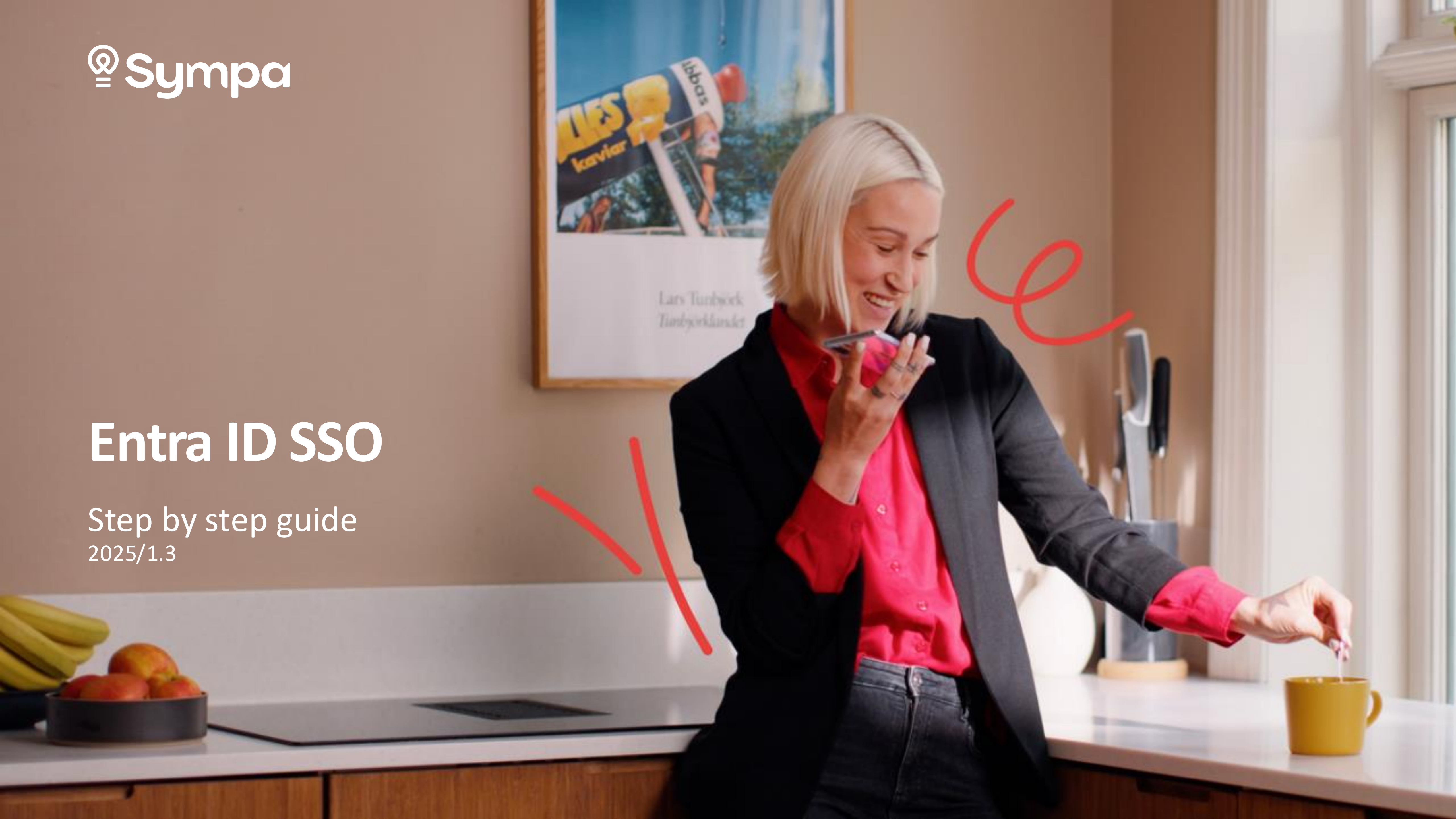
Sympa



Entra ID SSO

Step by step guide

2025/1.3

Sympa

Sympa login types

- **SSO** – Requires a UPN as the Sympa username.
- **Manual login** – Requires a unique, accessible email address as the username.
  - Test users
  - Employees not using SSO (if any)
  - Sympa system admins (if any)

Sympa

Entra ID SSO process

1. **Customer’s IT:**
   1. Ensure all SSO-users have a UPN
   2. Ensure all non-SSO users have unique email.
2. **Customer’s Entra ID Administrator:** Grant consent to Sympa to read user profiles in customer’s Entra ID (earlier Azure AD).
3. **Customer**: Define test user for the SSO.
4. **Sympa:** Switches the IAM solution.
5. **Customer:** Test and approve it!

