UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH
Centrum informačných a komunikačných technológií

Úsek informačnej a kybernetickej bezpečnosti
Tím na riešenie počítačových bezpečnostných incidentov (CSIRT-UPJS)

TLP:CLEAR

Nastavenie dvojfaktorového overovania v M365 / Setting up two-factor authentication in M365

TLP:CLEAR

Nastavenie dvojfaktorového overovania v Microsoft 365 2
Výber autentifikačnej metódy 2
Prvotné nastavenie 2
Autentifikačná metóda – overovací telefón / SMS správa 4
Autentifikačná metóda – mobilná aplikácia 5
Autentifikačná metóda – Windows aplikácia 8
Pridanie/Zmena/Odstránenie overovacej metódy 11
1. Pridanie novej overovacej metódy 11
2. Zmena už nastavenej overovacej metódy 12
3. Odstránenie už nastavenej overovacej metódy 13
Setting up two-factor authentication in Microsoft 365 14
Selecting an authentication method 14
Initial Setup 14
Authentication method – Verification via phone / SMS 16
Authentication Method – Mobile Application 17
Authentication method - Windows application 20
Add/Change/Remove Verification Method 23
1. Adding a new verification method 23
2. Changing an already set verification method 24
3. Delete an already set authentication method 24

Nastavenie dvojfaktorového overovania v Microsoft 365

Upozornenie: Viacfaktorové overenie je vyžadované pre prihlásenie do aplikácií Office 365 (Outlook, SharePoint, Teams, Word, Excel a i.) na novom zariadení (počítač, notebook, smartfón a pod.) pri prístupe z inej siete (napr. z domu) a pri prvom prihlásení z univerzitnej siete (eduroam). Overenie sa vyžaduje raz za 180 dní na jednotlivých zariadeniach, alebo vždy po odhlásení z účtu. Preto odporúčame pri vyzvaní, či chcete zostať prihlásení, vybrať možnosť „Áno“. Týmto spôsobom znížite počet požiadaviek na dvojfaktorové overenie.

Výber autentifikačnej metódy

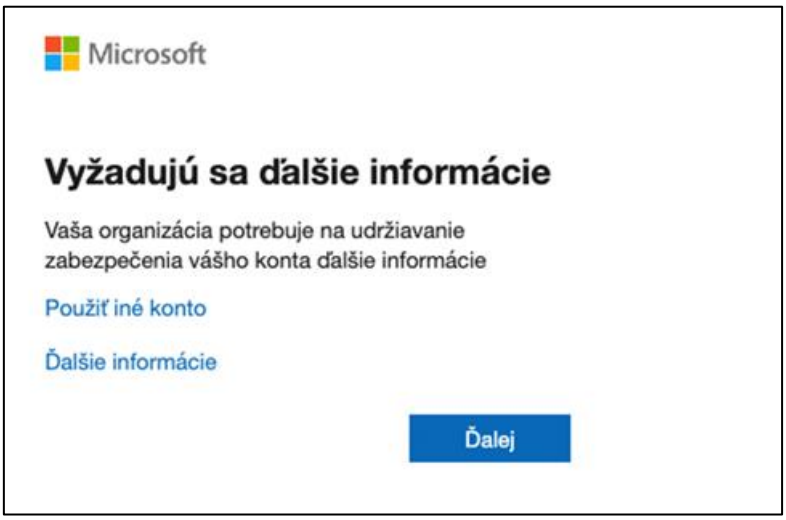
Po zapnutí dvojfaktorového overovania pre Váš účet je nutné vykonať prvotný výber autentifikačnej metódy. V rámci prvotného nastavenia máte na výber niekoľko možností:

- **Overovací telefón (/ SMS správa)** – bezplatné doručenie kódu formou SMS alebo hovorom na Vaše telefónne číslo.
- **Telefón do kancelárie** – telefonát na telefónne číslo Vašej kancelárie.
- **Mobilná aplikácia** – schválenie prihlásenia pomocou mobilnej aplikácie Microsoft Authenticator, ktorá je dostupná na platformách Android a iOS.
  Poznámka: V prípade zvolenia tejto metódy je vhodné nainštalovať si Microsoft Authenticator vopred. Odkazy na stiahnutia nájdete tu.

Prvotné nastavenie

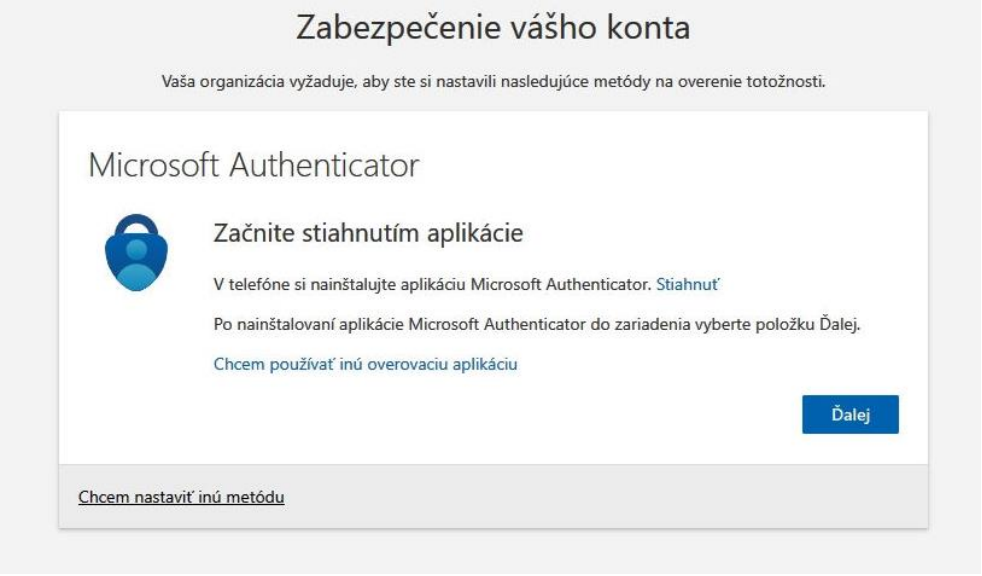
1. Stlačte tlačidlo „**Ďalej**“.

   Poznámka: V prípade, ak ste už prihlásení do svojho účtu a nezobrazuje Vám okno na ďalšie overenie zabezpečenia, je potrebné sa odhlásiť a znova prihlásiť. Po opätovnom prihlásení zvoľte možnosť Ďalej a postupujte podľa nasledujúcich krokov.



2. Ak chcete použiť na overenie aplikáciu, stlačte tlačidlo „**Ďalej**“. Ak ešte nemáte stiahnutú aplikáciu Microsoft Authenticator môžete kliknúť na „**Stiahnuť**“ a zobrazia sa Vám QR kódy na jej stiahnutie (Google Play, App Store).

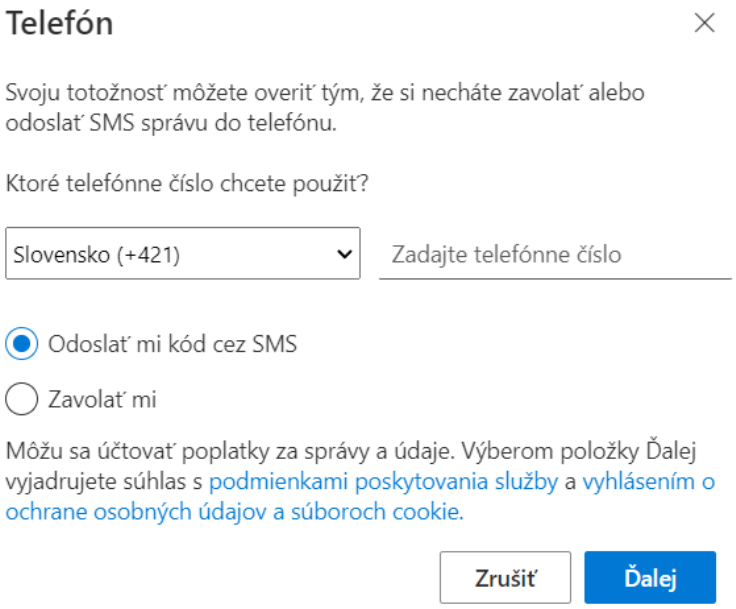
   Ak chcete použiť inú metódu, napríklad Overovací telefón (SMS správa)**,** stlačte možnosť „**Chcem nastaviť inú metódu**“, ktorá sa nachádza v ľavom dolnom rohu.





