2022-12-14

Setting up MFA (multi-factor authentication)

To improve the security when logging in with a JU account on private devices, a security method is needed, MFA. This method will make it harder for unauthorized people to access a JU account. MFA is not normally needed on JU computers. *Note that Mozilla Firefox will prompt the MFA verification on a JU device, whether it is in Private mode or not.*

JÖNKÖPING UNIVERSITY

Configure MFA

- The following information is displayed the first time you log in to Office365 (https://www.office.com) from a web browser on a private computer. Click **Next** to start the configuration.
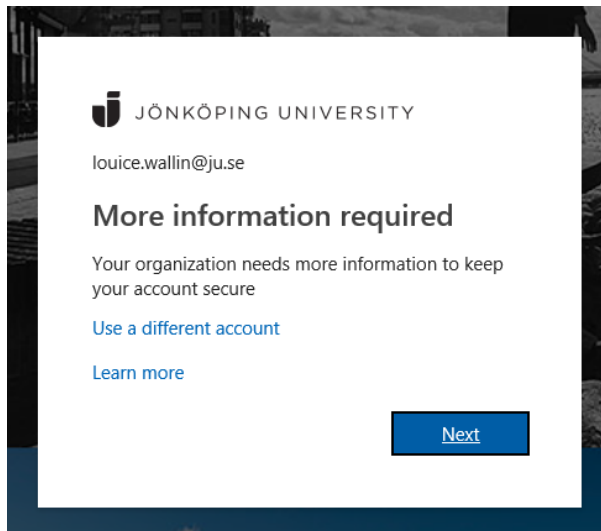
Choose authentication method

Microsoft Authenticator is set as default, if you want to change method, select **Choose security info.** If you want to add additional methods, read the part *Configure additional MFA methods* in the end of this manual.

- The following steps will show how to set up the *Microsoft Authenticator* app.
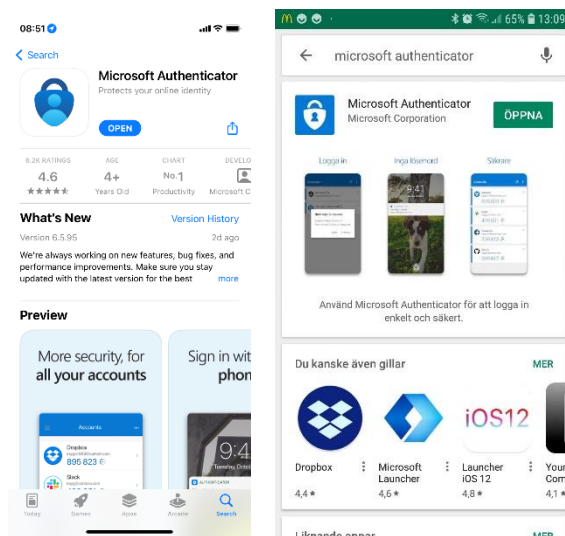

Click here if you want to use phone/text message for authentication instead.
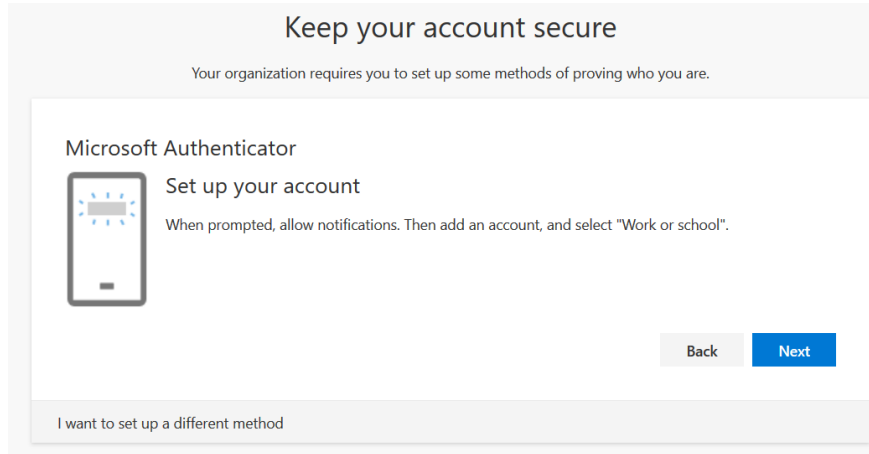
Install Microsoft Authenticator

