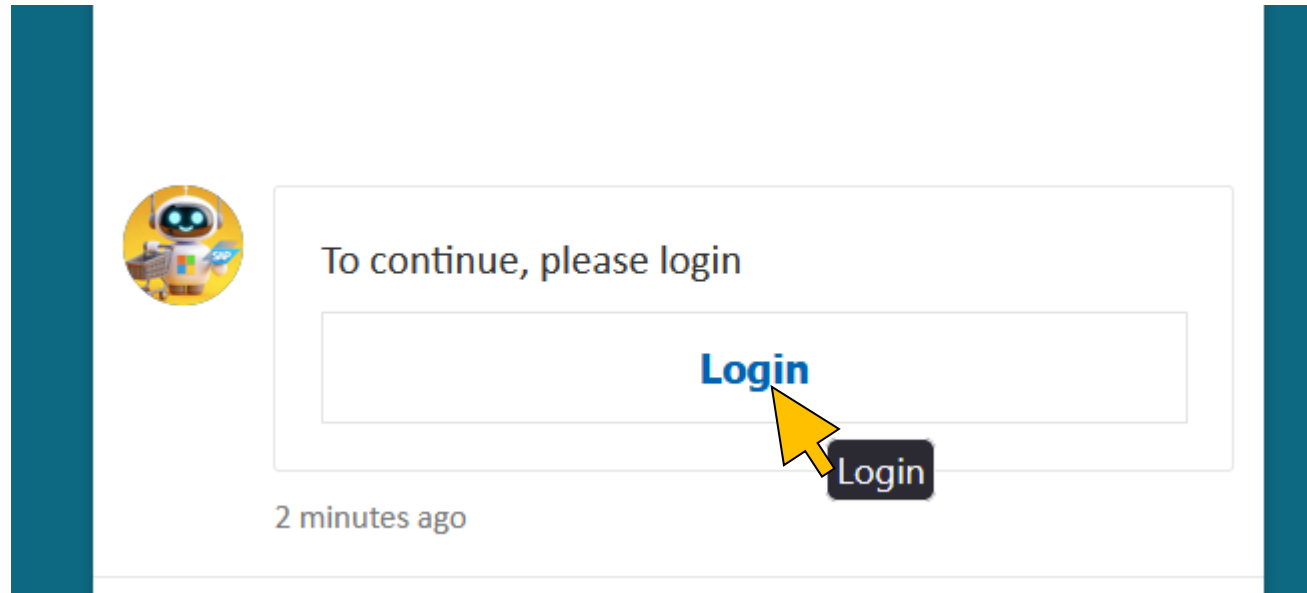
# 4.3 Start the conversation
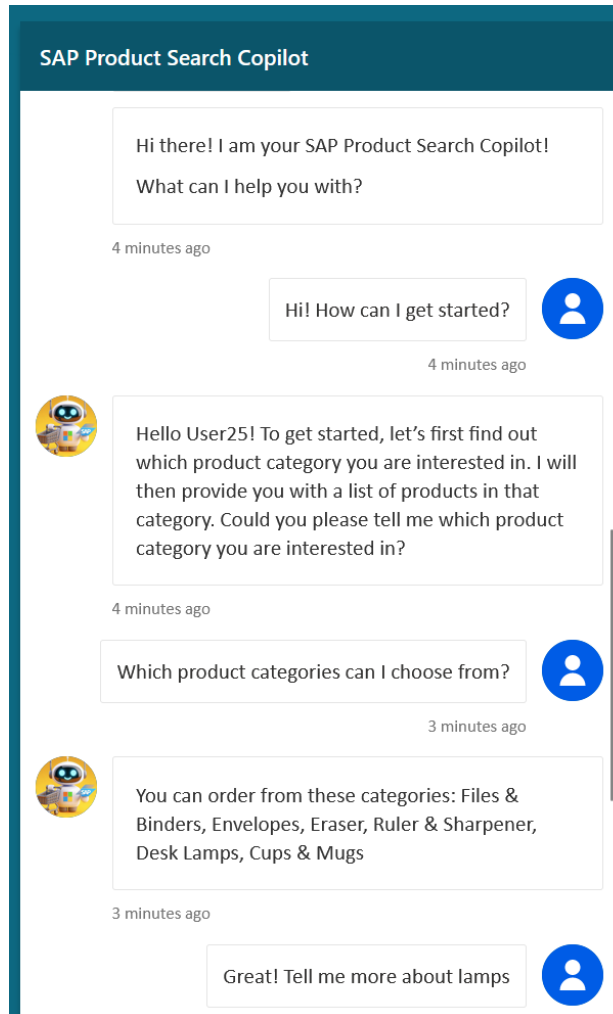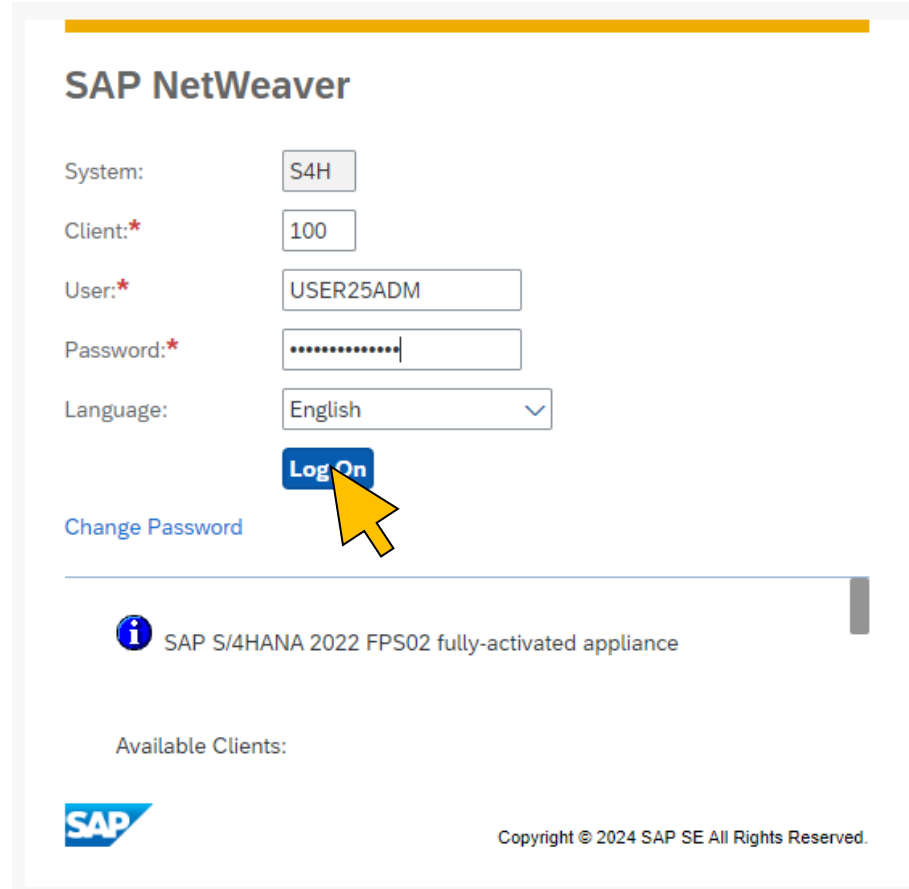