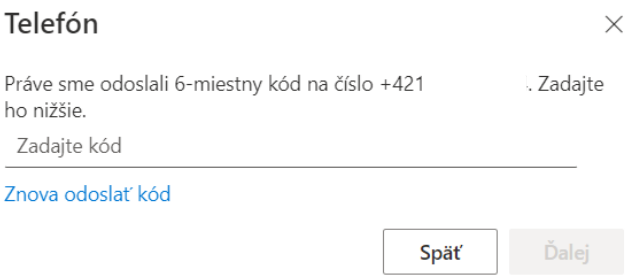
Autentifikačná metóda – overovací telefón / SMS správa

1. V prípade možnosti Overovací telefón si zvoľte predvoľbu (Slovensko (+421)) a zadajte svoje telefónne číslo.

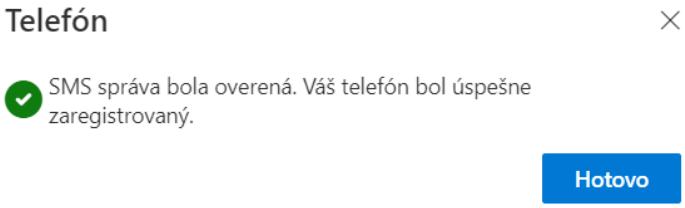


2. Zvoľte si spôsob – Odoslať mi kód cez SMS (odporúčané).

3. Zadajte overovací kód z SMS správy a kliknite na „**Ďalej**“.



4. Stlačte tlačidlo „**Hotovo**“.



Autentifikačná metóda – mobilná aplikácia

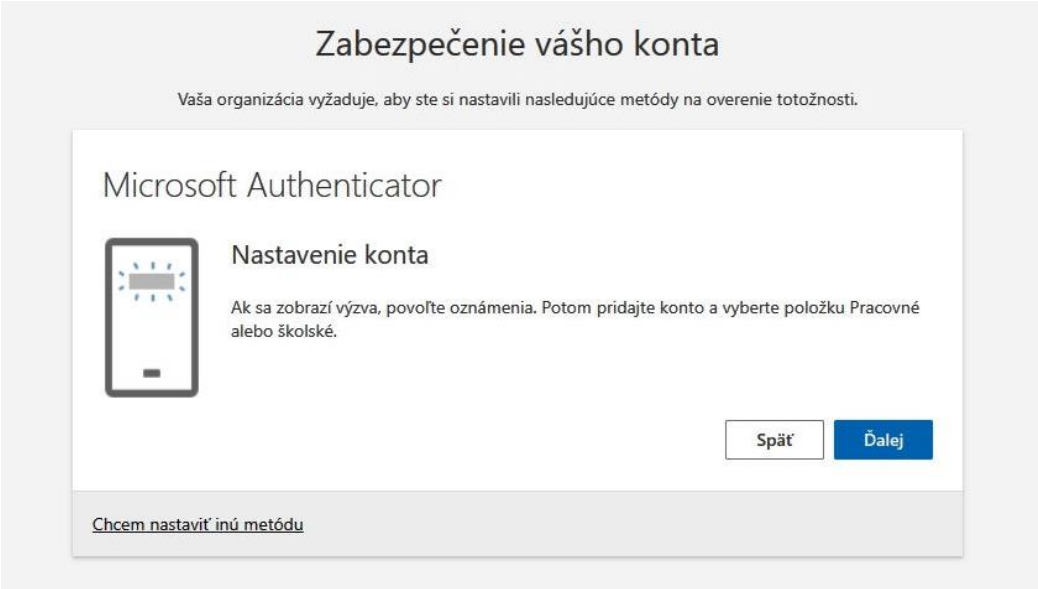
Microsoft Authenticator je bezplatná mobilná aplikácia, ktorej inštalácia je možná z obchodov s aplikáciami Google Play Store, Samsung Galaxy Store a Apple App Store na nasledovných odkazoch:

https://play.google.com/store/apps/details?id=com.azure.authenticator

https://galaxystore.samsung.com/detail/com.azure.authenticator

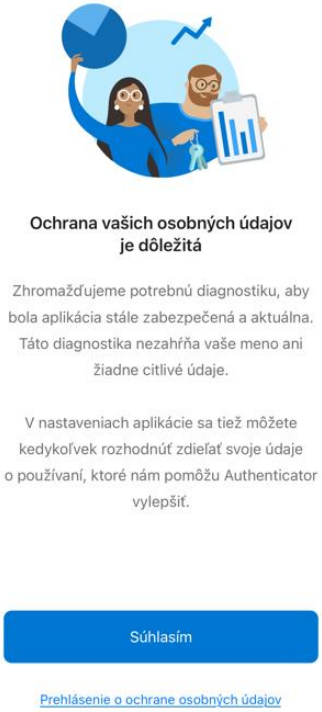
https://apps.apple.com/app/microsoft-authenticator/id983156458

1. V prípade ak ste stlačili tlačidlo “Ďalej“, teda je zvolené overenie Mobilnou aplikáciou sa Vám zobrazí nasledujúce okno. Znova stlačte tlačidlo „**Ďalej**“.



2. Ak ešte nemáte stiahnutú aplikáciu Microsoft Authenticator, stiahnite si ju na Vašom telefóne (napr. pomocou QR kódu ako bolo ukázané v prvej časti návodu).

3. Odsúhlaste prehlásenie o ochrane Vašich osobných údajov.



4. Kliknite na Pridať pracovné alebo školské konto.
   Do aplikácie sa **neprihlasujte**!

5. Naskenujte na telefóne QR kód (V prípade, že bude aplikácia žiadať o potvrdenie prístupu ku kamere, kliknite OK).

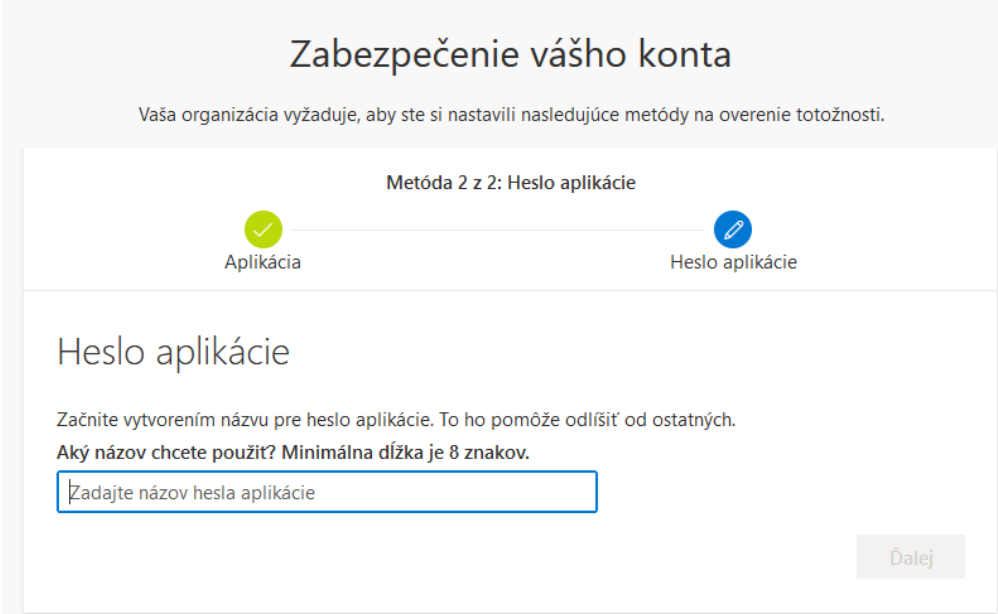
Poznámka: Ak máte problém s naskenovaním QR kódu, je možné taktiež vyplniť kód a URL adresu.