Details on the following slides.

During the onboarding project, test users will log in manually as non-SSO users (except when performing SSO testing).

1. Ensure UPN or unique email for every user.

Ensure all SSO-users have a UPN.

- UPN = User Principal Name
- UPN is used as a username in Sympa.
- UPN includes @ character

Ensure unique email for every non-SSO Sympa user.

If an employee has multiple user accounts (e.g. a test user or a Sympa system admin user), each account must also have a separate, unique email address. Test credentials are used in the Sympa onboarding project, while Sympa admin credentials are created following specific admin training.

- Use “+” sign in your non-SSO email **firstname.lastname+test@company.com**
  - The email will point to your regular email.
  - Must be supported by your company email provider. Most do support, some may not. **Please check with your email provider.**
- Alternatively, provide a separate email **firstname.lastname.test@company.com**
  - This new email can forward to your existing email account or be a separate account - whichever is more convenient for you

Sympa

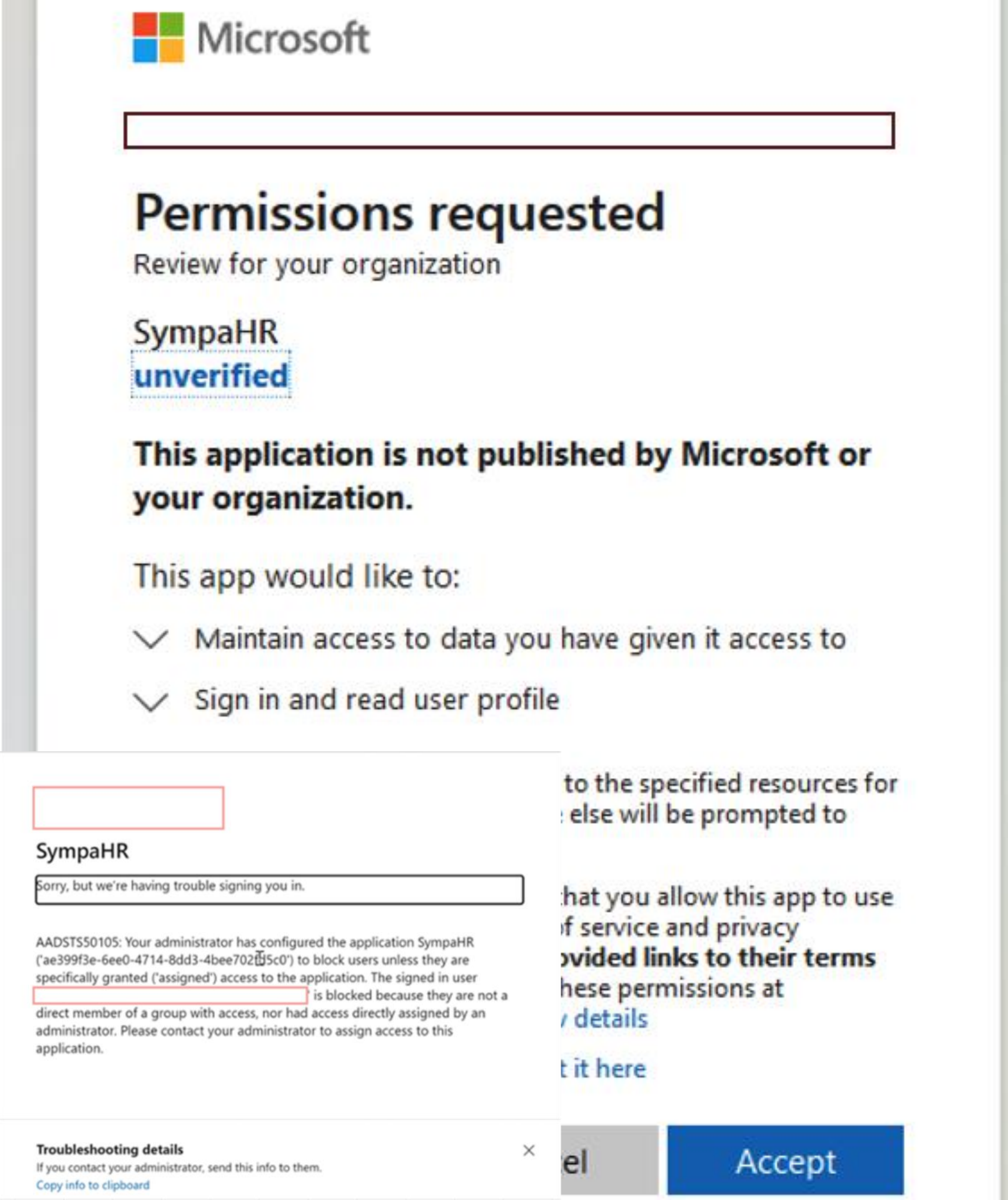
2. Customer’s Entra ID (Azure AD) Admin

Grant consent to **SympaHR** to read user profiles in customer’s Entra ID (Azure AD).

- Customer’s Entra ID (Azure AD) administrator: click this link *
