VŠEOBECNÁ FAKULTNÍ NEMOCNICE V PRAZE

NÁVOD

VPN pro externí účty

Nastavení Vícefaktorového ověřování

Obsah

Z důvodu bezpečnostních opatření je pro přístup do sítě VFN přes VPN **vyžadováno vícefaktorové ověření** (dále „**MFA**") **přes účet Office 365**. Ověření je nutné provádět **pomocí mobilní aplikaci Microsoft Authenticator** (možnost „notifikace z mobilní aplikace"). Jiné způsoby ověřování (kód z SMS, kód z aplikace, ...) pro VPN nefungují.

Aplikace Microsoft Authenticator

Aplikace je **zdarma dostupná pro všechny druhy mobilních operačních systémů** (Android, iOS, mobilní verze Windows) přes oficiální obchody.

Aplikaci nainstalujte, ale prozatím do ní nepřidávejte žádné účty. Účet do aplikace přidáte v průběhu nastavení MFA v prostředí Office 365.

Nastavení MFA při přihlášení do Office 365

Přes stránku office.com se **přihlaste do vašeho účtu Office 365 pro VFN** (účet@vfn.cz) – stejným účtem se také přihlašujte k Cisco AnyConnect.

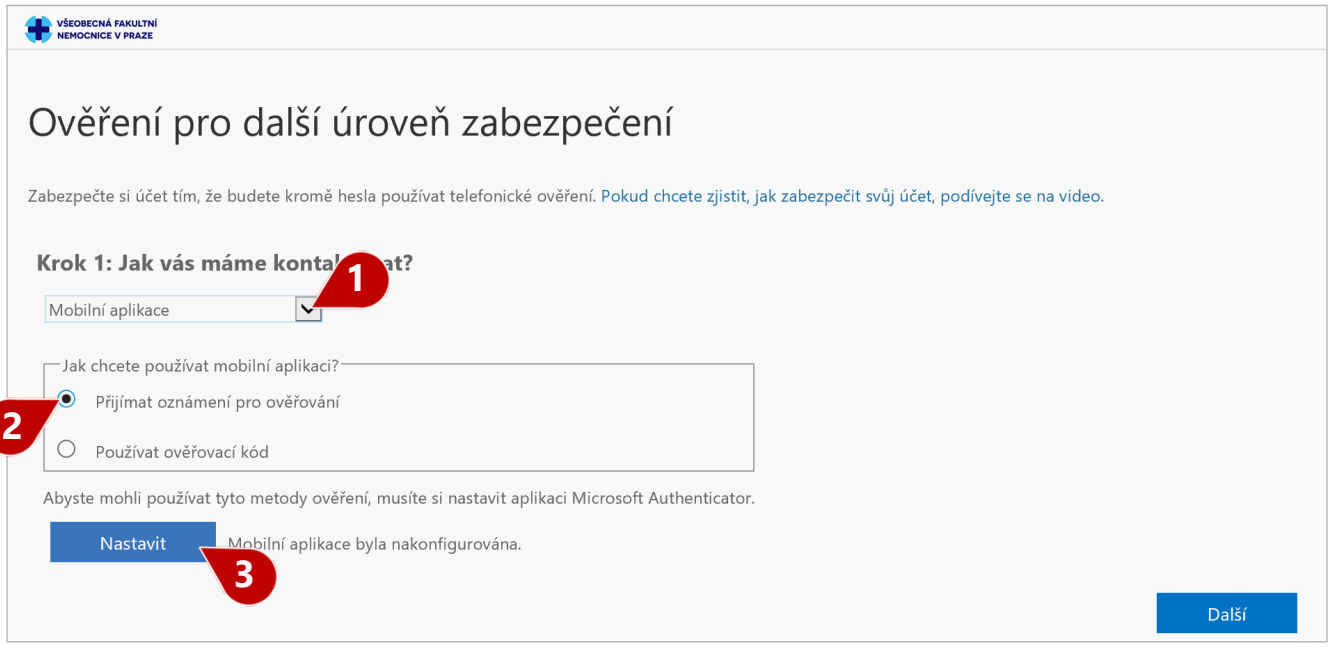
Vzhledem k tomu, že se do účtu přihlašujete poprvé, **spustí se kompletní průvodce zabezpečením Office 365, kterého je nastavení MFA součástí**.

