Configuring the app for two-factor authentication

This guide involves using a PC or Laptop to start the setup wizard and a mobile device to install Microsoft Authenticator or another authentication app.

The Microsoft Authenticator application can be easily installed on your mobile device by following these links.

Android: [link](#).

iPhone: [link](#).

Alternatively, simply search for “Microsoft Authenticator” in the device’s app store. A Microsoft guide to the Authenticator app is available at this [link](#).

Do you want to use another app or don’t have a smartphone to perform multi-factor authentication? No problem! It is possible to use TOTP-compatible third-party apps, both on computers and smartphones. A list of apps is available at this [link](#).

Setup Wizard (from PC or Laptop)

Access the following link with your username(at)usi.ch credentials: [https://aka.ms/mfasetup](https://aka.ms/mfasetup)

After the first login with the USI account, a message will appear asking for more information.

More information required

Your organisation needs more information to keep your account secure

Use a different account

Learn more
At this point, you will be asked to install the Microsoft Authenticator application or a different Authenticator (TOTP-compatible). Once installed, select "Next".

Now that the Authenticator app has been installed, you can add the USI account. Select "Next" to continue with Microsoft Authenticator. Or select “I want to use a different authenticator app” for the TOTP app. In this guide we show how to configure Microsoft Authenticator, for TOTP apps, and follow the vendor’s instructions, the procedure will be similar to the one illustrated here.
The procedure will now require opening the Authenticator app on the mobile device and adding the USI account by scanning the QR code on the screen.

Microsoft Authenticator

Scan the QR code

Use the Microsoft Authenticator app to scan the QR code. This will connect the Microsoft Authenticator app with your account.

After you scan the QR code, choose "Next".

Configuring the Authenticator app (from mobile device)

The steps within Microsoft Authenticator may vary slightly depending on the phone. Open the Authenticator app and click on the "+" symbol or, if you don't see it, click on the menu option with the 3 dots and then select "Add account".

Select "Work or school account".
Now select “Scan a QR code”. This should open the mobile device’s camera. Point the camera on the QR code on the setup screen and the Authenticator app will add your USI account. You can now select “Next” on the MFA setup screen on your PC and you will receive a notification from the Authenticator app. A number will appear on the screen. You must enter it in the Authenticator app to approve the request.

Once the request has been approved with the Authenticator app, the following confirmation screen will be displayed. Select “Next”.

At this point, you will receive confirmation that you have configured MFA on your account using the Authenticator app. Select "Done".
Change settings

You might want to change your MFA settings. For example, you might want to register the Authenticator app on a new phone or on a secondary phone. You can have up to 5 Authenticator apps registered for each account. Starting from Microsoft My Account (https://myaccount.microsoft.com), under “Security Info” select “Update Info”.

Take note of the current methods listed. If you have already set up MFA on your account using the Authenticator app, you should see it listed. The phone will be listed with an internal model number that may or may not match the name of the phone’s main model. Select “Add sign-in method” and from the drop-down list select “Authenticator App”.

You will then be asked which Authenticator app you are using. The recommended choice is Microsoft Authenticator.

Now follow the steps described above in the MFA wizard to set up your USI account on the Authenticator app on your new phone. Once the setup is complete, another Microsoft Authenticator will be listed on the account’s "Security Info" page. It is recommended to delete the old one for safety (unless you are still using it).
Stay signed in?

When you log in to your USI account, the following pop-up may appear asking if you want to “Stay registered?”. If you select Yes, account access will remain active until you explicitly disconnect from the account on that device/browser. If you access your account through Outlook on the web, this means that closing the browser will not interrupt the session and will not allow you to log out of the account. **It is not recommended to select** this option when accessing the USI account on machines shared with other users, as it could increase the risk of other users accessing the account.

---

**Stay signed in?**

Do this to reduce the number of times you are asked to sign in.

☐ Don't show this again

No  Yes