6. V okne pre nakonfigurovanie mobilnej aplikácie kliknite na „**Ďalej**“.

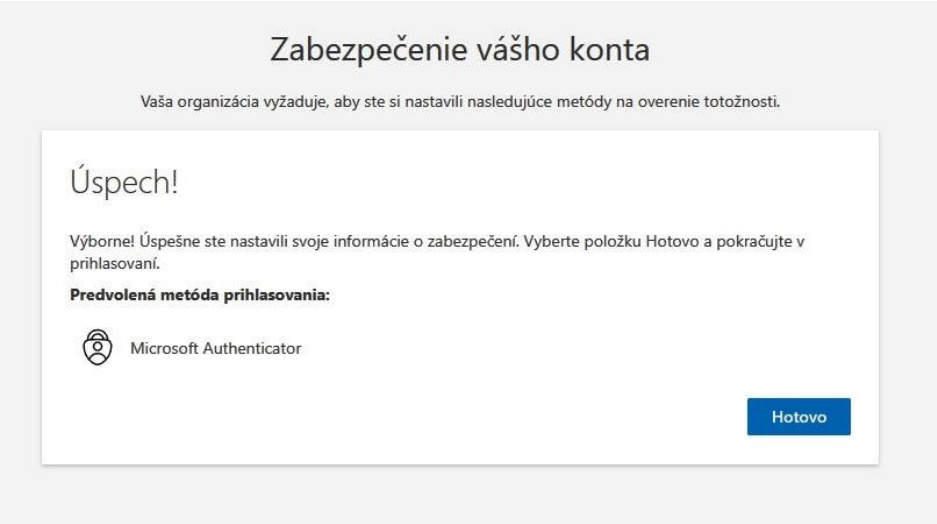
7. Tlačidlo „**Ďalej**“ by malo mať sivú farbu. V mobilnej aplikácii zadajte číslo zobrazené na obrazovke.

8. Následne sa tlačidlo „**Ďalej**“ z kroku 7. sfarbí na modro a môžete ho stlačiť.

9. V ďalšom kroku je potrebné si zvoliť ľubovoľný názov pre heslo aplikácie s minimálnou dĺžkou 8 znakov. Po stlačení tlačidla „**Ďalej**“ sa Vám zobrazí vygenerované heslo, ktoré slúži na autentifikáciu predovšetkým v starších verziách aplikácií. Z toho dôvodu Vám odporúčame si heslo uchovať. Pokračujte stlačením tlačidla „**Hotovo**“.



10. V poslednom kroku kliknite na tlačidlo „**Hotovo**“.

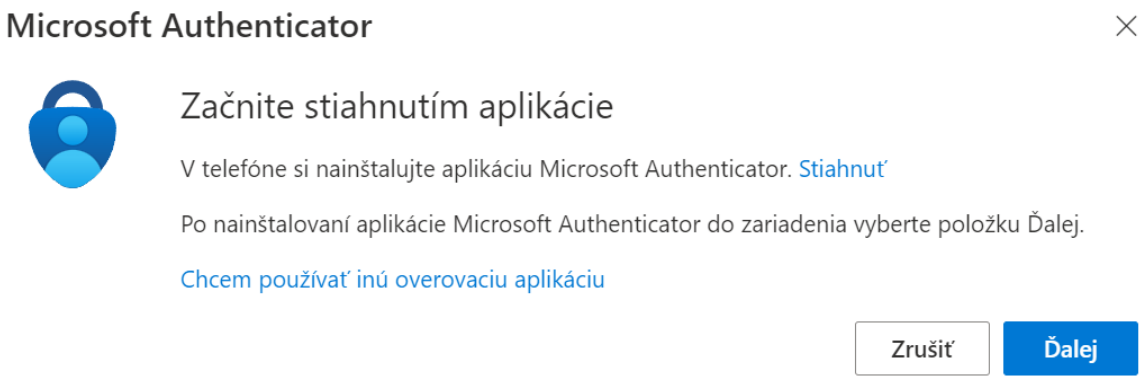


11. V prípade, ak sa Vám zobrazí požiadavka na schválenie prihlásenia, kliknite na „**Schváliť**“ v mobilnej aplikácii.

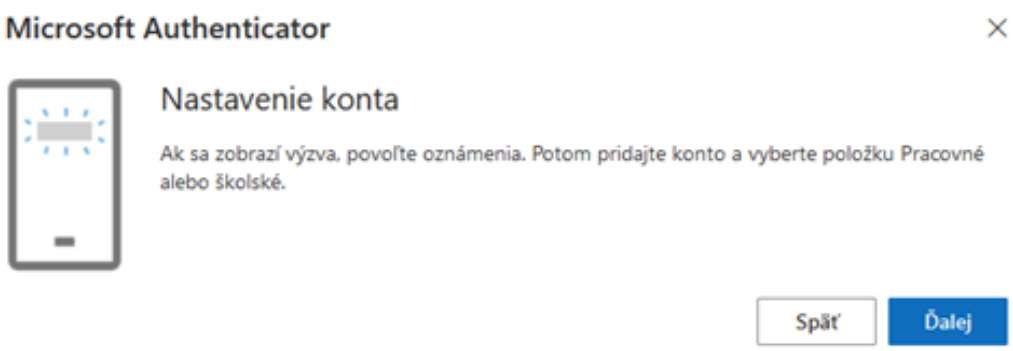
Autentifikačná metóda – Windows aplikácia

OTPKEY Authenticator je bezplatná Windows aplikácia, ktorej inštalácia je možná z obchodu Microsoft Store na nasledovnom odkaze:
https://apps.microsoft.com/store/detail/XP9MCL9T4JFZ0B?ocid=pdpshare

1. Ak ešte nemáte stiahnutú aplikáciu OTPKEY Authenticator, stiahnite si ju na Vašom počítači (napr. z obchodu Microsoft Store, ktorý sa nachádza v prvej časti návodu pre Windows aplikáciu). Následne stlačte tlačidlo „**Chcem použiť inú overovaciu aplikáciu**“.



