

TWO FACTOR AUTHENTICATION (MFA) CONFIGURATION

Two-factor authentication (MFA, MFA), sometimes called two-factor authentication or dual authentication, is a security process that requires more than one method of authentication to identify a user. This process is necessary to better protect user data and the resources that the user seeks to access.

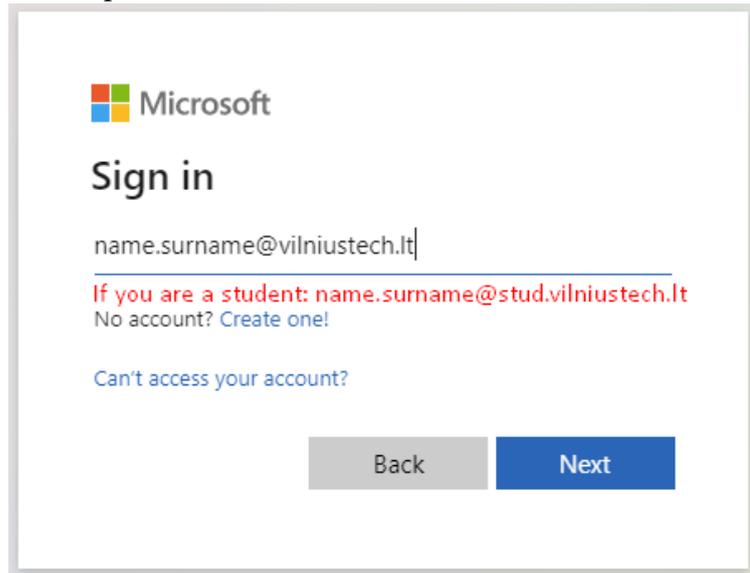
To perform the steps below, your mobile device and computer need internet access.

- **For Students:** use your student email address (name.surname@stud.vilniustech.lt)
- **For employees:** use your employee email address (name.surname@vilniustech.lt)
- If you are both an employee of VILNIUS TECH and a student of VILNIUS TECH, then MFA needs to be configured for the student and employee accounts.

Open the following link in your browser to start the MFA configuration process:

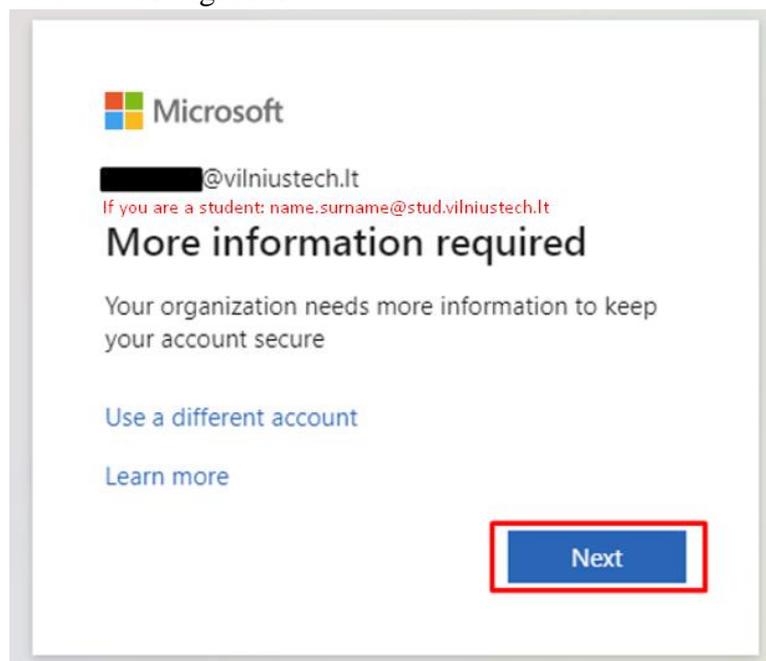
<https://aka.ms/mfasetup>

In the login window (<https://aka.ms/mfasetup>), enter the e-mail of the Employee or Student email address and password:



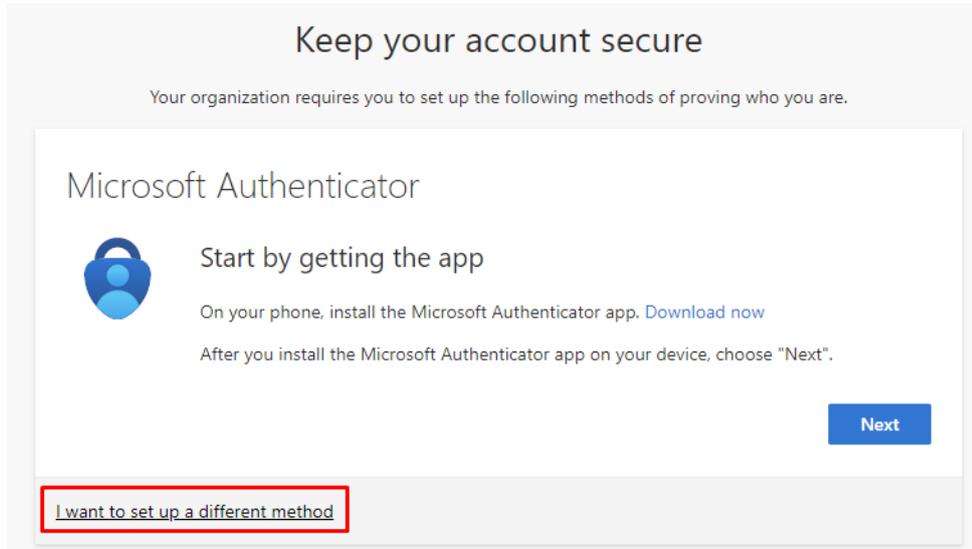
The image shows a Microsoft sign-in page. At the top left is the Microsoft logo. Below it is the text "Sign in". A text input field contains the email address "name.surname@vilniustech.lt". Below the input field, there is a red line of text: "If you are a student: name.surname@stud.vilniustech.lt". Underneath that is a blue link: "No account? Create one!". Further down is another blue link: "Can't access your account?". At the bottom right, there are two buttons: a grey "Back" button and a blue "Next" button.

Click *Next* to start the MFA configuration:



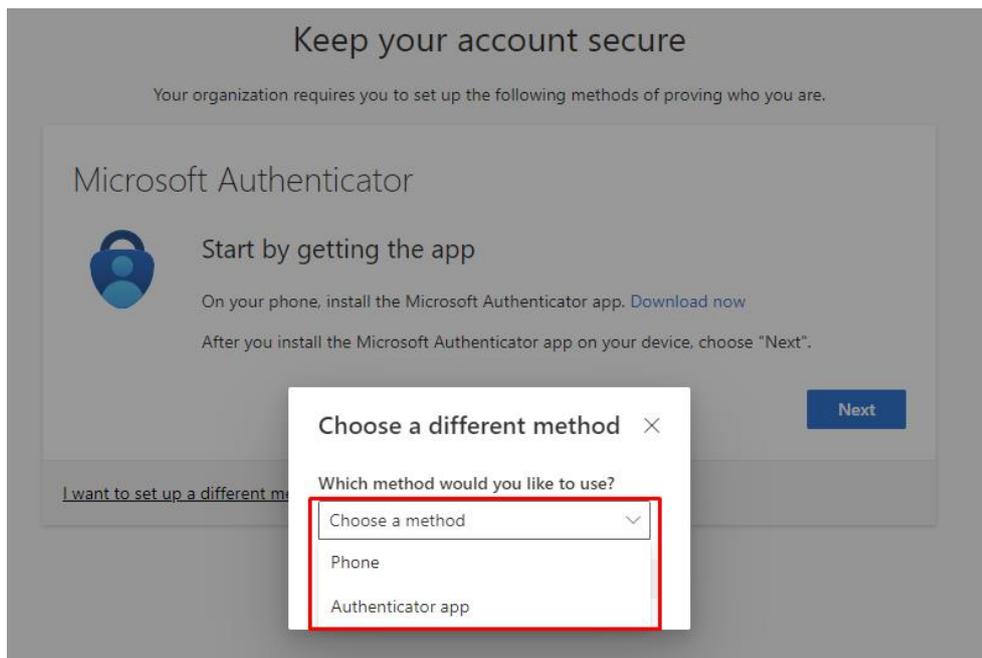
The image shows a Microsoft "More information required" screen. At the top left is the Microsoft logo. Below it is the text "@vilniustech.lt" with a black redaction box over the name part. Below that is a red line of text: "If you are a student: name.surname@stud.vilniustech.lt". The main heading is "More information required". Below that is the text: "Your organization needs more information to keep your account secure". There are two blue links: "Use a different account" and "Learn more". At the bottom right, there is a blue "Next" button, which is highlighted with a red rectangular border.

