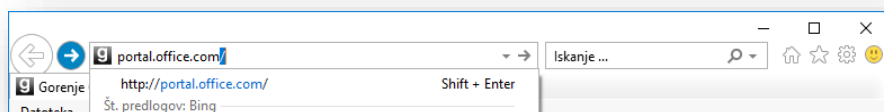


Activate multifactor authentication in Office 365

Please respect the environment. Do not print these instructions.

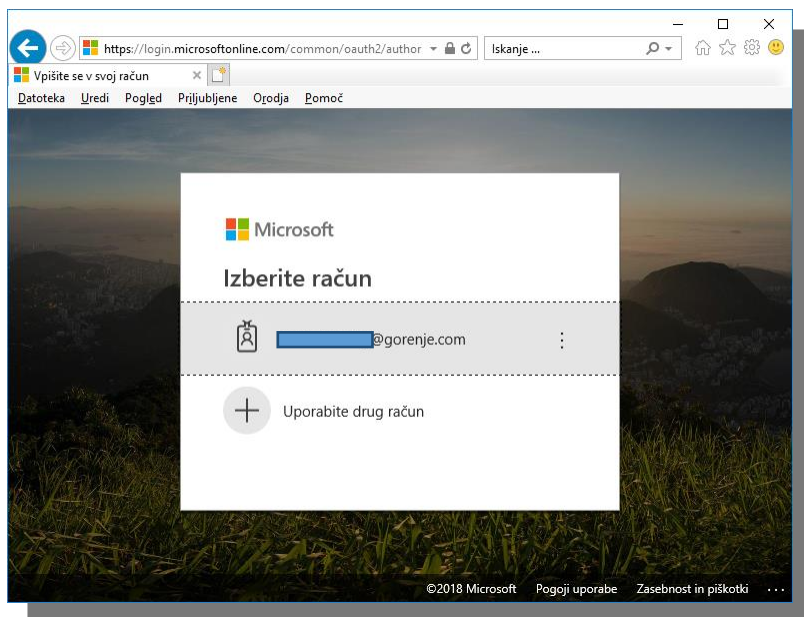
Office 365 services are constantly changing, therefore it is possible some steps described below may differ from actual Office 365 portal – changes might be in design, content or language used. We will try to keep these instruction as current as possible.

1. Web page portal.office.com



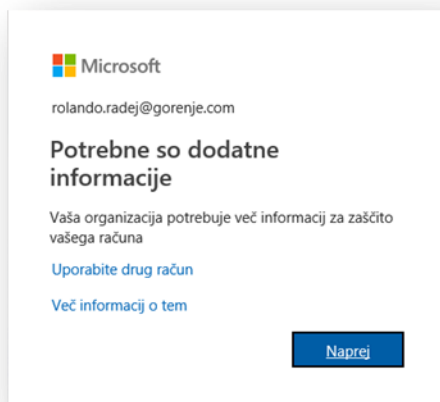
When your MFA is enabled, first visit the <https://portal.office.com>.

2. Sign in with your account



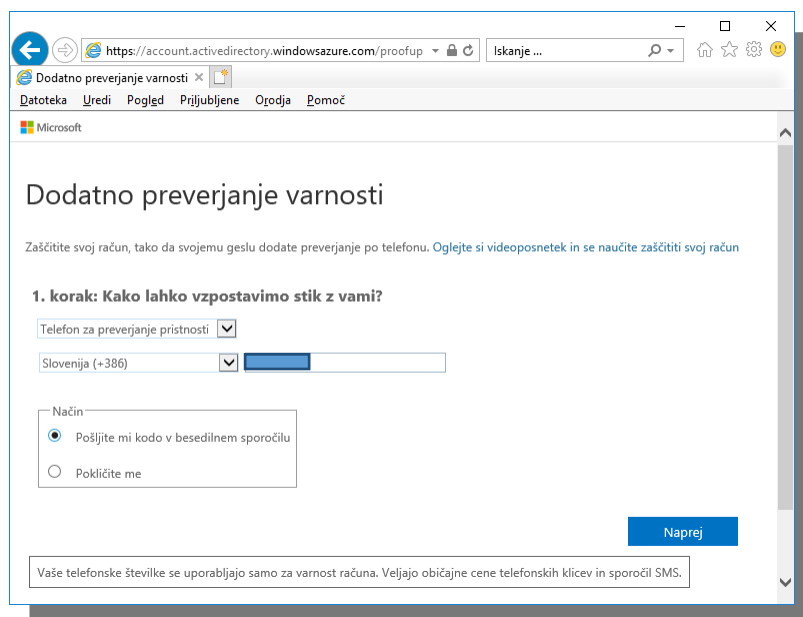
Enter your AD username as [name.surname@gorenje.com](#)