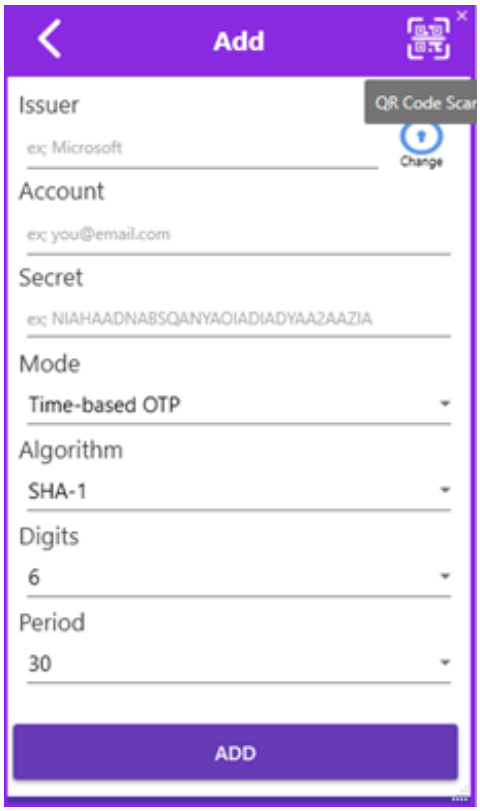
2. V prípade, ak ste stlačili tlačidlo „**Chcem použiť inú overovaciu aplikáciu**“, teda je zvolené overenie inou aplikáciou, sa Vám zobrazí nasledujúce okno. Teraz stlačte tlačidlo „**Ďalej**“.



3. V tejto časti sa vám zobrazí okno s QR kódom, ktorý je potrebné naskenovať aplikáciou. Otvorte aplikáciu OTPKEY Authenticator a v pravom hornom rohu kliknite na **tlačidlo ⊕ (biely krížik v kruhu)**, kde sa pridáva nový autentikátor.

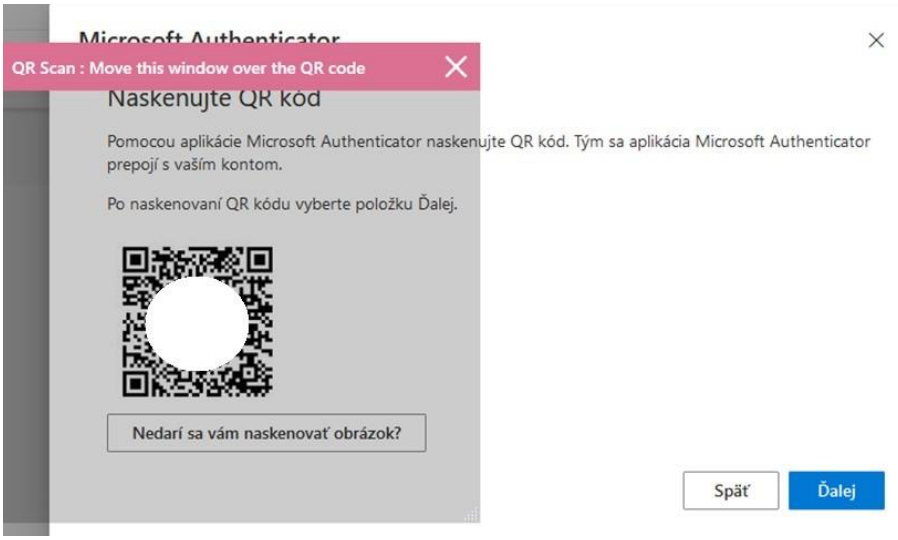


4. Následne v pravom hornom rohu kliknite na **tlačidlo** na skenovanie QR kódu.



5. Teraz sa Vám otvorí skener QR kódov, ktorý Vám umožní naskenovať QR kód zobrazený pri nastavovaní druhého faktora vo Vašom účte. Stačí posunúť skener tak, aby zachytil daný QR kód.

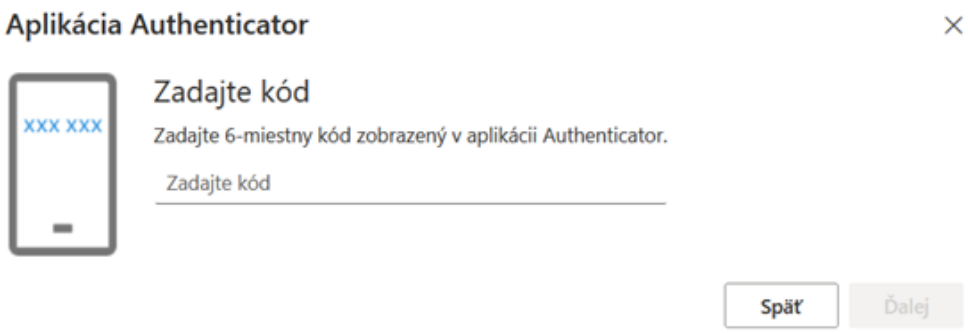
Poznámka: Ak máte problém s naskenovaním QR kódu, je možné taktiež vyplniť potrebné údaje ručne a to tak, že stlačíte tlačidlo „**Nedarí sa Vám naskenovat obrázok?**“. Následne v aplikácii do kolónky **Issuer** doplňte slovo Microsoft, do kolónky **Account** doplňte svoj účet na ktorom si nastavujete dvojfaktorové overovanie (napr. meno.priezvisko@upjs.sk) a do kolónky **Secret** doplňte Tajný kľúč, ktorý sa zobrazí pod tlačidlom „**Nedarí sa Vám naskenovat obrázok?**“



6. V okne pre nakonfigurovanie mobilnej aplikácie stlačte tlačidlo „**ADD**“. Tu sa Vám zobrazí 6-miestny kód, ktorý sa generuje každých 30 sekúnd.

7. V okne s QR kódom stlačte tlačidlo „**Ďalej**“.

8. V tomto kroku sa Vám zobrazí okno, kde si môžete vyskúšať funkčnosť overovania druhým faktorom. Tlačidlo „**Ďalej**“ by v tomto okamihu malo mať sivú farbu. Funkčnosť overovania druhým faktorom si môžete vyskúšať tak, že zadáte 6-miestny kód zobrazený v aplikácii Authenticator.



9. Následne sa tlačidlo „**Ďalej**“ z kroku 9. sfarbí na modro a môžete ho stlačiť.

10. V tomto okamihu je už všetko potrebné nastavené.

Pridanie/Zmena/Odstránenie overovacej metódy

Ak chcete pridať alebo zmeniť overovaciu metódu v dôsledku zmeny mobilného zariadenia, telefónneho čísla alebo z iných dôvodov, môžete tak urobiť kliknutím na tento odkaz: https://mysignins.microsoft.com/security-info.

Táto platforma poskytuje tri základné možnosti:

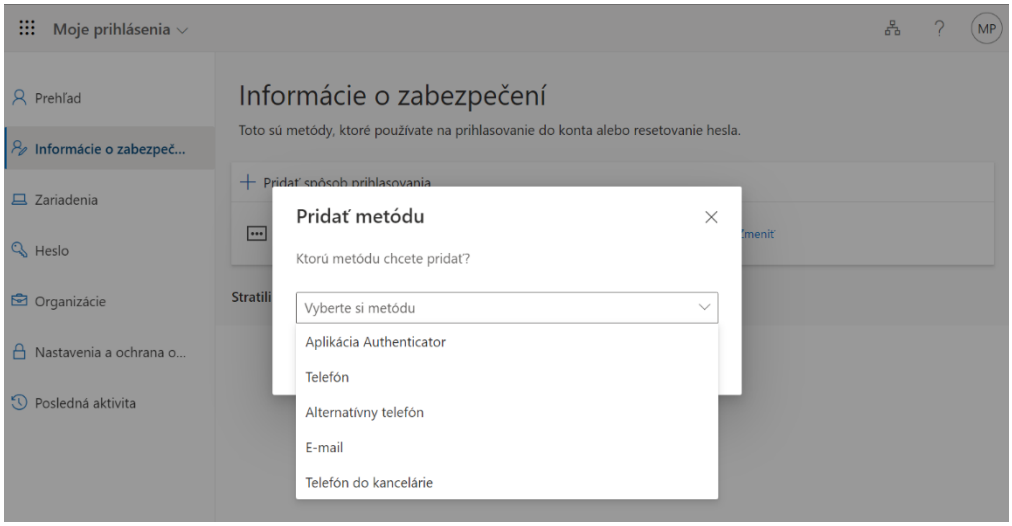
1. **Pridanie novej overovacej metódy**

   Táto možnosť Vám umožňuje pridať novú overovaciu metódu, napríklad pri kúpe nového telefónu, strate pôvodného, alebo pre použitie viacerých foriem autentifikácie.