Select the desired authentication method:



In the list, you can choose authentication between an app and a phone number. At least one must be selected, but 2 authentication methods can be configured.

Select the desired method and confirm the selection (*Confirm*):



MFA CONFIGURATION STEPS IF YOU SELECTED AN APP AS THE AUTHENTICATION METHOD

Configuration using Phone number is given below in the instructions. Step "Configuration steps for MFA using phone number as authentication method".



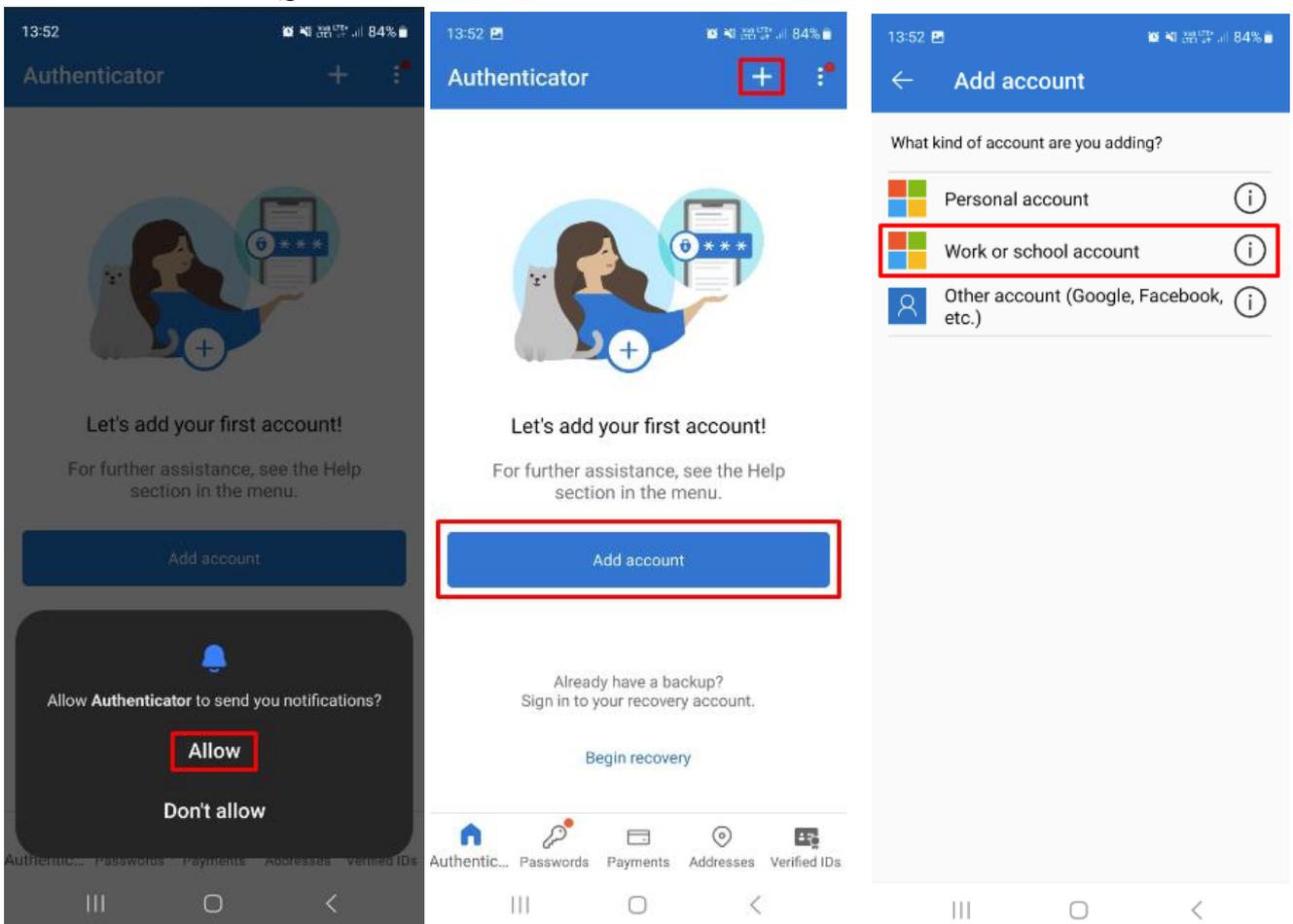
Download the app with this icon:

Download links:

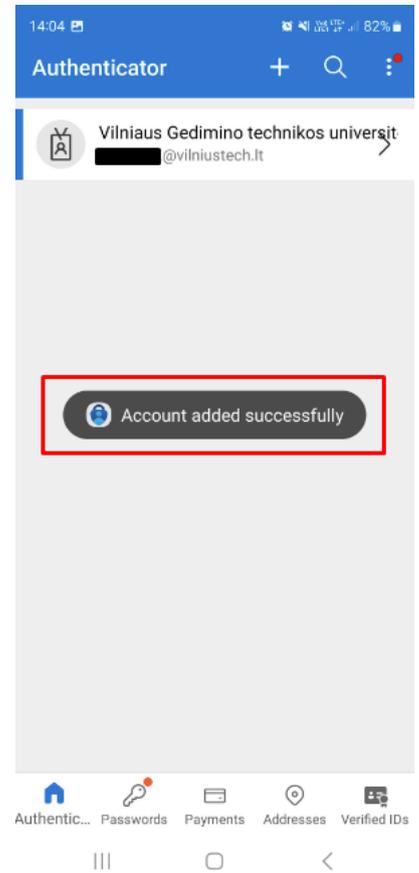
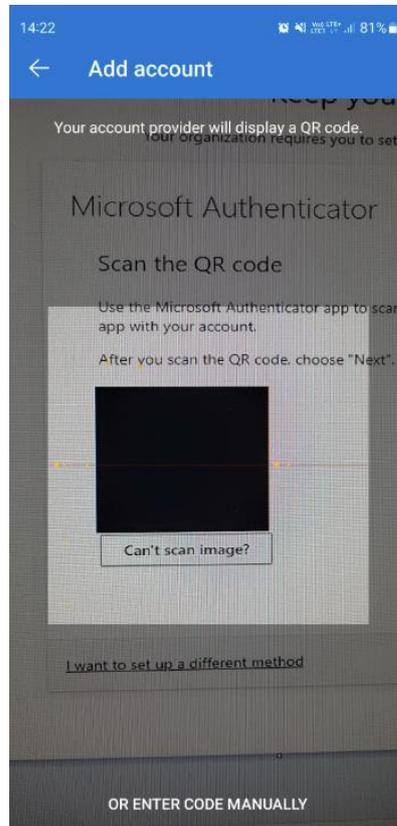
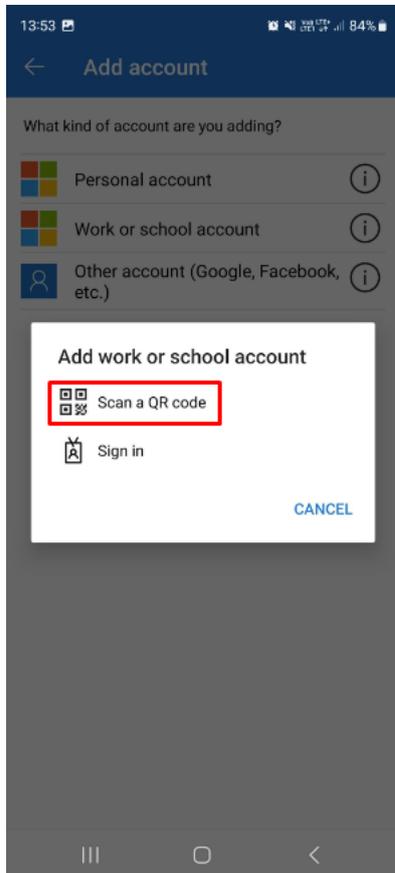
- Google play (Android):
<https://play.google.com/store/apps/details?id=com.azure.authenticator&gl=us>
- Apple store (iOS):
<https://apps.apple.com/us/app/microsoft-authenticator/id983156458>

Launch the app. **During the MFA configuration do not exit *Microsoft Authenticator* app:**

- Select Allow, so that the phone receives notifications about any connections to your account
- Select *Add account* or select the plus sign at the top of the screen
- Select *Work or school account*
- Select *Scan a QR code*



- **By using *Microsoft Authenticator* app** scan the QR code displayed on the computer screen **(there is no need to launch an additional camera app. QR code scanning is done using the *Microsoft Authenticator* app)**
- After successfully scanning the QR code, you will see a message that the account has been added, **however, after completing these steps, it is mandatory to make a first test confirmation (presented below in the instructions)**



After successfully scanning the QR code and adding the account to the app, click Next.