3. System notification about MFA



System informs you that additional information is needed. Click **Continue**.

4. Additional Security Verification page



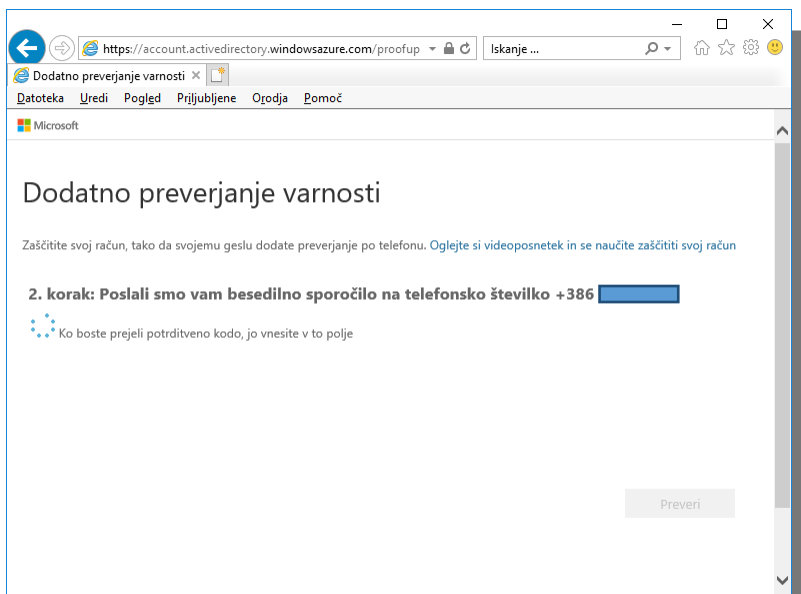
Select most suitable settings and press **Continue**.

These instructions cover verification by SMS (mobile text messages). You may use company assigned or your own mobile phone. This service is not available on landline phones.

Phone numbers that you use for MFA are not visible to anybody in Gorenje.

Settings may be different if you choose to use other authentication methods (phone calls, application...) – in such case please follow the instructions on the screen to configure MFA.

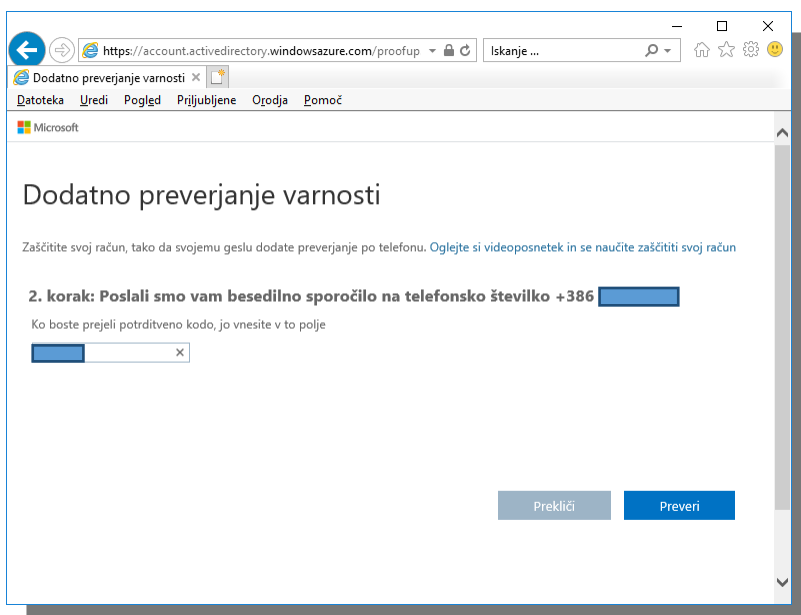
5. Wait for the confirmation code



The SMS message with confirmation code will be sent to a phone number you have provided in previous step.

