Kétfaktoros hitelesítés beállítása kliens felületen

A Debreceni Egyetem tanulmányi rendszerének kliens felületére való belépés biztonságának fokozása érdekében úgynevezett kétfaktoros azonosítási szolgáltatás kerül bevezetésre.

A kétfaktoros hitelesítő azonosítás azt jelenti, hogy a korábban megszokott Azonosító+Jelszó páros megadását követően minden egyes belépéskor egy 6 számjegyű token megadása is szükséges, amelyet egy Authentikátor (Hitelesítő alkalmazás) generál.

A kétfaktoros hitelesítés beállításának lépései:

1. Authentikátor (Hitelesítő alkalmazás) letöltése okoseszközre/számítógépre

↓

2. Regisztráció, kétfaktoros hitelesítés beállítása

↓

3. Az Authentikátor (Hitelesítő alkalmazás) használata (token megadása minden belépéskor)

1. Authentikátor (Hitelesítő alkalmazás) letöltése

Telepítsük okoseszközünkre/számítógépünkre az alább javasolt Authentikátorok egyikét!

Okoseszközre:

Google Authenticator:

- Android: https://play.google.com/store/search?q=google+authenticator&c=apps&hl=hu
- iOS: https://apps.apple.com/hu/app/google-authenticator/id388497605

Microsoft Authenticator:

- Android: https://play.google.com/store/apps/details?id=com.azure.authenticator&hl=hu
- iOS: https://apps.apple.com/hu/app/microsoft-authenticator/id983156458?l=hu

Számítógépre:

FortiToken:

- Windows: https://apps.microsoft.com/store/detail/fortitoken-windows/9P0TDH1J7WFZ?hl=en-us&gl=us
- macOS: https://apps.apple.com/us/app/fortitoken-mobile/id500007723

Step Two:

- https://steptwo.app/ csak macOS-re elérhető alkalmazás, amelyben a FortiTokenhez hasonlóan elvégezhető a kétfaktoros kulcs regisztrálása.

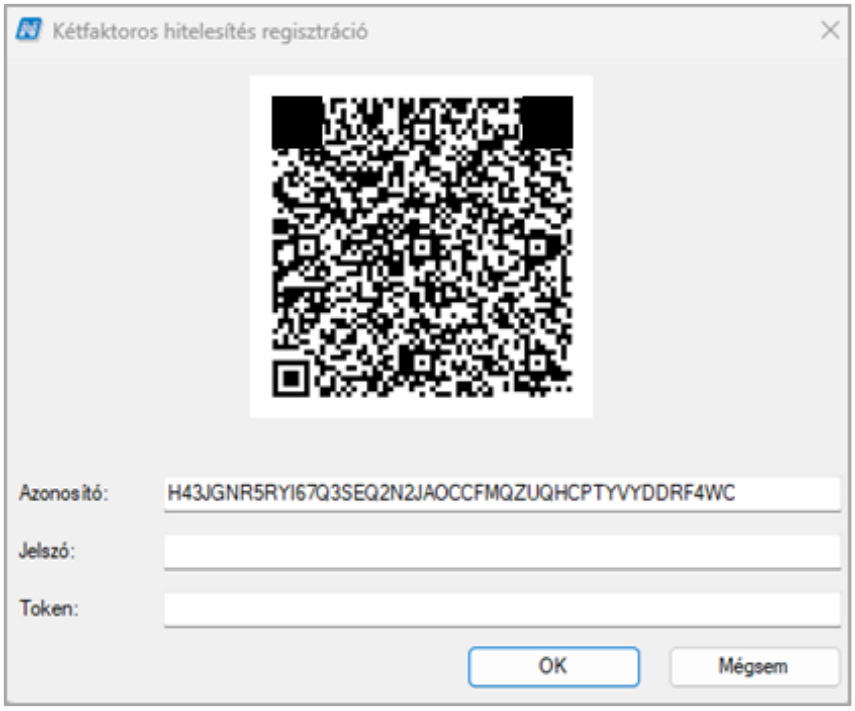
A felsorolt alkalmazások telepítése és használata ingyenes!

2. Regisztráció, kétfaktoros hitelesítés beállítása

2.1 Kétfaktoros hitelesítés regisztráció

Az 1. pont szerint a javasolt Authentikátorok egyikét szükséges telepíteni.

A Neptunba történő belépéskor, az Azonosító+Jelszó megadását követően az alábbi kétfaktoros hitelesítés regisztrációs ablak jelenik meg a kliens belépő oldalon:



Kétfaktoros hitelesítés regisztrációs ablak

Az előzetesen választott és okoseszközre letöltött Authentikátorral (Hitelesítő alkalmazással) be kell olvasni a megjelenített QR kódot, ezzel regisztrálva az Authentikátorban a kulcsot. A QR kód beolvasása helyett az **„Azonosító”** mezőben megjelenő karaktersor is bemásolható a számítógépre letöltött Authentikátorba. *(Több Authentikátorral használhatjuk ugyanazt a kétfaktoros regisztrációt, ha a karaktersort elmentjük/megőrizzük.)* Ezután az Authentikátor félpercenként generál egy 6 számjegyből álló tokent. A **„Token”** mezőben a sikeres regisztrálás után meg kell adni az **aktuális** 6 számjegyű tokent. A **„Jelszó”** mezőben a véglegesítéshez meg kell adni a **hálózati azonosítóhoz tartozó jelszót.**

Ezt a regisztrációt egyszer szükséges elvégezni, majd ezt követően minden belépéskor az Azonosító+Jelszó beírása után az Authentikátorban kapott **aktuális** 6 számjegyű tokent is meg kell adni! Az authentikáló alkalmazás a kód megadását követően bezárható, nem szükséges, hogy folyamatosan fusson.