- Before you continue, download and install the *Microsoft Authenticator* app on your phone (*AppStore* for iOS and *Play Store* for Android).
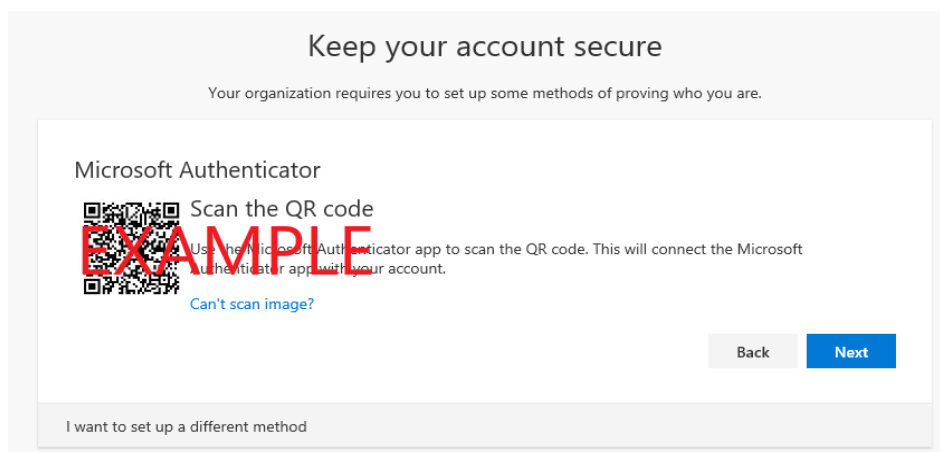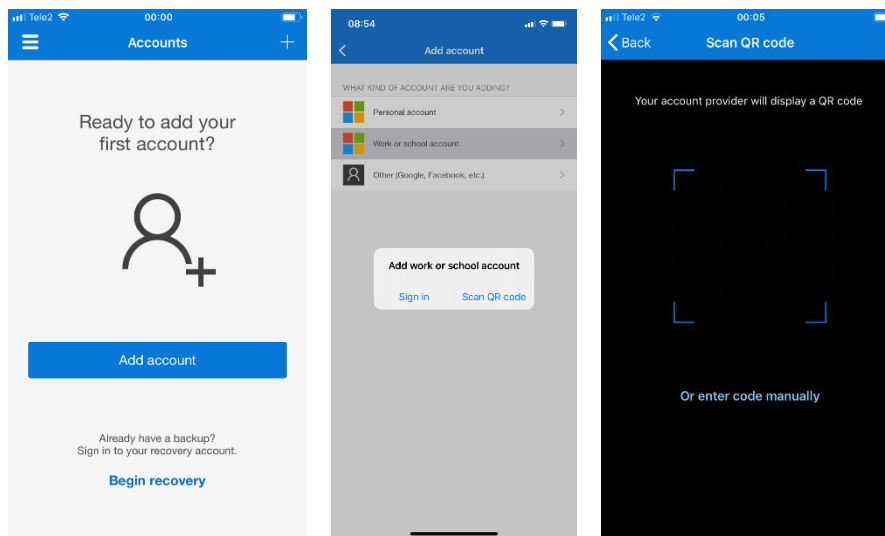
JÖNKÖPING UNIVERSITY

- When the app is installed, go back to the web browser and click **Next**, followed by **Next** on the dialog box *Set up your account.*
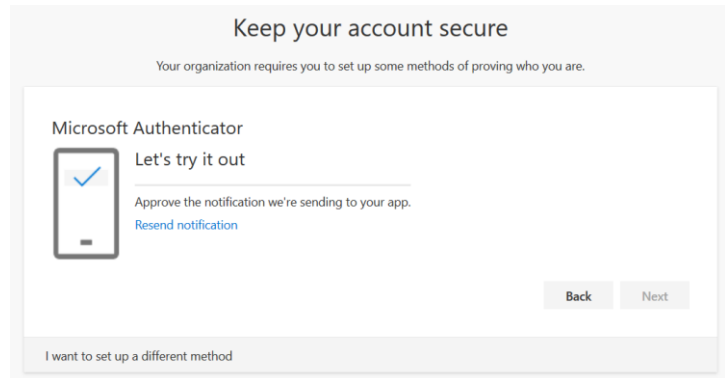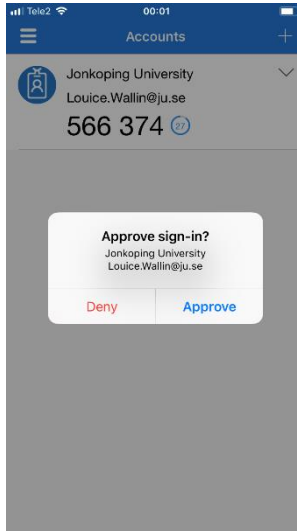