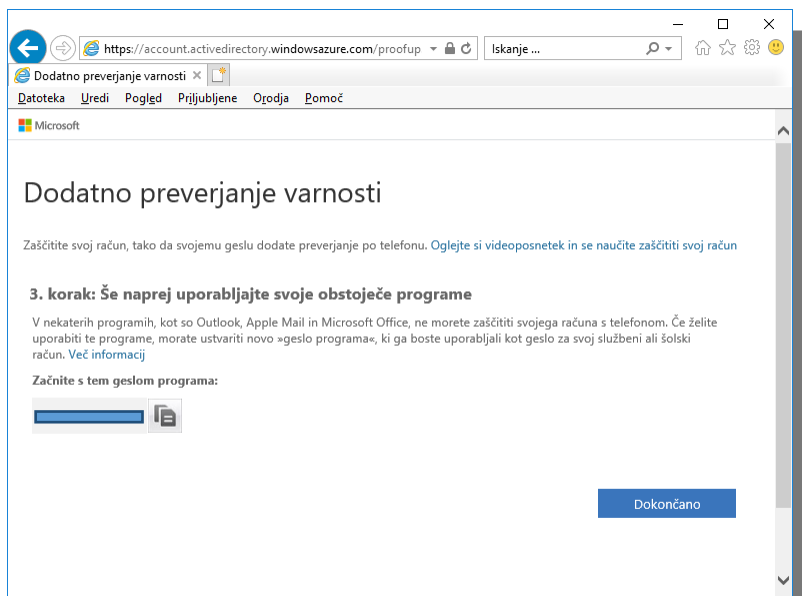
If you don't receive the SMS message in a few minutes, please repeat the previous step.

6. Enter the confirmation code



Enter the 6-digit kodo from the SMS and click **Check**

7. Finished

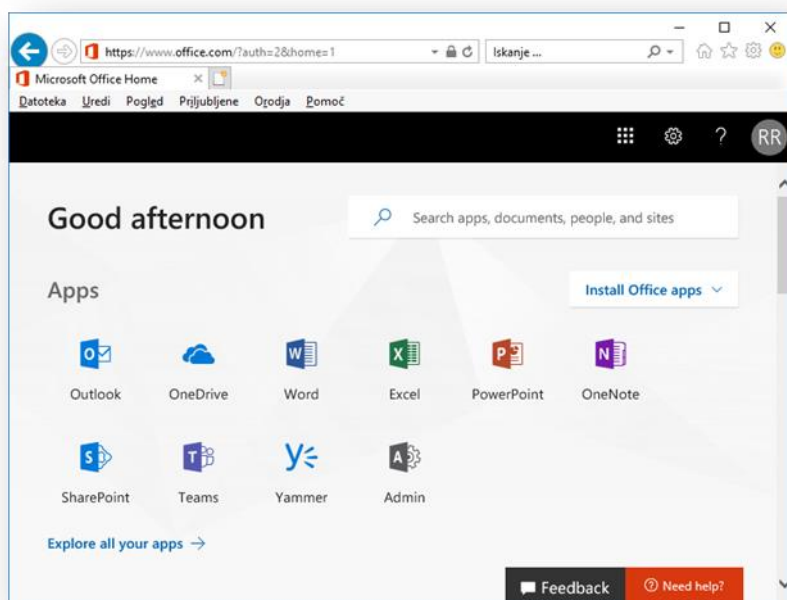


Congratulations. You have successfully configured your MFA. Click **Finish**.

