

Kétfaktoros hitelesítés

Első belépés, mindennapi használat és hozzáférés-helyreállítás

Biztonságosabb bejelentkezés két egymást kiegészítő azonosítási lépéssel

1. Jelszó	2. Egyszer használatos kód	3. Sikeres belépés
-----------	----------------------------	--------------------

RÖVIDEN Az első belépéskor az e-mailes kód vagy a hitelesítő alkalmazás közül kell elsődleges módot választani. Később a 2FA-beállításokban mindkettő bekapcsolható. Ha mindkettő aktív, a rendszer minden belépéskor megkérdezi, melyiket szeretné használni.

1. Az útmutató célja

Ez az útmutató bemutatja a kétfaktoros hitelesítés használatát az első belépéstől a mindennapi bejelentkezésen át a hozzáférés helyreállításáig. A leírás a felhasználói teendőkre összpontosít, ezért nem tartalmaz rendszerneveket, weboldalneveket vagy technikai háttérinformációkat.

A kétfaktoros hitelesítés a jelszó mellett egy rövid ideig vagy egyszer használható ellenőrző kódot is kér. Így a fiók akkor is nagyobb védelemben marad, ha a jelszó illetéktelen személy tudomására jut.

2. Amit érdemes előkészíteni

- A jelenlegi felhasználónevet és jelszót.
- Hozzáférést a fiókhoz tartozó e-mail-postafiókhoz.
- Hitelesítő alkalmazás használata esetén egy olyan mobilkészüléket, amelyen ilyen alkalmazás elérhető.
- Néhány percet az első beállítás megszakítás nélküli befejezésére.

FONTOS Az első belépés csak akkor fejezhető be, ha az új jelszó beállítása és a kiválasztott második hitelesítési mód ellenőrzése is sikeres.

3. A folyamat áttekintése

Helyzet	A rendszer működése	Felhasználói teendő
Első belépés	Kötelező jelszócsere, majd a második hitelesítési mód beállítása.	Új jelszó létrehozása, módszer kiválasztása, kód megadása.
Egy aktív módszer	A jelszó után automatikusan az aktív módszer következik.	Az e-mailben kapott vagy az alkalmazásban látható aktuális kód megadása.
Két aktív módszer	A jelszó megadása után választási lehetőséget ad.	Módszer választása, majd az ahhoz tartozó kód megadása.
Hozzáférés helyreállítása	Az alkalmazásos beállítás törlődik, az e-mail-es mód lesz aktív.	Belépés e-mail-es kóddal, majd szükség esetén új beállítás.

4. Első belépés és kezdeti beállítás

Az első belépés két egymást követő részből áll: először új jelszót kell beállítani, utána pedig ki kell választani és ellenőrizni a kétfaktoros hitelesítés elsődleges módját.

4.1 Új jelszó beállítása

1. **Jelentkezzen be a meglévő adataival.** A rendszer automatikusan a jelszócsere oldalra irányítja.
2. **Adja meg a jelenlegi jelszót.** Ez igazolja, hogy a módosítást a fiók tulajdonosa kezdeményezi.
3. **Írja be kétszer az új jelszót.** A két új jelszónak teljesen meg kell egyeznie.

JELSZÓKÖVETELMÉNYEK Az új jelszó legalább 8 karakterből álljon, tartalmazzon kisbetűt, nagybetűt és legalább egy számot.

Jelszó módosítása

Az első belépés folytatásához állítson be új jelszót.

Jelenlegi jelszó

Új jelszó

Új jelszó megerősítése

Az új jelszó legalább 8 karakter legyen, és tartalmazzon:

✓ kisbetűt

✓ nagybetűt

✓ legalább egy számot

Jelszó mentése és továbblépés

4.2 Hitelesítési mód kiválasztása

Az új jelszó megadása után válassza ki, melyik módszert szeretné elsődlegesen használni. Az első beállításkor az alábbi lehetőségek egyikét kell kiválasztani:

- E-mailes kód: a rendszer a fiókhoz tartozó e-mail-címre küldi az egyszer használható kódot.
- Hitelesítő alkalmazás: a mobilalkalmazásban megjelenő aktuális kódot kell megadni.

KÉSŐBB BŐVÍTHETŐ Az elsődleges mód beállítása után a Beállítások > 2FA-beállítások menüpontban a másik módszer is bekapcsolható. Ettől kezdve mindkét lehetőség aktív lehet.

Kétfaktoros hitelesítés beállítása

Válassza ki, melyik hitelesítési módot szeretné elsődlegesen használni.

☒ **E-mailes kód**
Az egyszer használható kód a fiókhoz tartozó e-mail-címre érkezik.

☐ **Hitelesítő alkalmazás**
A mobilalkalmazásban megjelenő aktuális kódot kell megadni.