   V časti Informácie o zabezpečení kliknite na tlačidlo **+ Pridať spôsob prihlasovania**.

   Vyberte medzi možnosťami: Overovací telefón (SMS), Telefón do kancelárie, alebo Aplikácia Authenticator (napr. Microsoft Authenticator, alebo OTPKeyAutheticator).

   Po vybraní metódy kliknite na tlačidlo „**Pridať**“.

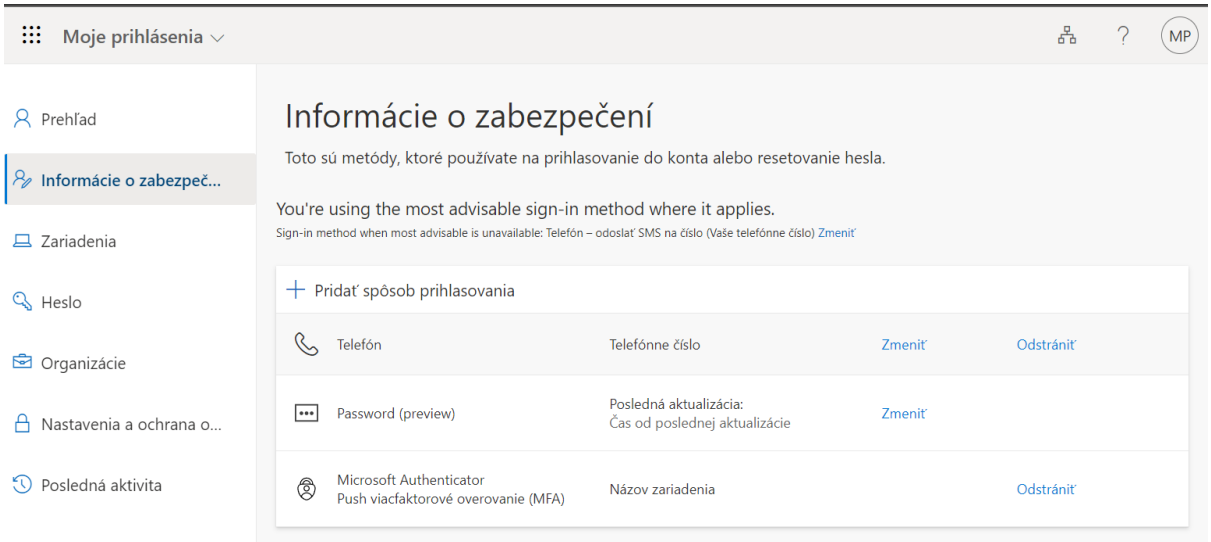


Ak ste vybrali konkrétnu overovaciu metódu, pokračujte podľa návodu pre danú metódu.

2. Zmena už nastavenej overovacej metódy

Poskytuje možnosť aktualizovať informácie o overovacej metóde, napríklad v prípade zmeny telefónneho čísla, alebo inej aktualizácie údajov.

Pri danej overovacej metóde, ktorú chcete upraviť stlačte tlačidlo „**Zmeniť**“. Tu môžete zadať Vaše nové údaje.



3. Odstránenie už nastavenej overovacej metódy

Umožňuje odstrániť neaktívne overovacie metódy, čo môže byť potrebné napríklad pri zmene zariadenia, alebo pri strate prístupu k niektorej z overovacích metód.

Pri danej overovacej metóde, ktorú chcete odstrániť stlačte tlačidlo „**Odstrániť**“. Ďalej môžete pokračovať pridaním novej overovacej metódy podľa bodu 1.

Setting up two-factor authentication in Microsoft 365

Please note: Multi-factor authentication is required for logging into Microsoft 365 applications (Outlook, SharePoint, Teams, Word, Excel, etc.) on a new device (computer, laptop, smartphone, etc.) when accessing from another network (e.g., home) and when logging in from the campus network (eduroam) for the first time. Authentication is required once every 180 days on individual devices, or whenever you log out of your account. Therefore, we recommend selecting "Yes" when prompted if you wish to remain logged in. This will reduce the number of requests for two-factor authentication.

Selecting an authentication method

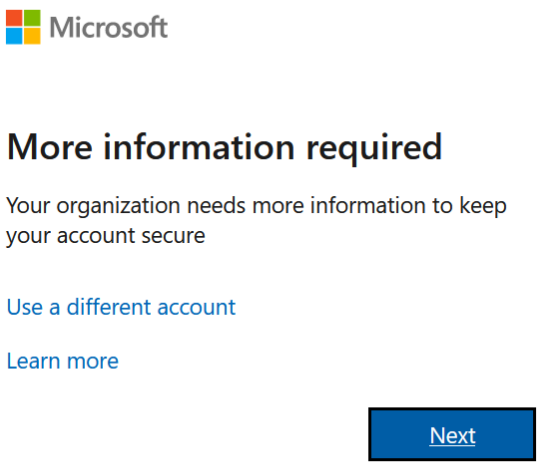
After activating two-factor authentication for your account, you must perform the initial selection of the authentication method. As part of the initial setup, you have several options to choose from:

- **Verification phone (SMS message)** – free of charge delivery of the code by SMS or call to your phone number.
- **Office phone** – call to your office phone or mobile device.
- **Authenticator App** – sign-in approval using the Microsoft Authenticator mobile application, which is available on Android and iOS platforms.
  Note: If you choose this method, it is recommended to install Microsoft Authenticator in advance. Download links can be found here.

Initial Setup

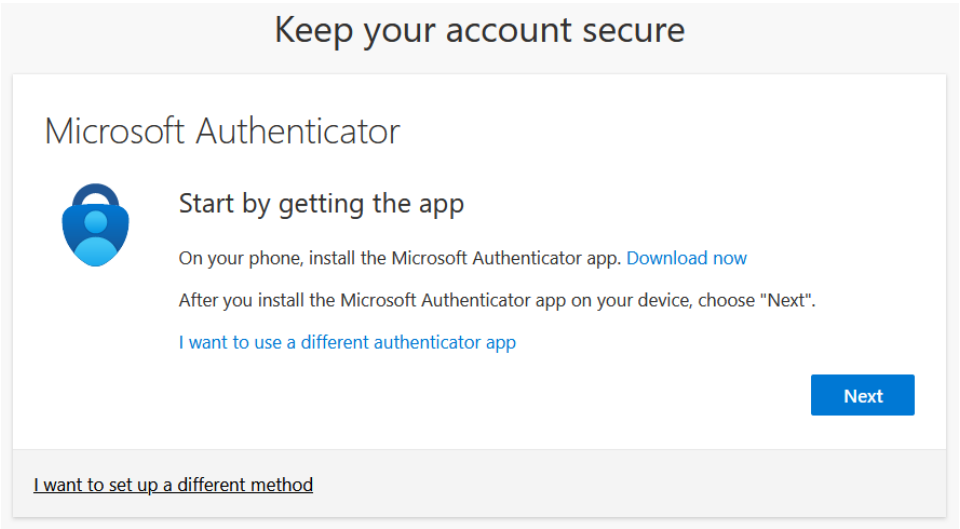
1. Press the "**Next**" button

   Note: If you are already logged into your account and the window for further security verification is not displayed, you need to log out and log in again. After logging in again, select Next and follow the next steps.



