Office 365 and Modern Authentication

Modern authentication uses an in-app browser to enable federated (and multifactor) scenarios in Office 365. This means Office 365 can be used with non-web clients when using a domain that is federated with SAML Identity Providers (IdPs) that are part of identity federations like SURFconext. For a compatibility list/list of clients that can authenticate via modern authentication, please see the Microsoft article "Updated Office 365 modern authentication".

- What is Modern Authentication?
- Security aspects
  - Verifying the authenticity of the login page
  - Two-factor authentication
  - Non-password authentication
- See also

What is Modern Authentication?

Modern Authentication is the term used by Microsoft for a new sign-in procedure implemented by Office clients that uses an embedded web browser to acquire authorisation to access a user's online resources hosted in Office 365. It is based on OAuth2 access tokens.

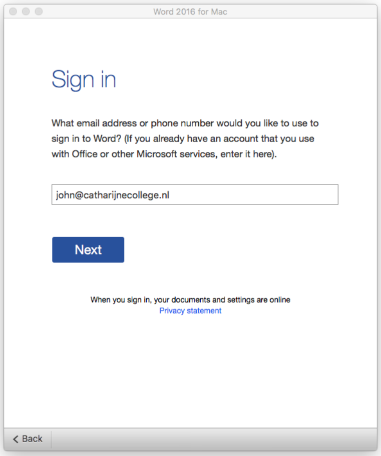
Modern authentication is available in Office 2016 for OSX and Windows, and on mobile clients (Windows mobile, iOS, Android). On Windows, Office 2013 clients also have modern authentication implemented, but this is disabled by default. Modern authentication can only be enabled through the registry.

Security aspects

Although an improvement over the sign-in process that was used before modern authentication in which user credentials were routed through Microsoft servers (at least when accessing Exchange mail over IMAP), there are still some security-related issues with non-web access to Office 365. This blog highlights what to look for for a secure login.

Verifying the authenticity of the login page

The in-app browser does **not** show an address bar or "lock" as an indication to what site it is connecting. See screenshots below.

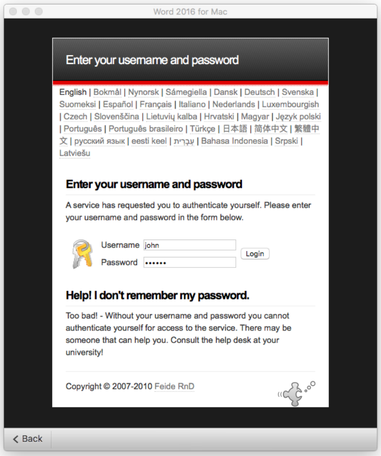


Sign in

What email address or phone number would you like to use to sign in to Word? (If you already have an account that you use with Office or other Microsoft services, enter it here).

john@catharijnecollege.nl

When you sign in, your documents and settings are online
Privacy statement



Enter your username and password

English | Bokmål | Nynorsk | Sámegiella | Dansk | Deutsch | Svenska | Suomeksi | Español | Français | Italiano | Nederlands | Luxembourgish | Czech | Slovenščina | Lietuvių kalba | Hrvatski | Magyar | Język polski | Português | Português brasileiro | Türkçe | 日本語 | 简体中文 | 繁體中文 | русский язык | eesti keel | עִבְרִית | Bahasa Indonesia | Srpski | Latviešu

Enter your username and password

A service has requested you to authenticate yourself. Please enter your username and password in the form below.

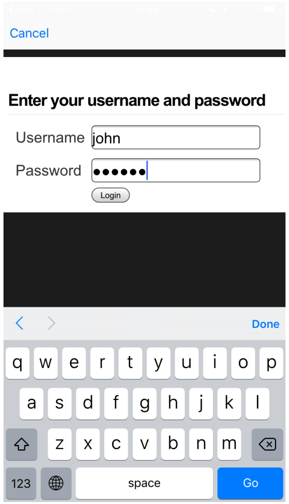
Username: john
Password: ••••••

Help! I don't remember my password.

Too bad! - Without your username and password you cannot authenticate yourself for access to the service. There may be someone that can help you. Consult the help desk at your university!

Copyright © 2007-2010 Feide RnD

Also on mobile clients (e.g. https://itunes.apple.com/us/app/microsoft-word/id586447913), there is no way for a user to verify the identity of the IdP. Even worse, the mobile interface seems to zoom in on username and password fields, making it harder to recognise the IdP login pages as visual clues like logos are no longer visible. See the screenshot below for an example.



Enter your username and password

Username john

Password ••••••

Organisations typically instruct their users on how to recognise phishing sites, and to verify the identity of the server they are authenticating to when asked to enter their password. For use with Microsoft's Office 365 clients, they should be explicitly instructed to make an exception for such clients. Note that signing in on clients in this way seems te be required only once (although we don't know yet how long the tokens are valid for).

Two-factor authentication

When logging in on a federated domain on a mobile platform, Microsoft's Authenticator is launched automatically. It is unclear why this happens, presumably it is incorrectly assumed that modern authentication is deployed because 2-factor authentication is enabled for that domain (a scenario where modern authentication is a requirement).

Non-password authentication

When authenticating at the IdP using an alternative authentication method, it may not be possible to sign in. This is due to the use of an embedded browser. For example, when authenticating using TLS client authentication, the client will not have access to the user's private key needed to authenticate to the server. A better approach would have been to use the system browser, which has additional usability benefits, such as integration with password managers.

See also

- How modern authentication works for Office 2013 and Office 2016 client apps
- Using Office 365 modern authentication with Office clients
- Enable Modern Authentication for Office 2013 on Windows devices
- Exchange Online: How to enable your tenant for modern authentication
- Office 2013 updated authentication enabling Multi-Factor Authentication and SAML identity providers
- Azure Active Directory Authentication Libraries
- Stack Overflow tag azure-active-directory