

2.2 Kétfaktoros hitelesítés

2.2.1 Kétfaktoros hitelesítésről bővebben

Mi ez?

Bejelentkezéskor a jelszava mellett egy hatjegyű kódot is meg kell adnia, amelyet a telefonján lévő hitelesítő alkalmazás (például Google Authenticator, Microsoft Authenticator) mutat. A kód 30 másodpercenként megváltozik, és mindig csak rövid ideig érvényes. Ezt a módszert TOTP-nek hívják, ami az angol *Time-based One-Time Password*, vagyis „időalapú egyszeri jelszó” rövidítése.

Hogyan működik?

Képzelve el, hogy Ön és az E-közüzem rendszer egy közös titkos jelszót kapnak, amelyet rajtunk kívül senki más sem ismer. A titkos jelszó alapján a pontos időből ugyanazt a számot lehet kiszámolni, ha valaki ismeri a titkot.

A beállításkor egy QR-kódot olvas be a telefonjával. Ez a QR kód átadja az E-közüzem által generált titkos jelszót az Ön authenticator alkalmazásának. Ettől kezdve a telefonja és a mi rendszerünk egymástól függetlenül, ugyanazzal a recepttel számolja ki az aktuális kódot. Amikor beírja a kódot, a rendszer ellenőrzi, hogy egyezik-e azzal, amit ő is kiszámolt. Ha igen, beléphet.

Fontos, hogy a telefonjának ehhez nincs szüksége internetkapcsolatra. Az alkalmazás nem kap üzenetet tőlünk, csak a telefon órájára és a beállításkor kapott titokra támaszkodik.

Miért előnyös ez felhasználói szempontból?

Egy ellopott jelszó így önmagában nem elég. Ha valaki megszerzi az Ön jelszavát, például egy adatszivárgásból vagy egy csaló e-mailből, akkor sem tud belépni, mert nincs nála az Ön telefonja.

A kódok gyorsan elévülnek. Még ha valaki meg is látja a kódját, fél percen belül használhatatlanná válik.

Biztonságosabb az SMS-nél. Az SMS-ben kapott kódokat el lehet téríteni, például ha valaki csalással megszerzi az Ön telefonszámát. A hitelesítő alkalmazás kódja nem utazik a hálózaton, így ezt a kockázatot elkerüli.

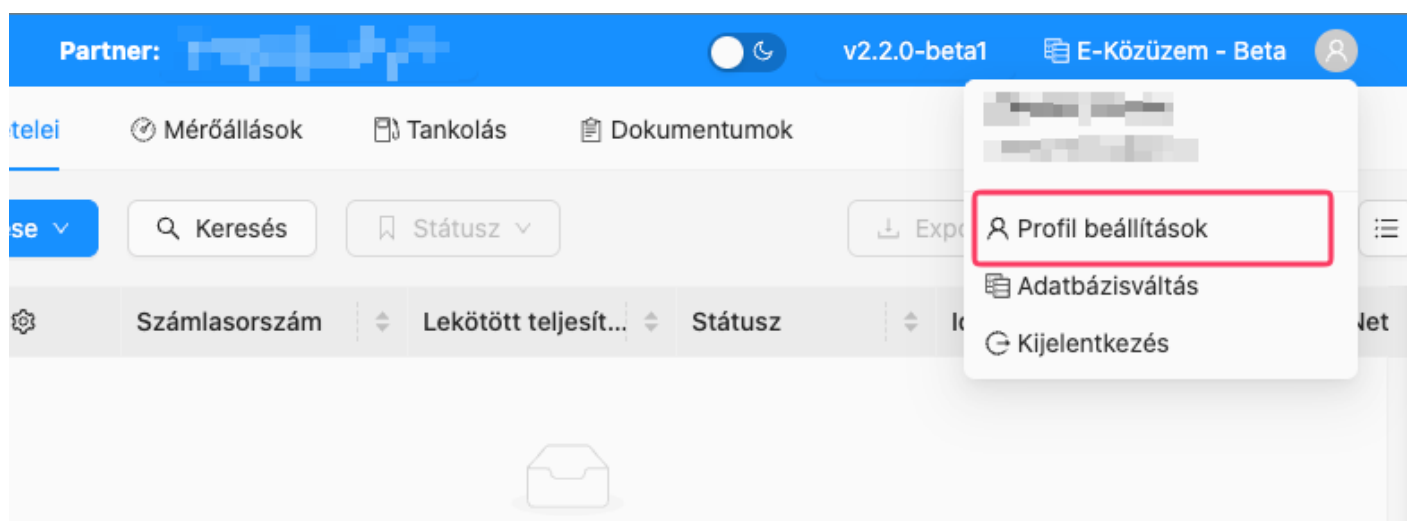
Mindenhol működik. Külföldön, repülőgépen vagy térerő nélkül is használhatja, és nem kerül pénzbe.

