

Modern hitelesítés alkalmazása a Kulcs-Könyvelés 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 bejelentkezés kérésén alapuló folyamat lépett.

A Kulcs-Könyvelés 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-Könyvelés 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 bejelentkezést 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 bejelentkezést 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-Könyvelés program által biztosított lehetőségek a modern hitelesítésre

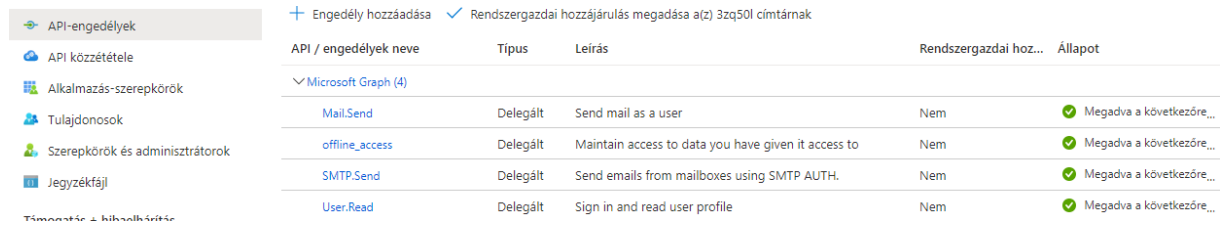
A Kulcs-Könyvelés program három különböző lehetőséget biztosít a modern hitelesítés használatára az e-mail küldés során:

- 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 bejelentkezést.

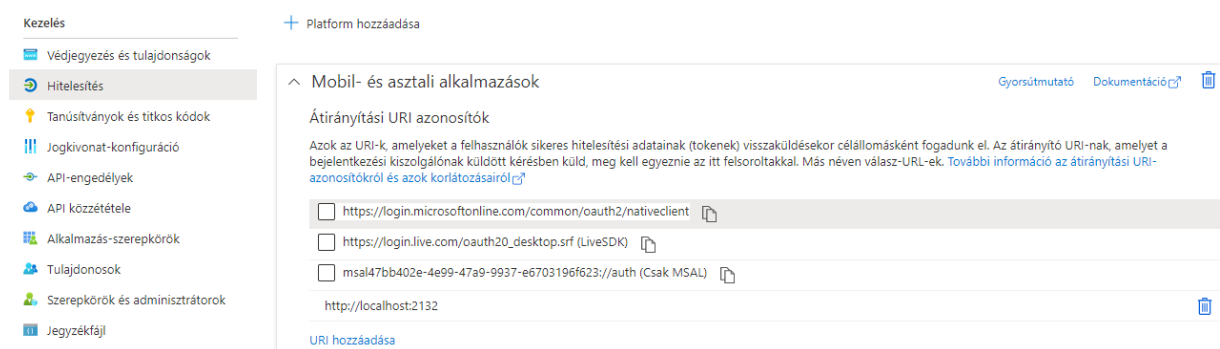
3.1 Microsoft SMTP + OAuth 2.0

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



API / engedélyek neve	Tipus	Leírás	Rendszergazdai hoz...	Állapot
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.

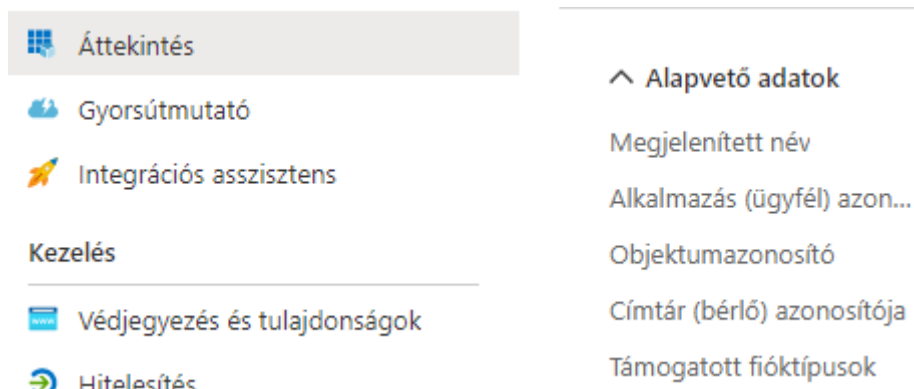


Kezelés	Platform hozzáadása
Hitelesítés	Mobil- és asztali alkalmazások
Átírányítási URI azonosítók	
Azok az URI-k, amelyeket a felhasználók sikeres hitelesítési adatainak (tokenek) visszaküldésekor célállomásként fogadunk el. Az átírányító URI-nak, amelyet a bejelentkezési kiszolgálónak küldött kérésben küld, meg kell egyeznie az itt felsoroltakkal. Más néven válasz-URL-ek. További információ az átírányítási URI-azonosítókról és azok korlátozásairól.	
<input type="checkbox"/>	https://login.microsoftonline.com/common/oauth2/nativeclient
<input type="checkbox"/>	https://login.live.com/oauth20_desktop.srf (LiveSDK)
<input type="checkbox"/>	msal47bb402e-4e99-47a9-9937-e6703196f623://auth (Csak MSAL)
<input type="checkbox"/>	http://localhost:2132

A Vállalati alkalmazást az alábbi linken lehet létrehozni és kezelni:

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

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



Áttekintés	Alapvető adatok
Gyorsútmutató	Megjelenített név
Integrációs asszisztens	Alkalmazás (ügyfél) azon...
Kezelés	Objektumazonosító
Védjegyzés és tulajdonságok	Címtár (bérlő) azonosítója
Hitelesítés	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.