Ihned po přihlášení se vám zobrazí informační okno „**Musíte zadat další informace**“. Jeho **potvrzením přes tlačítko** „**Další**“ se dostanete přímo ke konfigurátoru MFA – „**Ověření pro další úroveň zabezpečení**“.

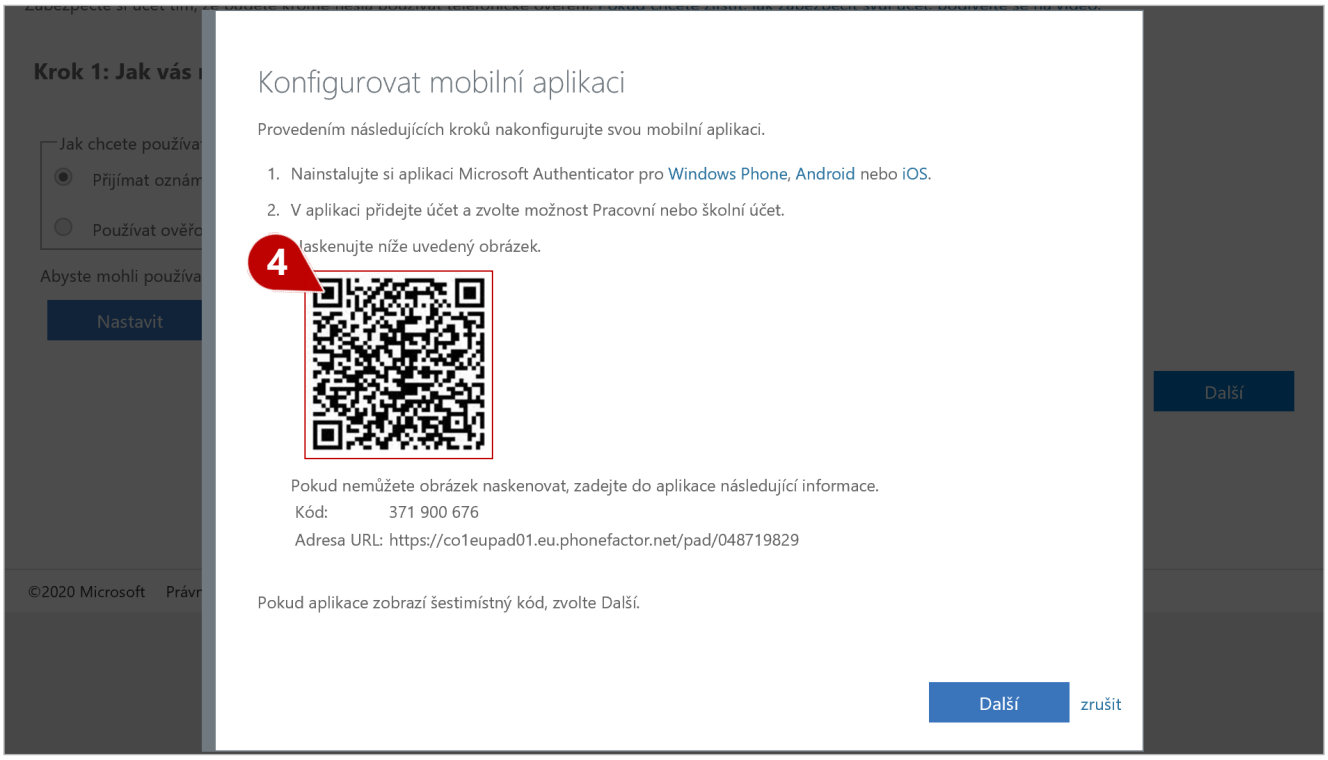
Krok 1: Jak vás máme kontaktovat?

Ze seznamu zvolte „**Mobilní aplikace**“ **(1)** a zaškrtněte „**Přijímat oznámení pro ověřování**“ **(2)**. Tím nastavíte způsob ověřování přes notifikaci z mobilní aplikace. Nyní je třeba nakonfigurovat aplikaci Microsoft Authenticator.

Klikněte na tlačítko „**Nastavit**“ **(3)**.



Vyskočí **informační okno s QR kódem (4)**.