Egy Authenticator alkalmazás, sok fiók. Ugyanabban az Authenticator alkalmazásban más szolgáltatások (e-mail, közösségi média, banki oldalak) kódjait is kezelheti.

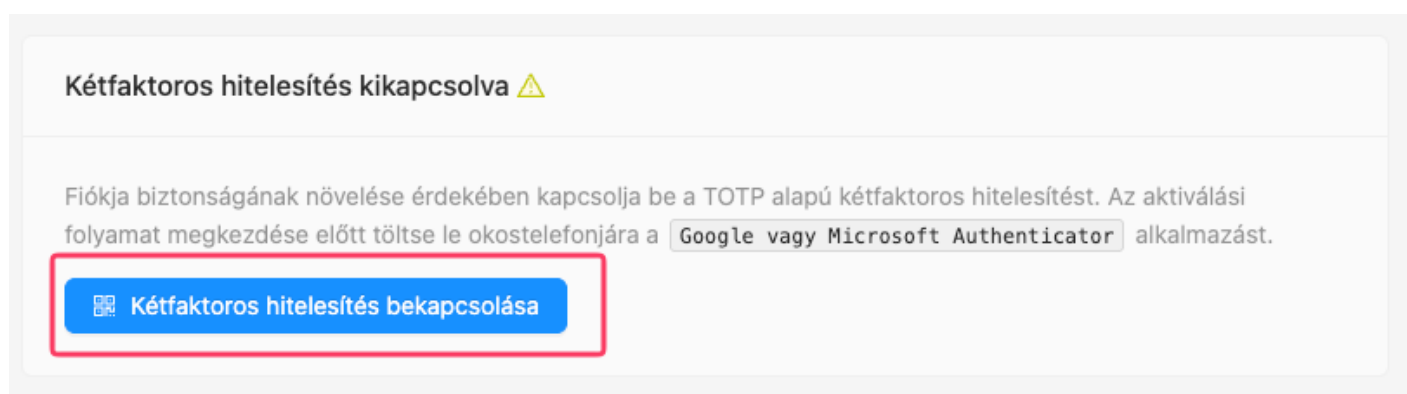
Ügyeljen arra, hogy a telefonján az idő automatikusan legyen beállítva, mert ha az óra elcsúszik, a kódok nem fognak egyezni. A beállításkor kapott helyreállító kódokat írja fel, és tartsa biztonságos helyen; ezekkel akkor is be tud lépni, ha elveszíti a telefonját. Telefoncsere előtt mindig költöztesse át a fiókjait az új készülékre, vagy kapcsolja ki, majd állítsa be újra a kétfaktoros azonosítást.

2.2.2 Kétfaktoros hitelesítés aktiválása

A kétfaktoros hitelesítés beállításához előbb lépjen be az alkalmazásba, válasszon intézményt, és partnert. A hitelesítési beállítások a jobb felső sarokban található Profil beállítások menüpontban érhetők el:



A kétfaktoros hitelesítés beállításához előbb regisztrálnia kell a mobileszközét a rendszerbe, hogy a rajta található Authenticator alkalmazás megkapja a hitelesítő kódok generálásához szükséges információkat. Az eszközregisztrálás megkezdéséhez kattintson a Kétfaktoros hitelesítés bekapcsolása gombra.



Az eszközregisztráció megkezdése előtt tölts le mobiltelefonjára (Android vagy iOS) a Microsoft vagy Google Authenticator alkalmazást. Az E-közüzem más hitelesítő alkalmazást is támogat, amelyek képesek TOTP kódok generálására, de a Microsoft és Google szoftvere a legelterjedtebb, így mi ezeket ajánljuk.