# 4.4 Continue until you get the details of a product you are interested in
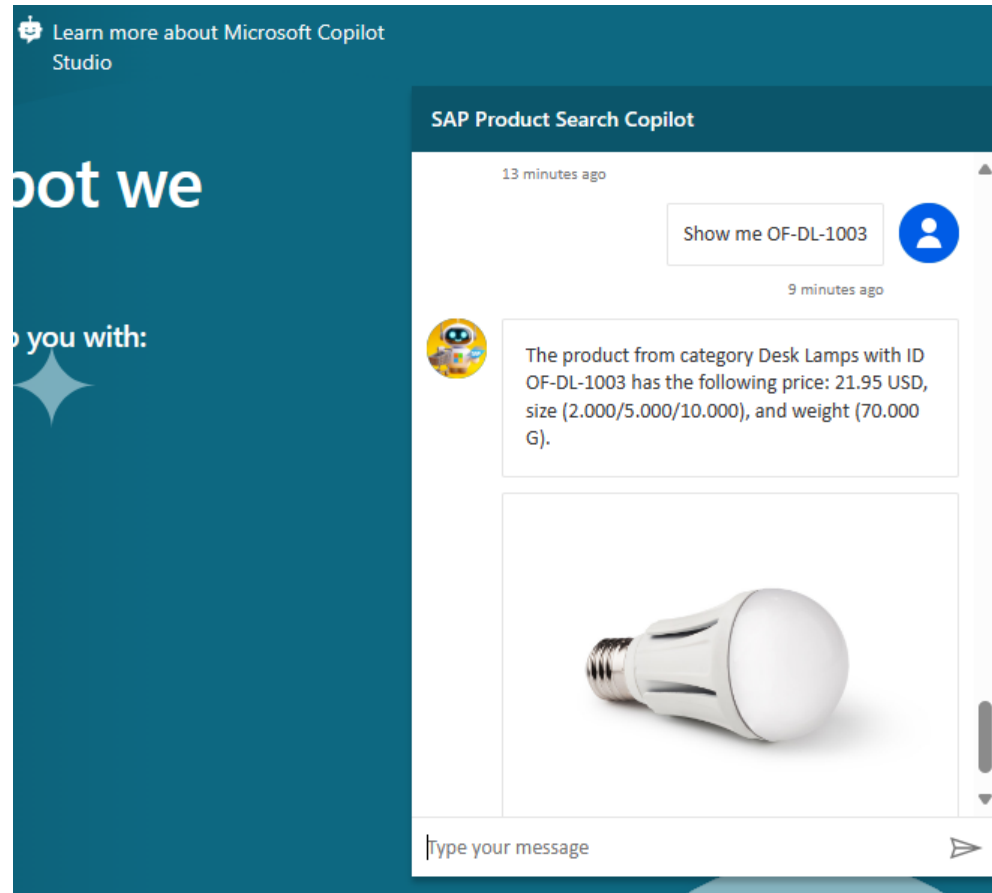
# Exercise 5