- Open *Microsoft Authenticator* on the phone. Select **Add account**, followed by **Work or school account,** select **Scan QR code** and then scan the QR code that is showing in the web browser.
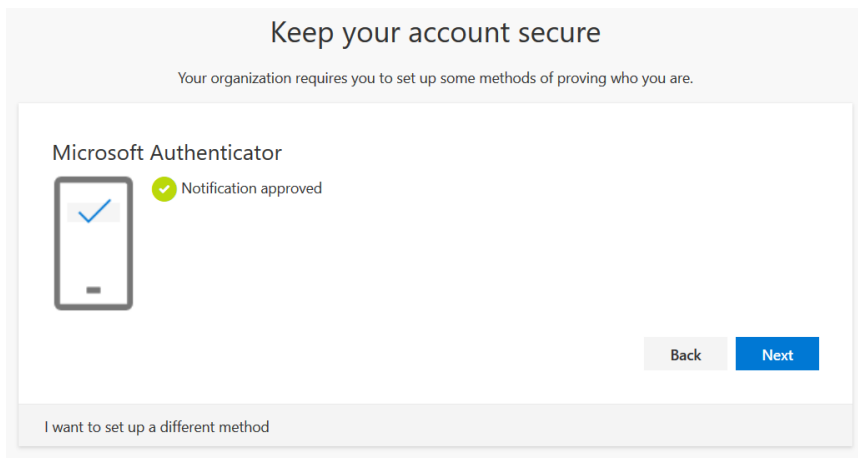
- When you have scanned the QR code, your JU account should come up as shown below. Click **Next** on the dialog box in the web browser and then **Approve** on the authenticator app.
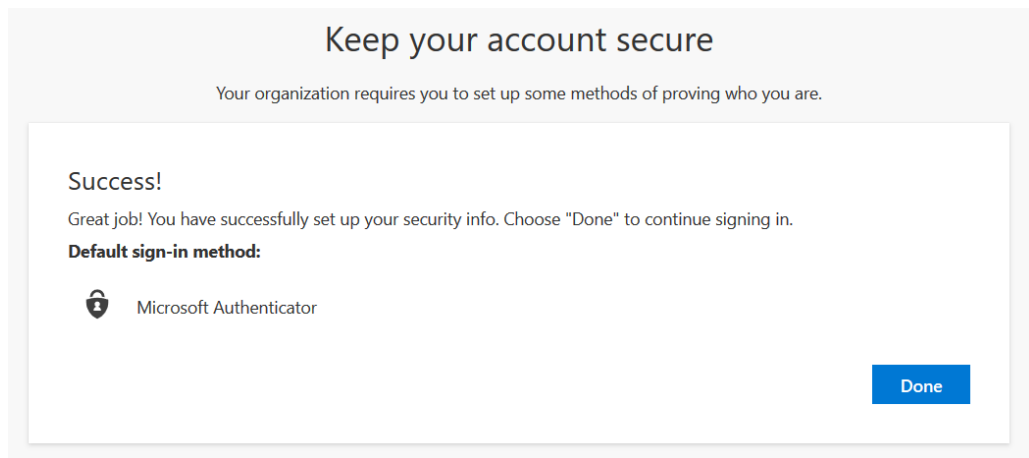

- Click **Next**.

- The message below will show when you're finished. Click **Done** and you are good to go.

Configure additional MFA methods

Phone, text message and authentication apps

By default, Microsoft will presume that the Microsoft Authenticator app has been set up for MFA verification, but it's recommended that you configure additional methods.

The available methods are:

- Get a **call** from Microsoft (N.B! This is an auto generated call from the US and the number is *+1(855) 330–8653*). Confirm the login with the *pound key (hashtag)*. You can set up two different phone numbers for verification.