2. If you want to use the application for verification, press the "**Next**" button. After clicking on "**Download now**", you will see QR codes for downloading the Microsoft Authenticator application (Google play, App Store).

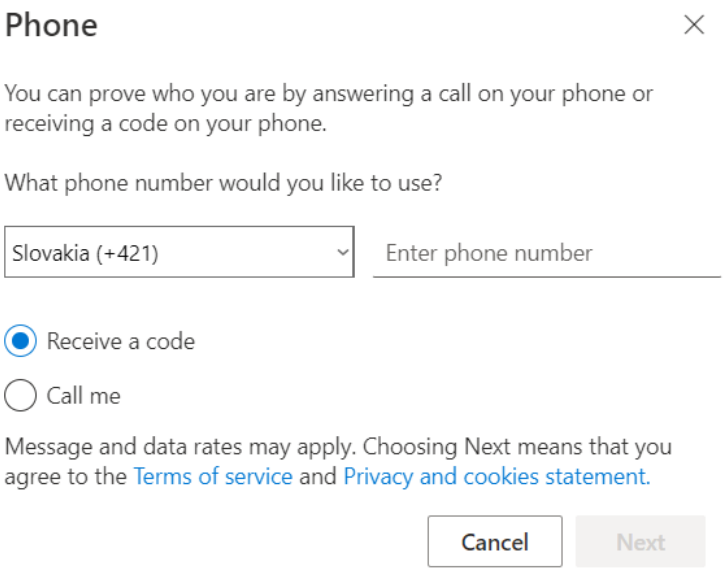
   If you want to use another method, such as Verification Phone (SMS message), press the "**I want to set up a different method**" option located at the bottom left corner.





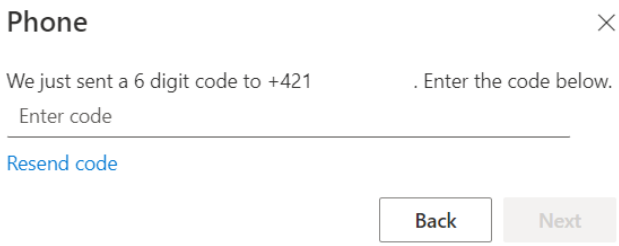
Authentication method – Verification via phone / SMS

5. In the case of Verification Phone option, choose your area code (Slovakia (+421)) and enter your phone number.

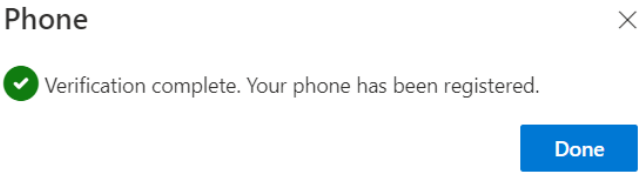


6. Choose a method – Receive a code (recommended).

7. Enter the verification code from the SMS message and press the "**Next**" button.



8. Press the "**Done**" button.



Authentication Method – Mobile Application

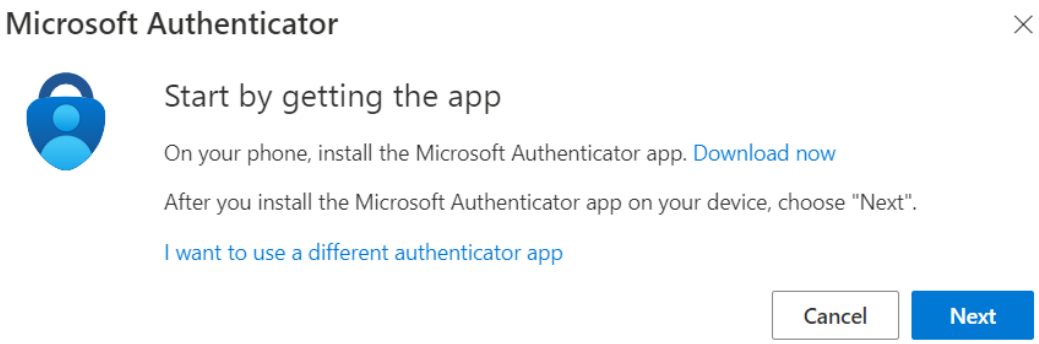
Microsoft Authenticator is a free mobile application that can be installed from the Google Play Store, Samsung Galaxy Store and Apple App Store at the following links:

https://play.google.com/store/apps/details?id=com.azure.authenticator

https://galaxystore.samsung.com/detail/com.azure.authenticator

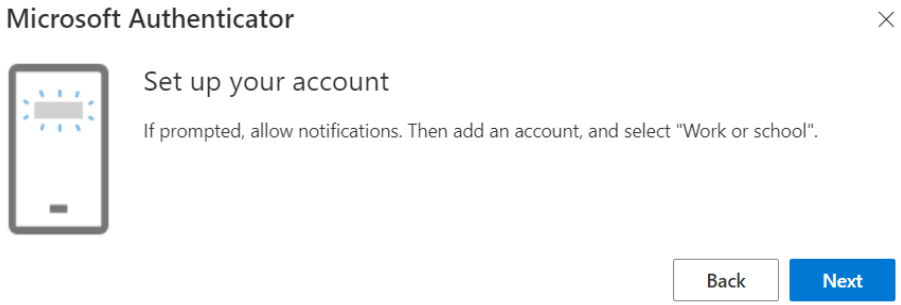
https://apps.apple.com/app/microsoft-authenticator/id983156458

1. If you haven't downloaded the Microsoft Authenticator app yet, you can click "Download" and you will see QR codes for download (Google Play, App Store). Then press the "**Next**" button.





2. If you have pressed the "**Next**" button, i.e., verification by the Mobile application is selected, the following window will appear. Press the "**Next**" button again.



3. Agree to the statement on the protection of your personal data.

4. Click “Add work or school account”.
   Do not log into the app!

5. Scan the QR code on your phone (if the application asks for confirmation of access to the camera, press the “**OK**“ button).

   Note: If you have a problem with scanning the QR code, it is also possible to fill in the code and the URL address.

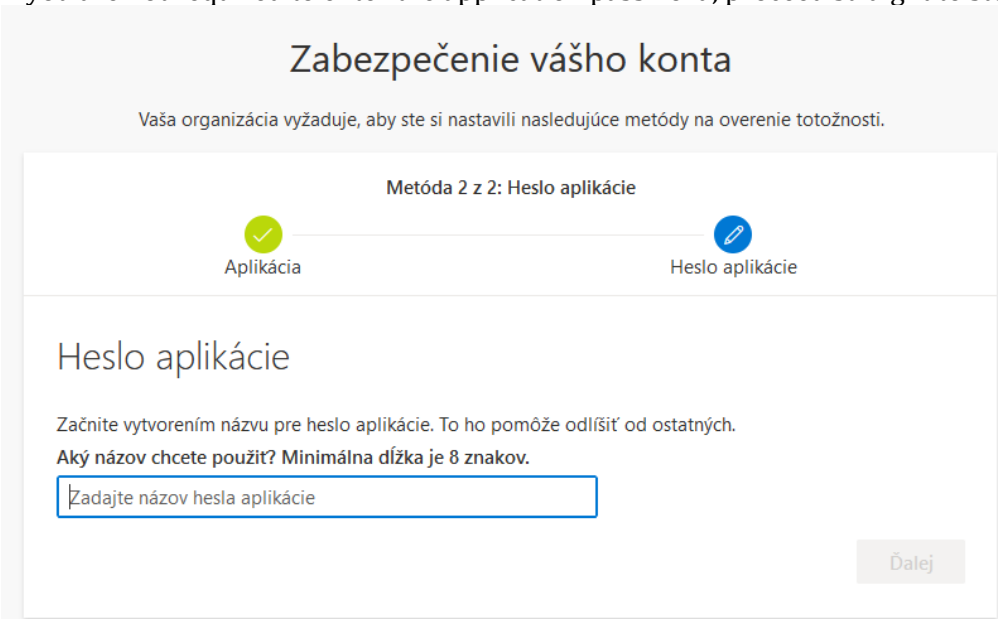
6. In the window for configuring the mobile application, press the “**Next**” button.