- Accept the permissions (see example on the right)

*The link: https://login.microsoftonline.com/common/adminconsent?client_id=43d906d7-880f-4ad1-b195-9d14383c87c9&redirect_uri=https%3A//www.sympahr.net/index.aspx

Note: You may encounter an error message like this if your username is different from the Sympa login username. This is expected, so you can ignore it.



Microsoft

Permissions requested

Review for your organization

SympaHR

unverified

This application is not published by Microsoft or your organization.

This app would like to:

Maintain access to data you have given it access to

Sign in and read user profile

to the specified resources for
else will be prompted to

hat you allow this app to use
f service and privacy
ovided links to their terms
hese permissions at
details

t it here

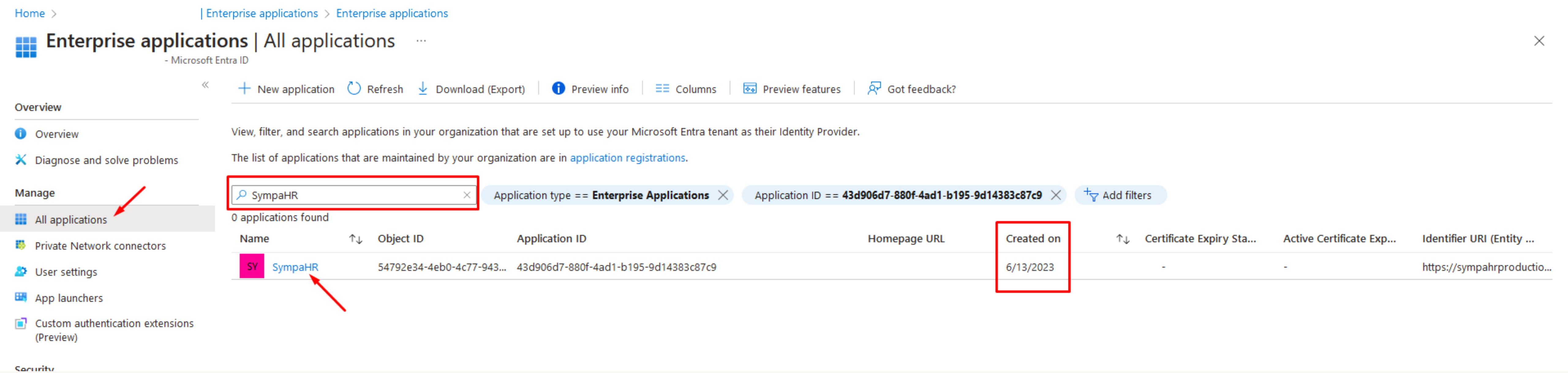
SympaHR

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

AADSTS50105: Your administrator has configured the application SympaHR ('ae399f3e-6ee0-4714-8dd3-4bee702[illegible]5c0') to block users unless they are specifically granted ('assigned') access to the application. The signed in user ' is blocked because they are not a direct member of a group with access, nor had access directly assigned by an administrator. Please contact your administrator to assign access to this application.