- **Text message**. Enter a mobile phone number to which you want to receive the message. A code will be sent as a text message, and you enter that code in the web browser

- Additional device with *Microsoft Authenticator* or another authentication app (e.g. *Google Authenticator*).
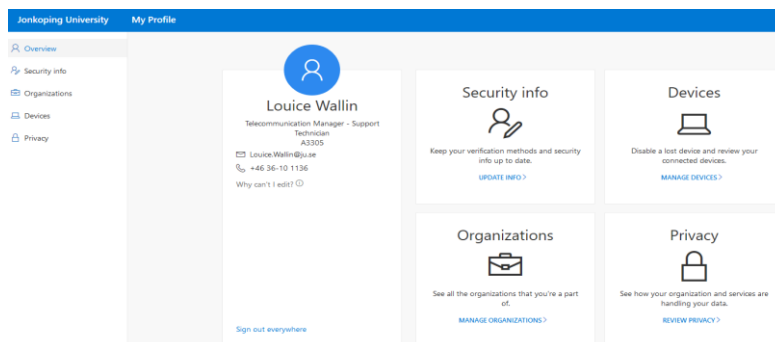
How to configure additional methods

- Log in to https://office.com and go to the O365 app launcher ⠿ in the upper left corner. Select **All apps** followed by **MFA – My Profile**.
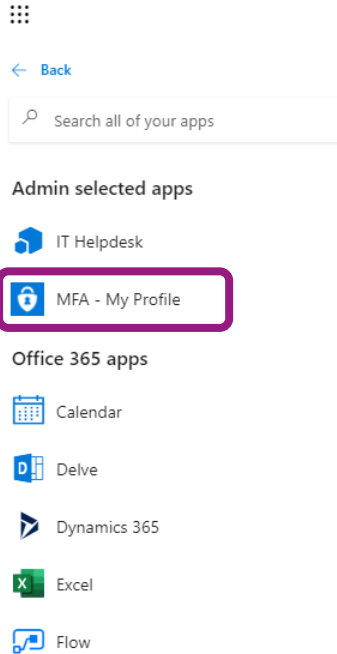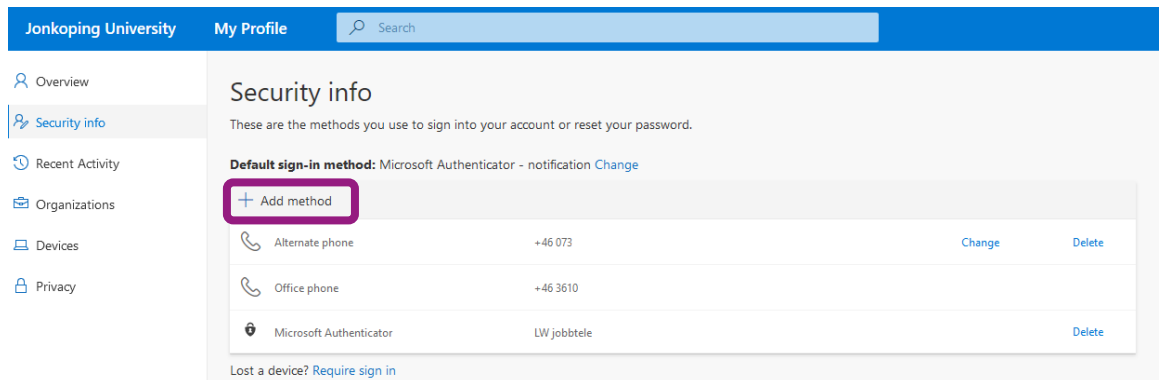

- The **My Profile** page will show information regarding security and MFA.
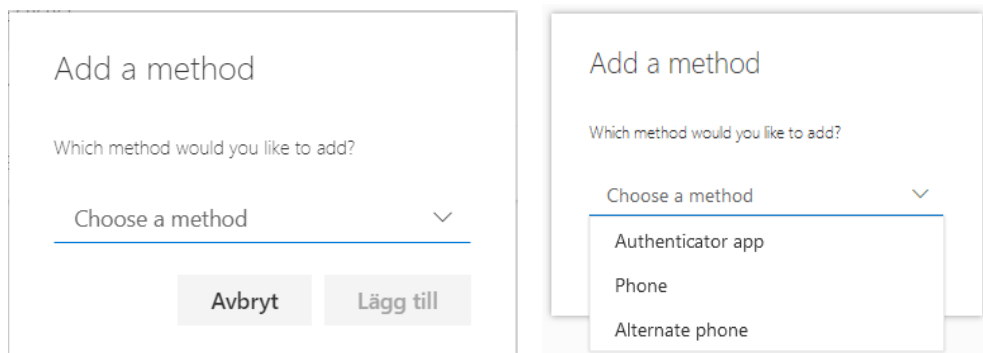
JÖNKÖPING UNIVERSITY

- If you want to add other MFA methods, go to *Security info*.
  For security reasons, you will have to log in one more time and verify with MFA, even on a JU device.