Change the user's authorizations in SAP

# 5.1 Access the SAP system as user USER<N>ADM with the [Web GUI](#), password Welcome24#1234

# 5.2 Enter transaction code PFCG (Role Maintenance) and hit Return
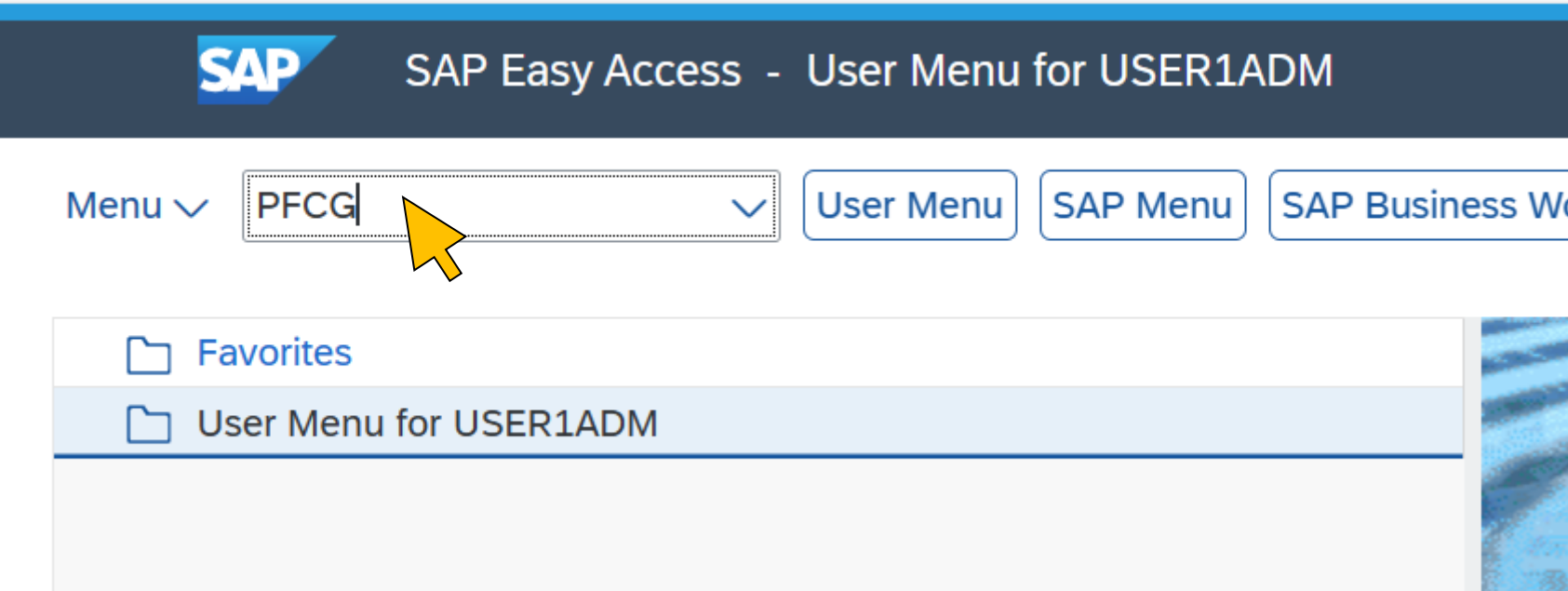
# 5.3 Enter PRODUCT_CATALOG_USER<N> in the Role field and hit the pencil button

