

Modern hitelesítés alkalmazása a Kulcs-Bér programban

Üzemeltetői segédlet

1 Mi a modern hitelesítés és miért van szükség a bevezetésére?

2021. szeptemberben a Microsoft közleményben jelentette be, hogy 2022. októbertől nem támogatja az online levelezőrendszereiben az egyszerű, felhasználónév és jelszó alapú hitelesítést a biztonsági kockázatok miatt.

[Basic Authentication and Exchange Online – September 2021 Update - Microsoft Community Hub](#)

A POP3, IMAP és SMTP szolgáltatásokat érintő változtatásokról 2022. októberben újabb közleményt adtak ki, egy december 31-ig tartó átmeneti időszakban biztosítanak lehetőséget az érintett szolgáltatások használatára, majd 2023. januártól az Exchange Online a modern hitelesítés használatával lesz elérhető.

[Deprecation of Basic authentication in Exchange Online | Microsoft Learn](#)

2 Az OAuth 2.0 hitelesítési folyamat

A OAuth 2.0 hitelesítés lényege, hogy a hagyományos, egyszerű felhasználónév és jelszó alapú azonosítás helyébe egy felhasználói belegegyezés kérésén alapuló folyamat lépett.

A Kulcs-Bér program a hitelesítés indításakor a Kliens azonosító és a hozzá tartozó, szolgáltatófüggő további adatok birtokában egy autentikációs kódot kér el az adott szolgáltatóhoz tartozó URL-ről, majd azt időkorlátos tokenekre cseréli REST hívásokkal.

Az autentikációs kód kiolvasását a Kulcs-Bér program beépített webszervere kezeli, a 2132-es portra visszairányítva. Ezért a helyi gépen a Windows vagy egyéb tűzfalon ezt a portot engedélyezni kell.

A felhasználói belegegyezést követően az e-mail küldés a felhasználói fiókot azonosító e-mail címmel történik a kapott tokenek felhasználásával. A fiókot azonosító e-mail címnek érvényesnek kell lennie az adott címtárban (például Azure Active Directory + Exchange Online).

A felhasználói belegegyezést az adott kliens gépen egyszer kell elkérni a modern hitelesítés beállító felületén.

Az implicit engedélyezési folyamat részletes leírása az alábbi linken található:

[OAuth 2.0 implicit engedélyezési folyamat – A Microsoft Identitásplatform - Microsoft Entra | Microsoft Learn](#)

3 A Kulcs-Bér program által biztosított lehetőségek a modern hitelesítésre

A Kulcs-Bér program három különböző lehetőséget biztosít a modern hitelesítés használatára az e-mail küldés során:

- Microsoft delegált OAuth 2.0 hitelesítés SMTP protokollal
- Google Cloud OAuth 2.0 hitelesítés SMTP protokollal
- Microsoft Graph API alapú nem delegált (szervezeti) hitelesítés HTTPS protokollal

A delegált és nem delegált hitelesítés közötti különbség, hogy a nem delegált esetben az Azure Active Directory adminisztrátora nem a felhasználókat társítja a Vállalati alkalmazáshoz, hanem az applikációt jogosítja fel arra, hogy a szervezet bármely felhasználója nevében e-mailt küldjön, így nincs szükség egyenként elkérni a felhasználói belegegyezést.

3.1 Microsoft SMTP + OAuth 2.0

Az OAuth 2.0 hitelesítés beállításához az Azure Active Directory adminisztrátorának egy új Vállalati alkalmazást kell létrehoznia a Kulcs-Bér program számára az alábbi engedélyekkel:

| API / engedélyek neve | Típus | Leírás | Rendszergazdai hoz... | Állapot |
|---|----------|---|-----------------------|--------------------------|
| + Engedély hozzáadása ✓ Rendszergazdai hozzájárulás megadása a(z) 3zq50l címárnak | | | | |
| ▼ Microsoft Graph (4) | | | | |
| Mail.Send | Delegált | Send mail as a user | Nem | Megadva a következőre... |
| offline_access | Delegált | Maintain access to data you have given it access to | Nem | Megadva a következőre... |
| SMTP.Send | Delegált | Send emails from mailboxes using SMTP AUTH. | Nem | Megadva a következőre... |
| User.Read | Delegált | Sign in and read user profile | Nem | Megadva a következőre... |

A Vállalati alkalmazás számára a Hitelesítés menüpontban meg kell adni, hogy a `http://localhost:2132` URL-re irányítsa át a kérés eredményét.