Troubleshooting details

If you contact your administrator, send this info to them.



Home > | Enterprise applications > Enterprise applications

Enterprise applications | All applications ···

- Microsoft Entra ID

Overview
- Overview
- Diagnose and solve problems

Manage
- All applications
- Private Network connectors
- User settings
- App launchers
- Custom authentication extensions (Preview)

Security

View, filter, and search applications in your organization that are set up to use your Microsoft Entra tenant as their Identity Provider.

The list of applications that are maintained by your organization are in application registrations.

SympaHR

Application type == **Enterprise Applications**

Application ID == **43d906d7-880f-4ad1-b195-9d14383c87c9**

0 applications found

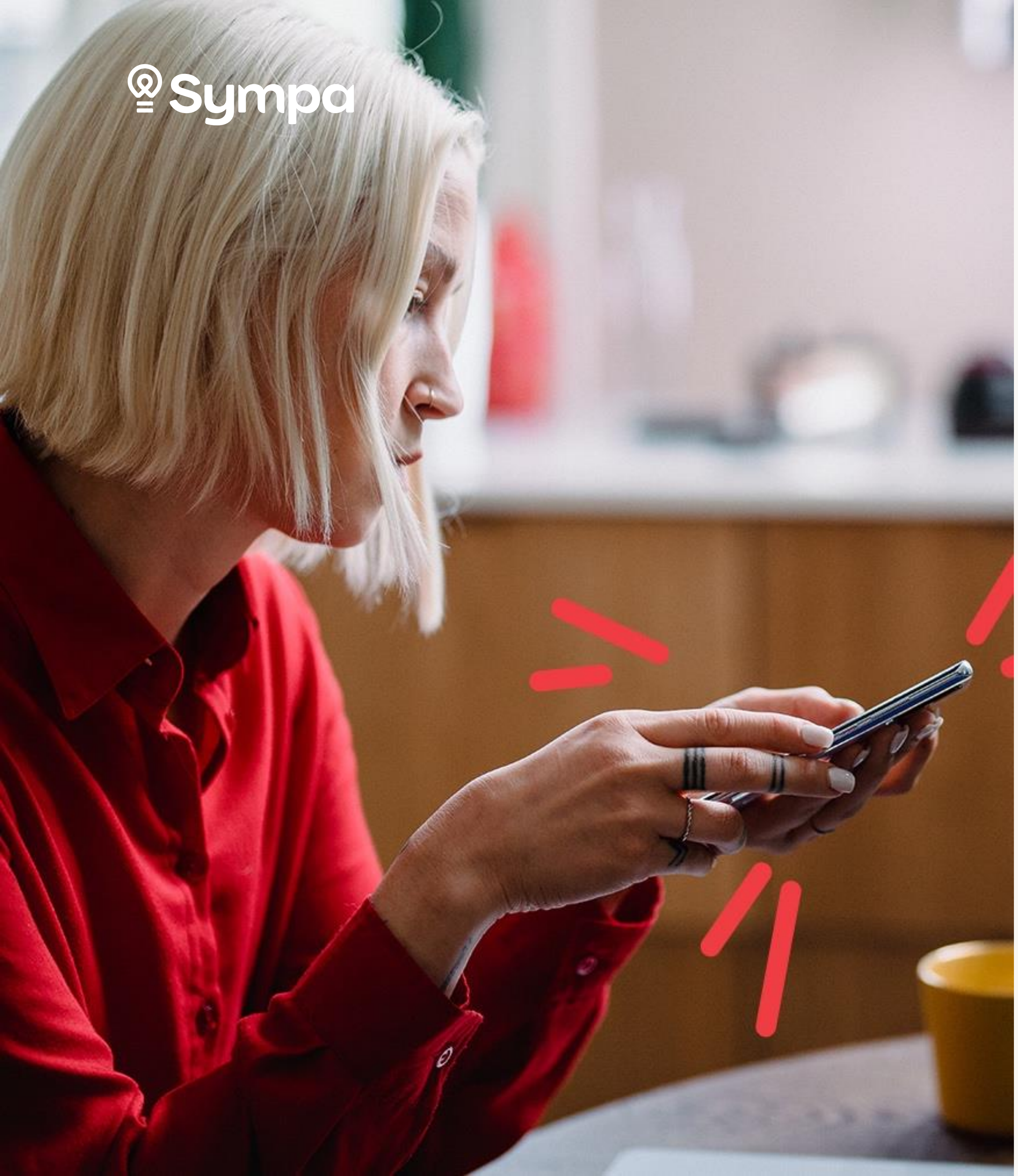
Name	Object ID	Application ID	Homepage URL	Created on	Certificate Expiry Sta...	Active Certificate Exp...	Identifier URI (Entity ...
SY SympaHR	54792e34-4eb0-4c77-943...	43d906d7-880f-4ad1-b195-9d14383c87c9		6/13/2023	-	-	https://sympahrproductio...