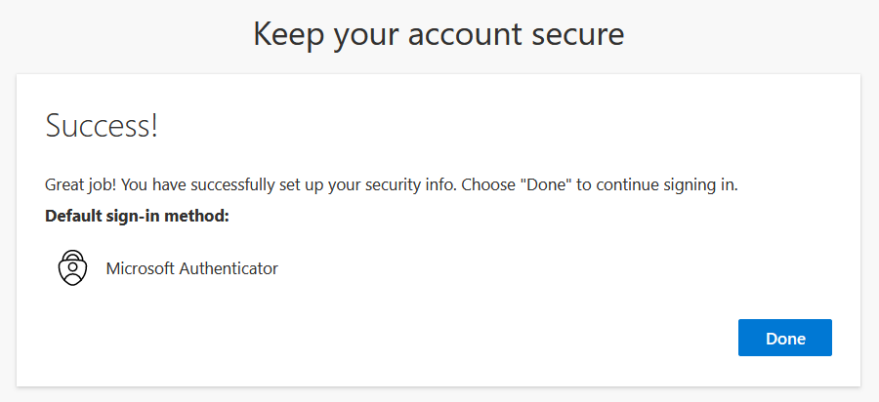
7. The “**Next**” button should be greyed out. In your mobile application fill in the number shown on the screen.

8. Then the "**Next**" button from step 7 will turn blue and you can press it.

9. In the next step, you need to choose an arbitrary name for the application password with a minimum length of 8 characters. After pressing the "**Next**" button, you will see the generated password, which is used for authentication, especially in older versions of the application. For this reason, we recommend that you save the password. Continue by pressing the "**Done**" button.

   If you are not required to enter the application password, proceed straight to step 11.



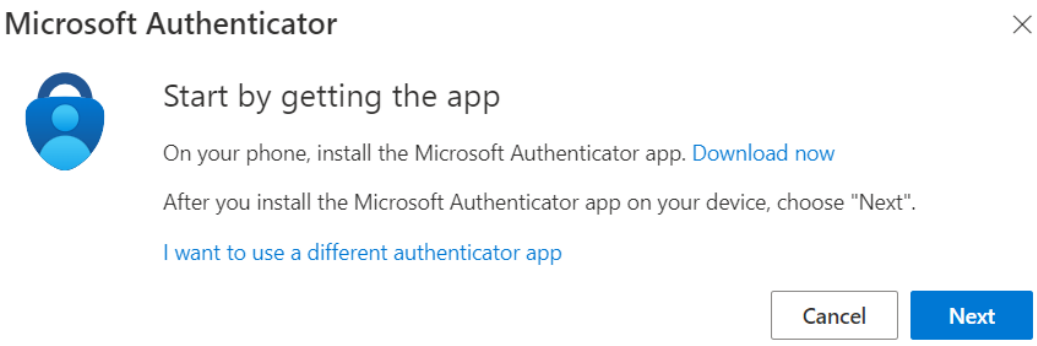


10. In the last step, press the "**Done**" button.

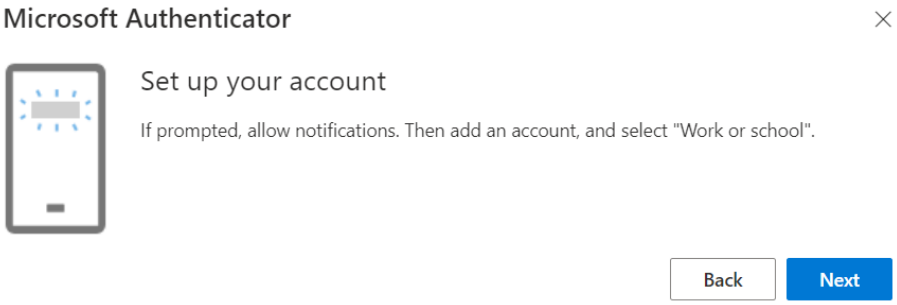
11. If you are prompted to approve your login, press the "**Approve**" button in the mobile app.

Authentication method - Windows application

OTPKEY Authenticator is a free Windows application that can be installed from the Microsoft Store at the following link:
https://apps.microsoft.com/store/detail/XP9MCL9T4JFZ0B?ocid=pdpshare



1. If you have not downloaded the OTPKEY Authenticator application yet, download it on your computer (e.g. from the Microsoft Store, which can be found in the first part of the Windows application guide). Then press the "**I want to use a different authenticator app**" button.

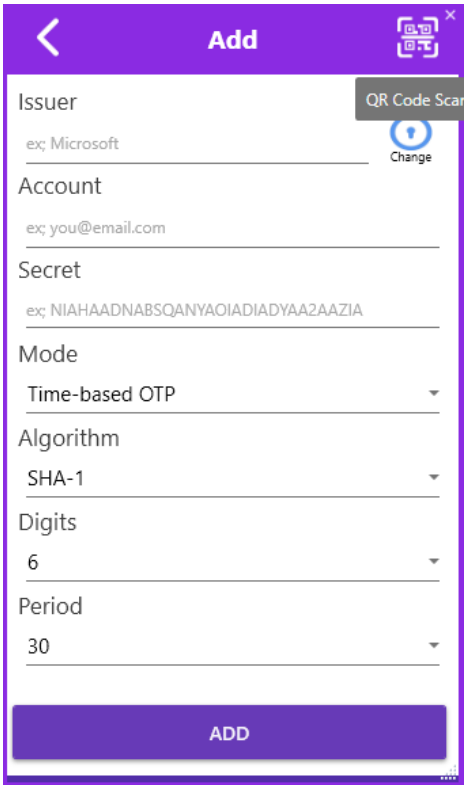


2. If you pressed the "**I want to use another authentication application**" button, i.e. authentication by another application is selected, you will see the following window. Now press the "**Next**" button.



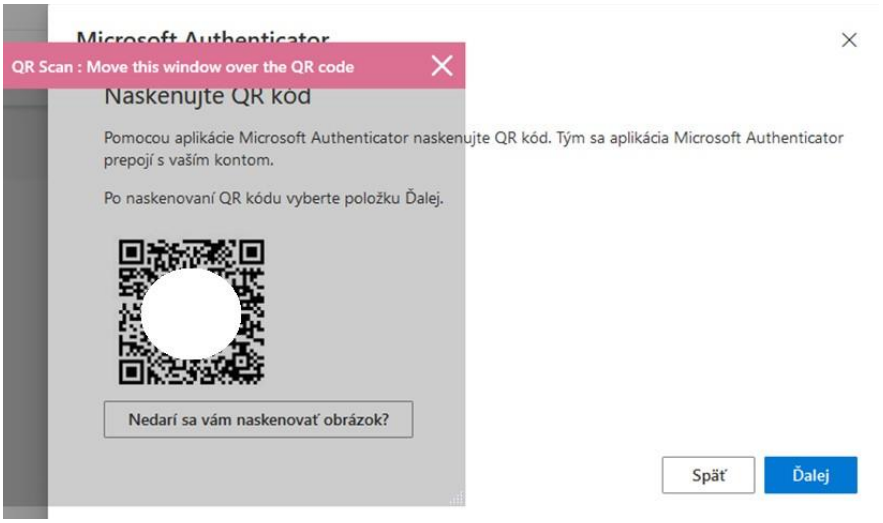
3. In this section, you will see a window with a QR code that needs to be scanned by the app. Open the OTPKEY Authenticator app and press the ⊕ **button (the white cross in the circle)** in the upper right corner to add a new authenticator.