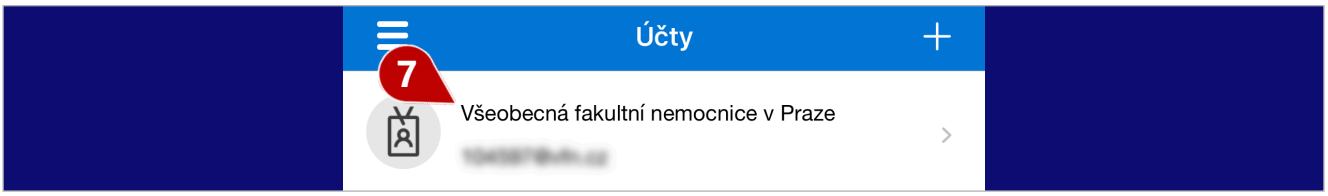


Na svém mobilním zařízení **otevřete aplikaci Microfost Authenticator**. V průběhu procesu se vás aplikace může zeptat na povolení přístupu k fotoaparátu. Přístup povolte.

Klikněte na tlačítko „**Přidat účet**“ **(5)**.

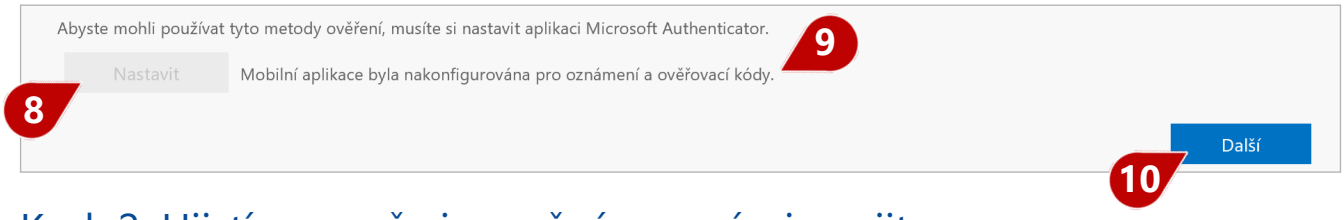
Zvolte „**Pracovní nebo školní účet**“ **(6)** a poté **načtěte přes fotoaparát QR kód**.

Účet VFN by se vám měl **načíst do aplikace (7)**.



Zpátky **v průvodci Office 365** klikněte na tlačítko „**Další**“pod QR kódem.

V kroku 1 vám tlačítko „**Nastavit**“ zašedne **(8)** a průvodce zobrazí informaci **(9)** o nakonfigurování mobilní aplikace. Potvrďte „**Další**“ **(10)**.



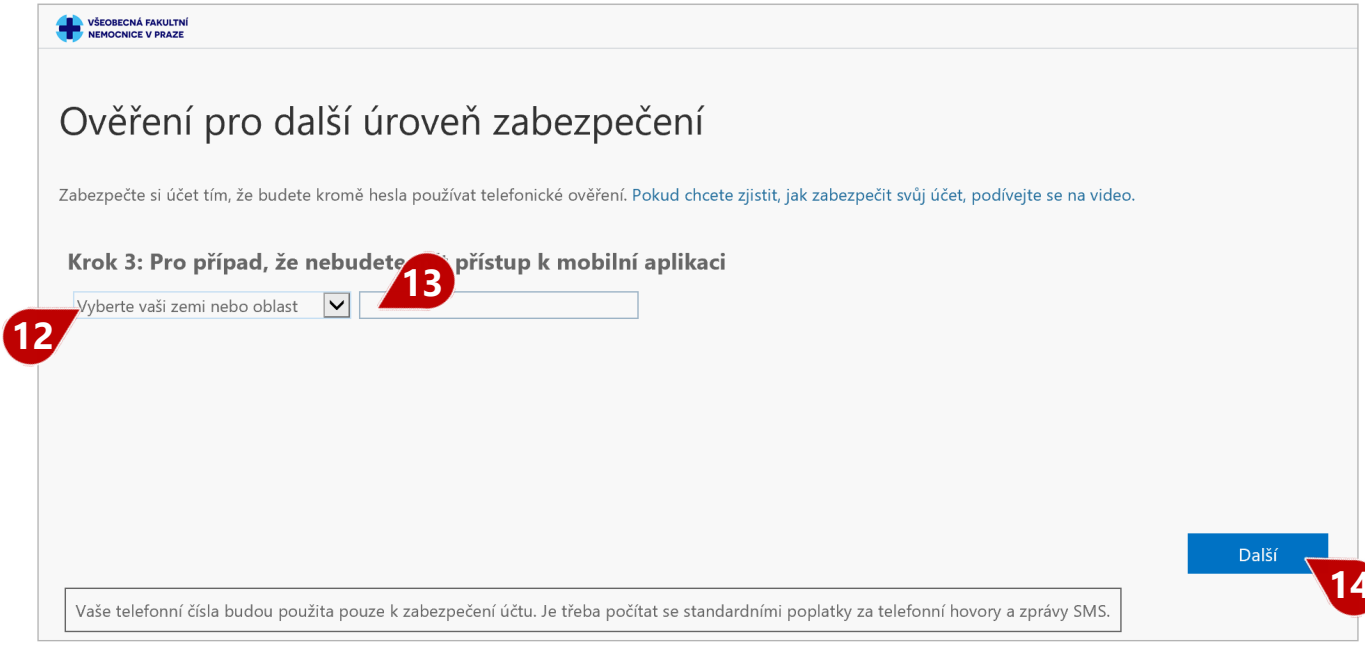
Krok 2: Ujistíme se, že je možné se s vámi spojit…

