VILNIAUS GEDIMINO
TECHNIKOS UNIVERSITETAS
INFORMACINIŲ TECHNOLOGIJŲ
IR SISTEMŲ CENTRAS

TWO FACTOR AUTHENTICATION (MFA) CONFIGURATION

Two-factor authentication (2FA, MFA), sometimes called two-factor authentication or dual authentication, is a security process that requires more than one means of authentication to authenticate a user. This process is needed for a better search for user data and resources to take advantage of.

Use the link (1st link) to successfully configure two-factor authentication:

1st link:: https://aka.ms/mfasetup

Your mobile device requires Internet access to complete the successful steps below.

Clicking on the link (1 link) will take you to the login page (Figure 1).

• For Students: Log in to the Student email address: (firstname.lastname@stud.vilniustech.lt).

• For Employees: Sign in with Employee Email address: (lastname.lastname@vilniustech.lt).

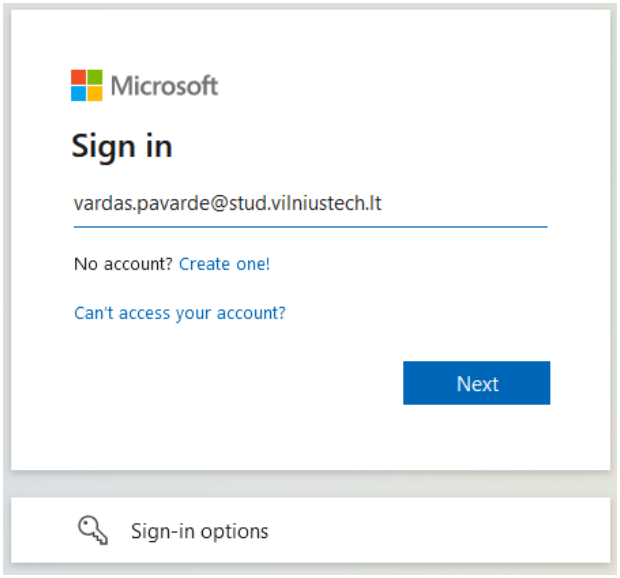

Figure 1. Login to Your account

After successfully logging in to your account, click Next (Figure 2):

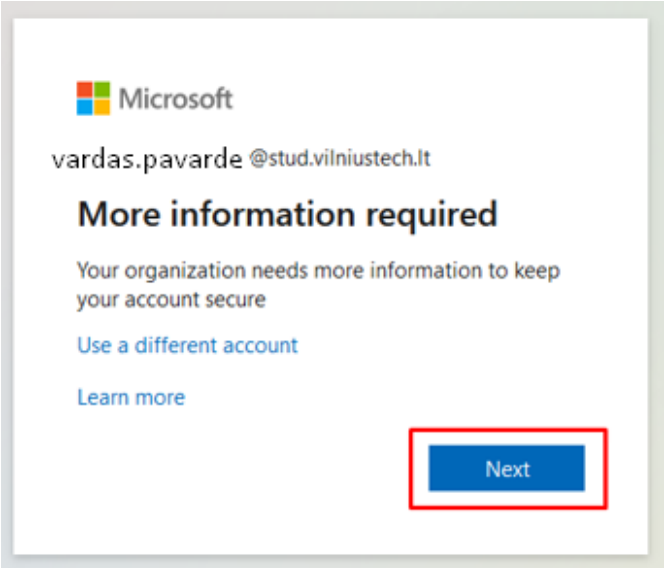

Figure 2. Select *Next*

Configure the settings (Figure 3):