A következő lépésben az E-közüzem meg fog jeleníteni Önnek egy QR kódot.

Kétfaktoros hitelesítés beállítása

1

Eszköz regisztrálása

2

Helyreállító kódok

Az Authenticator alkalmazásával olvassa be az alábbi QR kódot:



A QR kód beolvasása után írja be az Authenticator alkalmazásban megjelenő 6 számjegű kódot, majd kattintson a Megerősítés gombra:

|

Visszavonás

Megerősítés

Nyissa meg a választott Authenticator alkalmazását, majd rögzítsen új fiókot (a példában a Google Authenticator szerepel). Az Authenticator megnyitja a telefonja kameráját, amit az E-közüzem felületén látható QR kódra kell irányítani. A sikeres beolvasás esetén az Authenticator alkalmazásban megjelenik az E-közüzem fiókjához tartozó hitelesítő kód.

12:03



Google Authenticator



Keresés...



Beállítókulcs
megadása



QR-kód beolvasása





Az Authenticator alkalmazásban most megjelenő 6 számjegyű kódot írja be az E-közüzem felületen, a QR kód alatt található beviteli mezőbe, majd kattintson a Megerősítés gombra:

Kétfaktoros hitelesítés beállítása

1

Eszköz regisztrálása

2

Helyreállító kódok

Az Authenticator alkalmazásával olvassa be az alábbi QR kódot:



A QR kód beolvasása után írja be az Authenticator alkalmazásban megjelenő 6 számjegű kódot, majd kattintson a Megerősítés gombra:

8

5

6

0

5

0

Visszavonás

Megerősítés

A művelet sikerességével az E-közüzem meggyőződik arról, hogy az Ön készüléke helyesen elmentette a megosztott titkos jelszót, amivel így a telefonja is képes rövid életű hitelesítő kódokat generálni.

A második lépésben a felület 6 darab helyreállító kódot fog mutatni Önnek. Ezek a kódok olyan esetekben használhatók, ha a felhasználó elveszti hozzáférését a hitelesítő mobilkészülethez (pl.: véletlenül letörli az Authenticator alkalmazást vagy elromlik a telefon).

Kétfaktoros hitelesítés beállítása

✓

Eszköz regisztrálása

2

Helyreállító kódok

Amennyiben mobileszköze elveszik, elromlik, vagy az Authenticator alkalmazásához elveszti a hozzáférést, az alábbi helyreállító kódokat használhatja bejelentkezésakor.

Mindegyik kód csak egyszer használható! Kérjük, az alábbi kódokat mentse el biztonságos helyre (pl.: jelszókezelő alkalmazás)!

Új helyreállító kódokat bármikor generálhat a Profil beállítások oldalon. A kódok újragenerálásával a korábbi kódok inaktívvá válnak.

c7djjv5K8_NDF-P

QmByCiAH0ZjdrkOV

gNvLOit7gzU73_BC

hVJYYvb7pg_4EwV_

95AVCZZ0dzv1uokW

nweou-MA4N_3!PtU

Helyreállító kódok másolása

Visszavonás

Megértettem

Fontos: Ezeket a kódokat bejelentkezésakor beírhatja a 6 számjegyű hitelesítő kód helyett. Ha egy kóddal egyszer sikeresen bejelentkezett, utána már nem használható. Kérjük, ezeket a kódokat mentse el biztos helyre, hogy készülékmeghibásodás esetén is be tudjon jelentkezni az E-közüzembe!

Új helyreállító kódokat bármikor generálhat a Profil beállítások alatt. Ilyenkor a korábbi, még fel nem használt kódok érvénytelenné válnak.

Ha elmentette a helyreállító kódokat, kattintson a Megértettem gombra. Ezzel a kétfaktoros hitelesítés aktívvá válik a fiókjában, a következő bejelentkezésakor a rendszer már kérni fogja a 6 számjegyű hitelesítő kódot.