Nyní je nutné otestovat správnost nastavení MFA. **Office 365 vyšle výzvu na váš mobilní telefon, kterou je třeba schválit**. V mobilní aplikaci potvrďte správnost MFA tlačítkem „**Schválit**“ **(11)**.

Správnost potvrďte.

Krok 3: Pro případ, že nebudete mít přístup…

Vyberte **zemi, nebo oblast (12)** a **vložte vaše telefonní číslo (13)**, které chcete používat pro případ, že nebudete mít přístup k aplikaci. Jedná se o bezpečnostní pojistku, která je povinná. Potvrďte tlačítkem „**Další**“ **(14)**.



Tímto jste nastavili MFA způsobem vhodným pro práci s VPN. **Dále bude pokračovat průvodce zabezpečením účtu Office 365**, a to:

- ověřením hesla,
- testem ověření MFA
- a nastavení opatření pro možnosti obnovení vašeho účtu.

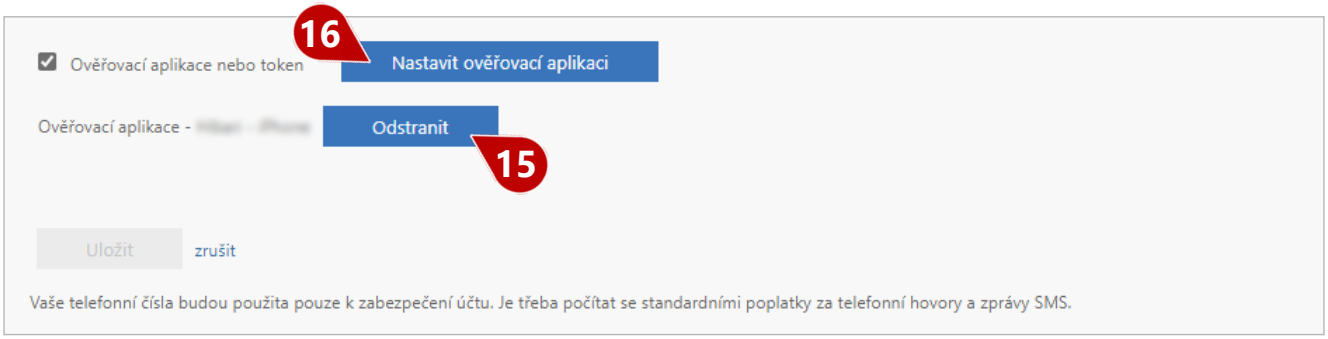
Změna nastavení MFA přes odkaz

Pokud nastala jakákoliv změna (nové mobilní zařízení, …) a potřebujete MFA změnit, či překonfigurovat aplikaci, **lze tak učinit jednoduše pomocí stránky https://aka.ms/mfasetup**.

Po přihlášení k vašemu účtu (upozorňujeme, že může být vyžadováno ověření MFA) se vám načte formulář pro změnu a konfiguraci nového způsobu ověřování – „**Ověření pro další úroveň zabezpečení**“.

