Pepita Group Zrt. - Jelszókezelés admin - házirend

1. Bevezetés a kétfaktoros hitelesítés (2FA) rendszeréhez

1.1 A 2FA bevezetésének célja

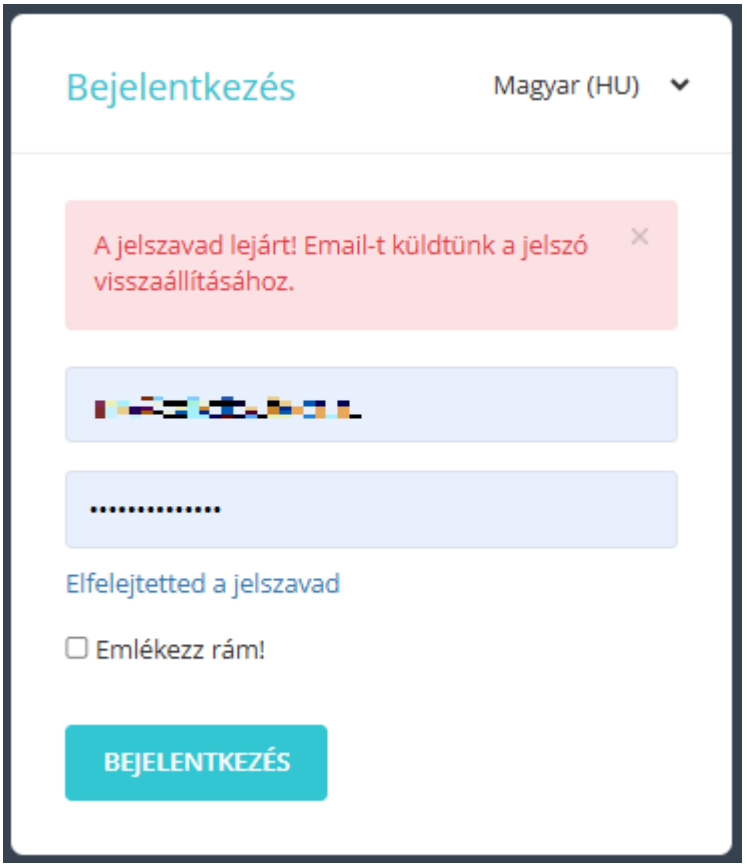
A rendszer biztonságának növelése érdekében bevezetésre kerül a kétfaktoros hitelesítés (2FA). Ennek célja, hogy a felhasználói fiókokhoz való hozzáférés ne csak jelszóval, hanem egy második azonosítási lépéssel is védett legyen.

1.2 Jelszavak érvényessége és cseréje

A jelenleg használt jelszavak 2026. május 15-ig maradnak érvényben. Ezt követően a rendszer nem fogadja el a régi jelszavakat, ezért azok megváltoztatása kötelezővé válik. A jelszócsere a határidő előtt is elvégezhető, opcionális jelleggel.

1.3 Lejárt jelszó kezelése

Amennyiben egy jelszó lejárt, a felhasználó bejelentkezéskor hibaüzenetet kap, amely jelzi, hogy új jelszó megadása szükséges. Ebben az esetben a rendszer útmutatást biztosít a jelszó megváltoztatásának folyamatához.



1.4 Jelszókövetelmények az új rendszerben

Az új jelszó megadásakor az alábbi biztonsági követelményeknek kell megfelelni:

- A jelszónak legalább 12 karakter hosszúnak kell lennie.

- A jelszó legfeljebb 64 karakter hosszú lehet.
- Tartalmaznia kell kis- és nagybetűt.
- Tartalmaznia kell legalább egy számot.
- Tartalmaznia kell legalább egy szimbólumot (például: #, $, @, _).
- Nem szerepelhet benne ugyanaz a karakter háromszor egymás után.
- A jelszó nem tartalmazhatja az e-mail cím helyi részét.
- A jelszó nem lehet az utolsó 5 használt jelszó egyike.

