

Activating Multi-Factor Authentication for SSO

Instructions

Effective as of June 1, 2026, version 5

Discovering
what
matters.

Contents

1	Introduction.....	3
2	Setting up multi-factor authentication for SSO	3
3	Authenticator app (OTP)	6
3.1	Setting up the authenticator app	7
4	Webauthn Register/Passkey/FIDO2.....	8
4.1	What is Passkey/FIDO2?	8
4.2	Setting up a passkey using the YubiKey as an example	8
5	SSO login with multi-factor authentication.....	10
5.1	Signing in with the authenticator app	10
5.2	Signing in with a passkey.....	12

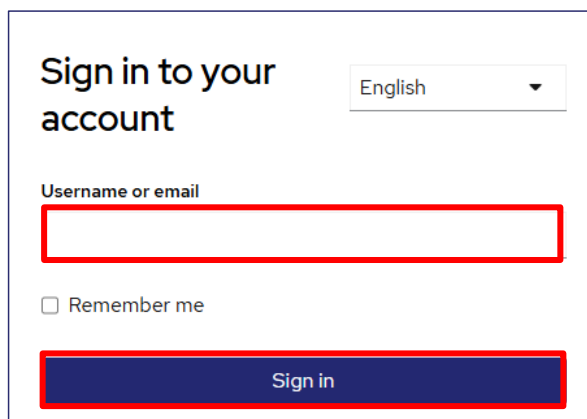
1 Introduction

Starting July 1, 2026, multi-factor authentication (MFA) will be required for all external users on the Single Sign-On portal (sso.fwf.ac.at). This means that you can no longer log in with a password on your cell phone or laptop. In the future, a password will only be required during **initial registration** on the Single Sign-On portal.

2 Setting up multi-factor authentication for SSO

Start by entering the URL <https://sso.fwf.ac.at/auth/realms/sso/account/#/> in your browser.

Enter your username and click **“Sign in”**:



Sign in to your account

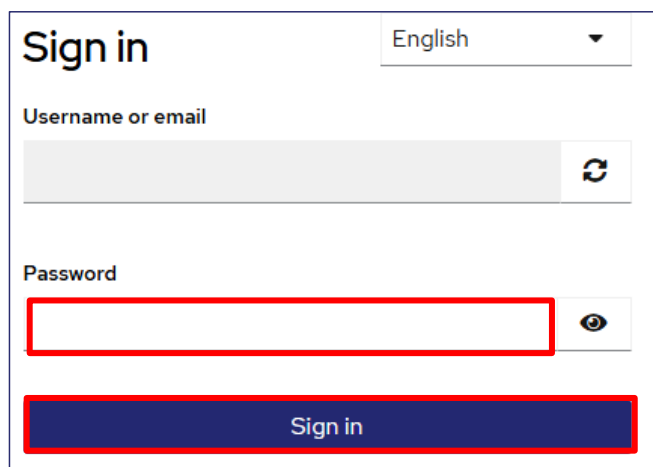
English ▼

Username or email

☐ Remember me

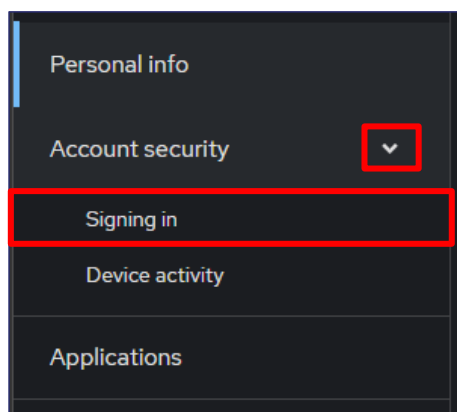
Sign in

Next, enter your password and click **“Sign in”**:



The image shows a 'Sign in' form. At the top left is the text 'Sign in'. To its right is a language dropdown menu showing 'English'. Below this is a label 'Username or email' followed by a text input field. To the right of the input field is a refresh icon. Below the username field is a label 'Password' followed by a password input field. To the right of the password field is an eye icon. At the bottom of the form is a large blue button with the text 'Sign in'. Red rectangular boxes highlight the password input field and the 'Sign in' button.