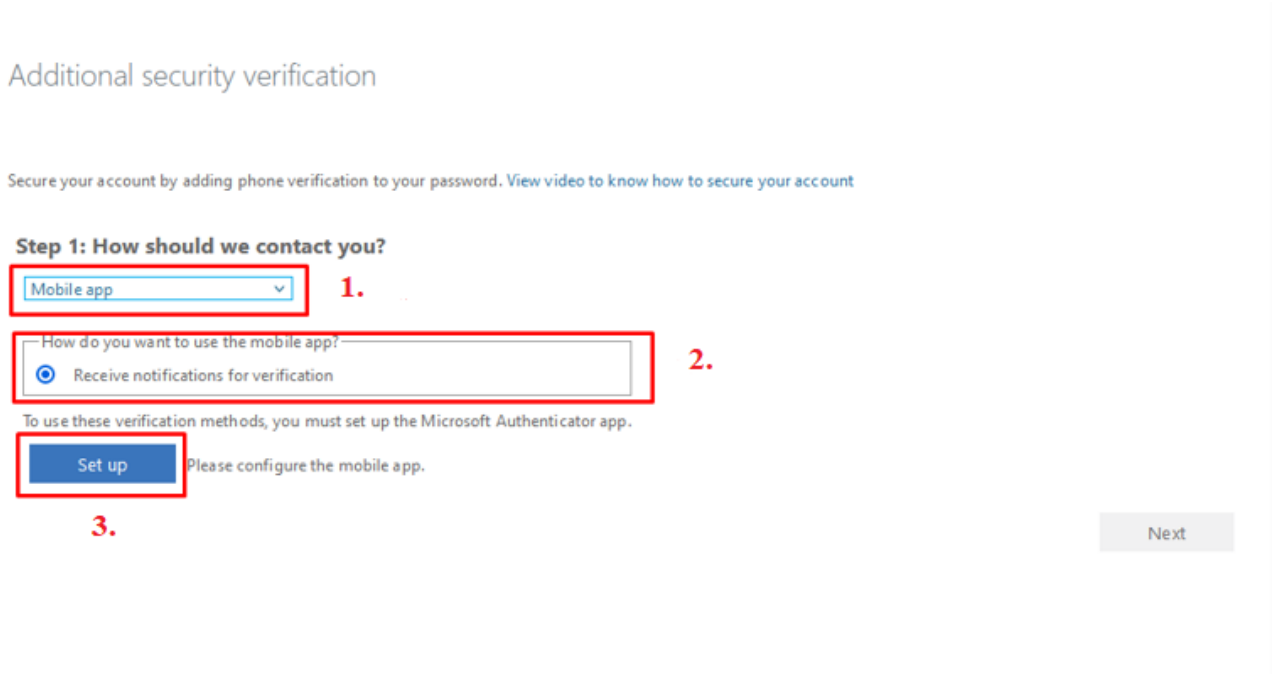

Figure 3. Configuring two-factor authentication

1. Choose a mobile app
2. Check the box
3. Click *Set up*. Clicking this button will generate a QR code for you to scan using the mobile app

- Download the Microsoft Authenticator app on your phone from the Google Play Store (Android OS) or Apple App Store (Apple iOS)
- Type "Authenticator" in the search

The App icon looks like this (Figure 4):

Figure 4. Icon of the Microsoft Authenticator App

1. Install the app on your mobile device
2. After launching the App, select *Scan a QR code*
3. Use the app to scan the QR code (Figure 5):

