Activate two-factor authentication in Microsoft 365

Introduction

Two-factor authentication (commonly referred to as 2FA, MFA, multi-factor authentication) adds another layer of protection for your UT account and protects it from being used for malicious purposes even if your password has leaked. You can check how it works here.

NB! We recommend the Microsoft Authenticator and Google Authenticator apps. In addition, we recommend adding an SMS method in case something happens to the smart device where the applications are installed.

Both a smart device and a computer are required for setup.

First-time setup

The requirement to setup two-factor authentication is enabled for all university staff and students starting June 13, 2023. During your next login to Microsoft-associated applications (Outlook, Teams, Moodle), you will be prompted for additional information and the setup of two-step authentication.
1. When first logging in to Microsoft services, you will be prompted with a More information required window. Click Next.
2. Select I want to use a different method.

3. From the drop-down menu, select Phone and click Confirm.
4. Select **area code Estonia (+372)** and enter your **phone number**. Then click **Next**.

5. A **message will be sent to your phone number**, the sender is Microsoft and the content is a 6 digit code.
6. Enter the code on your browser and click Next.

7. Your phone was registered successfully. Click Next.
8. To finish the setup, click Done.

9. The next time you log in to Office365, in addition to the password, you will also be asked for the code that came with the message.
   If you are at your home or work computer, you can let the computer remember it, i.e. within 90 days, you will no longer be asked for the second-level code at a specific computer.
Do not trust a device you are not sure about.
After typing in the code, click **Verify**.

**Enter code**

- We texted your phone +XXX XXXXXX50. Please enter the code to sign in.

778296

- Don’t ask again for 180 days

More information

**Two-factor authentication using Microsoft Authenticator**

1. Install the [Microsoft Authenticator](#) application on your smart device via [Google Play](#) or [App Store](#).
2. On your computer, go to 365.ut.ee or kiri.ut.ee.

3. Log in using the format username@ut.ee (login with username and password).

Microsoft

Sign in

Email, phone, or Skype

No account? Create one!

Can't access your account?

Back  Next
4. Click on your profile select View Account.
5. Select **Update info**.

6. Select **Add sign-in method**.
7. From the menu, select **Authenticator app** and click **Add**.

8. In the next window click **Next**.

**NB!** If you accidentally chose the wrong authentication method, or if you want to set up the Google Authenticator app or SMS authentication instead, select I want to use a different authentication app.
9. To start your account set up, click **Next**.

Microsoft Authenticator

Set up your account

If prompted, allow notifications. Then add an account, and select "Work or school".

10. Leave the next window open on your computer and pick up your smart device.

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".
11. In the Microsoft Authenticator application select **Add account**.
Ready to add your first account?

Any Microsoft account or other type of account you add will appear here.

Add account
11. Select Work or school account.

12. Select Work or school account.
13. Select **Scan QR code** and scan the QR code in section 10 (the window you left open on your computer).

14. The number **72** is displayed to test the application.

![Microsoft Authenticator](image)
15. Once again, pick up your smart device, enter the number 72 and click Yes.

16. A confirmation that everything is working is displayed in the computer view.

17. Microsoft Authenticator setup was successful.
18. The next time you log in to the UT Microsoft 365 account, in addition to the password, you will be prompted to insert the code displayed into the **Microsoft Authenticator** mobile application. When logging in from a web browser, it is possible to remember the device for 180 days, so that you do not have to re-enter the second level of verification every time.

**NB! Use it only for a personal or work computer.**
Approve sign in request

1. Open your Authenticator app, and enter the number shown to sign in.

   65

No numbers in your app? Make sure to upgrade to the latest version.

Don't ask again for 180 days

I can't use my Microsoft Authenticator app right now

More information

Süsteemi logimiseks kasutage palun kasutajatunnust kujul kasutaja@ut.ee (näiteks kasutaja Tuuli Tudeng sisestab tuuli12@ut.ee)

To log in please use the username in the form username@ut.ee (for example user Tuuli Tudeng must use tuuli12@ut.ee)
Two-factor authentication using Google Authenticator

1. Install Microsoft Authenticator on your smart device via Play store or App store.
2. On your computer, go to 365.ut.ee or kiri.ut.ee, click your profile, select View Account, select Update info.
3. Select **Add sign-in method**.
4. Select I want to use a different authenticator app and click Next.

Microsoft Authenticator

Start by getting the app

On your phone, install the Microsoft Authenticator app. Download now

After you install the Microsoft Authenticator app on your device, choose "Next".

I want to use a different authenticator app

Cancel  Next

5. A QR code will be displayed. Keep this window open.

Authenticator app

Scan the QR code

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

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

Can't scan image?

Back  Next
6. Pick up your smart device and scan the QR code by clicking **Scan a QR code in Google Authenticator application**.

![Scan a QR code](image.png)

7. After scanning the QR code, Google Authenticator two-factor authentication is activated.

![Two-factor authentication using SMS](image.png)

**Two-factor authentication using SMS**

1. On your computer, go to [365.ut.ee](http://365.ut.ee) or [kiri.ut.ee](http://kiri.ut.ee), click your profile, select View Account, select Update info.
2. Select Add sign-in method.

Add sign-in method
3. From the drop-down menu, select **Phone** and click **Add**.

   **Add a method**

   Which method would you like to add?

   ![Select Phone](image)

   ![Add button](image)

4. Select **area code Estonia (+372)** and enter your phone number. Then click **Next**.

   **Phone**

   You can prove who you are by texting a code to your phone.

   What phone number would you like to use?

   ![Select area code](image)

   ![Text me a code](image)

   Message and data rates may apply. Choosing Next means that you agree to the **Terms of service** and **Privacy and cookies statement**.

   ![Cancel](image)

   ![Next button](image)
5. A message will be sent to your phone number, the sender is Microsoft and the content is a 6 digit code.

6. Enter the code on your browser and click Next.

7. SMS authentication is activated. To finish, press Done.

8. After setting up, the mobile phone number to which it is associated will be displayed.
9. The next time you log in to Office365, in addition to the password, you will also be asked for the code that came with the message. If you are at your home or work computer, you can let the computer remember it, i.e. within 180 days, you will no longer be asked for the second-level code at a specific computer.

*NBI!* Do not trust a device you are not sure about.

---

**Enter code**

☐ We texted your phone +XXX XXXXXX50. Please enter the code to sign in.

**Code**

☑ Don't ask again for 180 days

Having trouble? Sign in another way

More information

[Verify]