- Here you can see the methods that you have configured and select which method that you want as default.
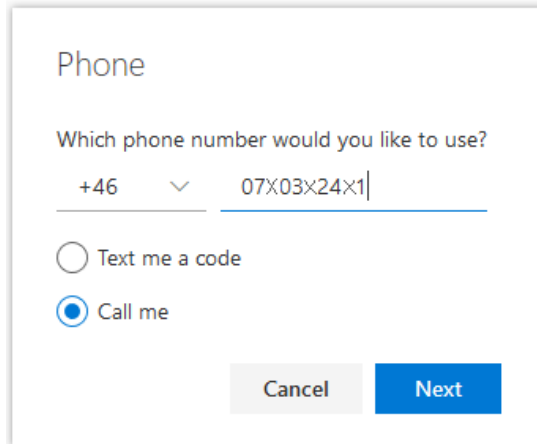

- Select *Add method* to add another method.

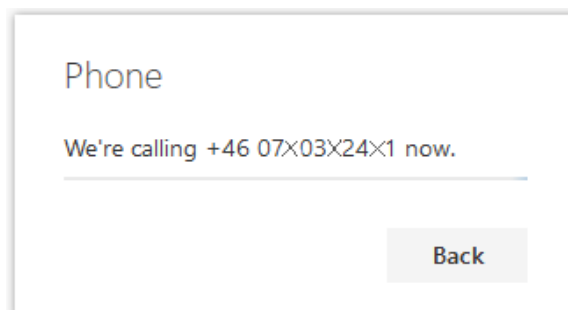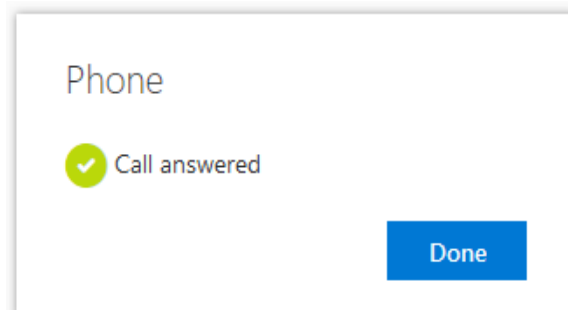- For example, select *Phone* to add a phone number.

JÖNKÖPING UNIVERSITY

- Select *Text me a code* if you want to receive a text message with a generated code for verification or *Call me* to receive an auto generated call. Click **Next**.

- The system will now verify the number that you have entered. Approve the request on the actual device.

JÖNKÖPING UNIVERSITY

Description of the options on *My Profile*:

- *Security info*:
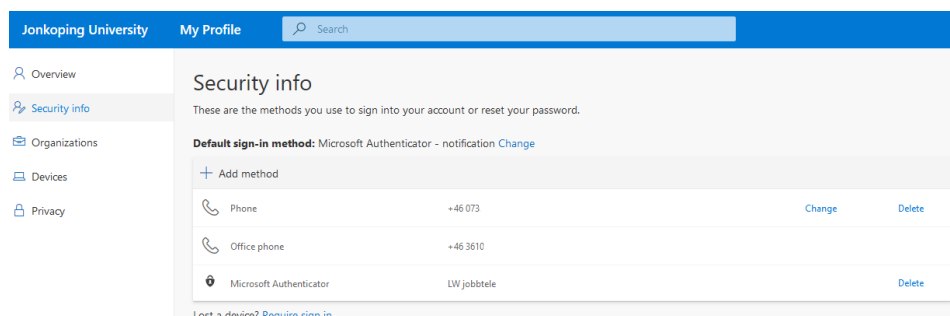
In this view you can see all your configured log in methods. It is recommended to use *Microsoft Authenticator* primarily and supplement with a cell phone number. You can also change default method and remove devices that you no longer want to use for authentication.