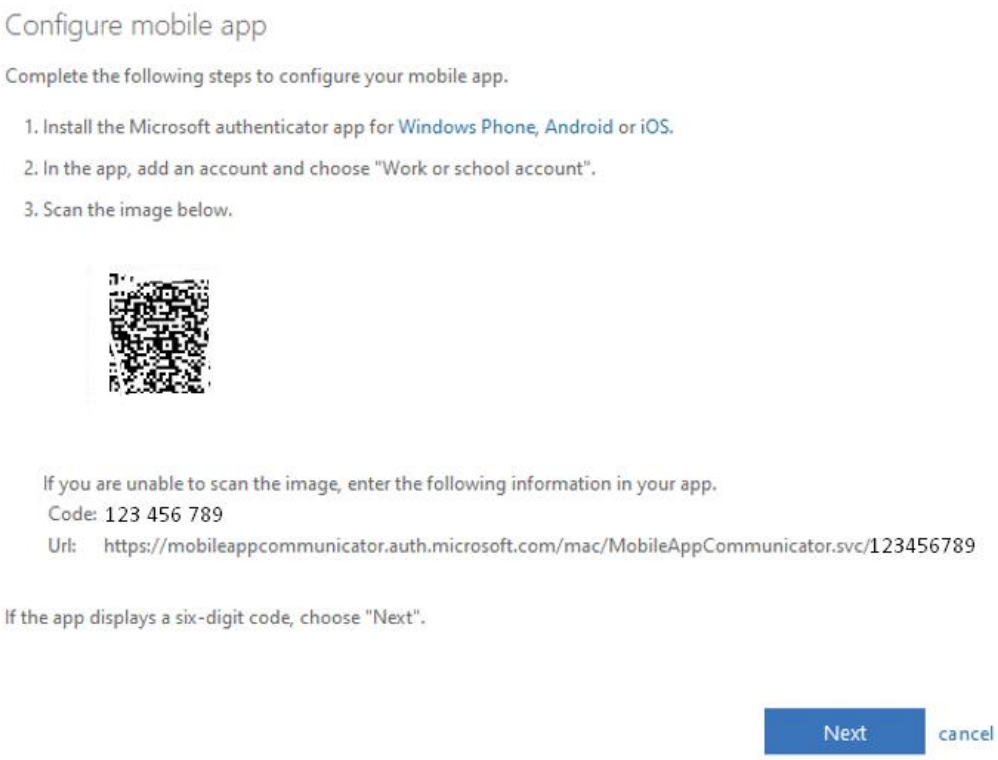

Figure 5. Scanning the QR code

There is a chance that the QR code will not be scanned the first time, so you will be redirected to the next window where you will need to enter the code and URL link (Figure 6). You can also press *Cancel* and press *Set Up* again - a new QR code will be generated, which you can scan again using the app:

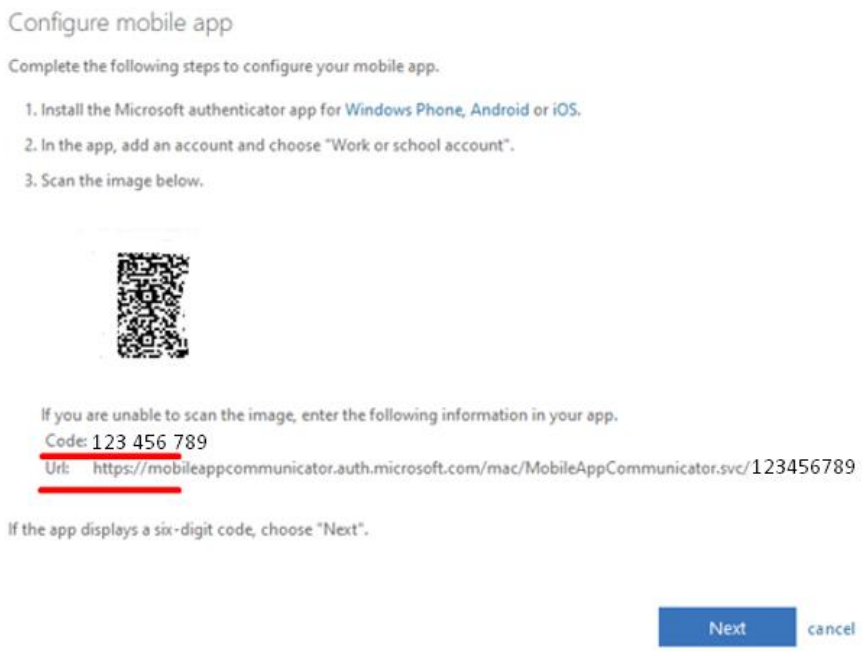

Figure 6. Code and URL link

- After you have scanned the QR code using the Microsoft Authenticator App (if that did not work, make sure you entered the code and the URL link into the App before proceeding further), click Next (Figure 6).
- You should receive a notification on your phone when you need to activate your account. Agree to the message.