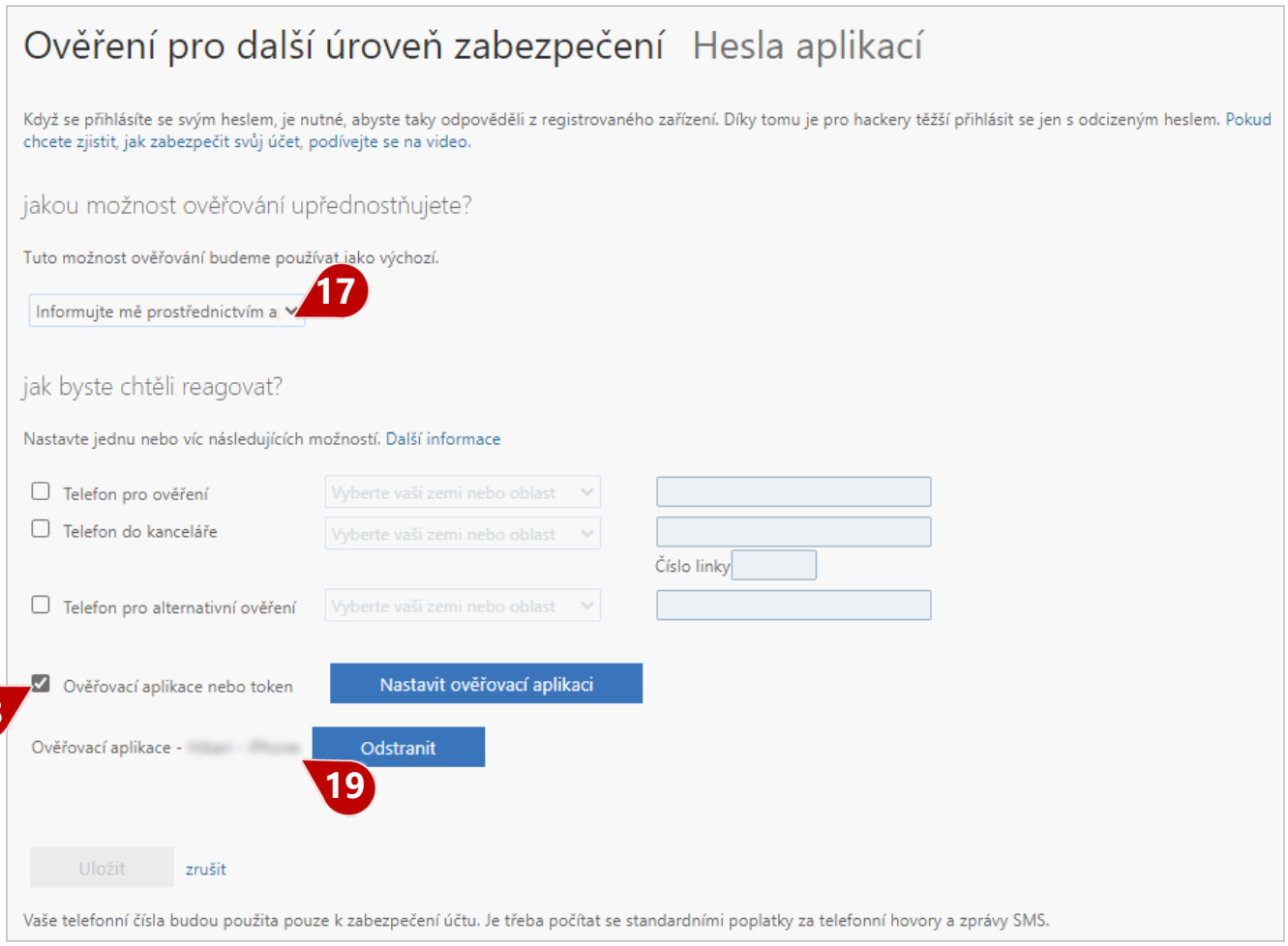
Rekonfigurace aplikace

V seznamu ověřovacích aplikací **odstraňte (15) zařízení, které již nebudete používat**. Proces může chvíli trvat. Poté klikněte na tlačítko „**Nastavit ověřovací aplikaci**“ **(16)**. Zobrazí se vám okno s QR kódem.



Na novém zařízení spusťte aplikaci Microsoft Authenticator a dále pokračujte dle pokynů popsaných v kapitole „**Krok 1: Jak vás máme kontaktovat?**“ na stránce 2.

Na závěr si nezapomeňte zkontrolovat, že máte vybráno „**Informujte mne prostřednictvím aplikace**“ **(17)**, zatrženo „**Ověřovací aplikace nebo token**“ **(18)** a **správný název zařízení**, kde máte aktivovanou aplikaci **(19)**.



Pokud je třeba, uložte.

Kontakty

V případě problémů s VPN kontaktujte Dispečink ÚI na e-mailu: dispecink@vfn.cz či na telefonním čísle: +420 224 962 119.