- If you want to change the default method for MFA, Click **Change** at *Default sign-in method*.
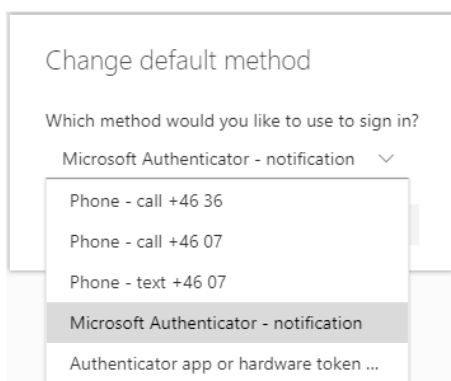
*In this example, you can choose between receiving a call, receiving a text message or approve with **Microsoft Authenticator:***
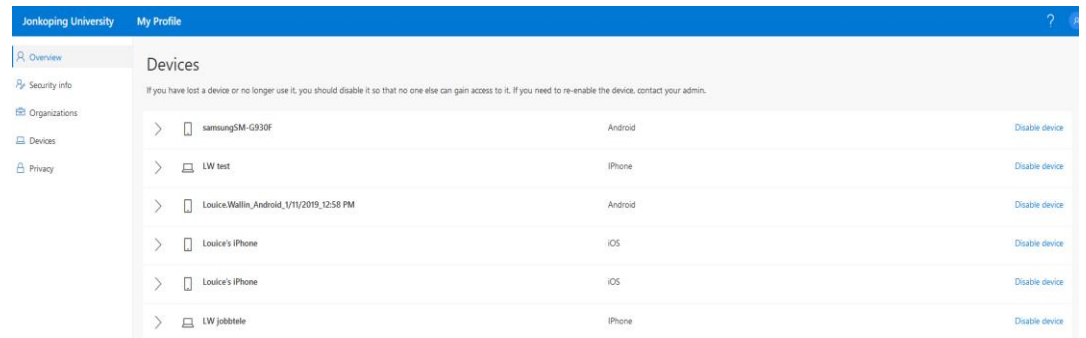***Notification**: Receive a prompt in the Microsoft Authenticator app to approve the login (recommended method).*
***App or hardware token**: A six-digit code that changes every 30 seconds that you enter at login.*
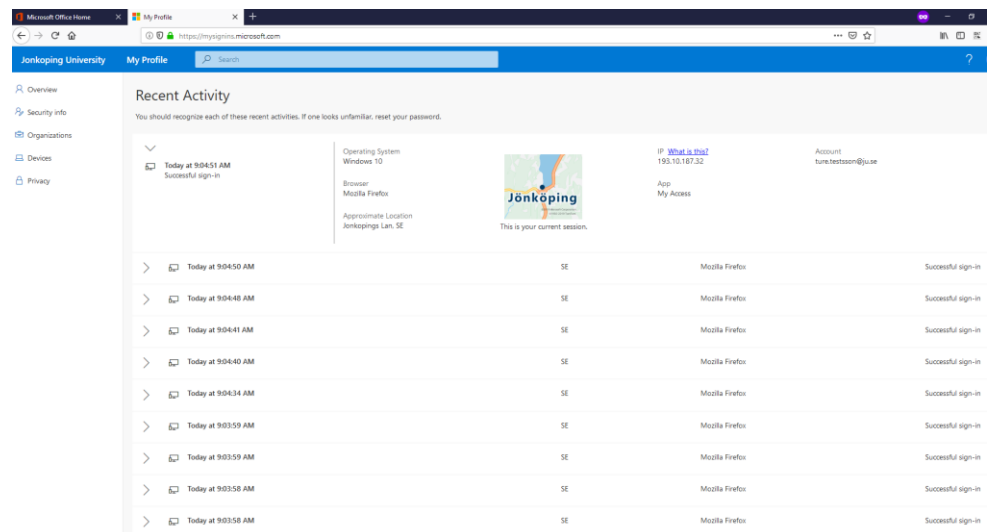
o *Devices*:

This view is showing your registered devices. It will also show private devices where you have, for example, installed the Office suite. Here you can also remove devices that you no longer use.

If you want to see information about recent successful sign ins/attempted sign ins on your account, go to https://mysignins.microsoft.com/.