1.5 Jelszó érvényességi ideje 2FA használata esetén

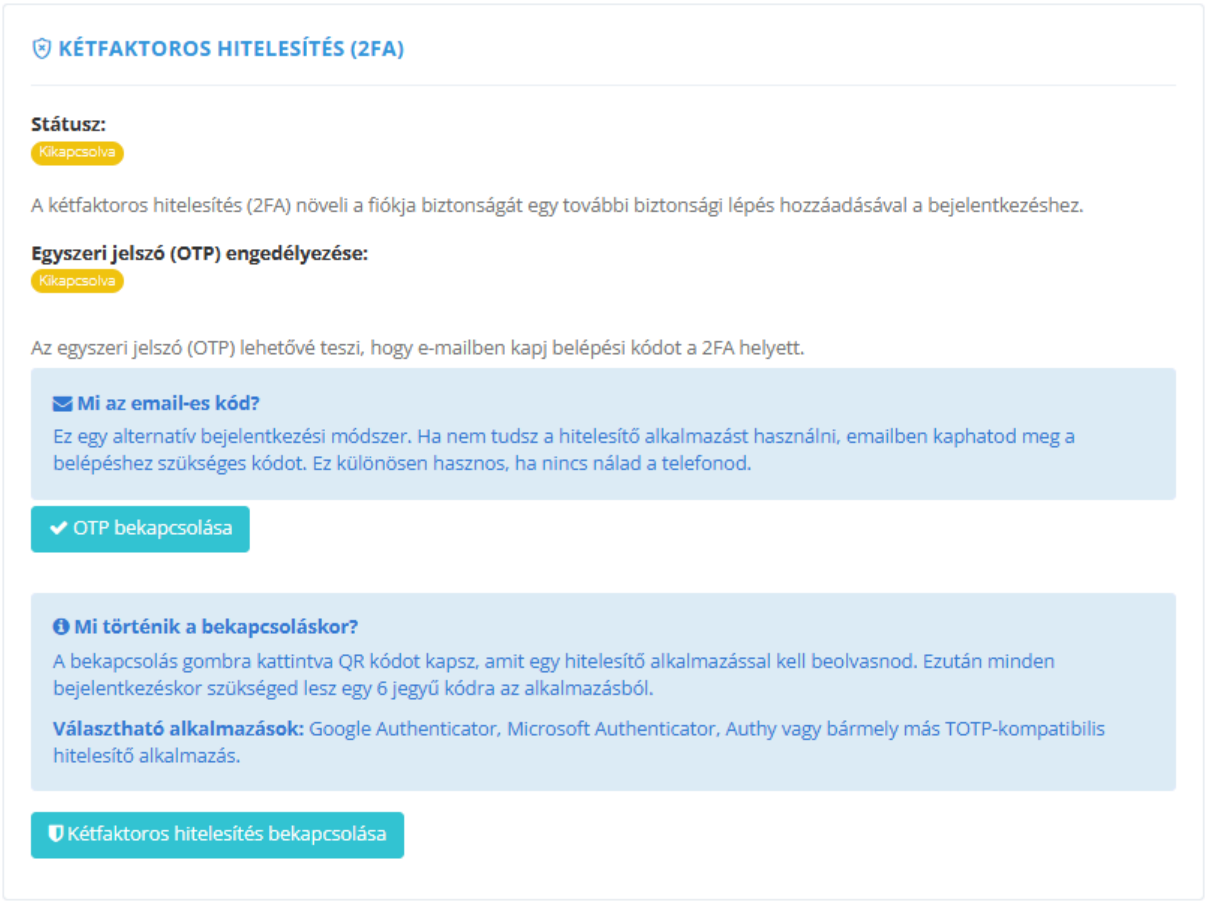
Amennyiben a felhasználó bekapcsolja a kétfaktoros hitelesítést (2FA), a beállított jelszó érvényességi ideje 1 évre módosul.

2. Kétfaktoros hitelesítés (2FA) bekapcsolása

A rendszer magasabb védelmi szintje érdekében javasoljuk partnereink számára a kétfaktoros hitelesítés bekapcsolását.