Change the MFA settings

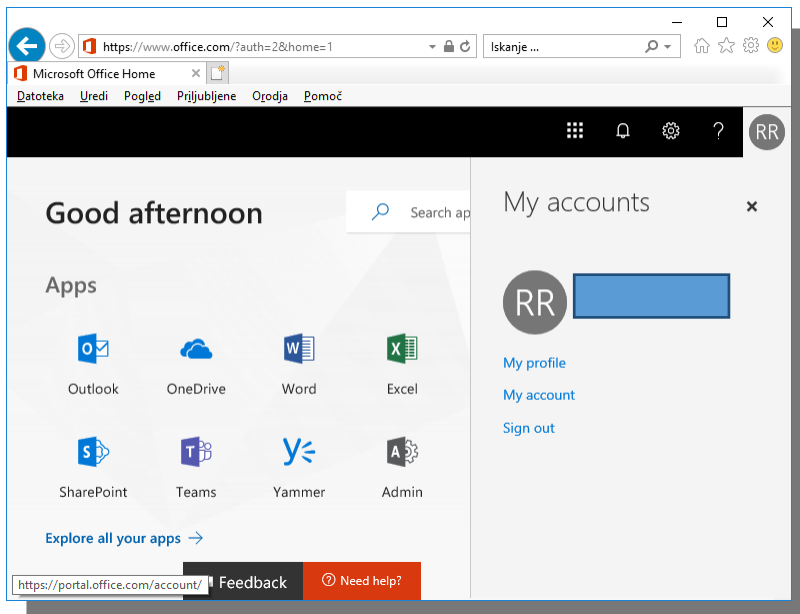
You can change your MFA settings on the Office Portal

1. Open the Office Portal



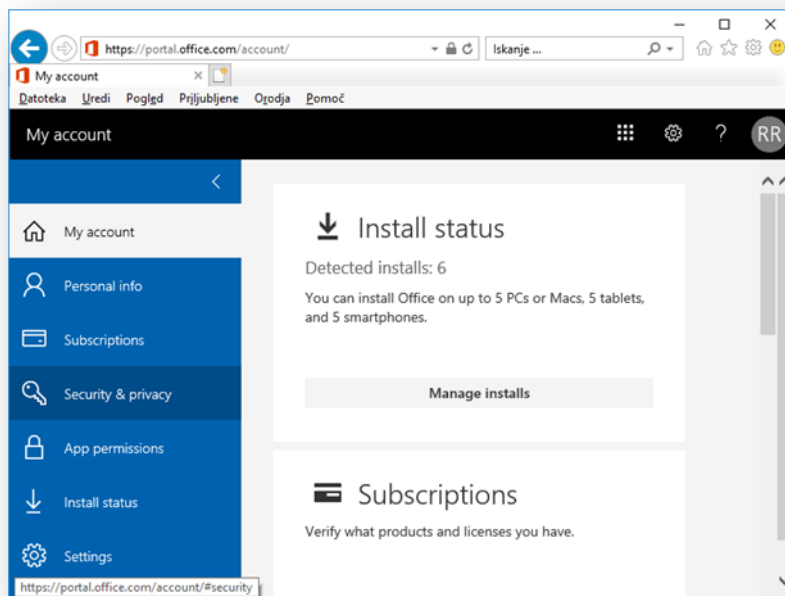
Sign in to <https://portal.office.com>

2. Account properties



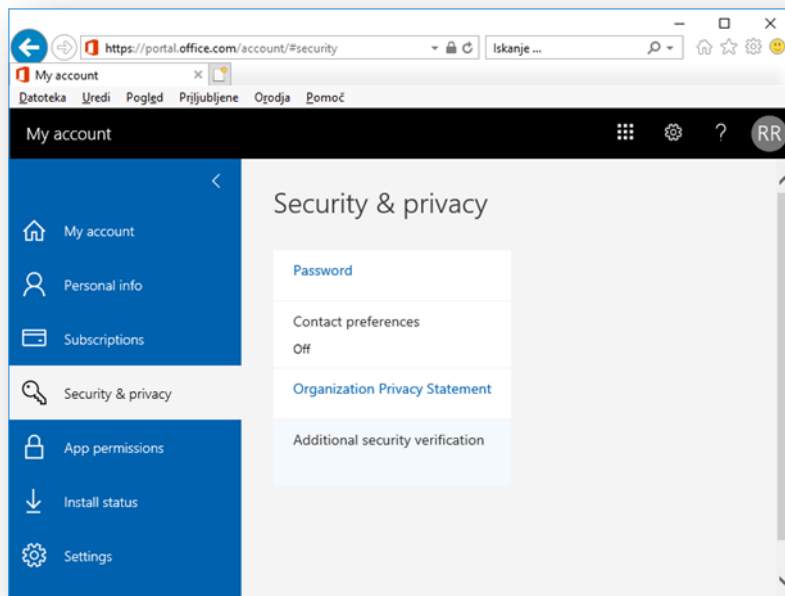
Click on the round icon in top right corner. A menu will open - select **My Account**

