

# Dvoufaktorové ověřování při přihlašování do Webglobe Admin

Poslední aktualizace 12 září, 2024

V dnešní době již klasické uživatelské jméno a heslo k přihlášení nestačí. Pokud se do vašeho počítače nebo jiného zařízení dostane virus, může všechna vaše jména a hesla odeslat na internet, kde je může získat potenciální útočník. Ke kombinaci jména a hesla se lze dostat také v případě, že se připojujete prostřednictvím veřejných (nezabezpečených) sítí wi-fi, například v kavárnách, hotelech nebo na letišti, kam se jméno a heslo přenáší z vašeho zařízení nezabezpečeným způsobem.

## Nastavení v aplikaci Webglobe Admin

Pokud máte zájem o zvýšení zabezpečení svého účtu správce, doporučujeme aktivovat dvoufaktorové ověřování pro přihlašování do aplikace Webglobe Admin.

Chcete-li tuto možnost aktivovat, nejprve se přihlaste [ke svému účtu](#) a poté přejděte do části **Můj účet – Změna hesla** v levém sloupci. Na zobrazené obrazovce stačí kliknout na druhou záložku s názvem **Dvoufaktorové ověřování**.

Pro dokončení nastavení naskenujte zobrazený QR kód pomocí chytrého telefonu prostřednictvím aplikace pro dvoufaktorové ověřování, například *Google authenticator* ([iOS/Android](#)) nebo *Authy*. Po naskenování QR kódu aplikace vytvoří účet pro Webglobe Admin a zobrazí šestimístné číslo, které je třeba zadat do pole pro ověření v aplikaci Webglobe Admin, a klikněte na tlačítko **Aktivovat**. Tento úkol však musíte dokončit před vypršením platnosti kódu.

**PROFIL**
[Detail profilu](#)
[Správa přihlášení](#)
[Telekód](#)
**KONTAKTY**
[REGISTRAČNÍ KONTAKTY](#)
[PŘIHLAŠOVACÍ ÚČTY](#)
[EXTERNÍ ÚČTY](#)
[CENÍK DOMÉN](#)
[GIT](#)
[PŘEHLEDY](#)
[+ NOVÁ SLUŽBA](#)
[WEBGLOBE ACADEMY](#)
[POŽADAVEK](#)
[NÁPOVĚDA](#)
[+420 603 111 111](#)
[HELPDESK@WEBGLOBE.CZ](#)
[ČESKY](#)
[REFRESH ACL](#)
**Změna hesla pro uživatele JAN2231**
[Změna hesla](#) [Změna přihlašovacího jména](#) **[Dvoufaktorová autentifikace](#)** [IP ochrana + GeolP](#) [MojeID](#)

Dvoufaktorová autentifikace předchází narušením bezpečnosti pomocí dodatečného ověření Vaší identity. Jednorázové hesla jsou generována náhodně a nedají se opakovaně použít. Můžete si zvolit buď generování hesla prostřednictvím aplikace ve Vašem mobilním telefonu (One-Time Password) nebo ověření prostřednictvím SMS zprávy zaslané na zadané telefonní číslo.

Pro použití One-Time Password budete nejdříve potřebovat si stáhnout a nainstalovat do Vašeho mobilního telefonu aplikaci na generování jednorázových hesel (např. google authenticator nebo authy). Potom si kliknete na "Aktivovat" a aplikaci si naskenujete zobrazený QR kód. Při následujícím přihlášení budete ve druhém kroku vyzváni na zadání jednorázového hesla - to Vám vygeneruje aplikace ve vašem telefonu. V případě zadání správného jednorázového hesla budete úspěšně přihlášení. Pro SMS verifikaci je potřebné zadat číslo mobilního telefonu, na který budou posílány SMS zprávy s jednorázovým klíčem potřebným pro přihlášení se do Vašeho účtu.

 Typ dvoufaktorové autentifikace OTP - One Time Password - Pomocí aplikac

QR kód


 Privátní klíč `I4R5SS3L6KXR5POII5DQQLONHSPMGU4U`

Verifikační kód




## Doporučené aplikace OTP pro smartphone

### Google Authenticator

- [Android](#)
- [iOS](#)

### Authy 2-faktorové ověřování

- [Android](#)
- [iOS](#)