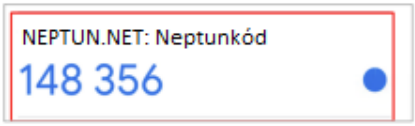
2.2 Authentikátorok használata, a kétfaktoros hitelesítés beállítása

Okoseszközön Google Authenticatort használva:

Miután okoseszközünkre sikeresen telepítettük az alkalmazást, megnyitjuk azt, majd jobb oldalon alul a + jelre kattintva a „QR kód beolvasása” lehetőséget válasszuk.

Kulcs létrehozása

A QR kód beolvasása után azonnal megkezdődik a token generálás. A kulcs neve „NEPTUN.NET” és a felhasználó Neptunkódja lesz.



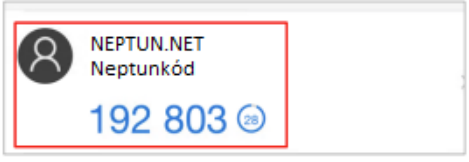
Kulcs neve és Generált token

Okoseszközön Microsoft Authenticatort használva:

Megnyitjuk az alkalmazást, majd jobb oldalon a + jelre kattintva a megjelenő opcióknál az „Egyéb (Google, Facebook stb.)” opciót válasszuk.

Kulcs létrehozása

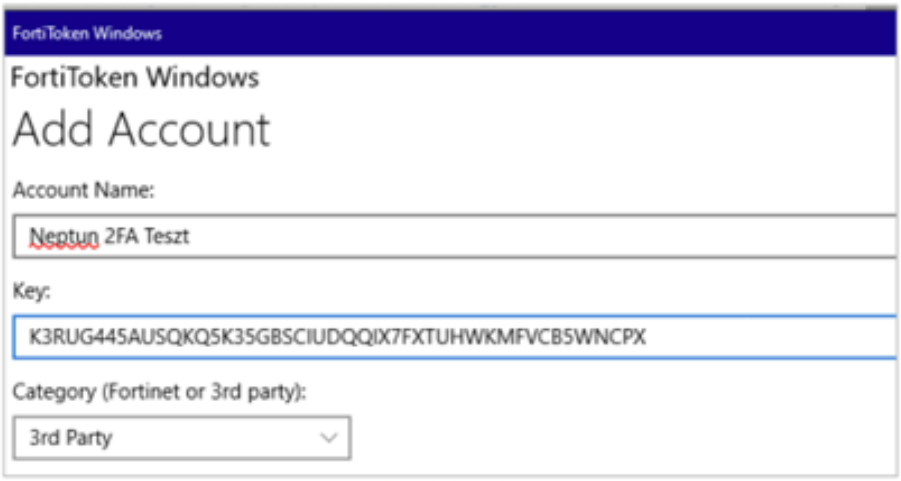
A QR kód beolvasása után azonnal megkezdődik a token generálás. A kulcs neve „NEPTUN.NET” és a felhasználó Neptunkódja lesz.



Kulcs neve és Generált token

Számítógépen FortiTokent használva:

A letöltést követően meg kell nyitni a **FortiToken** alkalmazást. A felület jobb alsó részén a „+ Add” gombra kattintva kezdhető meg a beállítás. Az „Account Name” mező szabadon tölthető, ez lesz a neve a kulcsnak. A „Key” mezőben azt a másolható karaktersort kell megadnunk, ami a Neptunban a regisztrációs ablakon belül az „Azonosító” mezőben jelenik meg. A „Category (Fortinet or 3rd party)” mezőben pedig a „3rd Party” lehetőséget kell kiválasztani. Az adatok megadását követően a felület jobb alsó felén rákattintunk a „✓ Done” feliratú gombra.