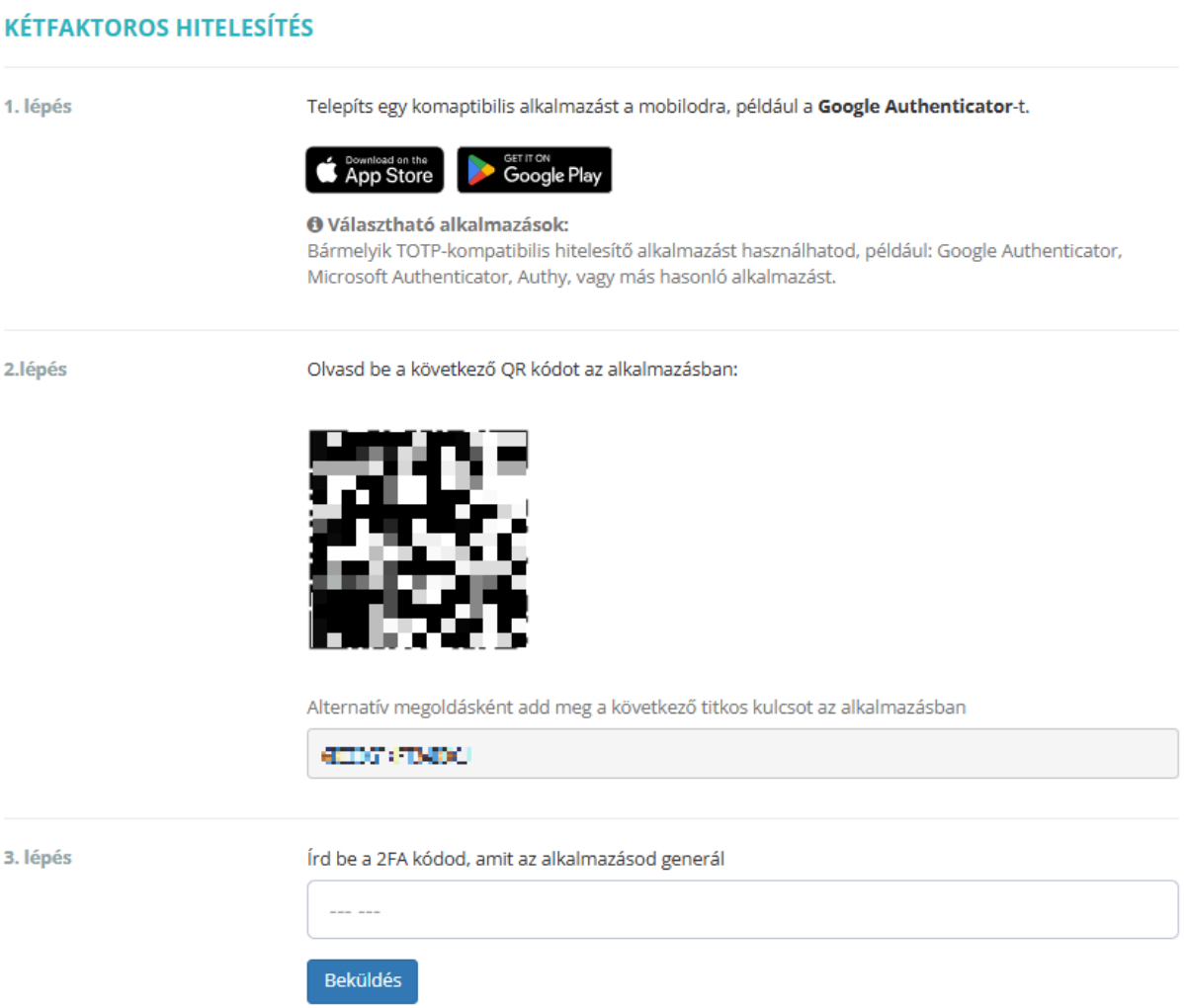
2.1 A 2FA aktiválásának elérése

A kétfaktoros hitelesítés bekapcsolása bejelentkezést követően érhető el. Az oldalsó menüsorban válassza a **Felhasználók** menüpontot, majd azon belül a **Kétfaktoros hitelesítés** fület.
Az aktiválás elindításához kattintson a **„Kétfaktoros hitelesítés bekapcsolása”** gombra.



2.2 Átirányítás az aktiváló felületre

A gombra kattintást követően a rendszer automatikusan átirányítja az aktiváló felületre, ahol a 2FA beállítás elvégezhető.



2.3 Szükséges alkalmazás

Az aktiváláshoz egy hitelesítő (authenticator) alkalmazás szükséges. Például használható a Microsoft Authenticator alkalmazás, amely elérhető Android és iOS eszközökre is.

2.4 QR-kód beolvasása és kód megadása

Az aktiváló felületen megjelenő QR-kódot be kell olvasni az authenticator alkalmazással.
A sikeres beolvasást követően az alkalmazás egy 6 számjegyű biztonsági kódot generál.