- In the next step, select your country (It does not have to be Lithuania as shown in the screenshot) (Figure 7).
- Provide your mobile phone number (Figure 7):

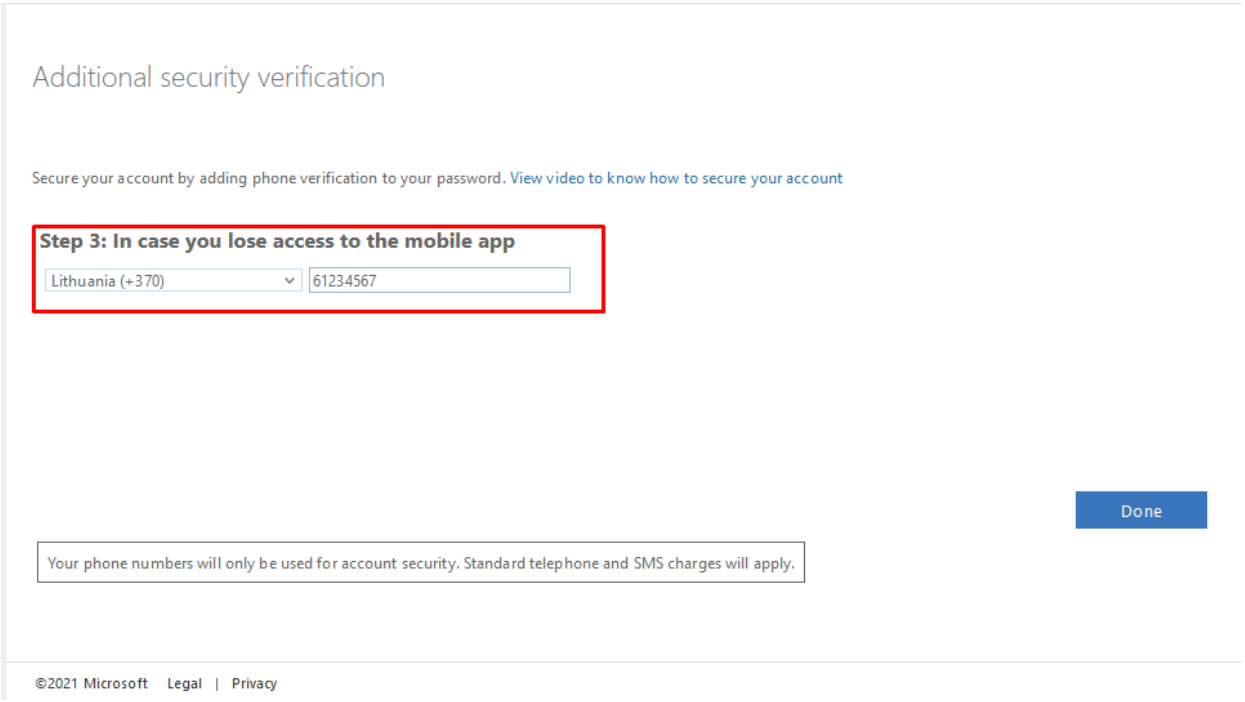

Figure 7. Additional protection to prevent account loss

- Select *Done*
- You will be redirected to another window asking you to confirm the login on your mobile device (Microsoft Authenticator app)
- Accept the message on the mobile device (Microsoft Authenticator app)

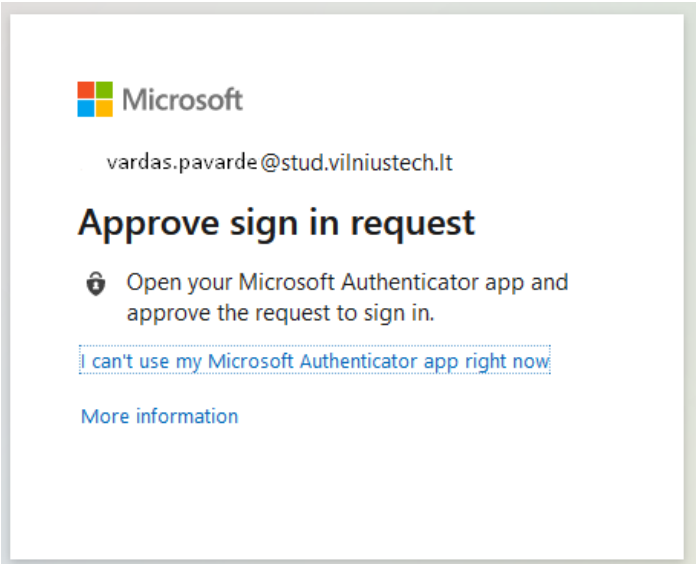

Figure 8. Account Login Confirmatio

After confirming the login in the mobile app, you will be redirected to a window where you will see a summary of two-factor authentication (MFA) (Figure 9). You can change the basic settings there.