# 5.4 Switch to tab Authorizations and click Change Authorization Data

# 5.5 Expand the authorization object tree and click the Edit button for the PDCATEGORY authorization field

# 5.6 Click on the value help button of the 'From' field

Field values

Object: S_EPM_PD    EPM: Authorization object for protecting Product data
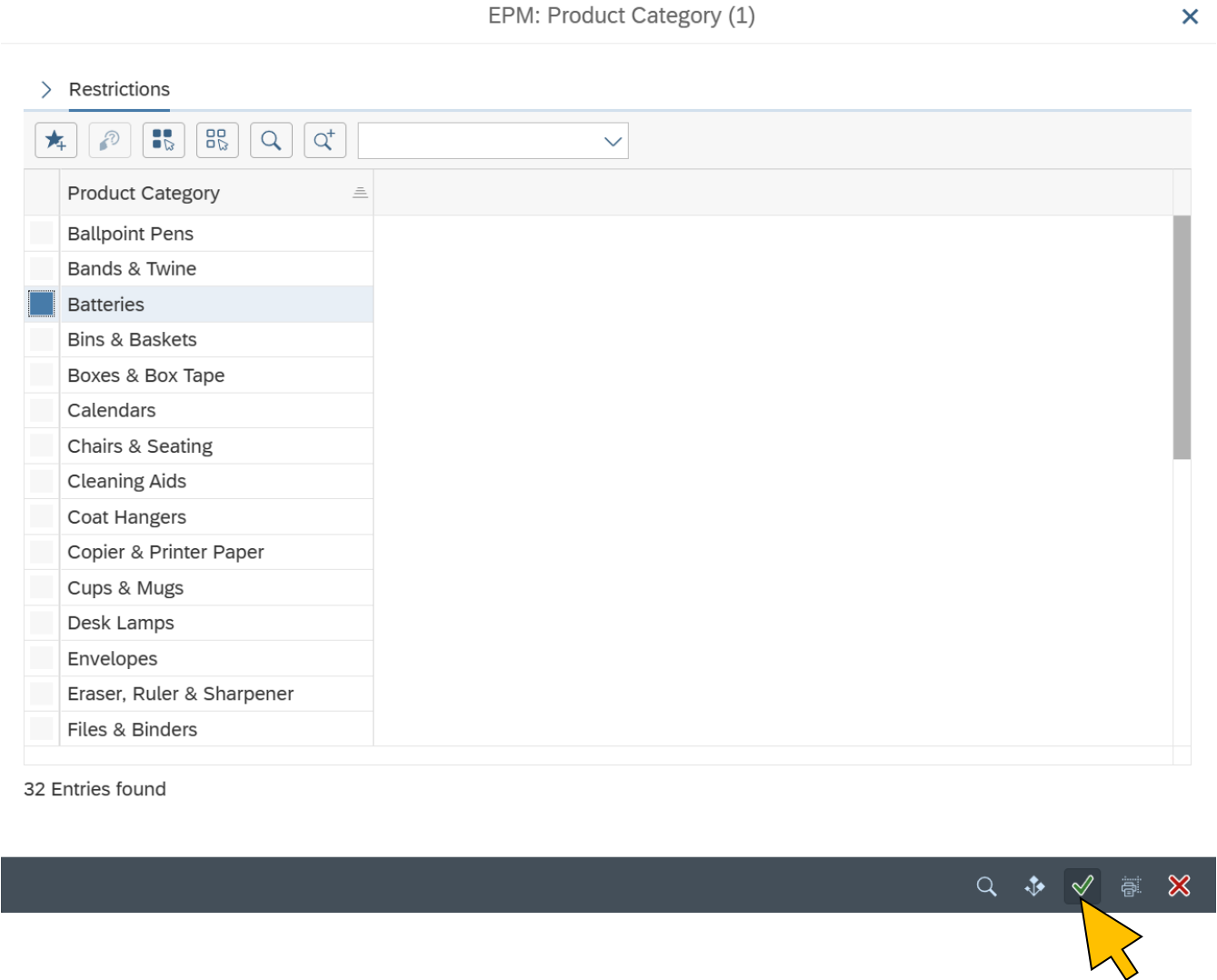
Field Name: PDCATEGORY    EPM: Product Category