JÖNKÖPING UNIVERSITY

Try out the alternate MFA method

- Open a web browser on a private device or open a web browser in Incognito/InPrivate mode on a JU computer. You can also use Mozilla Firefox on a JU computer. Go to https://office.com.

- Log in but stop at the step **Approve sign in request** and select **I can't use my Microsoft Authenticator app right now**.
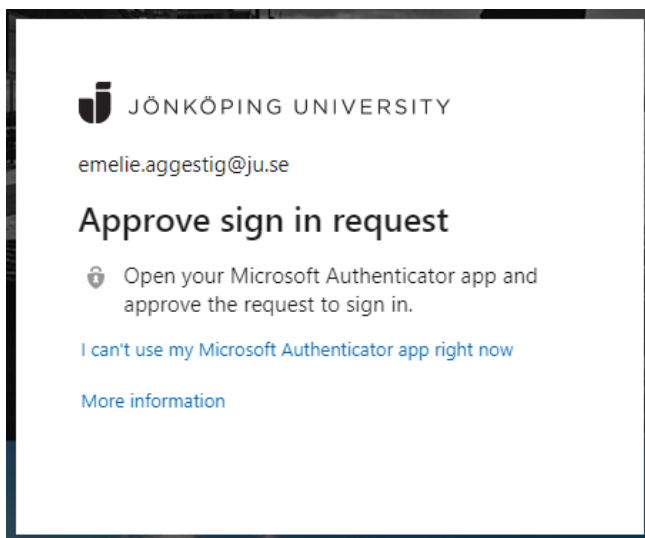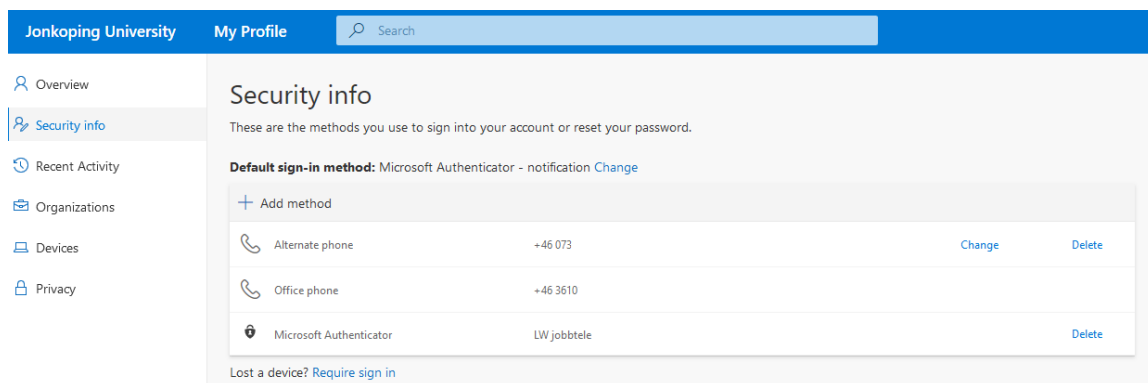

- Select the method that you want to try.
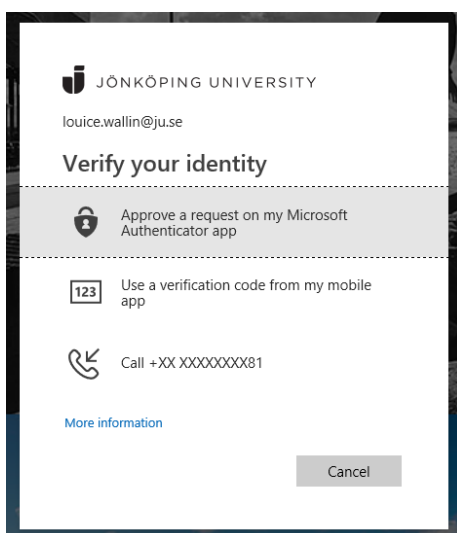
Delete MFA methods

- Log in to https://office.com and go to the O365 app launcher ⠿ in the upper left corner. Select **All apps** followed by **MFA – My Profile.**

- Go to **Security info** to view you configured methods.

- Click **Delete** on the method that you want to remove.
  Note! Keep at least one of the methods you've added yourself. If you delete all methods you need to contact IT helpdesk to be able to log in again.

- Open *Microsoft Authenticator* (or the authentication app that you are using) and select the account that you want to remove, tap on the cogwheel in the upper right corner and select **Remove account.**