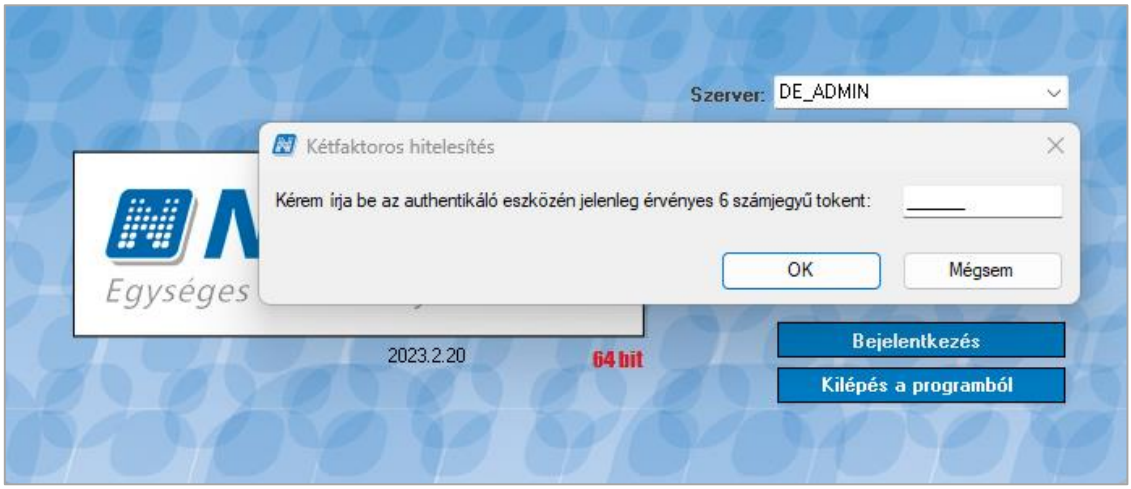


Adatok kitöltése

3. Az Authentikátor (Hitelesítő alkalmazás) használata (token megadása minden belépéskor)

A sikeresen beállított kétfaktoros hitelesítést követően minden belépéskor a kliens belépő felületen az Azonosító+Jelszó magadása után megjelenik a „Kétfaktoros hitelesítés” felugró ablak. Itt a korábban sikeresen regisztrált Authentikátorban generált 6 számjegyű tokent kell megadni.

A belépéshez kattintsunk az „OK” gombra.



Token megadása

4. Egyéb információk, technikai feltételek, segítség

A kétfaktoros hitelesítés szolgáltatás feltételei:

- A **Google Authenticator** elérhető iOS 13.0 verzió vagy felett, Android 4.4 verzió vagy felett.
  A **Microsoft Authenticator** elérhető iOS 11.0 verzió vagy felett, Android 6.0 verzió vagy felett.
  A **FortiToken** elérhető Windows 10 verzió 14393.0 vagy felett, macOS 11.0 vagy felett.
  Az **Authy** elérhető macOS 10.11 vagy felett, Linux-on (Ubuntu, Linux Mint, Debian, Manjaro).
- Internetkapcsolat a Neptun Egységes Tanulmányi Rendszert futtató eszközön. A választott authentikáló alkalmazás telepítéséhez szükséges internetkapcsolat, viszont a kulcs regisztrációjánál és a folyamatos használatnál a 6 számjegyű token generálásához már nincs szükség internetre.
- Okoseszköz (Android vagy iOS operációs rendszert futtató eszköz) vagy számítógép
- Hitelesítő alkalmazás megléte az 1-es pontban választott eszközön
- A DE Neptun rendszerében kliens jogosultság

Mire szükséges figyelni a kétfaktoros hitelesítés használatakor:

- Új eszköz vásárlásakor, ha nem kerülnek át az alkalmazások az új készülékre, akkor a kétfaktoros hitelesítés törlése szükséges, majd újra regisztrálása az új eszközön. Amennyiben segítségre van szüksége, kérjük jelezze a neptun@unideb.hu e-mail címen.
- Újra regisztráláskor a korábbi fiókot törölni kell az Authentikátorban.
- Pontosan adjuk meg a generált tokent! Elírás esetén nem fogunk tudni belépni.
- Több Authentikátorral használhatjuk ugyanazt a kétfaktoros regisztrációt, ha a QR kódhoz tartozó másolható karaktersort megőrizzük.
- Azon felhasználók, akik egyszerre több Neptun szolgáltatáshoz is rendelkeznek hozzáféréssel (oktatói, hallgatói, kliens adminisztrátori), az egyik felületen keresztüli regisztrációnál létrehozott token-nel mindegyik felülethez hozzá fognak férni. A hitelesítés regisztrációt csak egyszer kell elvégezni.
- Az **éles és a teszt klienshez** két külön kétfaktoros regisztráció szükséges. Amennyiben Microsoft Authenticator-t választottunk, az egyik kliens regisztrációját követően át kell neveznünk a kulcsot egy tetszés szerinti névre, hogy a másik kliens regisztrációja sikeres legyen.
- Sikertelen regisztráció után, amennyiben a QR-kódot tartalmazó ablakot már bezártuk, de a választott Hitelesítő alkalmazásunkban az ehhez tartozó fiók már létrejött, akkor az újbóli regisztráció előtt a korábban létrejött kód fiókot mindenképp törölni szükséges az alkalmazásban, mivel az már nem lesz érvényes, használható.

Technikai segítség:

Amennyiben a kétfaktoros hitelesítéssel kapcsolatosan technikai segítségre van szüksége, kérjük, hogy a problémát részletezve, képernyőképet csatolva és **Neptunkódját** feltüntetve a következő e-mail címen jelezze: neptun@unideb.hu