2. Customer’s Entra ID (Azure AD) Admin

Log in to the Azure Portal and Grant consent on behalf of all users (see the screenshots). You should select the one created in the previous step.

Depending on your configurations you may need to do some extra steps. For example, If needed, you can whitelist Sympa's manual login link for the admins and possible non-SSO users:

https://www.sympahr.net/index.aspx?y=**YOURORGANISATION**&logintype=manual
(replace the **YOURORGANISATION** with your organisation differentiator)



3. Define test user

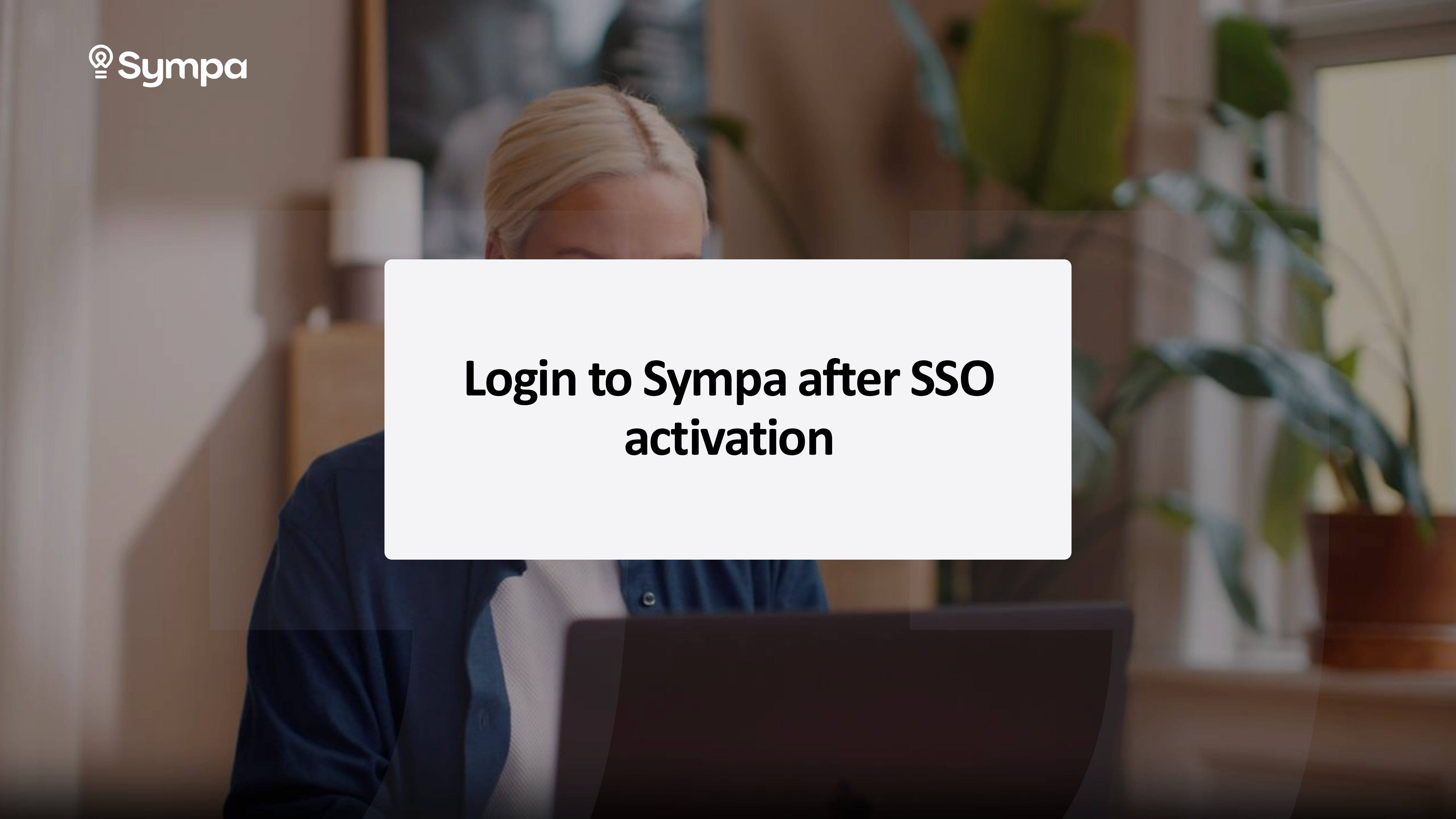
- Select a real Sympa user to test the SSO, such as someone from HR or IT.
- Request the UPN of the selected test user from your Entra ID administrator.
- Share the following information for Sympa to create a real user account for testing:
  - Employee's first and last name
  - UPN
  - Employee ID