Keep your account secure

Your organization requires you to set up the following methods of proving who you are.

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".



Can't scan image?

[Back](#) [Next](#)

[I want to set up a different method](#)

After selecting *Next*, you will see a message on the computer screen that you need to confirm the connection to your account on the phone:

Keep your account secure

Your organization requires you to set up the following methods of proving who you are.

Microsoft Authenticator



Let's try it out

Approve the notification we're sending to your app.

[Back](#) [Next](#)

[I want to set up a different method](#)

After confirming the message on the phone, a message will appear on the computer screen that the connection has been successfully confirmed. Click *Next*.

Keep your account secure

Your organization requires you to set up the following methods of proving who you are.

Microsoft Authenticator



✔ Notification approved

Back Next

[I want to set up a different method](#)

Click *Done*.

Keep your account secure

Your organization requires you to set up the following methods of proving who you are.

Success!

Great job! You have successfully set up your security info. Choose "Done" to continue signing in.

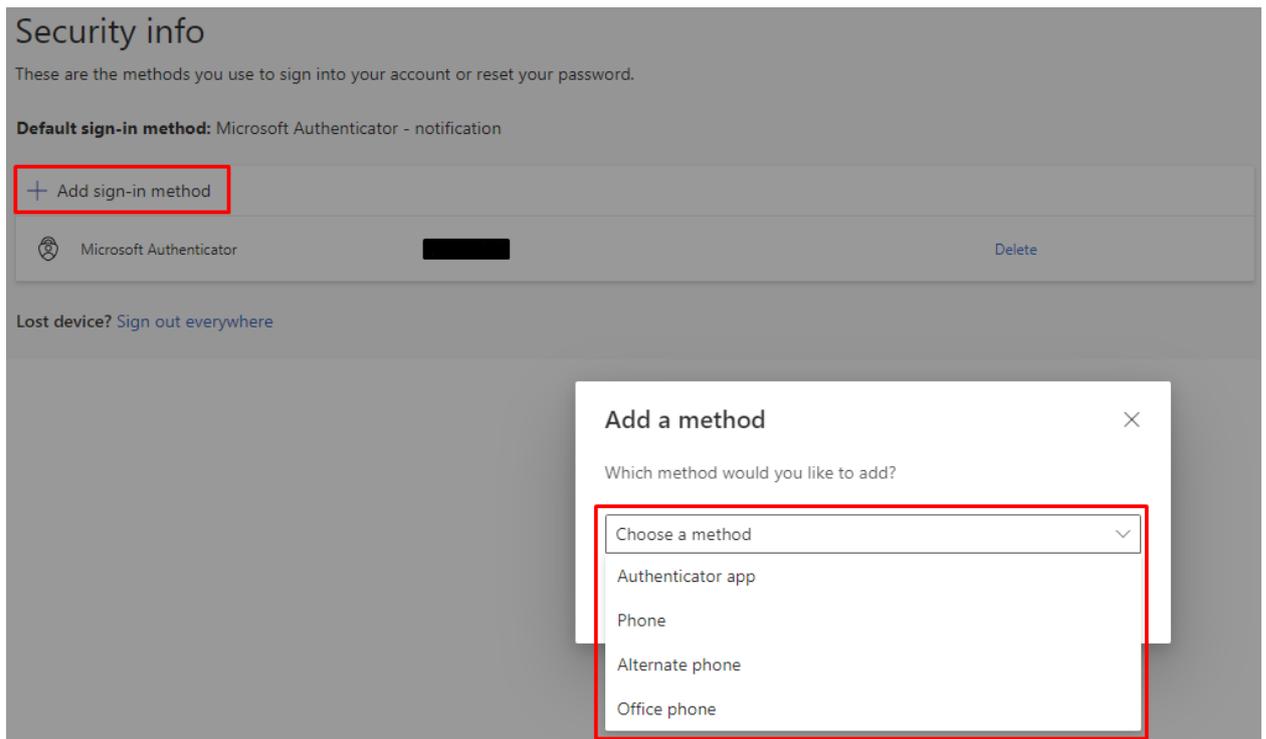
Default sign-in method:



Microsoft Authenticator

Done

After successful configuration, you will be redirected to a page where you can add another, additional authentication method (this is optional):

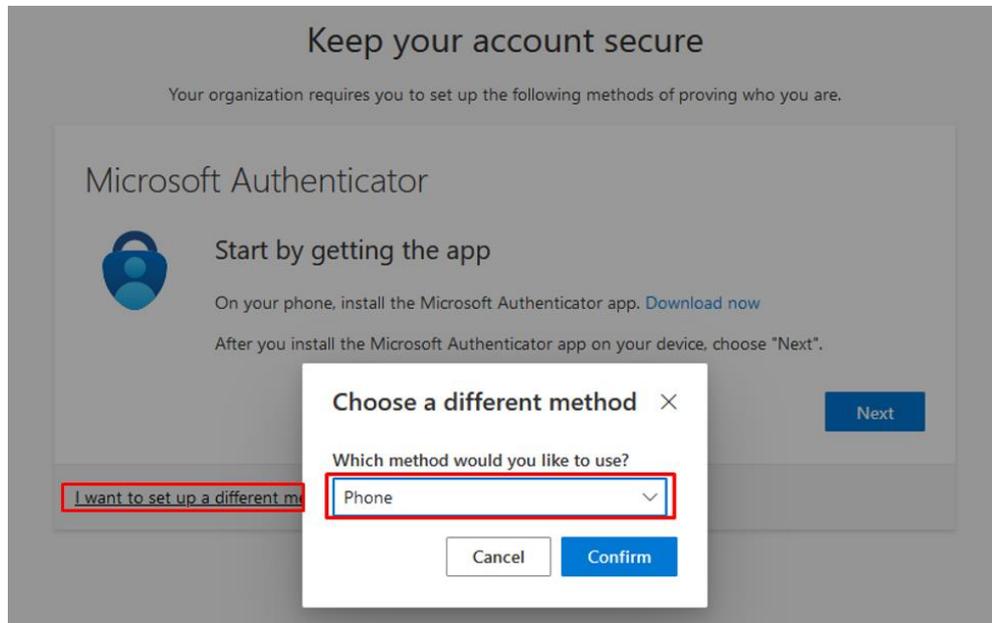


You can make future changes to your account's MFA configuration using this link: <https://mysignins.microsoft.com/security-info>

MFA configuration using the *Microsoft Authenticator* app is complete.

CONFIGURATION STEPS FOR MFA USING PHONE NUMBER AS AUTHENTICATION METHOD

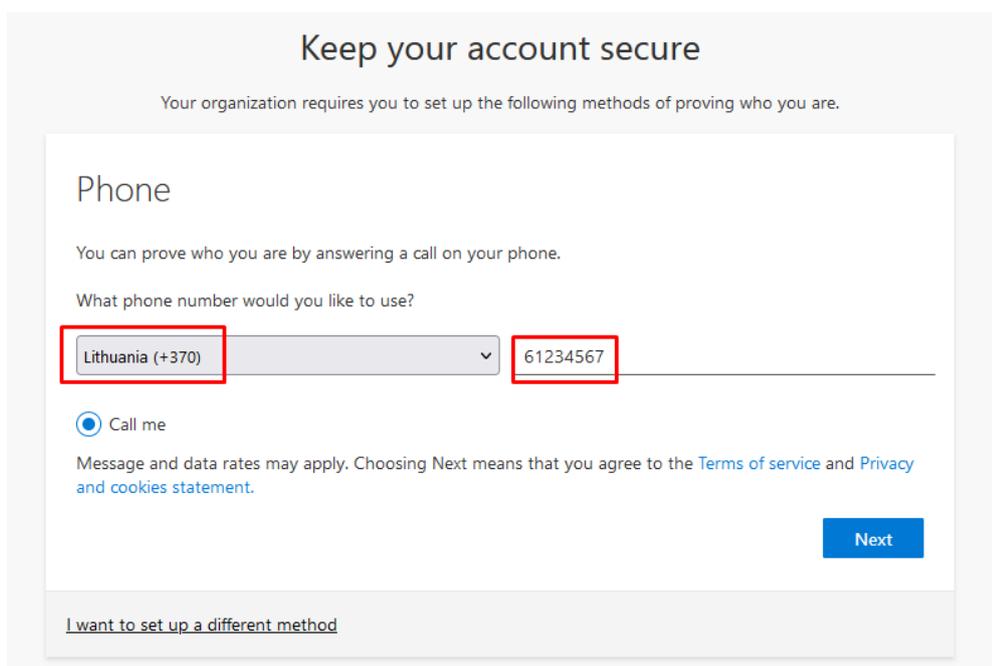
Confirm the choice to authenticate using a phone number (*Confirm*):



Choose from the list which country your phone number belongs to.