Kezelés + Platform hozzáadása

Mobil- és asztali alkalmazások

Átírányítási URI azonosítók

Azok az URI-k, amelyeket a felhasználók sikeres hitelesítési adatainak (tokenek) visszaküldésekor célállomásként fogadunk el. Az átírányító URI-nak, amelyet a bejelentkezési kiszolgálónak küldött kérésben küld, meg kell egyeznie az itt felsoroltakkal. Más néven válasz-URL-ek. További információ az átírányítási URI-azonosítókról és azok korlátozásairól

- <https://login.microsoftonline.com/common/oauth2/nativeclient>
- https://login.live.com/oauth20_desktop.srf (LiveSDK)
- <msal47bb402e-4e99-47a9-9937-e6703196f623://auth> (Csak MSAL)

<http://localhost:2132>

URI hozzáadása

A Vállalati alkalmazást az alábbi linken lehet létrehozni és kezelni:

https://portal.azure.com/#view/Microsoft_AAD_IAM/StartboardApplicationsMenuBlade~/AppAppsPreview/menuId~/null

Az Áttekintés menüpontban található a Kulcs-Bér program beállításához szükséges azonosítók:

Áttekintés

Gyorsútmutató

Integrációs asszisztens

Kezelés

Védjegyzés és tulajdonságok

Hitelesítés

Alapvető adatok

Megjelenített név

Alkalmazás (ügyfél) azon...

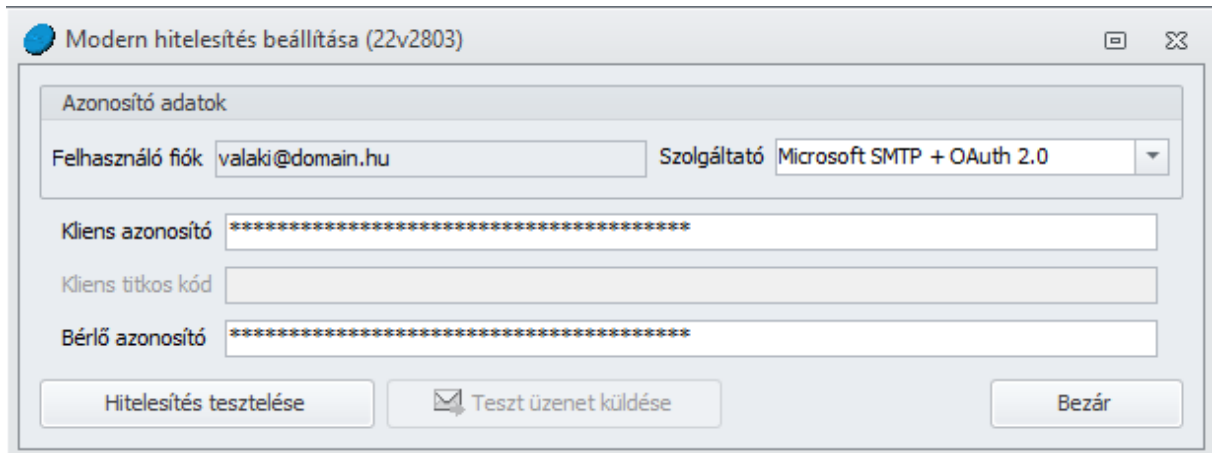
Objektumazonosító

Címtár (bérlő) azonosítója

Támogatott fióktípusok

A Microsoft SMTP OAuth 2.0 hitelesítés használatakor a felhasználói fiók mellett a Kliens azonosítót (az Azure portalon regisztrált applikáció Application ID-ja, magyarul Alkalmazás (ügyfél) azonosító) és a Címtár (bérlő) azonosítót (az Azure-t használó szervezet Tenant ID-ja) is meg kell adni.

Az adatok a Hitelesítés tesztelése gombbal mentődnek el, egyúttal a program tájékoztat a hitelesítés eredményéről és amennyiben sikeres volt, azonnal lehetőség van teszt üzenet küldésére.



A Hitelesítés tesztelése során létrejön egy ún. Refresh token, ez biztosítja, hogy ne kelljen minden e-mail küldéskor elkérni a felhasználói bejelentkezést. A token élettartama a Microsoft OAuth 2.0 esetében biztonsági beállításoktól függően legalább 90 nap, amennyiben ennél hosszabb ideig nem történik e-mail küldés, erről hibaüzenet tájékoztatja a felhasználót, ilyenkor a Kulcs-Bér rendszergazda számára a hitelesítési folyamat megismétlésével van lehetőség újabb Refresh token beszerzésére.