3. Account settings



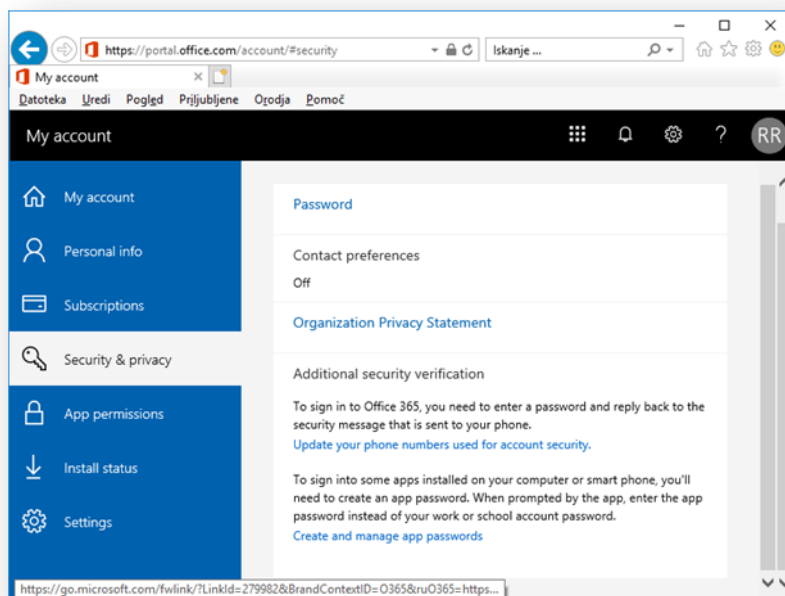
Select **Security & privacy**

4. Security & privacy



Select **Additional security verification**

5. Additional security verification



Click on **Update your phone numbers used for account security**

6. Additional security verifications

Additional security verification App Passwords

When you sign in with your password, you are also required to respond from a registered device. This makes it harder for a hacker to sign in with just a stolen password. [View video to know how to secure your account](#)

what's your preferred option?

We'll use this verification option by default.

Text code to my authentication p

how would you like to respond?

Set up one or more of these options. [Learn more](#)

☒ Authentication phone Slovenia (+386)

☐ Office phone Slovenia (+386)

Here you can select additional phone numbers, change existing phone numbers or activate the Authenticator mobile application.

7. Entering additional phone numbers

Additional security verification App Passwords

We'll use this verification option by default.

Text code to my authentication p

how would you like to respond?

Set up one or more of these options. [Learn more](#)

☒ Authentication phone Slovenia (+386)

☒ Office phone Slovenia (+386) Extension Contact your administrator for office number. Do not use extension.

☐ Alternate authentication phone Select your country or region

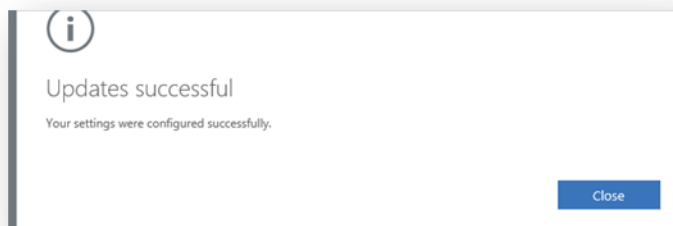
☒ Authenticator app Mobile app has been configured.

Your phone numbers will only be used for account security. Standard telephone and SMS charges will apply.

You can manually enter additional phone numbers or simply check to use your office phone number. If your stated office phone number is not the right one, please contact the IT Helpdesk.

Click **Save** to store settings.