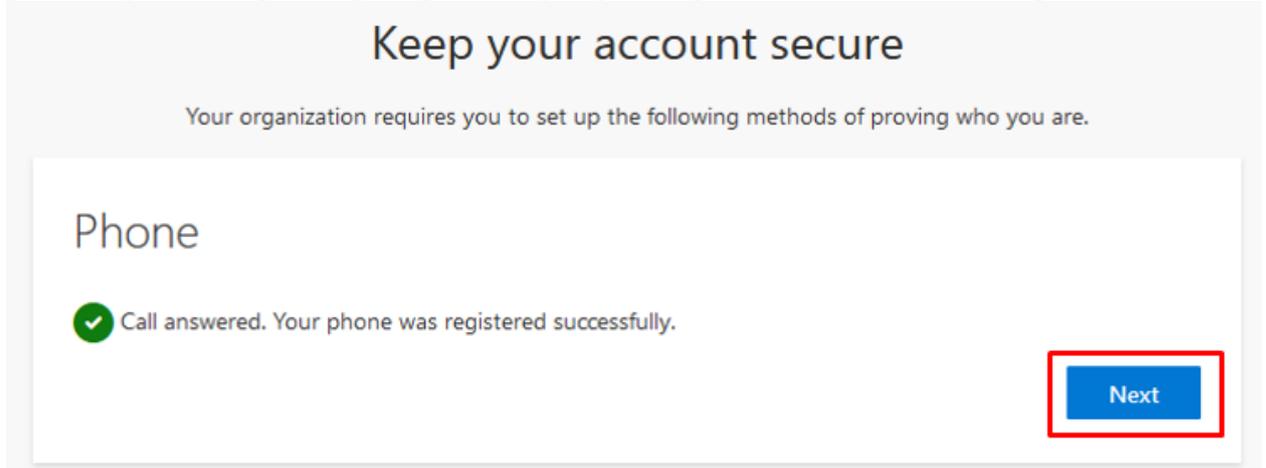
If it is a Lithuanian number, then it must be entered in the box on the right in the following format: 61234567. The number must begin with the number 6.

+370..., 86... and other formats entered in the box are invalid:

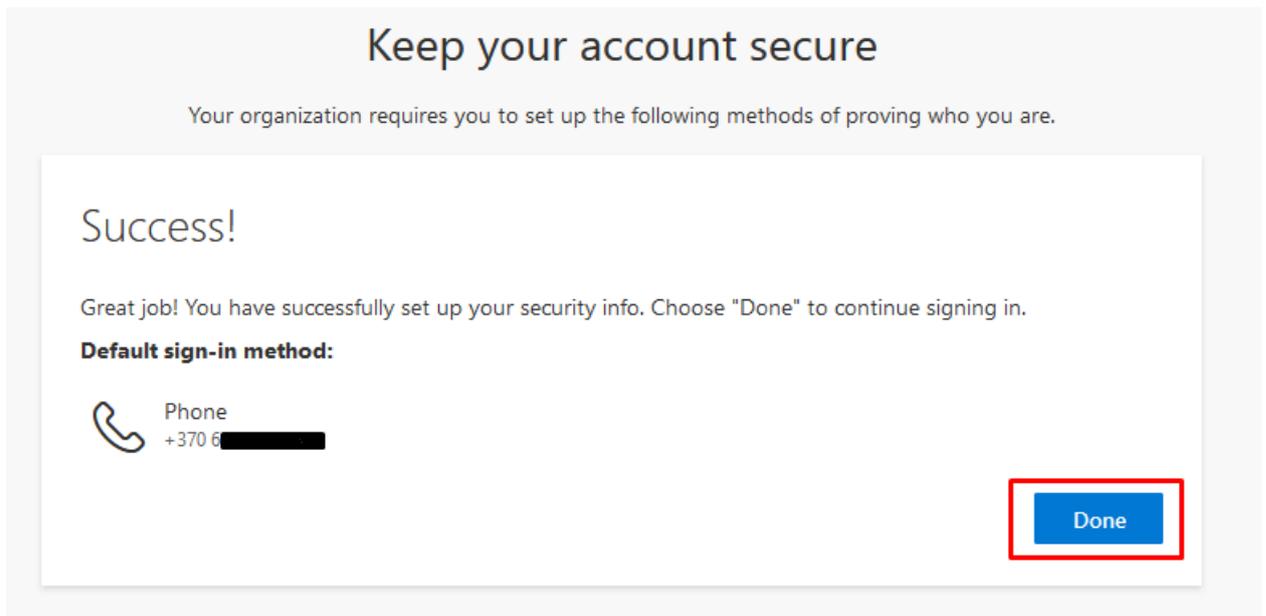


After clicking *Next*, you will need to enter automatically generated characters (letters, numbers) presented in image format (*captcha*). It is important to enter upper and lower case letters as shown.

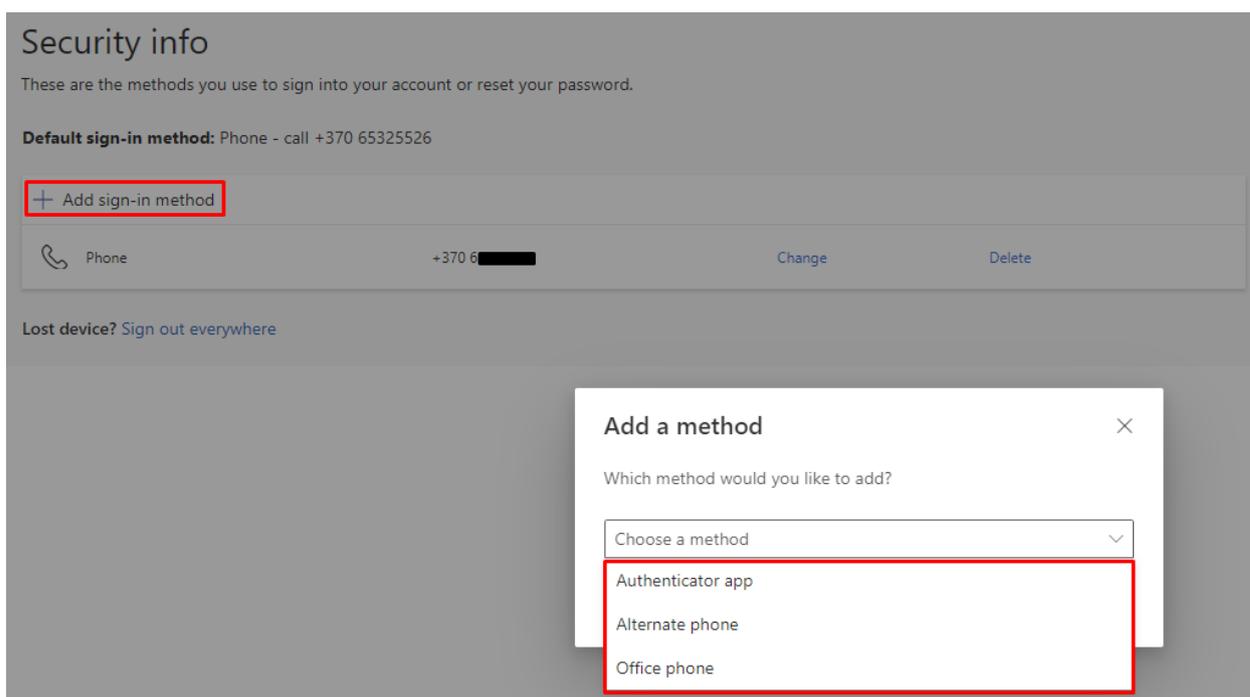
When you receive a call, you will be asked (in English or Lithuanian) to confirm or cancel the connection. If you are not currently connecting to the account, you should press 0 (zero), then the account will be blocked, but if the connection is made by you, then you need to select the pound key #. After pressing the pound key #, your login will be confirmed/accepted. Select *Next*.



Click *Done*.



After successful configuration, you will be directed to a page where you can add another, additional authentication method (this is optional):



You can make future changes to your account's MFA configuration using this link: <https://mysignins.microsoft.com/security-info>

MFA configuration using phone number as authentication method is complete.

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