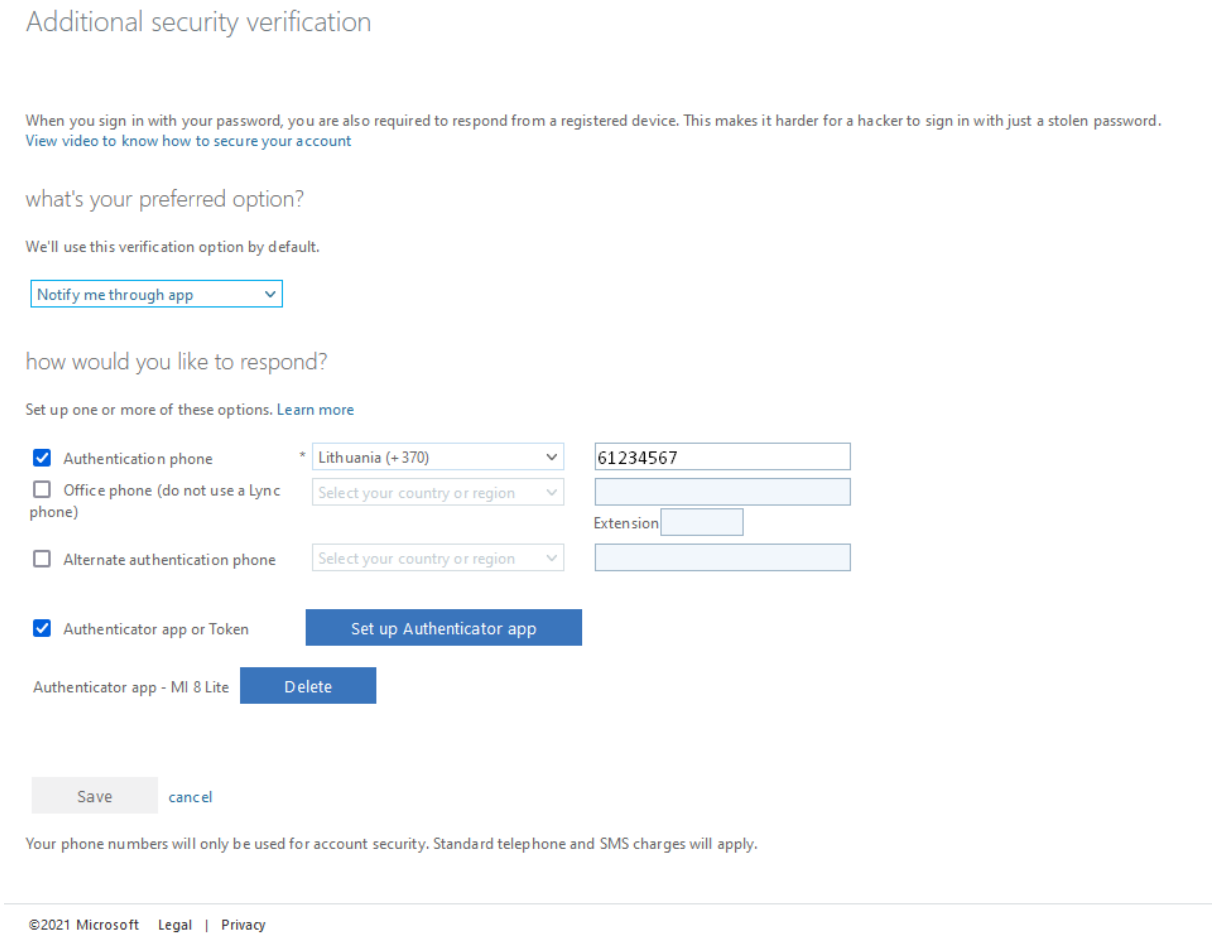

Figure 9. Summary of two-factor authentication (MFA) settings

If you are satisfied with all the settings you have configured, **no action is required in this window**. You can sign out of your account and turn off this window (you'll see your email address at the top right of the screen. Click on it and select Sign out).

If you have any questions, register the application using this link: https://pagalba.vgtu.lt/, select English language (EN) on the top right of the screen, select section **IT Helpdesk**.