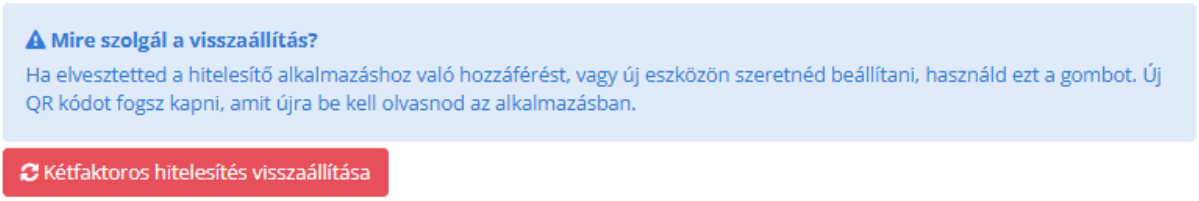
Ezt a kódot a megfelelő mezőbe kell beírni, majd a **„Beküldés”** gombra kattintva véglegesíthető a kétfaktoros hitelesítés aktiválása.

2.5 Megjegyzés a 2FA aktiválási folyamat megszakításáról

Amennyiben a kétfaktoros hitelesítés (2FA) aktiválási folyamata bármilyen okból megszakításra kerül, a folyamat nem vész el.

2.6 A 2FA kezelésére vonatkozó korlátozások és helyreállítás

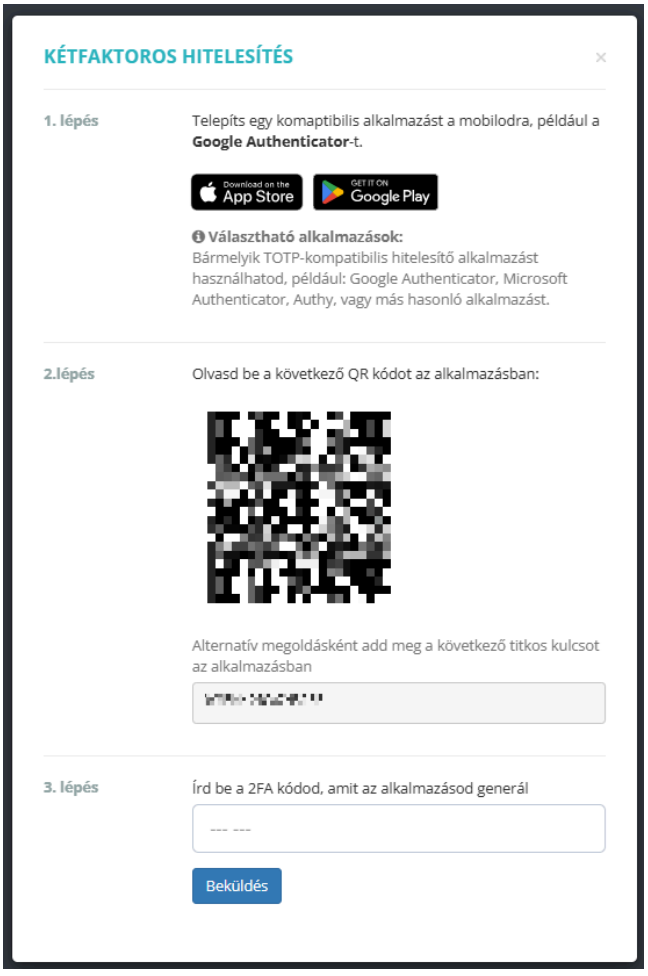
A kétfaktoros hitelesítés bekapcsolását követően annak kikapcsolására nincs lehetőség. A rendszer kizárólag a 2FA működéséhez használt titkoskulcs törlését teszi lehetővé.



Amennyiben a felhasználó bármilyen okból elveszíti a hozzáférést az authentikáló alkalmazáshoz (például eszközcsere vagy alkalmazás törlése miatt), a hozzáférés helyreállítása az ügyfélszolgálaton keresztül történik.

Az ügyfélszolgálat a titkoskulcs visszaállítását követően lehetőséget biztosít új eszköz regisztrálására vagy a kétfaktoros hitelesítés újbóli aktiválására.

A felhasználó kijelentkezést, majd újbóli bejelentkezést követően ismét lehetőséget kap az aktiválás befejezésére, a korábban ismertetett lépések végrehajtásával.



3. Egyszer használatos jelszó (OTP) használata

3.1 Az egyszer használatos jelszó bekapcsolása

Az egyszer használatos jelszó (OTP) funkció a **Kétfaktoros hitelesítés** fülön érhető el. A megfelelő opció kiválasztásával aktiválható a szolgáltatás.