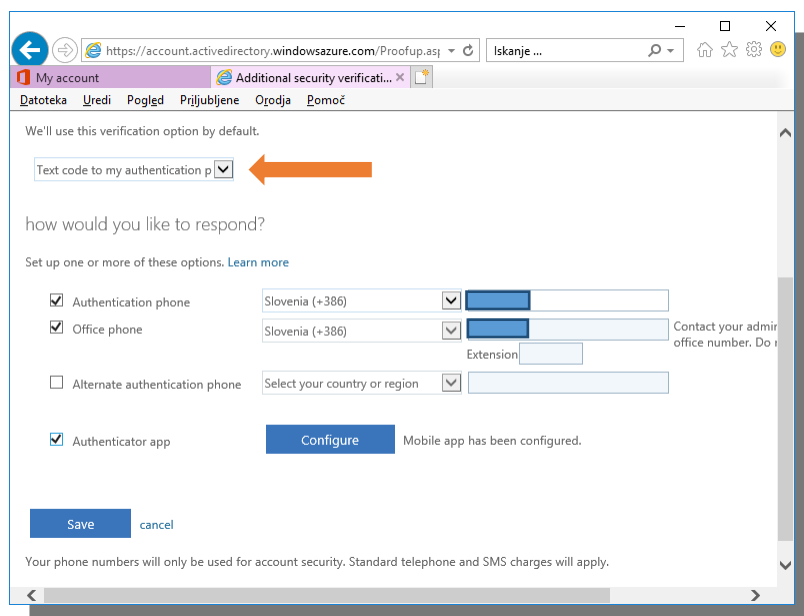
8. Finally



This concludes configuring the MFA.

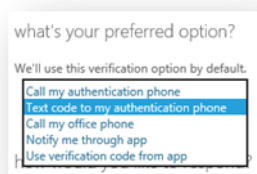
Select preferred MFA method

1. Follow the steps from “Change MFA settings” up to step 6



Select the drop-down list with preferred option (see the arrow above).

2. Select the preferred option

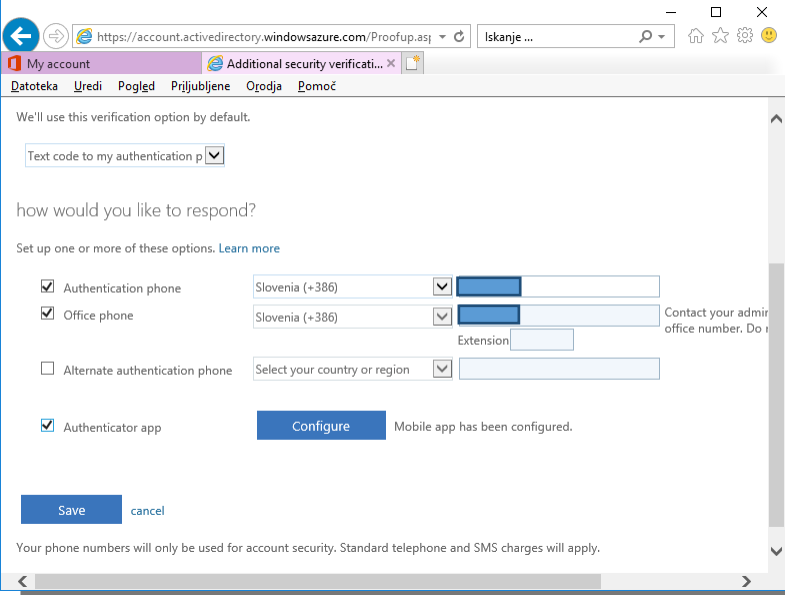


Select the preferred option and click **Save**.

Configuring the mobile application

To use mobile application Authenticator, follow these steps:

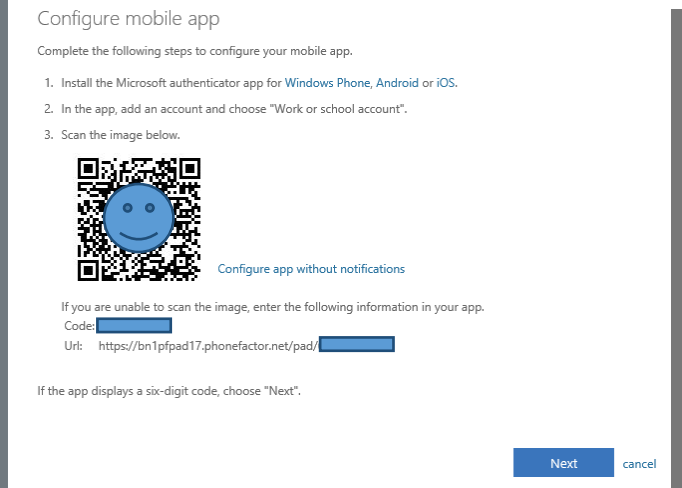
3. Follow the steps from “Change MFA settings” up to step 6