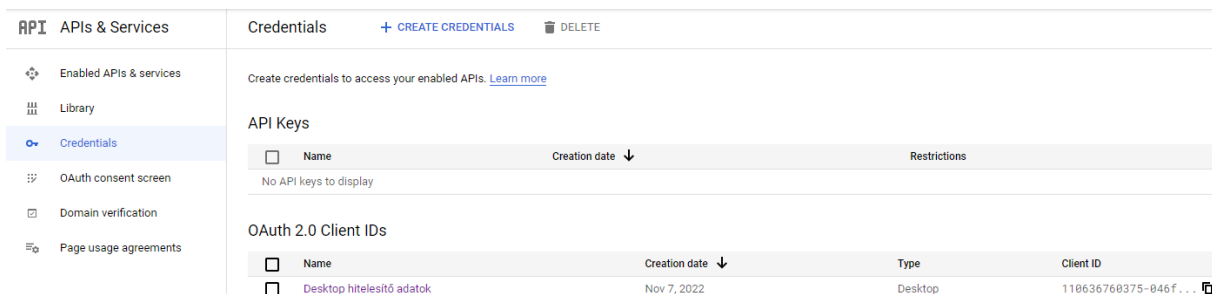
Bővebb információk az alábbi linken találhatóak:

[Configurable token lifetimes - Microsoft Entra | Microsoft Learn](#)

3.2 Google mail + OAuth 2.0

Azoknak a vállalatoknak, ahol már korábban bevezették a Google Cloud OAuth 2.0 hitelesítés használatát, a Kulcs-Bér program lehetőséget biztosít az egyszerű felhasználónév + jelszó alapú azonosítás helyett a magasabb biztonságú beállításokra.

A hitelesítő adatok a Google Cloud konzol (<https://console.cloud.google.com>) APIs & Services menüpontban a kiválasztott projekt Credentials menüjéből érhetők el:



| API Keys | | | |
|------------------------|---------------|--------------|--|
| Name | Creation date | Restrictions | |
| No API keys to display | | | |

| OAuth 2.0 Client IDs | | | |
|---|---------------|---------|----------------------|
| Name | Creation date | Type | Client ID |
| Desktop hitelesítő adatok | Nov 7, 2022 | Desktop | 110636760375-046f... |

A Kulcs-Bér program modern hitelesítés beállító felületén a hitelesítő adatokat értelem szerűen kell megadni, a Kliens azonosító a Client ID, a Kliens titkos kód a Client secret.

A Hitelesítés tesztelése és a teszt üzenet küldése megegyezik a Microsoft OAuth 2.0 pontban részletezett folyamattal, a böngészőbe kiirányítást követően a felhasználói belegegyezés elkérése után küldhetők SMTP protokollal az e-mail üzenetek.

A Microsoft autorizációs folyamathoz hasonlóan a felhasználói belegegyezés elkérésekor létrejön ebben az esetben is egy ún. Refresh token, annak érdekében, hogy ne kelljen minden e-mail küldésekor megismételni az autorizációt. Amennyiben hosszabb ideig nem történik e-mail küldés, a Refresh token érvénytelenségének lejáratára vagy a Refresh token hiányára vonatkozó hibaüzenet keletkezhet, ekkor meg kell ismétetni a hitelesítés tesztelését a beállító felületen.

3.3 Microsoft Graph + HTTPS (szervezeti)

A nem delegált, Graph API alapú hitelesítés beállításai három ponton térnek el a 3.1-ben részletezett OAuth 2.0-tól:

Nincs szükség a böngészőbe kiirányításra, ezért a `http://localhost:2132` átirányítás beállítása sem szükséges

Az Azure Active Directory adminisztrátora a Vállalati alkalmazásnak adja meg a jogot, hogy a szervezet bármelyik felhasználói fiókja nevében e-mailt küldhessen, ezért nincs szükség felhasználónként belegegyezés kérésére

Az alábbi API engedélyek beállításával van lehetőség a Kulcs-Bér program Graph API alapú használatára:

| Kezelés | Konfigurált engedélyek | | | | | | | | | | | | | | | | | | | | |
|--|--|-------------------------------|-----------------------|----------------------------|-----------------------|---------|-----------------------|--|--|--|--|-----------|------------|-----------------------|------|----------------------------|-----------|----------|-------------------------------|-----|----------------------------|
| <ul style="list-style-type: none"> Védjegyzés és tulajdonságok Hitelesítés Tanúsítványok és titkos kódok Jogkivonat-konfiguráció API-engedélyek API közzététele Alkalmazás-szerepkörök | <p>Az alkalmazások a hozzájárulási folyamat részeként jogosultak az API-k hívására, ha erre a felhasználók/rendszergazdák engedélyeket adnak. A konfigurált engedélyek li szerepelnie kell az alkalmazás igényeinek megfelelő összes engedélynek. További információ az engedélyekről és a hozzájárulásról</p> <p>+ Engedély hozzáadása ✓ Rendszergazdai hozzájárulás megadása a(z) 3zq50l című tárnak</p> <table border="1"> <thead> <tr> <th>API / engedélyek neve</th> <th>Tipus</th> <th>Leírás</th> <th>Rendszergazdai hoz...</th> <th>Állapot</th> </tr> </thead> <tbody> <tr> <td colspan="5">▼ Microsoft Graph (2)</td> </tr> <tr> <td>Mail.Send</td> <td>Alkalmazás</td> <td>Send mail as any user</td> <td>Igen</td> <td>✓ Megadva a következőre...</td> </tr> <tr> <td>User.Read</td> <td>Delegált</td> <td>Sign in and read user profile</td> <td>Nem</td> <td>✓ Megadva a következőre...</td> </tr> </tbody> </table> | API / engedélyek neve | Tipus | Leírás | Rendszergazdai hoz... | Állapot | ▼ Microsoft Graph (2) | | | | | Mail.Send | Alkalmazás | Send mail as any user | Igen | ✓ Megadva a következőre... | User.Read | Delegált | Sign in and read user profile | Nem | ✓ Megadva a következőre... |
| API / engedélyek neve | Tipus | Leírás | Rendszergazdai hoz... | Állapot | | | | | | | | | | | | | | | | | |
| ▼ Microsoft Graph (2) | | | | | | | | | | | | | | | | | | | | | |
| Mail.Send | Alkalmazás | Send mail as any user | Igen | ✓ Megadva a következőre... | | | | | | | | | | | | | | | | | |
| User.Read | Delegált | Sign in and read user profile | Nem | ✓ Megadva a következőre... | | | | | | | | | | | | | | | | | |

Az Azure Active Directory adminisztrátora az alkalmazás számára létrehoz egy titkos kódot, ezzel igazolva a hitelesítő adatok megbízhatóságát:

Kezelés

- Védjegyzés és tulajdonságok
- Hitelesítés
- Tanúsítványok és titkos kódok**
- Jogkivonat-konfiguráció
- API-engedélyek
- API közzététele
- Alkalmazás-szerepkörök
- Tulajdonosok

Az alkalmazásregisztrációs tanúsítványok, a titkos kódok és az összevont hitelesítő adatok az alábbi lapokon találhatóak.

Tanúsítványok (0) **Titkos ügyfélkódok (1)** Összevont hitelesítő adatok (0)

Egy titkos sztring, mellyel az alkalmazás jogkivonatokat kérésekor igazolja az identitását. Alkalmazásjelszónak is nevezik.

+ Új titkos ügyfélkód

| Leírás | Lejárát | Érték ⓘ |
|-------------------------------|---------------|----------|
| Mail.Send alkalmazás engedély | 2023. 03. 09. | bró***** |

A Kliens azonosító (Alkalmazás azonosító) és Bérő azonosító megegyezik az Microsoft OAuth 2.0 esetében ismertettekkel, a Kliens titkos kód a Microsoft szóhasználatában a Titkos klienskód.

Modern hitelesítés beállítása (22v2803)

Azonosító adatok

Felhasználó fiók: valaki@domain.hu Szolgáltató: Microsoft Graph + HTTPS (szervezeti)

Kliens azonosító: *****

Kliens titkos kód: *****

Bérő azonosító: *****

Hitelesítés tesztelése Teszt üzenet küldése Bezár

Az adatok a hitelesítés tesztelésekor tárolódnak el, azonnali lehetőség van ebben az esetben is a teszt üzenet küldésére.

Az Azure Active Directory az online felhasználói felületen nem biztosít lehetőséget az applikációhoz rendelt felhasználói fiókok korlátozására, ugyanakkor PowerShell scriptekkel biztonsági csoporthoz rendelhető az e-mail küldés lehetősége, így megoldható, hogy a nem delegált Graph alapú működés esetén is kizárólag a szervezet Exchange Online felhasználói fiókjainak egy meghatározott köre legyen jogosult a Vállalati alkalmazáson keresztüli e-mail küldésre.

Erről bővebben az alábbi linken található információk:

[Limiting application permissions to specific Exchange Online mailboxes - Microsoft Graph | Microsoft Learn](#)