4. Then press on the button in the top right corner to scan the QR code.



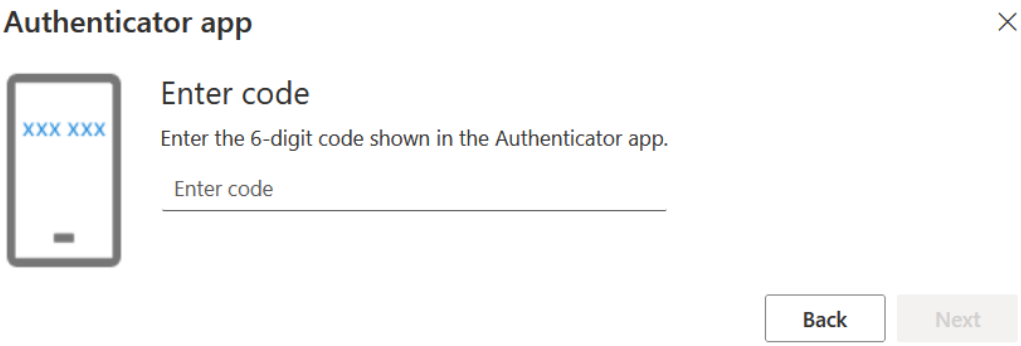
5. Now the QR code scanner will open, allowing you to scan the QR code displayed when setting up the second factor in your account. Simply move the scanner over to capture the QR code.

Note: If you have a problem with scanning the QR code, it is also possible to fill in the necessary data manually by pressing the "**Can't scan the image?**" button.
Then in the application, in the **Issuer** field add the word Microsoft, in the **Account** field add your account for which you are setting up two-factor authentication (e.g. name.surname@upjs.sk), and in the **Secret** field add the Secret Key that appears under the "**Can't scan your image?**" button.



6. In the window for the mobile application configuration, press the "**ADD**" button. Here you will see a 6-digit code that is being generated every 30 seconds.

7. In the window with the QR code, press the "**Next**" button.



8. In this step, you will be presented with a window where you can test the functionality of the second factor authentication. The "**Next**" button should be greyed out at this point. You can test the second factor authentication functionality by entering the 6-digit code displayed in the Authenticator application.

9. Then the "Next" button from step 9 will turn blue and now you can press it.

10. At this point, everything you need is already set.

Add/Change/Remove Verification Method

If you want to add, change or remove an authentication method due to a change of mobile device, phone number or for other reasons, you can do so by clicking this link: https://mysignins.microsoft.com/security-info.

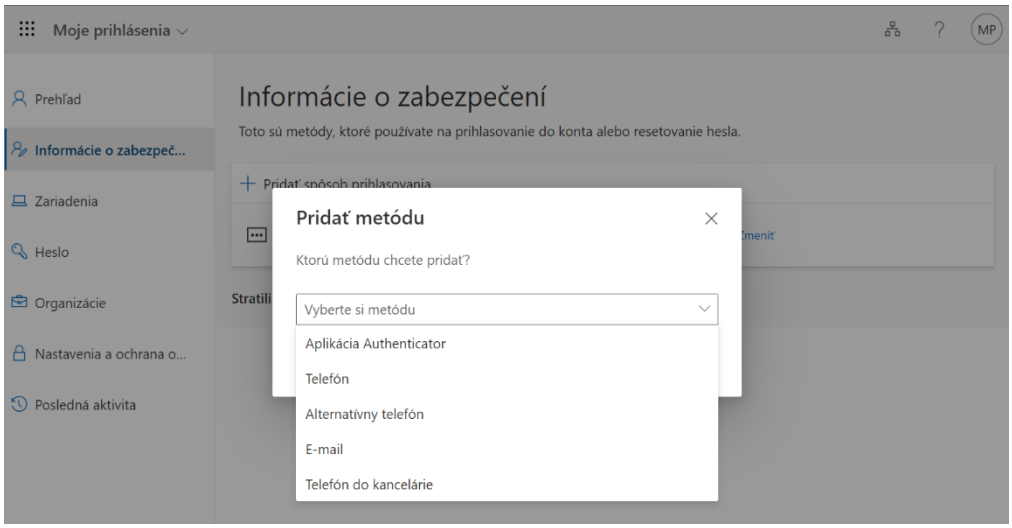
1. **Adding a new verification method**

This option allows you to add a new authentication method, such as when you get a new phone, loose your old one, or when you want to use multiple forms of authentication.

Under Security Info, press **+ Add sign-in method**.

Choose between the options: Verification phone (SMS message), Office phone, or Authenticator App (e.g., Microsoft Authenticator or OTPKeyAutheticator).

After selecting the method, click the "**Add**" button.

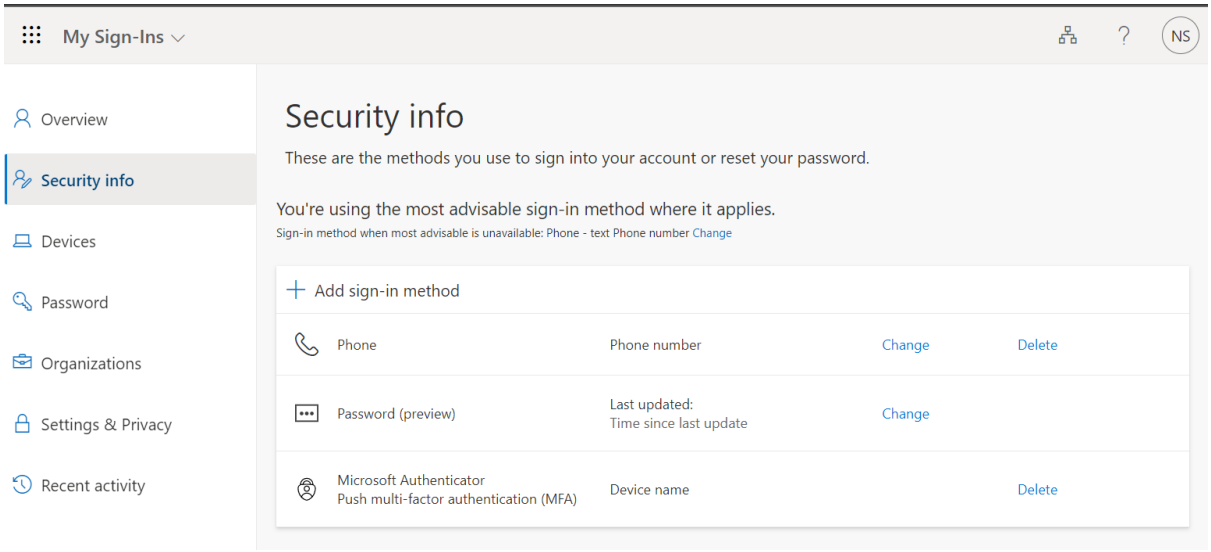


If you have selected a specific verification method, follow the instructions for that method.

2. Changing an already set verification method

This option provides the ability to update the authentication method information, for example, if your phone number changes or if you otherwise update your personal information.

For a given verification method that you want to modify, press the "**Change**" button. Here you can enter your new information.



3. Delete an already set authentication method

These options allow you to remove inactive authentication methods, which may be necessary, for example, when you change devices or lose access to one of the authentication methods.

For a given authentication method you want to delete, press the "**Delete**" button.
You can continue by adding a new authentication method according to point 1.