The screenshot shows a web browser window with the URL <https://account.activedirectory.windowsazure.com/Proofup.aspx>. The page title is "Additional security verification". It shows a dropdown menu for "Text code to my authentication p" and a section titled "how would you like to respond?". Under "Set up one or more of these options. Learn more", there are four options: "Authentication phone" (checked), "Office phone" (checked), "Alternate authentication phone" (unchecked), and "Authenticator app" (checked). The "Authenticator app" option has a "Configure" button and the text "Mobile app has been configured." Below the options are "Save" and "cancel" buttons. At the bottom, a note states: "Your phone numbers will only be used for account security. Standard telephone and SMS charges will apply."

Enable **Authenticator app** and click **Configure**.

4. Reading the QR code



The screenshot shows a page titled "Configure mobile app". It contains the following instructions:

1. Install the Microsoft authenticator app for **Windows Phone, Android** or **iOS**.
2. In the app, add an account and choose "Work or school account".
3. Scan the image below.

Below the instructions is a QR code with a blue smiley face in the center. To the right of the QR code is a link: [Configure app without notifications](#).

Below the QR code, it says: "If you are unable to scan the image, enter the following information in your app."

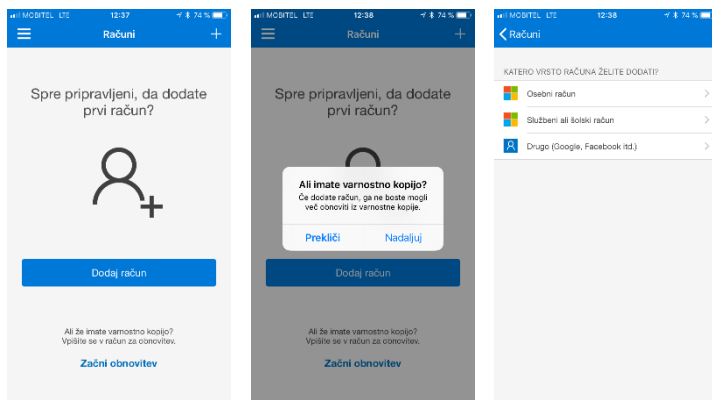
Code: [redacted]
Uri: <https://bn1pfpad17.phonefactor.net/pad/> [redacted]

At the bottom, it says: "If the app displays a six-digit code, choose 'Next'."

At the bottom right are "Next" and "cancel" buttons.

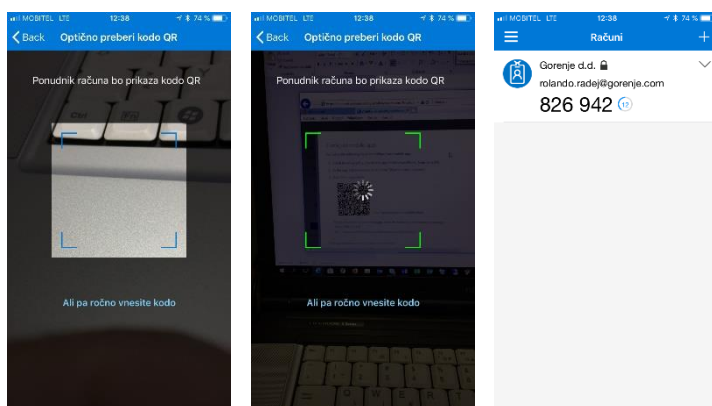
Open the **Authenticator** application on your mobile device

5. Mobile Authenticator



Select **Add account**, **Continue** and **Business or school account**.

6. Reading the QR code



Present the QR code to the phone and the application will activate automatically.

7. Finish the configuration

To finish the configuration on the Office portal click **Save**.