The screenshot shows a dialog box titled "E-mail adatainak beállítása". It has three main sections: "Hitelesítés típusa" (Authentication type) with "Modern hitelesítés" checked; "Azonosítási adatok" (Identification data) with "Felhasználói fiók" (User account) set to "valaki@domain.hu", "Szolgáltató" (Provider) set to "Microsoft SMTP + OAuth 2.0", and "Port" set to "2132"; and "Hitelesítési adatok" (Authentication data) with three masked input fields for "Kliens azonosító" (Client ID), "Kliens titkos kód" (Client secret), and "Bérlő azonosító" (Tenant ID). At the bottom, there are buttons for "Hitelesítés tesztelése", "Teszt e-mail küldése", "Rendben", and "Mégse".

A Hitelesítés tesztelése során létrejön egy ún. Refresh token, ez biztosítja, hogy ne kelljen minden e-mail küldéskor elkérni a felhasználói beleegyezést. 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-Könyvelés 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](#)

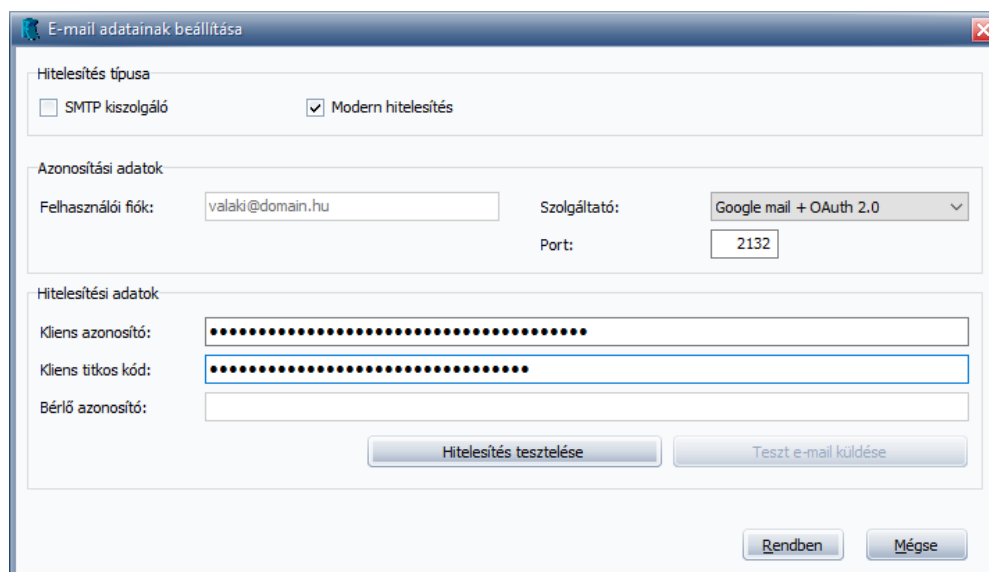
3.2 Google mail + OAuth 2.0

Azoknak a vállalatoknak, ahol már korábban bevezették a Google Cloud OAuth 2.0 hitelesítés használatát, a Kulcs-Könyvelés 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:

APIs & Services		Credentials		+ CREATE CREDENTIALS		DELETE	
Enabled APIs & services		Create credentials to access your enabled APIs. Learn more					
Library		API Keys					
Credentials		No API keys to display					
OAuth consent screen		OAuth 2.0 Client IDs					
Domain verification							
Page usage agreements							
		Name	Creation date	Type	Client ID		
		Desktop hitelesítő adatok	Nov 7, 2022	Desktop	118636768375-046f...		

A Kulcs-Könyvelés program modern hitelesítés beállító felületén a hitelesítő adatokat értelemszerűen 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 ismételní 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-Könyvelés program Graph API alapú használatára:

Kezelés

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

Konfigurált engedélyek

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](#)

+ Engedély hozzáadása ✓ Rendszergazdai hozzájárulás megadása a(z) 3zq50l címárnak

API / engedélyek neve	Típus	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

- Védjegyezés 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 jogkivonatok kérésekor igazolja az identitását. Alkalmazásjelszónak is nevezik.

+ Új titkos ügyfélkód

Leírás	Lejárat	Érték
Mail.Send alkalmazás engedély	2023. 03. 09.	br6*****

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.

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](#)