

# Microsoft Office 365

Microsoft Office 365 consists of a number of online services: Exchange Online, Sharepoint Online and Skype for Business Online (formerly known as Lync Online). As far as the web interfaces to these services is concerned, it is possible to authenticate to these services using SURFconext. Non-web clients (i.e. any software that is not a browser, like mail apps) require other solutions for federated authentication to work. For more information why this is, see [SURFconext and rich clients](#) and [Achtergrond](#). SURFnet has an environment to test common scenario's of how Dutch institutions would connect to Office365.

What does and doesn't work can be found at [Ways of connecting with Office 365 and consequences](#). A summary of the current findings is as follows:

- For a non-federated connection (on-premise institution AD synchronised with Microsoft Azure AD):
  - In this scenario, password hashes are synched with the Microsoft-cloud.
  - Passwords are relayed over Microsoft infrastructure.
  - This scenario is the easiest to use for both administrators and users.
- Federated, with Microsoft technology (ADFS):
  - This scenario requires some extra configuration to make everything work.
  - As long as Modern Authentication is configured in the Office tenant, institution passwords will not be relayed over Microsoft infrastructure (when 'basic authentication' is configured an administrator is unable to prevent a user to configure an IMAP connection, thereby relaying the institution password).
  - If users use clients that don't support modern authentication (like Thunderbird), they need to use Application Specific Passwords.
  - When requesting support from Microsoft, since all components are Microsoft-components, Microsoft won't point to other parties as a possible cause of the problem.
- Federated, via SURFconext:
  - In this scenario passwords will never be relayed over the Microsoft-cloud (SURFconext does not support passing passwords).
  - As in the previous federated scenario, with Microsoft technology, some configuration is required and users with certain clients will need to use Application Specific Passwords.
  - When requesting support from Microsoft, they are likely unfamiliar with SURFconext, and it could be they state SURFconext is (causing) the problem. SURFconext could come to the conclusion everything works as expected. This process can cause delays in problem resolution.
- Good to know: our knowledge partner, 2AT, expects it should be easy to start of using Office 365 using SURFconext, but switch to one of the other scenario's if that would be desirable later on.

More details can be found in [Ways of connecting with Office 365 and consequences](#) and the pages below.

We have also tested Office365 with SURFsecureID, which also works with Office365. The results can be found [here](#).

Besides the info on this wiki, you might also be interested in [what SURFmarket offers around Office365](#).

In case you have questions about Office365 with SURFconext or SURF Strong Authentication, you can contact the SURFconext team via email: [support@surfconext.nl](mailto:support@surfconext.nl).