Full authorization

Value Intrvl

| 'From' | 'To' | |
|---|---|---|
| ☐ Cups & Mugs | es & Binders | |
| ☐ | | |
| ☐ | | |
| ☐ | | |

# 5.7 Select a different product category, e.g. Batteries, and confirm with OK

EPM: Product Category (1)                                                    ✕

> Restrictions

| Product Category |
|---|
| Ballpoint Pens |
| Bands & Twine |
| Batteries |
| Bins & Baskets |
| Boxes & Box Tape |
| Calendars |
| Chairs & Seating |
| Cleaning Aids |
| Coat Hangers |
| Copier & Printer Paper |
| Cups & Mugs |
| Desk Lamps |
| Envelopes |
| Eraser, Ruler & Sharpener |
| Files & Binders |

32 Entries found

# 5.8 Also change the 'To' field by clicking on the value help

Field values                                                    ✕

Object:  S_EPM_PD      EPM: Authorization object for protecting Product data acc...
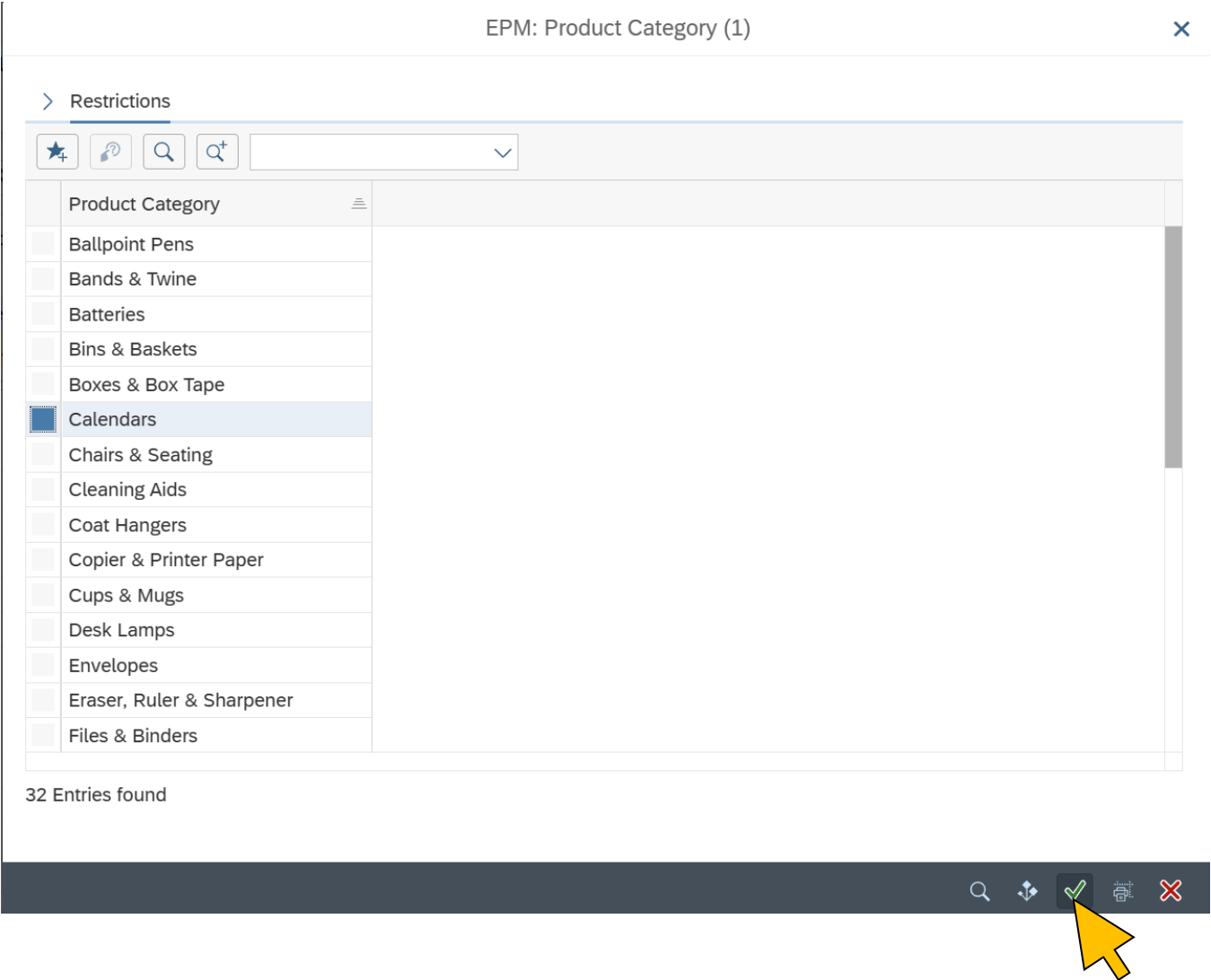
Field Name:  PDCATEGORY    EPM: Product Category

Full authorization

Value Intrvl                                                    ⚙

| | 'From' | 'To' | |