Next, select **“Signing in”** from the **“Account security”** drop-down menu:



Now you need to select the desired authentication method:

- To set up an authenticator app with TOTP (time-based one-time password), select **“Set up Authenticator application.”** For further steps, please see [section 4.1.](#)
- If you want to set up a passkey (for example a YubiKey) as a second factor, select **“Set up Passkey.”** For further steps, please see [section 5.2.](#)

Two-factor authentication

Authenticator application

Enter a verification code from authenticator application.

Authenticator application is not set up.

Passkey

Use your Passkey to sign in.

Passkey is not set up.

Set up Authenticator application

Set up Passkey

3 Authenticator app (OTP)

To enable multi-factor authentication, you must have an authenticator app (OTP – one-time password) installed on your smartphone.

Most smartphones already come with at least one app of this kind preinstalled.

If you do not currently have an OTP app installed on your smartphone, you will need to download one from your device's app store before beginning the setup process.

The most commonly used apps for this purpose are "Google Authenticator" and "Microsoft Authenticator." Some alternative apps include "FortiToken Mobile" and "FreeOTP."

For more information on this topic, see, for example:

<https://www.onlinesicherheit.gv.at/Services/News/Authenticator-Apps.html> (in German)

3.1 Setting up the authenticator app

Open the authenticator app on your phone and scan the QR code on the screen.

Enter the one-time code generated by the app and a device name, then click “**Submit.**”

Mobile Authenticator Setup

English

You need to set up Mobile Authenticator to activate your account.

1. Install one of the following applications on your mobile:

FreeOTP

Microsoft Authenticator

Google Authenticator

2. Open the application and scan the barcode:



Unable to scan?

3. Enter the one-time code provided by the application and click Submit to finish the setup.
Provide a Device Name to help you manage your OTP devices.

One-time code *

Device Name

☒ Sign out from other devices

Submit

Once the token has been saved successfully, SSO setup is complete and you can close the window.

4 Webauthn Register/Passkey/FIDO2

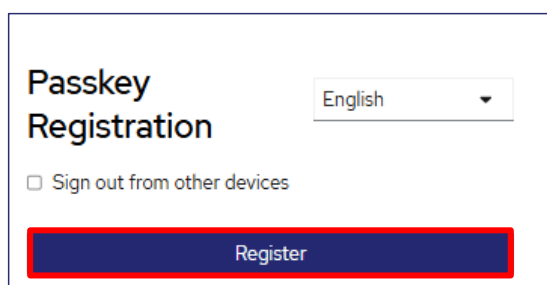
4.1 What is Passkey/FIDO2?

FIDO2 is a modern, highly secure authentication standard. Instead of a code, identity is verified using a cryptographic key stored on the device. A passkey can be stored on a hardware token (e.g., YubiKey) or directly on a compatible device (e.g., Windows Hello, Face ID).

Please note: FIDO2 is not supported by all YubiKey models. On older models (e.g., YubiKey 4), only FIDO U2F is available. Be sure to check which model you have before proceeding with setup.

4.2 Setting up a passkey using the YubiKey as an example

After selecting **“Set up Passkey”** or **“Webauthn Register – Use your Passkey to sign in.”** (see section 2 or 3), you will see the following window. Please click **“Register”**:



Passkey
Registration

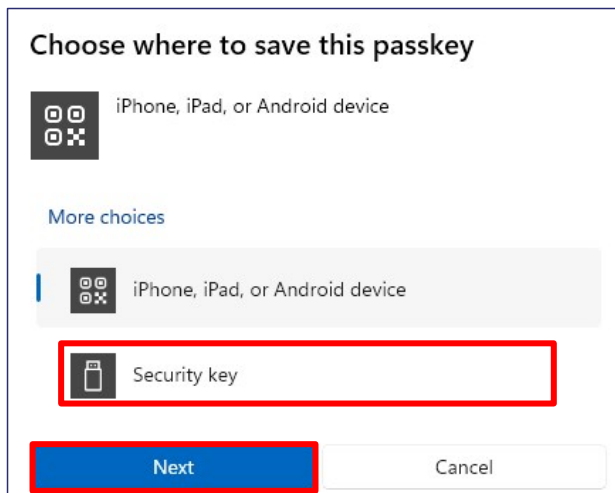
English ▼

☐ Sign out from other devices

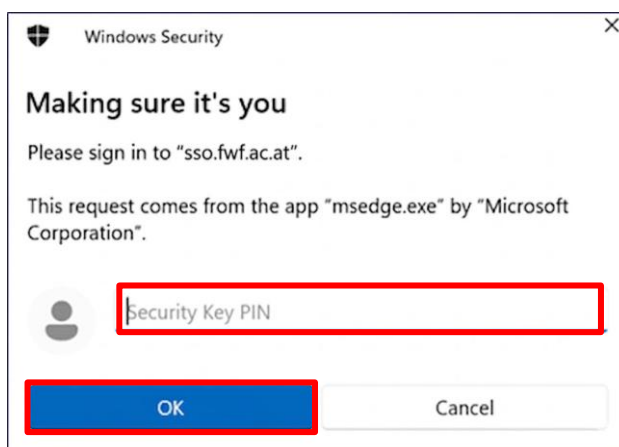
Register

To continue the process, you will need to re-enter your login credentials (FWF username and password) in the next step.

Select **“Security key”** and then **“Next”**:



Next, enter your YubiKey PIN Security key and confirm by clicking **“OK”**:



Enter a passkey name (the display name you choose) and confirm by clicking **“OK”**:

Once the token has been saved successfully, SSO setup is complete and you can close the window.

5 SSO login with multi-factor authentication

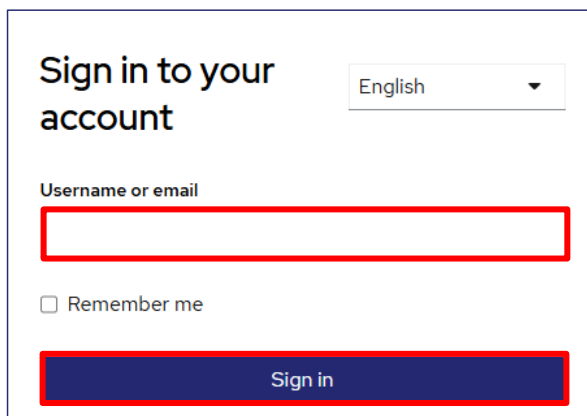
After you have successfully registered, you can log in via the login page (SSO – Single Sign-On) in two ways: using an authenticator app or a passkey.

Kommentiert [SS1]: Hier evtl. die URL anführen/verlinken?

Kommentiert [2]:

5.1 Signing in with the authenticator app

Enter your FWF username or email address and click **“Sign in”**:



The screenshot shows a login form titled "Sign in to your account". To the right of the title is a language dropdown menu set to "English". Below the title is a label "Username or email" followed by a text input field. Underneath the input field is a checkbox labeled "Remember me". At the bottom of the form is a dark blue button with the text "Sign in". Red rectangular boxes highlight the text input field and the "Sign in" button.

Open the authenticator app on your smartphone.

Take the one-time code generated by the app and enter it in the **“One-time code”** field. Confirm by clicking **“Sign in”**:

Sign in

English ▼

Username or email

↺

One-time code

Sign in

5.2 Signing in with a passkey

Enter your FWF username or email address and click **“Sign in”**:

Sign in to your account

English ▼

Username or email

☐ Remember me

Sign in

Click **“Sign in with Passkey”**:

Passkey login

English ▼

Username or email

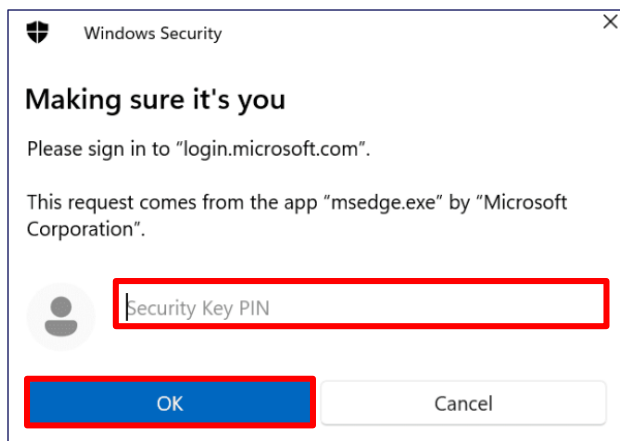
 **Passkey (Default Label)**
Created Jun 16, 2026, 11:38 AM

Sign in with Passkey

Select “**Security key**” and then “**Next**”:



Enter your YubiKey PIN security key and click “**OK**” to confirm:



Press the flashing button on the YubiKey with your finger:

Kommentiert [SS3]: Ganz zum Schluss nach Übernahme aller Änderungen bitte das Inhaltsverzeichnis aktualisieren.