4. Sympa switches you to the SSO

Once the previous steps are done by your Entra ID (Azure AD) Administrator, Sympa will switch to the SSO solution on the agreed date.

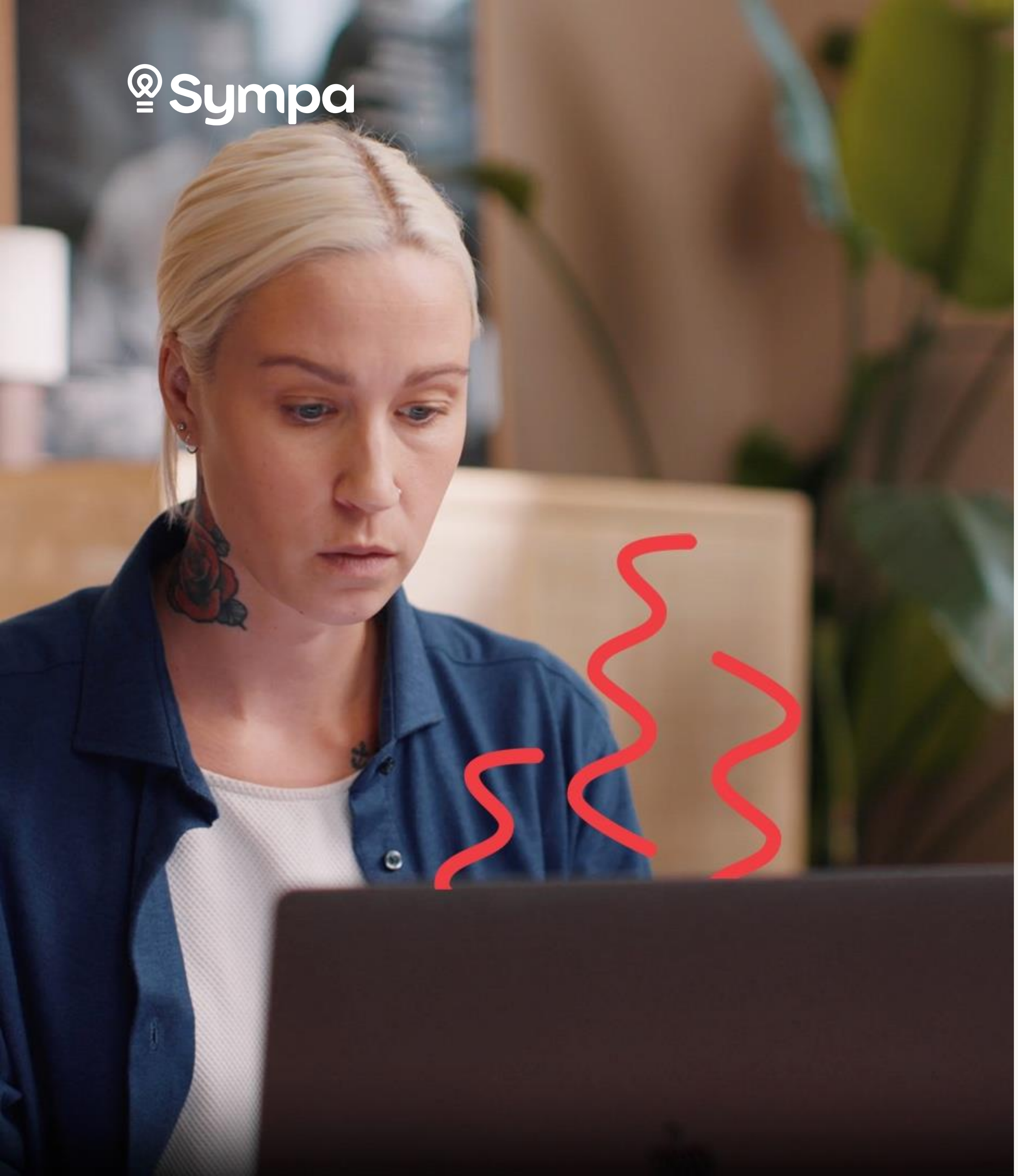
4. Test the SSO login

- Test the login with the user guide on the following pages.
- In case you will have both SSO and non-SSO users, test both logins.
- Do not add any data for the test users in Sympa!
- Please note that the user will be deactivated after approval to prevent login before go-live.



Login to Sympa after SSO activation

Users with SSO



Test user log in with SSO

1. Please ask the person testing the SSO to log in to Sympa.
   - Use the link in format: https://www.sympahr.net/[yourorganisation]
2. Do not add any data for this employee!
3. Please note that the user will be deactivated after approval to prevent login before go-live.
4. The test is considered successful if the employee can log in to Sympa, allowing you to mark this task as approved.