A másik módszer később a 2FA-beállításokban szintén bekapcsolható.

Tovább

4.3 A beállítás ellenőrzése

1. **Kérje le vagy olvassa le a kódot.** E-mailes módszernél ellenőrizze a postafiókot; alkalmazásos módszernél nyissa meg a hitelesítő alkalmazást. (A hitelesítő alkalmazás installálásához kérjük olvassa el a Hitelesítő alkalmazások rövid útmutatóját)
2. **Adja meg a kódot.** A számokat pontosan, a megjelenített sorrendben írja be.
3. **Fejezze be a belépést.** Sikeres ellenőrzés után az új jelszó és a kétfaktoros beállítás is érvénybe lép.

Amennyiben a Hitelesítő alkalmazást választotta, első belépéskor egy QR kódot fog látni a weboldalon.

Ezt a QR kódot kell szkennelnie a telefonjával, a hitelesítő alkalmazáson belül. Így történik meg az összekapcsolás. Szkennelés után a telefonon található hitelesítő alkalmazásnál megjelennek a 30 másodpercenként frissülő számok. Ezt a számot kell beírni az aktiváláshoz. Hitelesítő alkalmazás telepítéséhez kérjük töltse le és olvassa el a weboldalon található másik leírást is!

Hitelesítő alkalmazás beállítása

Kapcsolja össze a fiókját a hitelesítő alkalmazással.



1. Nyissa meg a hitelesítő alkalmazást a telefonján.
2. Válassza a QR-kód beolvasását vagy új fiók hozzáadását.
3. Olvassa be a bal oldalon látható QR-kódot.

Az alkalmazás ezután egy hatjegyű kódot jelenít meg.

A beállítás befejezéséhez írja be ezt a kódot alább.

Az alkalmazásban megjelenő kód

123 456

Összekapcsolás és ellenőrzés

A QR-kód csak az első beállításkor szükséges.

5. Mindennapi bejelentkezés

5.1 Ha egyetlen módszer van bekapcsolva

Ha csak az e-mailes vagy csak a hitelesítő alkalmazásos módszer aktív, a rendszer nem jelenít meg választási kérdést. A jelszó megadása után automatikusan az egyetlen aktív módszerhez tartozó ellenőrzés következik.

1. **Adja meg a felhasználónevét és jelszavát.** A rendszer automatikusan felismeri az egyetlen aktív második hitelesítési módot.
2. **Adja meg az ellenőrző kódot.** E-mailes módnál a kiküldött kódot, alkalmazásos módnál az alkalmazásban megjelenő számokat írja be.
3. **Folytassa a belépést.** Helyes kód esetén a megszokott kezdőoldal jelenik meg.

5.2 Ha mindkét módszer be van kapcsolva

Ha az e-mailes és a hitelesítő alkalmazásos módszer is aktív, a rendszer a felhasználónév és a jelszó megadása után minden alkalommal megkérdezi, melyik 2FA-módot szeretné használni.

- E-mailes mód választásakor a rendszer új ellenőrző kódot küld a fiókhoz tartozó e-mail-címre. A belépéshez ezt a kódot kell visszaírni.
- Hitelesítő alkalmazás választásakor nem e-mail érkezik: az alkalmazásban megjelenő aktuális számokat kell beírni.

A VÁLASZTÁS CSAK KÉT AKTÍV MÓDNÁL JELENIK MEG Ha csak az egyik módszer aktív, a rendszer kihagyja ezt a kérdést, és automatikusan az aktív módszer ellenőrző képernyőjét nyitja meg.

5.3 E-mailben kapott kód használata

- A kód a kiküldéstől számított 2 percig használható fel.
- Mindig a legutóbb kapott, még érvényes kódot adja meg.
- Ha az üzenet nem látható, ellenőrizze a levélszemét vagy kéretlen üzenetek mappáját is.
- Lejárt kód esetén kérjen új kódot, majd az új üzenetben szereplő értéket használja.

IDŐKORLÁT A 2 perces érvényességi idő biztonsági korlátozás. A kódot célszerű közvetlenül a beérkezés után megadni.

E-mailes ellenőrzés



Az ellenőrző kódot elküldtük a fiókhhoz tartozó e-mail-címre.
A kód a kiküldéstől számított 2 percig használható fel.

Ellenőrző kód

123 456

Kód ellenőrzése

Nem érkezett meg az üzenet?

Új kód kérése

Mindig a legutóbb kiküldött kódot használja.

5.4 Hitelesítő alkalmazás kódjának használata

- Nyissa meg a korábban beállított hitelesítő alkalmazást.
- Keresse meg a fiókhhoz tartozó bejegyzést.
- Írja be az éppen megjelenő kódot, majd erősítse meg a belépést.

TIPP Ha a kód hamarosan megváltozik, várja meg a következő kódot, és azt adja meg. Így több idő marad a beírásra.