2.2.3 Új helyreállító kódok generálása

Amennyiben Ön már aktiválta a kétfaktoros hitelesítést, de több helyreállító kódot is felhasznált vagy elvesztette a meglévőket, akkor a Profilbeállítások alatt bármikor újakat generálhat a Új helyreállító kódok generálása gombra kattintva:

Kétfaktoros hitelesítés bekapcsolva 

A kétfaktoros hitelesítés kikapcsolásával csökken fiókjának védelme.

 Új helyreállító kódok generálása

 Kétfaktoros hitelesítés kikapcsolása

Új helyreállító kódok

Amennyiben mobil eszköze elveszik, elromlik, vagy az Authenticator alkalmazásához elveszti a hozzáférést, az alábbi helyreállító kódokat használhatja bejelentkezéskor.

Mindegyik kód csak egyszer használható! Kérjük, az alábbi kódokat mentse el biztonságos helyre (pl.: jelszókezelő alkalmazás)!

Új helyreállító kódokat bármikor generálhat a Profil beállítások oldalon. A kódok újragenerálásával a korábbi kódok inaktívvá válnak.

LFvuMpDxtAjcc2vc

HX1UHQK/B3s?x2MA

d/M88X7csQ2H_FkD

txYX!KdD3Haz!mT7

_1MrUbL5TaH93kww

f6qaQiPEuD3GU?Az

 Helyreállító kódok másolása

Visszavonás

Alkalmazás

2.2.4 Kétfaktoros hitelesítés kikapcsolása

Amennyiben fiókjában szeretné kikapcsolni a kétfaktoros hitelesítést, azt szintén a Profil beállítások alatt teheti meg. Ehhez kattintson a Kétfaktoros hitelesítés kikapcsolása gombra:

Kétfaktoros hitelesítés bekapcsolva 

A kétfaktoros hitelesítés kikapcsolásával csökken fiókjának védelme.

 Új helyreállító kódok generálása

 Kétfaktoros hitelesítés kikapcsolása

A kétfaktoros hitelesítés bekapcsolása ajánlott! Kérjük, csak abban az esetben kapcsolja ki, ha régi Authenticator alkalmazásához elvesztette hozzáférését, és új eszközt szeretne regisztrálni a fiókhoz. Ilyenkor kikapcsolhatja rövid időre a funkciót, de minél előbb regisztrálja új hitelesítő eszközét!

2.2.5 Bejelentkezés kétfaktoros hitelesítéssel

A kétfaktoros hitelesítéssel való bejelentkezés ugyan úgy indul, mint a sima beléptetés. Előbb adja meg e-mail címét és jelszavát, majd kattintson a Bejelentkezés gombra.

A rendszer előbb megvizsgálja, hogy a megadott adatok helyesek-e, és ha szükséges kétfaktoros hitelesítést, azt jelezni fogja a felületen:

⚠ Kétfaktoros hitelesítés szükséges!



Bejelentkezés

E-mail cím

revesz.ferenc@gs.hu

Jelszó

.....

Hitelesítő kód

123456

Adja meg az Authenticator alkalmazásban megjelenő kódot vagy egyik helyreállító kódját!

[Elfelejtett jelszó](#)

[Bejelentkezés](#)



A Hitelesítő kód mezőbe írja be az Authenticator alkalmazásban megjelenő, az E-közüzem fiókjához tartozó aktuális 6 jegű hitelesítő kódot.

A Bejelentkezés gombra való kattintás után 2 perc áll rendelkezésére, hogy beírja a hitelesítő kódot. Ha kifut az időből, a rendszer hibaüzenetben jelzeni fogja, hogy újra be kell jelentkeznie! Ilyenkor frissítse a weboldalt, és lépjen meg ismét.

Amennyiben Authenticator alkalmazásához elvesztette a hozzáférést, beírhatja valamelyik helyreállító kódját is. Ilyen esetben kérjük, hogy azonnal kapcsolja ki a kétfaktoros hitelesítést, és kapcsolja vissza újra az új eszközének regisztrálásával.

A rendszer 5 sikertelen hitelesítő kód próba után 5 percre tiltja a bejelentkezést a fiókjához.

Változat #3

Révész Ferenc hozta létre 27 október 2026 10:45:26

Révész Ferenc frissítette 27 október 2026 11:46:00