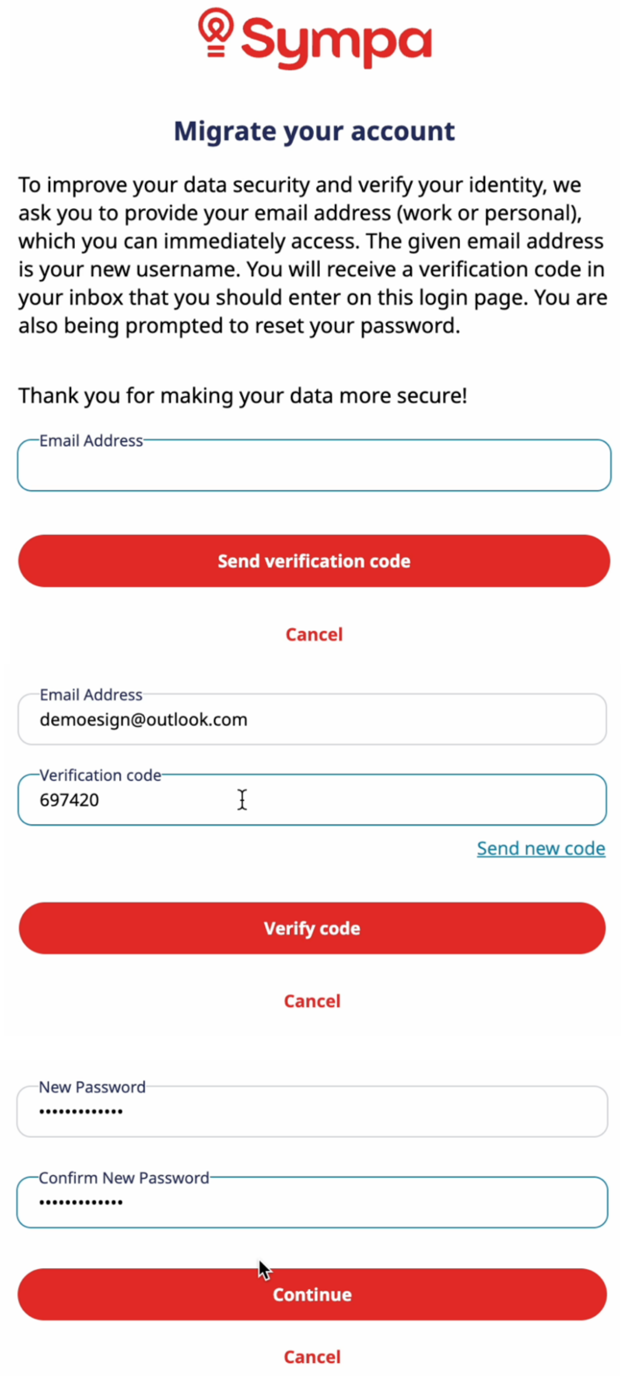
Sympa

Non-SSO Users

Non-SSO login after the update

Your Sympa Onboarding project’s test users will follow this after the SSO is activated.

1. Use the manual login link, and type in your username and password.
2. Again, provide your account's email address, click “Send verification code”.
3. Enter the verification code sent to your email, click “Verify code”.
4. Provide a new password. By clicking “Continue”, you are directed to the Sympa homepage.
5. Migration is complete!



Migrate your account

To improve your data security and verify your identity, we ask you to provide your email address (work or personal), which you can immediately access. The given email address is your new username. You will receive a verification code in your inbox that you should enter on this login page. You are also being prompted to reset your password.

Thank you for making your data more secure!