6. Hitelesítési módok kezelése

Bejelentkezés után a Beállítások > 2FA-beállítások menüpontban külön-külön kezelhető az e-mailes és a hitelesítő alkalmazásos módszer. Az első belépéskor kiválasztott mód mellé a másik is bekapcsolható, így mindkettő egyszerre aktív lehet.

KÉT AKTÍV MÓD Ha mindkét módszer aktív, a rendszer minden bejelentkezéskor - a felhasználónév és a jelszó megadása után - választást kér. A választás határozza meg, hogy e-mailes kódot küldjön, vagy az alkalmazás aktuális kódját kérje.

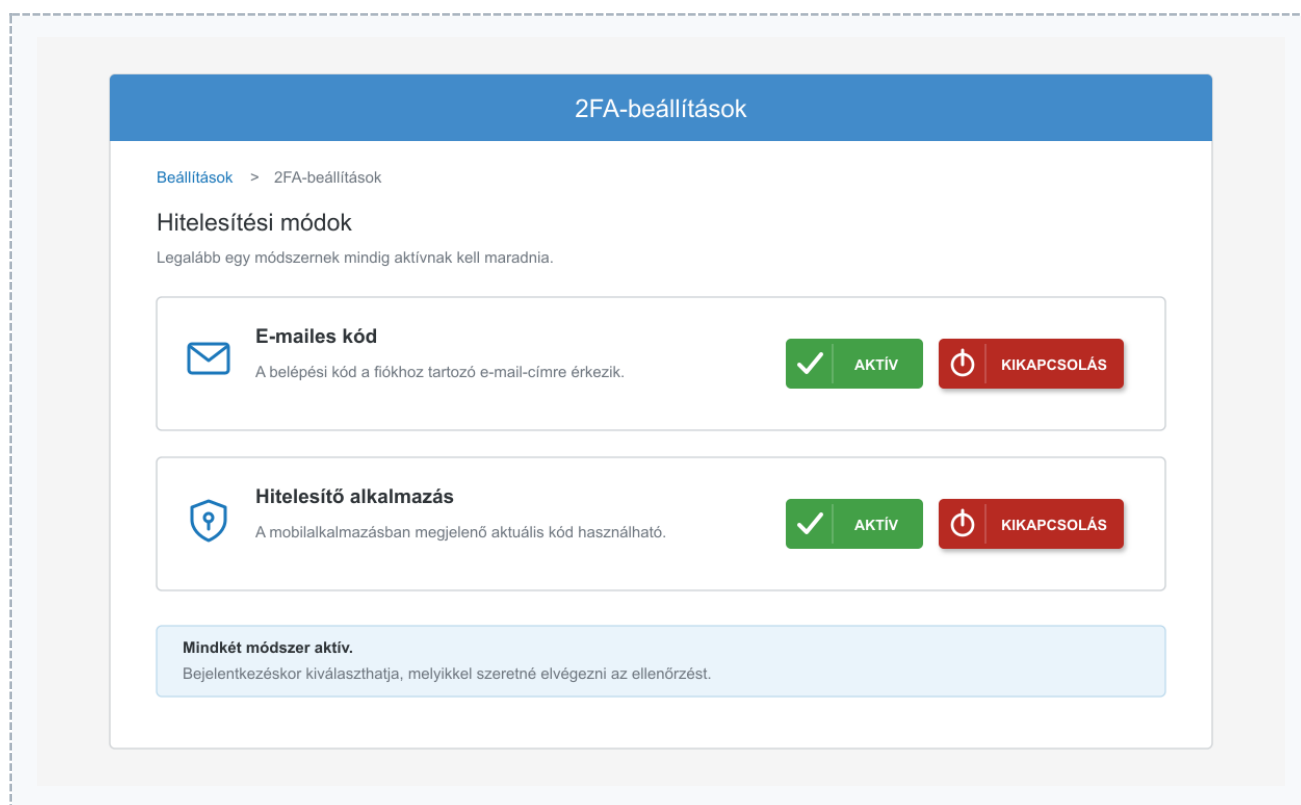
6.1 Új módszer bekapcsolása

1. **Nyissa meg a Beállítások > 2FA-beállítások menüpontot.** Itt külön sorban látható a két hitelesítési mód aktuális állapota.
2. **Kapcsolja be a másik módszert.** Az elsődleges mód mellett az e-mailes és az alkalmazásos lehetőség egyszerre is aktív lehet.
3. **Ellenőrizze a beállítást egy kóddal.** A módszer csak sikeres kódellenőrzés után válik használhatóvá.

6.2 Módszer kikapcsolása

MINDKETTŐ SOHA NEM LEHET KIKAPCSOLVA Egy hitelesítési mód csak akkor kapcsolható ki, ha a másik módszer már aktív. A rendszer nem engedi, hogy az e-mailes és az alkalmazásos módszer egyszerre kikapcsolt állapotba kerüljön.