|---|---|---|---|
| ☐ | Batteries | Files & Binders | ⧉ |
| ☐ | | | |
| ☐ | | | |

# 5.9 Change the value, e.g. to Calendars, and click OK

EPM: Product Category (1)                                              ✕

> Restrictions

[★⁺] [🔍] [🔍] [🔍⁺]  [                    ▽]

| Product Category | ≡ |
|---|---|
| ☐ Ballpoint Pens | |
| ☐ Bands & Twine | |
| ☐ Batteries | |
| ☐ Bins & Baskets | |
| ☐ Boxes & Box Tape | |
| ☐ Calendars | |
| ☐ Chairs & Seating | |
| ☐ Cleaning Aids | |
| ☐ Coat Hangers | |
| ☐ Copier & Printer Paper | |
| ☐ Cups & Mugs | |
| ☐ Desk Lamps | |
| ☐ Envelopes | |
| ☐ Eraser, Ruler & Sharpener | |
| ☐ Files & Binders | |

32 Entries found

                                              🔍  ⤧  ✔  ⊟  ✖

# 5.10 Click Save

# 5.11 Click Save

# 5.12 Click Generate

# 5.13 Click Exit

# 5.14 Back on the Demo website, click Start over

# 5.15 Ask the copilot again from which categories you can choose from to see the changes made in the backend

Microsoft

Thank you

# Please provide your feedback for this session