3.2 Az OTP használatának feltétele

Az egyszer használatos jelszó kizárólag a kétfaktoros hitelesítés (2FA) engedélyezésével együtt használható.
Önállóan, 2FA nélkül az OTP alapú bejelentkezés nem érhető el.

3.3 Az OTP működése

Az OTP lehetővé teszi, hogy a felhasználó bejelentkezés során ne authentikáló alkalmazást használjon, hanem egy egyszer használatos kóddal azonosítsa magát.

3.4 Kód kiküldése és használata

Bejelentkezéskor a rendszer egy egyszer használatos biztonsági kódot küld a felhasználó regisztrált e-mail címére.
A kapott kód megadásával a felhasználó sikeresen be tud jelentkezni a rendszerbe.

4. Bejelentkezés a fiókba 2FA használatával

4.1 Bejelentkezési folyamat indítása

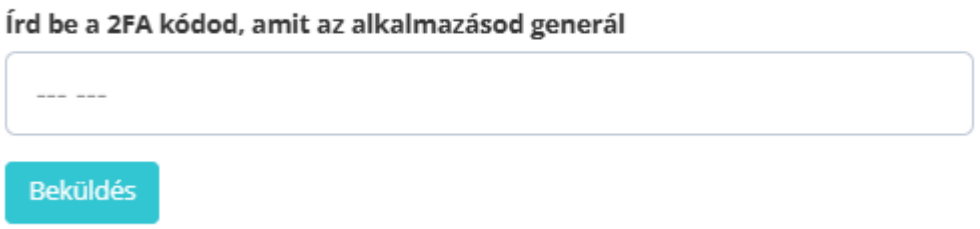
A felhasználónév és jelszó helyes megadását követően a „Bejelentkezés” gombra kattintva egy további azonosítási panel jelenik meg.

Ezen a felületen egy beviteli mező található a 6 számjegyű biztonsági kód megadására, valamint egy „Egyszerhasználatos jelszó kérése” gomb.

4.2 Bejelentkezés authentikáló alkalmazással

Az authentikáló alkalmazásban megjelenő 6 számjegyű kódot a megfelelő mezőbe kell beírni.

A „Beküldés” gombra kattintva – helyes kód megadása esetén – a felhasználó sikeresen belép a rendszerbe.

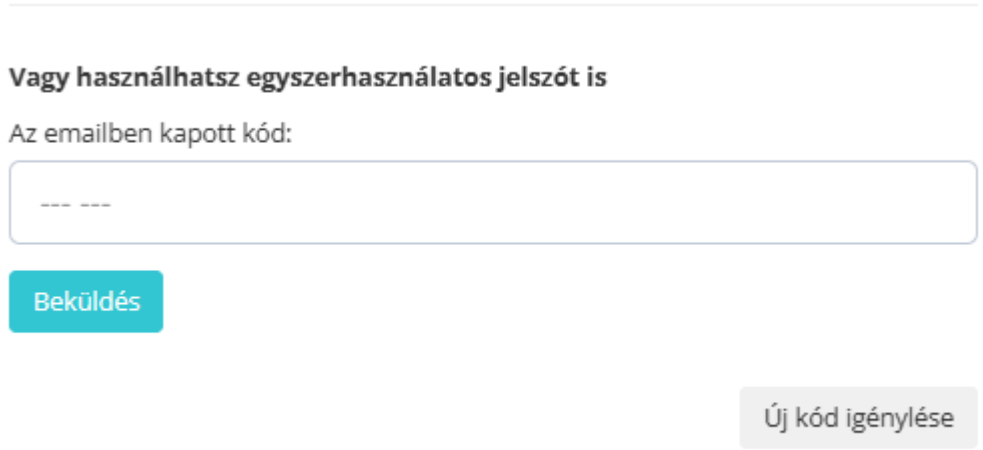


4.3 Bejelentkezés egyszer használatos jelszóval (OTP)

Az „Egyszerhasználatos jelszó kérése” gombra kattintva a felület módosul, és megjelenik egy új beviteli mező.

Ide az e-mailben kiküldött 6 számjegyű egyszer használatos kódot kell megadni.

A kód megadását követően a „Beküldés” gombra kattintva – helyes kód esetén – a bejelentkezés sikeresen megtörténik.



4.4 Új egyszer használatos kód igénylése

Amennyiben a felhasználónak új kódra van szüksége (például a korábbi lejárt vagy nem érkezett meg), az „Új kód igénylése” gombra kattintva lehet új egyszer használatos jelszót kérni.