Ha az egyik módszert szeretné kikapcsolni, előbb kapcsolja be és egy kóddal ellenőrizze a másikat. Csak ezután válik kikapcsolhatóvá a már nem használt módszer. A fiókon tehát mindig legalább egy aktív 2FA-mód marad.



7. Hozzáférés helyreállítása

Ha a hitelesítő alkalmazás már nem érhető el - például készülékcseré, elveszett telefon vagy törölt alkalmazás miatt -, jogosult adminisztrátor helyreállíthatja a kétfaktoros belépést.

7.1 Mi történik helyreállításkor?

- A korábbi hitelesítő alkalmazásos beállítás törlődik.
- Az e-mailes hitelesítés bekapcsolódik, és a következő belépéskor ezt kell használni.
- A helyreállítás nem ad hozzáférést az e-mail-postafiókhoz; ahhoz továbbra is a felhasználónak kell hozzáférnie.

7.2 Teendők a helyreállítás után

1. **Jelentkezzen be a szokásos felhasználónévvel és jelszóval.** A rendszer e-mailes ellenőrző kódot kér.
2. **Adja meg az e-mailben kapott kódot.** A kódot a 2 perces érvényességi időn belül használja fel.
3. **Nyissa meg a kétfaktoros beállításokat.** Szükség esetén állítsa be újra a hitelesítő alkalmazást.
4. **Ellenőrizze az új módszert.** Ha az alkalmazásos módszer már aktív, az e-mailes módszer megtartható vagy kikapcsolható.

HA AZ E-MAIL SEM ÉRHETŐ EL Ne próbálkozzon találmra más e-mail-címmel. Forduljon a kijelölt ügyfélszolgálathoz vagy rendszergazdához a fiókhoz tartozó cím ellenőrzéséért.

Amennyiben 5x egymás után helytelen jelszót, vagy hitelesítő kódot ír be, a rendszer automatikusan kitiltja. A tiltás feloldásához kérjük forduljon az adminisztrátorokhoz!

8. Gyakori helyzetek és megoldások

Helyzet	Javasolt teendő
Nem érkezik meg az e-mail-es kód.	Várjon rövid ideig, frissítse a postafiókot, ellenőrizze a levélszemét mappát, majd szükség esetén kérjen új kódot.
A rendszer szerint lejárt a kód.	Kérjen új kódot. A korábbi kód helyett mindig a legutóbb kiküldöttet adja meg.
A beírt alkalmazáskód nem fogadható el.	Várja meg a következő kódot, írja be pontosan, és ellenőrizze, hogy a megfelelő fiók bejegyzését nézi.
Nem tudom kikapcsolni az egyik módszert.	Előbb kapcsolja be és ellenőrizze a másik módszert. A rendszer csak akkor engedi a kikapcsolást, ha a másik már aktív; mindkettő egyszerre soha nem lehet kikapcsolva.
Új telefonom van, a régi alkalmazás nem érhető el.	Kérjen hozzáférés-helyreállítást, lépjen be e-mail-es kóddal, majd állítsa be újra a hitelesítő alkalmazást.
Nincs hozzáférésem a fiókhoz tartozó e-mailhez.	Forduljon a kijelölt ügyfélszolgálathoz vagy rendszergazdához; az e-mail-cím módosítását ne próbálja kerülőúton megoldani.

9. Első belépés előtti gyors ellenőrzőlista

- ☐ Ismerem a jelenlegi bejelentkezési adataimat.
- ☐ Hozzáférek a fiókhoz tartozó e-mail-postafiókhoz.
- ☐ Kiválasztottam, hogy e-mail-es vagy alkalmazásos hitelesítést szeretnék használni.
- ☐ Olyan új jelszót készítettem elő, amely megfelel a követelményeknek.
- ☐ A beállítást egy alkalommal, megszakítás nélkül végig tudom vinni.
- ☐ Tudom, hogy később a 2FA-beállításokban mindkét módszert aktiválhatom, de legalább az egyiknek mindig aktívnak kell maradnia.

10. Biztonságos használat röviden

- Az ellenőrző kódot ne ossza meg más személlyel.
- Csak olyan belépési kérést hagyjon jóvá, amelyet Ön kezdeményezett.
- Ha váratlanul kap kódot, ne használja fel, és szükség esetén jelezze az esetet az illetékes támogatási csatornán.
- Készülékcsere vagy e-mail-hozzáférési probléma esetén még a régi hozzáférés megszűnése előtt frissítse a beállításokat, ha erre van lehetőség.

LÉNYEG A belépéshez a jelszó és egy aktuális ellenőrző kód szükséges. A fiókon mindig legalább egy második hitelesítési mód aktív marad.