Email Address

Email Address: demoesign@outlook.com

Verification code: 697420

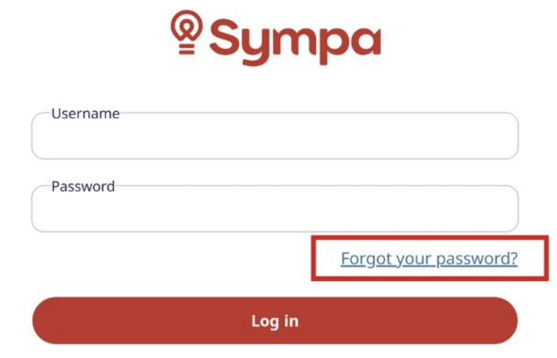
New Password: •••••••••••••

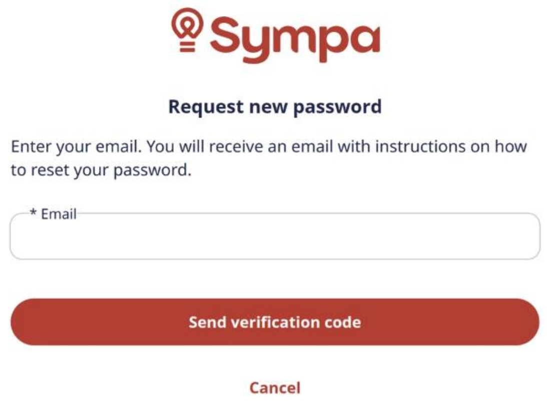
Confirm New Password: •••••••••••••

First-time login without SSO

You will create your password during your first login. Your employees will follow this after the Sympa Go-live.

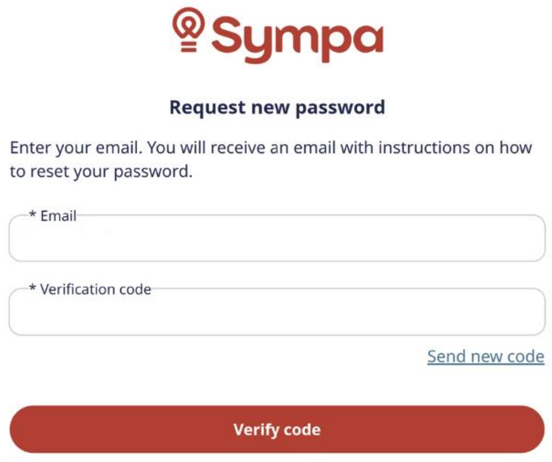
1. Go to the login page.
2. Click *Forgot your password?*
3. Enter your email address (which is used as your username).
4. You will receive an email with a verification code. Enter the code in the designated field to verify your email, then proceed to create your password.





Request new password

Enter your email. You will receive an email with instructions on how to reset your password.



Request new password

Enter your email. You will receive an email with instructions on how to reset your password.